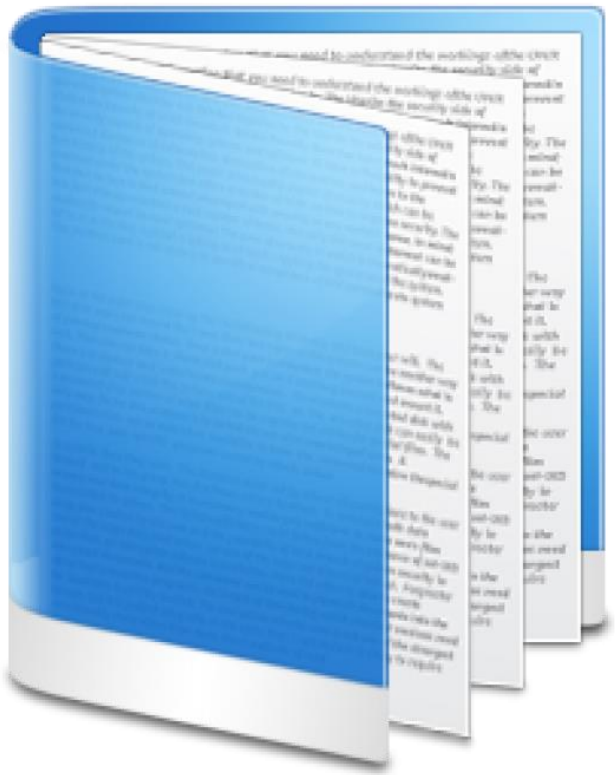
УНИВЕРСИТЕТ ИТМО

В.М. Коржук, И.Ю. Попов, А.А. Воробьева

ЗАЩИЩЕННЫЙ ДОКУМЕНТООБОРОТ. ЧАСТЬ 1



Санкт-Петербург

2021

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

В.М. Коржук, И.Ю. Попов, А.А. Воробьева

ЗАЩИЩЕННЫЙ ДОКУМЕНТООБОРОТ. ЧАСТЬ 1

Учебно-методическое пособие

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки 10.03.01 Технологии защиты информации
в качестве Учебно-методического пособия для реализации основных
профессиональных образовательных программ высшего образования бакалавриата

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург
2021

Коржук В.М., Попов И.Ю., Воробьева А.А., Защищенный документооборот. Часть 1: Учебно-методическое пособие – СПб: Университет ИТМО, 2021. – 67 с.

Рецензент(ы):
Арустамов Сергей Аркадьевич, д.т.н., профессор факультета безопасности информационных технологий, сотрудник международного научного центра «Нелинейные и адаптивные системы управления» Университета ИТМО.

Защищенный документооборот в современном мире является сложным, комплексным процессом. Особенную актуальность вопросы обеспечения информационной безопасности документов получают в условиях внедрения и перехода на электронный документооборот. В данном учебно-методическом пособии рассмотрены такие темы, как юридическая сила документа, защита документов на бумажных носителях, защита электронных документов, системы электронного документооборота, вопросы роуминга в системах электродного документооборота при международном взаимодействии. Каждая тема содержит перечень контрольных вопросов, способствующих проверке знаний студента. В приложении содержатся кейсы для лучшего усвоения материала.

Пособие предназначено для студентов старших курсов факультета безопасности информационных технологий Университета ИТМО, специализирующихся по направлению подготовки 10.03.01 «Технологии защиты информации».

Университет ИТМО – ведущий вуз России в области информационных

и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Содержание

Введение

Защищенный документооборот в современном мире является сложным, комплексным процессом. Особенную актуальность вопросы обеспечения информационной безопасности документов получают в условиях внедрения ECM-систем и перехода на электронный документооборот. В данном учебно-методическом пособии рассмотрены такие темы, как юридическая сила документа, защита документов на бумажных носителях, защита электронных документов, простая и усиленная электронная подпись, системы электронного документооборота, вопросы роуминга в системах электродного документооборота при международном взаимодействии. Каждая тема содержит перечень контрольных вопросов, способствующих проверке знаний студента. В приложении содержатся кейсы для лучшего усвоения материала.

Представленное учебно-методическое пособие предназначено для студентов старших курсов факультета безопасности информационных технологий Университета ИТМО, специализирующихся по направлению подготовки 10.03.01 «Технологии защиты информации».

1. Бумажный документооборот

1.1 Понятие документа

Документирование информации развивается параллельно становлению социальной системы. Документами, как известно, можно считать наскальные рисунки, отражающие важные события в жизни древнего человека; глиняные дощечки с зарубками, означавшие, например, количество переданной в соседнее поселение рыбы или берестяные свитки, содержащие информацию о каких-либо событиях.

Поскольку документ так или иначе является продуктом общества, он влияет на формирование и характер общественных отношений. К примеру, появление печатных станков в 15 веке и пишущих машинок в 18 веке позволило упростить и обеспечить повсеместное распространение книг и печатных документов и, соответственно, ускорить темпы развития общественных отношений [1]. Однако изучение документа и документооборота невозможно вне социальной среды, где он сформировался и функционирует. О различных функциях документа будет рассказано далее.

В России первый государственный стандарт, описывающий сферу документооборота и включающий в себя базовые понятия, появился и был утвержден в 1970 г. Это был ГОСТ 16487-70 «Делопроизводство и архивное дело». В нем определение понятия документ выглядело следующим образом: «Документ - средство закрепления различным способом на специальном материале информации о фактах, событиях, явлениях объективной действительности и мыслительной деятельности человека». В тоже время данное определение пришлось пересмотреть через некоторое время из-за критики того факта, что в таком формате средством закрепления информации наравне с документом может быть письмо, схема или даже аудиозапись [2].

В 1983 году в результате появился пересмотренный и обновленный вариант в виде нового ГОСТ 16487-83 «Делопроизводство и архивное дело. Термины и определения». В нем под документом понимался «…материальный объект с информацией, закреплённой созданным человеком способом для её передачи во времени и пространстве». Но и в таком формате ученые и делопроизводители нашли уязвимое место: поскольку фактически в это время уже существовала концепция электронного документа, определять документ только как материальный объект было некорректно [3].

В современном ГОСТ Р 7.0.8-2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» дана наиболее корректная и общепризнанная трактовка: документ – это зафиксированная на носителе информация с реквизитами, позволяющими ее идентифицировать [4].

1.2 Классификация документов

Поскольку документы сопровождают практически каждое изменение, касающееся субъекта некоторых отношений, возможно представить несколько вариантов классификации документов.

Документов по происхождению делятся на следующие виды:

–личного происхождения;

–официальные;

–служебные.

Документами личного происхождения являются документы, появившиеся по желанию частного лица, то есть составленные лицом вне сферы его служебной деятельности или выполнения общественных обязанностей. Личные документы являются частной собственностью лица и охраняются авторским правом. Также к документам такого вида относят так или иначе (оформление личных документов не является строго регламентированным) документированную информацию о частной жизни человека: в качестве примера могут выступать мемуары, личная переписка, рукописи, дневники.

Официальный документ — документ, созданный юридическим или физическим лицом, оформленный и удостоверенный в установленном порядке. Среди них можно выделить:

–официальные личные документы. К ним относятся паспорта, права, документы, удостоверяющие личность, подтверждающие уровень образования и специальность и так далее;

–официальные управленческие документы. В основном такие документы создаются в процессе делопроизводства и отображают все основные управленческие функции.

Служебный документ — официальный документ, используемый в текущей деятельности организации. Чаще всего служебный документ содержит информацию об организации и ее функционировании; подписываются такие документы определенными ответственными лицами.

Документы по способу документирования делятся на следующие виды:

–письменный документ;

–текстовый документ;

–рукописный документ;
–машинописный документ;
–электронный документ;
–изобразительный документ;
–фотодокумент;
–фонодокумент;
–кинодокумент.

Письменный документ — документ, информация которого зафиксирована любым типом письма.

Текстовый документ — документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи.

Рукописный документ — письменный документ, при создании которого знаки письма наносят от руки.

Машинописный документ — письменный документ, при создании которого знаки письма наносят техническими средствами.

Электронный документ — документ, информация которого представлена в электронной форме.

Изобразительный документ — документ, содержащий информацию, выраженную посредством изображения какого-либо объекта.

Фотодокумент — изобразительный документ, созданный фотографическим способом.

Фонодокумент — документ, содержащий звуковую информацию, зафиксированную любой системой звукозаписи.

Кинодокумент — изобразительный или аудиовизуальный документ, созданный кинематографическим способом.

В стандартном варианте, в процессе документооборота в любой компании обрабатываются только текстовые документы, созданные рукописным и машинописным способом или представленные в электронной форме. Для создания и обработки других видов документов (видеодокументов, аудиозаписей - например, записанной в Zoom-е защиты лабораторной работы) должны существовать отдельные специальные подразделения организации.

Виды документов в зависимости от отношения к аппарату управления:

Входящие документы (поступившие в организацию).
Исходящие документы (отправляемые из организации).
Внутренние документы (создаваемые и используемые в данной организации).

Виды документов по числу затронутых вопросов

Простые документы (письма, заявления) содержат изложение одного вопроса.

Сложные документы, в отличии от простых, могут включать несколько вопросов. Сложные документы могут касаться нескольких должностных лиц, структурных подразделений, учреждений (приказы, протоколы, инструкции).

По ограничению доступа документы разделяются на:

–секретные;

–для служебного пользования;

–несекретные (открытые / общего доступа).

Секретные документы содержат в себе информацию ограниченного доступа, представляющую особую ценность для государства. На таких документах в правом верхнем углу ставится гриф секретности (отметка об ограничении доступа - об этом будет рассказано далее) - С (секретно), СС (совершенно секретно) и ОС (особой важности). Создание, ознакомление, изменение и даже уничтожение таких документов строго регламентируются. Для доступа к данным документам требуются разрешение на доступ - допуск к секретной информации.

Документы для служебного пользования (гриф ДСП) содержат несекретные сведения и могут использоваться сотрудниками внутри организации. Работа с документами, содержащими гриф ДСП, также строго регламентирована.

По способу изложения текста документы делятся на следующие виды:

–индивидуальные;

–типовые;

–трафаретные.

В **индивидуальных** документах содержание излагается в виде связного текста. Составитель (исполнитель) индивидуального документа готовит оригинальный текст, посвященный одному (или нескольким) вопросу, для выполнения конкретной управленческой задачи. Эти документы представляют собой традиционный литературный текст.

Типовые документы используются для документирования однотипных (повторяющихся) ситуаций, они составляются на основе образца (например, типовые письма, инструкции, договоры и др.). В документоведении метод типизации используется для создания типовых форм документов и текстов, то есть образцов или эталонов, на основе которых создаются конкретные документы. Типовой текст — текст-

образец, на основе которого создаются в последующем тексты аналогичного содержания.

В **трафаретных** документах структура изложения текста формализована, в них используются заранее подготовленные стандартные фразы или отдельные части постоянно повторяющегося текста и пропуски для заполнения переменной информации. Наиболее известным видом таких документов является анкета или справка. Такие документы, как правило, напечатаны на бланке, содержащем постоянную информацию, а переменная вписывается от руки. Вариант использования трафаретных текстов — введение их в память компьютера (шаблон текстовых редакторов).

По степени подлинности документы делятся на следующие виды:

–подлинники;

–дубликаты;

–копии.

Подлинник официального документа (оригинал) — первый (или единственный) экземпляр документа, обладающий юридической силой. Подлинник удостоверяет собственноручная подпись должностного лица, гриф утверждения, оттиск печати, регистрационный индекс. Подлинник обязательно содержит сведения, подтверждающие его достоверность (об авторе, времени и месте создания).

Дубликат документа — повторный экземпляр официального документа, имеющий юридическую силу подлинника и сопровождаемый отметкой «дубликат». Оформление дубликатов практикуется в случаях потери или порчи подлинника; например, при утрате выпускником диплома об образовании учебное заведение по запросу предоставит ему дубликат утерянного диплома.

Копия документа — документ, полностью воспроизводящий информацию подлинного документа и все его внешние признаки или часть их, не имеющий юридической силы.

Исторически копии появились в то же время, что и документ, поскольку была необходимость оставлять напоминание о том, что содержалось в оригинальном документе. На Руси все документы и их копии писались от руки - из-за этого устаревшим названием копии был «список» (от гл. списывать). В 19 веке появились первые машинописные копии; о простоте скан-копий или электронных копий можно не упоминать. Существовала отдельная должность в российских учреждениях — копиист — такой сотрудник занимался как раз копированием различных документов.

Заверенная копия документа — копия документа, на которой в соответствии с установленным порядком проставляют необходимые реквизиты, придающие ей юридическую силу.

Наряду с термином «копия» используется термин «заверенная копия». ГОСТ Р 51141-98 определяет его следующим образом: «Заверенная копия – копия документа, на которой в соответствии с установленным порядком проставляют необходимые реквизиты, придающие ей юридическую силу». Заверенная копия документа является аналогом подлинника документа [5].

Порядок заверения копий установлен ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов». Стандарт устанавливает следующее: «При заверении соответствия копии документа подлиннику ниже реквизита «Подпись» проставляют заверительную надпись: «Верно»; должность лица, заверившего копию; личную подпись; расшифровку подписи (инициалы, фамилию); дату заверения. Допускается копию документа заверять печатью, определяемой по усмотрению организации» [6].

По срокам хранения документы делятся на:

–*документы постоянного хранения;*

–*долговременного/длительного хранения* (свыше 10 лет)*;*

–*временного* (до 10 лет) *хранения.*

Сроки хранения документов определяются Федеральной архивной службой с указанием сроков хранения.

По способу передачи документов различают:

–*письма;*

–*телеграммы;*

–*телефонограммы;*

–*телексы;*

–*факсограммы;*

–*электронные сообщения* [7].

1.3 Функции документа

В классических учебных пособиях по документоведению и делопроизводству [8] выделяются следующие функции документов:

1. ***Информационная***: определяется потребностью документирования, хранения и предоставления информации.

2. ***Коммуникативная***: документы являются средством обмена информацией. Поскольку обмен информацией возможен между минимум двумя субъектами, предполагается существование источника документа

(отправителя) и приемника документа (получателя). Однако из-за культурных особенностей, географической удаленности или даже разницы во времени могут возникнуть сложности при восприятии передаваемой в документах информации. Такие сложности носят название «информационный барьер». При этом барьеры могут возникнуть как со стороны источника, так и со стороны приемника, и быть объективными (не зависящими от человека) и субъективными.

Исследователи выделяют следующие информационные барьеры:

–*Языковые* (национально-языковые) барьеры обусловлены незнанием либо слабым знанием языков.

–*Семантические* (терминологические) барьеры появляются в результате различного толкования разными людьми слов, терминов, символов.

–*Государственно-политические* барьеры связаны с различиями в политических режимах, законодательстве, регуляции информационно-документационных процессов различных государств.

–*Экономические* барьеры связаны с отсутствием или дефицитом финансовых средств для производства, передачи, потребления информации.

–*Пространственные* (географические) барьеры возникают вследствие удаления источника и приёмника информации друг от друга в пространстве.

–*Временные* (исторические) барьеры связаны с разделением источника и приёмника информации во времени.

–*Режимные* барьеры ограничивают доступ к документированной информации.

–*Ведомственные и бюрократические* барьеры обусловлены разветвлённой, иерархической структурой системы управления и самоуправления.

–*Технические* барьеры возникают вследствие нехватки или технической несовместимости оборудования.

–*Идеологические* барьеры возникают между отдельными людьми или социальными группами вследствие наличия у них разных систем взглядов на окружающую действительность, различного вероисповедания и т.п. Идеологические барьеры могут стать (и неоднократно становились) причиной острых социальных конфликтов.

–*Психологические* барьеры связаны с особенностями восприятия информации конкретным человеком, с особенностями его памяти.

3. ***Социальная***: состоит в запечатлении, сохранении и передаче социальной информации; документ является не только продуктом определенных социальных отношений, но и сам может воздействовать на эти отношения.

4. ***Специальные*** функции документа:

–*управленческая* — в ней документ выступает как средство управления деятельностью;

–*организационная* — документ устанавливает или упорядочивает действия участников правовых отношений;

–*правовая* — документ может являться письменным доказательством и быть источником права;

–*общекультурная* — способность документа сохранять и передавать культурные традиции, эстетические нормы, ритуалы, принятые в обществе;

–*историческая* — документ является историческим источником.

Приведенная классификация на самом деле не является однозначной: в редких случаях можно сказать, что определенный документ выполняет только одну функцию; чаще всего документ несет в себе совокупность функций. Например, приказ об отчислении выполняет информационную, коммуникативную, историческую, правовую, управленческую и организационную функции.

1.4 Оформление документов, реквизиты документов

Для того, чтобы документы имели юридическую силу и могли исполнять свои функции, существуют определенные правила оформления документов. Наиболее важные из них представлены ниже. Документы могут создаваться на бумажном носителе и в электронной форме с соблюдением установленных правил оформления документов.

Размеры бумаги

Все виды документов оформляются на бумаге определенных размеров (Табл. 1) — форматов, данные требования относительно деловых документов оговорены в ГОСТ Р 7.0.97–2016 [9].

Таблица 1. Размеры бумаги для документов

Формат	Размер, мм	Применение
А3	297х420	Для больших таблиц, схем, диаграмм, приложений
А4	210х297	Приказы, письма и другие организационно-распорядительные документы
А5	148х210	Приказы, письма и другие организационно-распорядительные документы
А6	105х148	Разного рода справки

Применение стандартных форматов в делопроизводстве дает возможность использовать средства автоматизации при составлении и обработке документов: к примеру, использование определенных шаблонов облегчает задачу системам распознавания образов и их операторам.

Размеры полей

Согласно ГОСТу 7.0.97–2016 для приказов, управленческих документов и деловых писем используются минимальные поля следующих размеров:

– 20 мм - левое;

– 10 мм - правое;

– 20 мм - верхнее;

– 20 мм - нижнее.

Научные отчеты, рефераты, курсовые и дипломные работы, диссертации следует оформлять, соблюдая следующие размеры полей: левое — не менее 30 мм, правое — не менее 10 мм, верхнее — не менее 15 мм, нижнее — не менее 20 мм. Аналогичные размеры полей должна иметь текстовая часть документов, подготавливаемых для типографического издания.

Если документ хранится больше 10 лет — левое поле должно быть минимум 30 мм. Логичным является удовлетворение данного требования для бумажных документов, так как их скрепляют или сшивают в дела — специальные папки — и сдают на хранение в архив. Вопрос актуальности данного требования для электронных документов остается открытым, но, скорее всего, для унификации требований по оформлению действует и для электронных документов.

Допускается создание документов на лицевой и оборотной сторонах листа. При двустороннем создании документов ширина левого поля на лицевой стороне листа и правого поля на оборотной стороне листа должны быть равны, то есть они должны отражаться зеркально по отношению друг к другу. Например, если на одной стороне листа левое поле равняется 20 мм, а правое — 10 мм, то на оборотной стороне листа левое должно быть 10 мм, а правое — 20 мм. Это также делается для удобства при скреплении, сшивке и хранении документов.

Шрифты, отступы и выравнивание

Для создания документов необходимо использовать свободно распространяемые бесплатные шрифты. Рекомендуемые размеры — № 12, 13, 14. При составлении таблиц допускается использовать шрифты меньших размеров.

Абзацный отступ текста документа — 1,25 см. Заголовки разделов и подразделов печатаются с абзацным отступом или центрируются по ширине текста. Многострочные реквизиты печатаются через один межстрочный интервал, составные части реквизитов отделяются дополнительным интервалом.

Текст документа печатается через 1-1,5 межстрочных интервала. Если документ готовится для издания с уменьшением масштаба, текст печатается через два интервала. Интервал между буквами в словах - обычный. Интервал между словами - один пробел.

Текст документа выравнивается по ширине листа (по границам левого и правого полей документа). Длина самой длинной строки реквизита при угловом расположении реквизитов должна быть не более 7,5 см. Длина самой длинной строки реквизита при продольном расположении реквизитов должна быть не более 12 см.

Нумерация страниц

Если документ содержит более двух страниц (то есть является многостраничным), то все страницы, кроме первой, нумеруются. При этом, если страницы документы печатаются с двух сторон листа, то нумеруются обе стороны (логично, что одна сторона имеет нечетный номер, другая — четный). По требованиям указанного ГОСТа номер страницы наносится на верхнем поле листа посередине, на расстоянии не менее 1 см от верхнего края. В классическом формате номер пишется арабскими цифрами без знаков препинания, без указания слова «стр.» и знаков «тире».

Реквизиты документа

Для унификации вида документа существует понятие формата (или формуляра) документа. Речь идет не о файловом расширении, а о форме представления документа. Обязательные элементы, составляющие структуру или формат документа, называются реквизитами.

Различные документы состоят из разного набора реквизитов. Число реквизитов, характеризующих документы, определяется целями создания документа, его назначением, требованиями к содержанию и форме данного документа, способом документирования. Для некоторых документов число и состав реквизитов строго регламентированы и установлены законодательными и нормативными актами. Отсутствие или неправильное указание какого-либо реквизита в таком документе делает его недействительным.

Формат, свойственный определенному виду документа, например приказа, акта или заявления, называется типовым формуляром. Типовой формуляр характеризуется конкретным количеством обязательных

реквизитов, расположенных в строго определенной последовательности на определенных местах. Например, в формуляр заявления входят следующие реквизиты: адресат, автор, указание вида документа, текст, подпись, дата.

В соответствии с ГОСТом существует 30 реквизитов:

01 - герб (Государственный герб Российской Федерации, герб субъекта Российской Федерации, герб (геральдический знак) муниципального образования);

02 - эмблема;

03 - товарный знак (знак обслуживания);

04 - код формы документа;

05 - наименование организации - автора документа;

06 - наименование структурного подразделения - автора документа;

07 - наименование должности лица - автора документа;

08 - справочные данные об организации

09 - наименование вида документа;

10 - дата документа;

11 - регистрационный номер документа;

12 - ссылка на регистрационный номер и дату поступившего документа;

13 - место составления (издания) документа;

14 - гриф ограничения доступа к документу;

15 - адресат;

16 - гриф утверждения документа;

17 - заголовок к тексту;

18 - текст документа;

19 - отметка о приложении;

20 - гриф согласования документа;

21 - виза;

22 - подпись;

23 - отметка об электронной подписи;

24 - печать;

25 - отметка об исполнителе;

26 - отметка о заверении копии;

27 - отметка о поступлении документа;

28 - резолюция;

29 - отметка о контроле;

30 - отметка о направлении документа в дело.

Расположение реквизитов различается для формата А4 углового бланка (рисунок 2) и для формата А4 продольного бланка (рисунок 3).

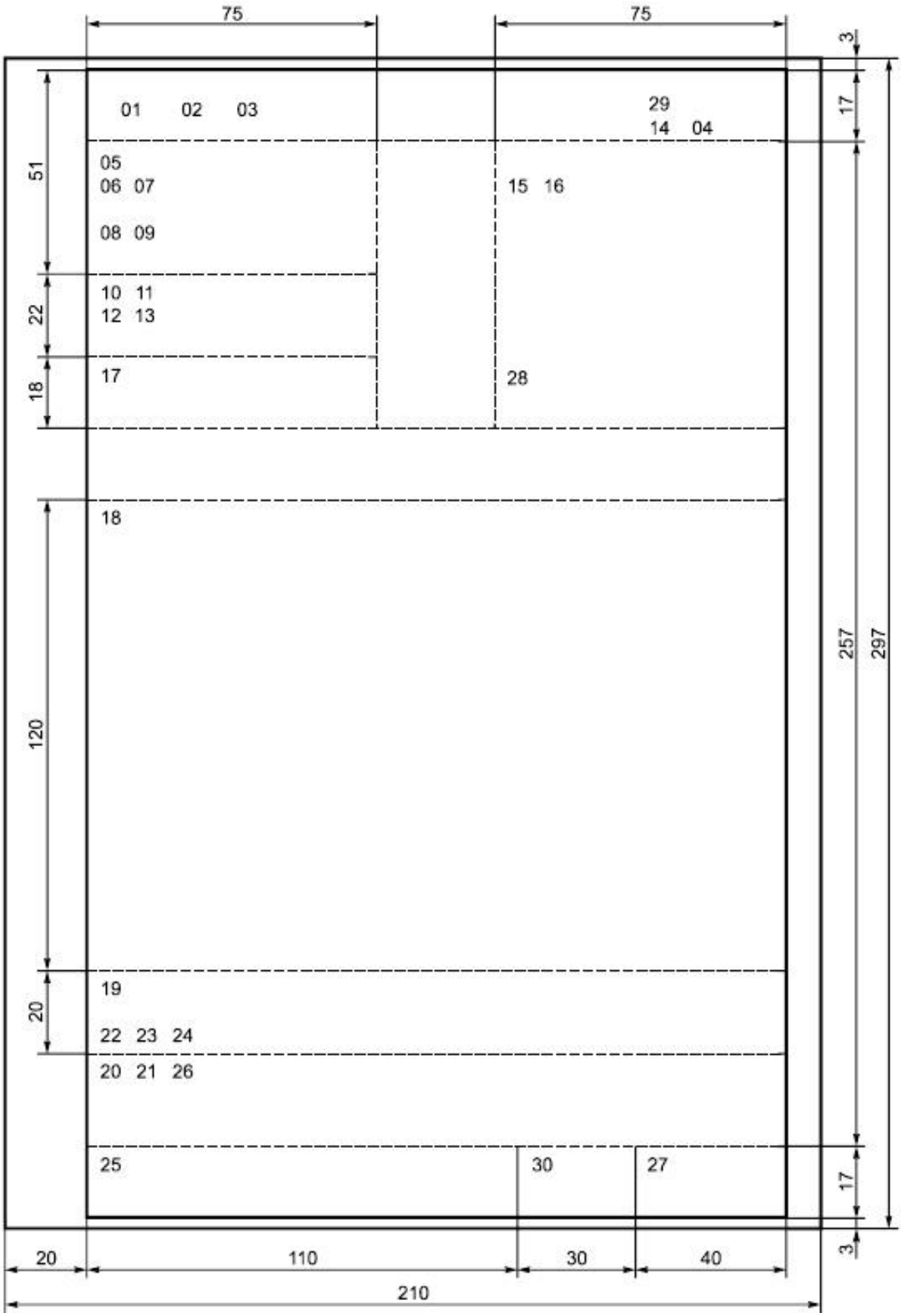


Рисунок 2 — Расположение реквизитов на угловом бланке листа А4 [9]

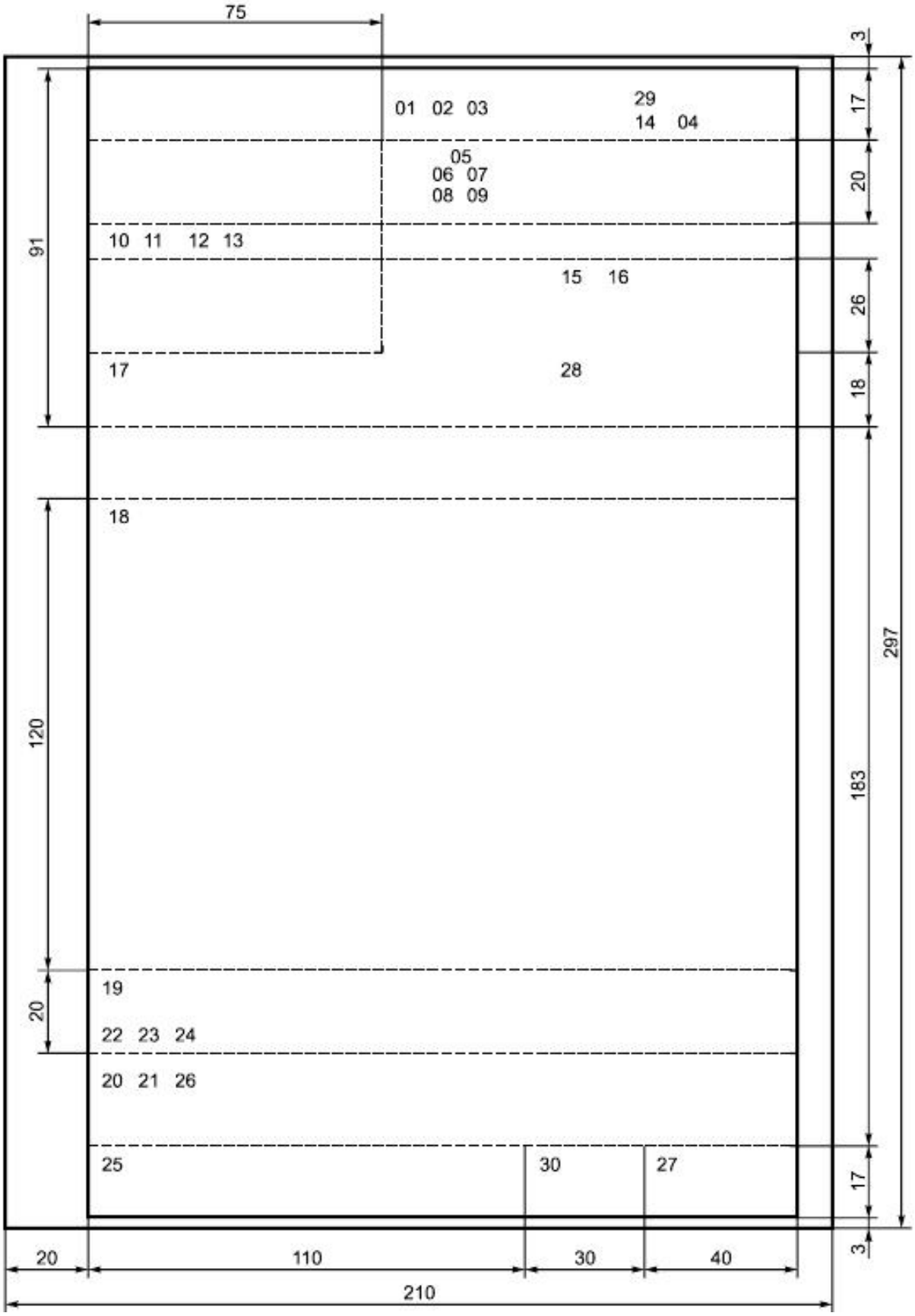


Рисунок 3 — Расположение реквизитов на продольном бланке листа А4 [9]

1.5 Юридическая сила документа

В соответствии с ГОСТ Р 7.0.8-2013, юридическая сила документа — свойство официального документа вызывать правовые последствия. Юридическая значимость документа – свойство документа выступать в качестве подтверждения деловой деятельности либо событий личного характера.

При создании документа необходимо:

–соблюдать при его подготовке действующие нормы законодательства;

–издавать документы только в пределах своей компетенции;

–соблюдать действующие в определенное время общегосударственные правила составления и оформления документов.

К числу наиболее юридически значимых реквизитов относятся: наименование организации, дата и регистрационный номер документа, подпись, печать, грифы согласования и утверждения.

Для обладания юридической силой документ, как было упомянуто ранее, должен иметь определенный набор реквизитов. Например, письмо должно иметь адрес отправителя и получателя, исходящий номер и дату, заголовок, сам текст письма и подпись. Приказ должен содержать название вида документа (собственно «ПРИКАЗ»), текст определенного содержания, даты и так далее. Для некоторых документов также необходим официальный бланк организации. Для определенных видов документов в действующих правилах оформления разработаны требования к реквизитам, удостоверяющим их юридическую силу.

Отсутствие необходимых реквизитов или неправильное их оформление может привести к тому, что документ не будет иметь юридической силы (в случае, когда документ не имеет подписи или даты, он даже не рассматривается). Если же в документе нет заголовка к тексту (например, в письме это необязательно) или отметки о приложении, то это приведет лишь к некоторым временным и трудозатратам в работе с документом, но не повлечет за собой нарушение юридической значимости.

Подпись

Широкое распространение подпись как таковая получила относительно недавно: раньше ей пользовались только представители элиты, аристократии и дворянства в России, Европе и Азии, остальным же людям приходилась придерживаться классических «предшественников» современной подписи — крестик, палочка или любой другой символ, отражающий деятельность человека.

На сегодняшний день подпись является обязательным реквизитом любого документа. Должностное лицо, проставляя подпись в документе, берет на себя ответственность за:

–достоверность документа;

–все возможные последствия исполнения (введения в действие) документа.

Право подписи предоставляется определенным лицам и может быть закреплено: в уставе предприятия; в положении о предприятии (о структурном подразделении); в инструкции по делопроизводству; в должностной инструкции работника; в приказе о распределении обязанностей.

Документы организации подписывает руководители организации (директор/ректор и тому подобные) или его заместители. Документы структурных подразделений подписывают соответственно их руководители.

По ряду вопросов правом подписи могут обладать другие работники, например ведущие специалисты предприятия. Подпись ставится на первом экземпляре документа, при необходимости — на других экземплярах, например при заключении договора.

Факсимиле

В том случае, когда необходимо иметь аналог собственноручной подписи для подписания большого количества документов, возможно изготовление её в виде штампа. Штамп может быть использован для удостоверения полномочий должностного лица. Обычно факсимильная подпись применяется в компаниях с большим объемом документооборота и в тех случаях, когда руководитель имеет высокую занятость или необходимо подписать документы ввиду отсутствия руководителя на рабочем месте.

Определение факсимиле встречается в ГК РФ и в п. 7 приложения №1 к Постановлению Правительства Москвы от 21.02.2006 года № 112-ПП «О регламенте Правительства Москвы». Конкретные случаи и порядок воспроизведения факсимиле специальными законами не регламентированы. У делопроизводителей и бухгалтеров возникает путаница, на каких документах можно ставить факсимиле, а на каких требуются живая подпись.

Право на заверение документа факсимиле имеет только один человек в организации. Зачастую это человек, представляющий интересы организации. В качестве такого доверенного лица выбирают главного бухгалтера. Для того чтобы можно было использовать факсимиле от имени

руководителя, необходимо утвердить локальный нормативный акт. В нем должен быть определен перечень лиц, которые наделяются правом визировать документы факсимиле, и список документов, к которым применяется штамп. При подготовке такого документа прописывается порядок изготовления, учета, хранения и уничтожения факсимиле.

Дата документа

Отсутствие даты на документе делает его недействительным, поэтому дата является важнейшим реквизитом документа.

Печать

Юридически значимый реквизит применяется в целях заверения подписи должностного лица на наиболее важных (или финансовых) документах является печать.

Печать свидетельствует о:

– *подлинности документа;*

– *принадлежности документа к указанной на печати организации.*

Печать проставляется на документах, издание которых влечет за собой:

– *какие-либо правовые последствия,* например создание, реорганизацию предприятия;

– *материальные последствия,* например передачу материальных ценностей, удостоверение права организации или отдельного лица на что-либо.

Гриф утверждения

Некоторые документы приобретают юридическую силу только с момента их утверждения руководителем или вышестоящим органом.

Гриф утверждения — это реквизит официального документа, придающий нормативный или правовой характер его содержанию. Обязательному утверждению подлежат: уставы, положения о предприятиях (филиалах); штатные расписания; акты проверок, акты приема-передачи; должностные инструкции; сметы, бизнес-планы, отчеты ит. п.

Регистрационный номер

Регистрационный номер свидетельствует о том, что документ прошел все стадии обработки, зарегистрирован и тем самым является официальным документом организации [4].

1.6 Наказания за подделку документов

В УК РФ [10] есть несколько статей, в соответствии с которыми определяется, как и кого наказывать за подделку бумаг. Под данным

понятием в ст. 327 Уголовного кодекса понимается изготовление фальшивых удостоверений или других официальных бумаг, в которых уточняется, какие права они предоставляют или от каких обязанностей освобождают.

Они могут быть фальсифицированы полностью (когда все части образцов не являются оригинальными, вплоть до используемой бумаги) или частично.

В удостоверениях должно быть указано, кому оно принадлежит, кем данная личность является (пенсионер, полицейский, водитель и так далее). Чтобы понять, является ли бумага официальным документом, нужно обратить внимание на следующее:

– Наличие официального источника происхождения.

– Определенная форма и реквизиты образца.

– Соответствие установленной процедуре изготовления.

– На официальной бумаге должны быть:

– Штамп организации и необходимые данные о ней.

– Подпись с указанием должности лица, его оформившим.

– Данные адресата.

Все доверенности, заявления, договора после того, как на них появится подпись любого компетентного органа (нотариуса, должностного лица), становятся официальной бумагой. Проездные и единые билеты (железнодорожные, авиабилеты) заверять не нужно: они и так считаются официальными документами.

Сами по себе подпись, печать и штамп ничего собой не представляют. Однако без них договоры, постановления, отчеты не действительны. Появление на бумаге подлинной подписи (подписей) означает, что лицо, которому принадлежит автограф, с содержимым документа ознакомлен и согласен. Если же она ненастоящая, то заверенная бумага не имеет юридической силы. Поэтому подделка подписей, печатей и штампов (вне зависимости от способа их получения) рассматривается как фальсификация документа.

В каждом отдельном случае воспроизведение фальшивой подписи рассматривается отдельно. Связано это с тем, что юридические последствия наступают не всегда. Например, если жена распишется вместо мужа при получении посылки и при этом не откроет ее, уголовное дело заводиться не будет. А вот в протоколе о дорожно-транспортном происшествии, к примеру, ставить фальшивую подпись нельзя, так как бумага имеет юридическую силу.

Подпись считается подделанной, если ее:

– Перерисовали от руки.

– Скопировали при помощи стекла, копировальной бумаги, специальной техники.

– Поставили без ведома владельца (в случае с подписью, нанесенной на штамп).

За все деяния, связанные с подделкой документов, в зависимости от их степени значимости, предусматривается штраф и ограничение свободы на срок до трех лет.

1.7 Угрозы безопасности документов

С каждым днем мы постоянно сталкиваемся с процессом документооборота, если соотнести поток документов с каналом связи, то мы получим довольно упорядоченный поток документированных данных различных сфер деятельности. В данном процессе очень большую роль играет процесс защиты документов от множества угроз. Самыми вероятными угрозами являются следующие:

– несанкционированный доступ к документам;

– случайные или умышленные действия сотрудников в процессе документооборота;

– кража или уничтожение документа;

– подмена и фальсификация документа.

Для соблюдения правил безопасности бумажных документов необходимо реализовать следующие задачи:

1. Ограничить доступ любого лица к документам, а также к копиям, черновикам и другим составным частям.
2. Организовать и обеспечить физическую безопасность документов с целью их сохранности.
3. Обеспечить сохранность информации, хранящейся в документах [11].

1.8 Методы защиты бумажных документов

Для защиты документа можно применять ряд специальных технологий и/или организационных мероприятий. Совокупность некоторых особенностей защищенного документа позволяет установить его подлинность. В большинстве случаев используются различные визуальные характеристики документа. При этом средства защиты разделяются на два вида:

– *для потребителя;*
– *для специалиста.*

Для потребителя самым главным фактором отличия подлинного документа от поддельного является быстрота и визуальная наглядность. К такому примеру защиты подлинного документа можно привезти водяной знак, который виден на свету.

Для специалистов важно подтвердить подлинность с помощью специальных технологий или средств. К примеру, инфракрасная защита на водяных знаках — её можно увидеть только тогда, когда имеется специализированная инфракрасная лампа.

Главная цель защиты документа — это невозможность получить фальсификат документа.

Защита документа делится на три основные вида:

– *технологическая защита;*
– *полиграфическая защита;*
– *физико-химическая защита.*

К технологической защите относится в первую очередь защита самой подложки бумажного носителя. Самыми распространенными методами защиты в данном случае являются:

– *водяной знак;*
– *защитные нити;*
– *защитные волокна;*
– *изменяющиеся краска;*
– *голографическая защита;*
– *оптические свойства самой бумаги.*

К полиграфической защите относятся методы, связанные со способом нанесения самой краски. Выделяют следующие методы:

– *высокая / плоская / глубокая / трафаретная печать;*
– *микропечать;*
– *совмещенные / скрытые изображения.*

К физико-химической защите относится добавление специальных веществ в состав бумаги, благодаря которому любое травление документа становится бессмысленным или раскрывает факт самого процесса травления. Важно отменить, что факт использования защиты такого рода может быть обнаружен лишь с помощью специальных приборов, в этом и заключается отличие от технологической защиты, где процесс проверки

подлинности основан исключительно на визуальном подходе. К физико-химическим методам относятся:

– *люминесцентная защита;*
– *инфракрасная защита;*
– *магнитная защита* [12].

1.9 **Документоведение**

Документоведение — это наука, которая изучает классификацию документов, варианты организации документооборота, систему строительства документирования. Документоведение занимается всеми видами, жанрами и формами документов, а также всеми системами и подсистемами документации. При этом в основном акцент ставится на документы и системы документации, связанные со стороной руководства. Документоведение является теоретической базой для делопроизводства, документной лингвистики, организации секретарского обслуживания.

Основной задачей, поставленной перед документоведением, является теоретическое обоснование процессов документационного обеспечения аппарата управления. В определенном смысле содержание понятия «документоведение» можно трактовать как теорию делопроизводства. В то же время такой рабочий процесс, как получение, распространение, регистрация документов, контроль исполнения, справочная работа, классификации документов, процедуры проверки ряда документов, их хранения и использования являются предметом делопроизводства [7].

1.10 **Документооборот**

Документооборот — движение документов в организации с момента их создания, исполнения, передачи на хранение или уничтожения. Изначально документооборот являлся одной из составляющих частей делопроизводства, но в настоящее время разница между этими двумя понятиями практически стерлась.

Деятельность любой организации характеризуется набором взаимосвязанных документов соответствующего объема, содержания и функционала. «Совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к оформлению» составляет систему документации организации.

Любой документ вне зависимости от его структуры или содержания проходит ряд стадий, которые в целом называются жизненным циклом документа:

– *документы создаются;*
– *рецензируются и исправляются;*

– *формально или неформально утверждаются;*
– *распространяются или публикуются для более широкой аудитории;*
– *выполняют свою основную функцию и попадают в архив;*
– *при необходимости извлекаются из архива, а затем снова архивируются.*

Необходимо также учитывать, что в процессе делопроизводства возможно повторение некоторых стадий.

Отдельно можно выделить следующие этапы обработки входящих и исходящих документов:

– *прием и первичная обработка;*
– *предварительное рассмотрение и распределение;*
– *регистрация документов;*
– *направление на исполнение и исполнение документов;*
– *оформление и удостоверение документов;*
– *отправка.*

Вопросы контроля исполнения и хранения документов обычно представляют собой особый класс задач делопроизводства. Вся документация организации по отношению к аппарату управления делится на три документопотока: входящие документы (поступившие в организацию извне от каких-либо субъектов), исходящие документы (отправленные из организации внешним субъектам) и внутренние документы (функционирующие и регулирующие отношения внутри организации) [13].

1.11 Служба ДОУ

Делопроизводство (или документационное обеспечение управления) — вид государственной, муниципальной, научной, коммерческой и некоммерческой деятельности, связанной с вопросами документирования и организации работы с документами. Документооборот или делопроизводство относится к соответствующей службе — службе ДОУ. В Российской Федерации данная деятельность регламентирована ГОСТ Р 7.0.97-2016.

Функции службы ДОУ

Обычно функция обеспечения централизованного документооборота возлагается на специализированный отдел. Но данная практика применима для крупных компаний; в небольших организациях функции всей службу документационного обеспечения управления передаются секретарю руководителя компании. В общем, служба ДОУ может быть представлена в

организации как самостоятельным структурным подразделением, так и отдельным сотрудником

Основными задачами службы ДОУ являются: обеспечение первичной обработки входящих документов, предварительного рассмотрения документов, регистрация, передача документов на рассмотрение руководству, передача документов на исполнение, исполнение документов, контроль исполнения документов, хранение исполненных документов, организация подготовки и отправки исходящих документов, организацию создания и исполнения внутренних документов.

В службе ДОУ условной организации, согласно нормам, должны работать три человека. В первую очередь в компании появляются секретарь и делопроизводитель.

Секретарю целесообразно передать:

–контроль оформления документов, представляемых на подпись руководителю;

–представление документов на подпись руководителю;

–направление документов на исполнение;

–контроль исполнения документов.

Вся эта деятельность связана с работой с директором и исполнителями, которых назначает директор. Кроме того, эти задачи не требуют немедленного исполнения, и секретарь сможет сам планировать свой день, оставив время для приема посетителей, организации совещаний, выполнения поручений руководителя и прочих обязанностей, напрямую не связанных с делопроизводством.

Делопроизводитель получит в сферу своей ответственности следующие процессы:

–прием и предварительное рассмотрение входящих документов;

–регистрация входящих документов;

–контроль оформления исходящих документов;

–регистрация исходящих документов;

–отправка документов по почте;

–регистрация внутренних документов;

–заверение копий документов.

Третьему работнику отдела достанутся следующие функции:

–разработка номенклатуры дел;

–организация хранения документов;

–разработка, внедрение и ведение Табеля и Альбома унифицированных форм документов;

–разработка и внедрение локальных нормативных актов, регламентирующих процессы делопроизводства.

Организация службы ДОУ

В практике работы организации традиционно существуют два подхода к формированию отдела документационного обеспечения управления.

–отдел планируется заранее, а количество и функционал работников, должностные инструкции разрабатываются до того, как подразделение будет создано.

–отдел развивается спонтанно, часто «вырастая» из одного секретаря.

Работу по распределению обязанностей лучше всего производить поэтапно:

1 - определение процессов делопроизводства, применяемых в организации.

2 - определение объема документооборота и динамики его роста.

3 - приведение численности персонала службы ДОУ в соответствие с нормами.

4 - распределение функций между сотрудниками.

5 - планирование взаимозаменяемости работников [14].

Инструкция по делопроизводству

В России существует инструкция по делопроизводству (документационному обеспечению управления), являющаяся базовым документом, регламентирующим правила обработки документов при создании, редактировании, утверждении и последующих этапах жизненного цикла. Несмотря на то, что существуют типовые варианты инструкций по делопроизводству, предполагается, что каждая организация «донастраивает» инструкцию в соответствии со своими особенностями.

Указанная инструкция, иными словами, является подробной методикой по работе с документами. Разрабатывается инструкция по делопроизводству непосредственно службой ДОУ в большей степени для сотрудников организации, так или иначе имеющих дело с документами, чем для внутреннего пользования.

В процессе формирования инструкции выделяются следующие этапы:

–сбор и анализ материала;

–разработка проекта инструкции, ее согласование и утверждение;

–внедрение инструкции в организации.

В общем, инструкция по документационному обеспечению управления используется для унификации процессов обработки документов в компании. Как у любого документа верхнего уровня, у инструкции есть

определенная цель, заключающаяся в повышении эффективности работы с документами и качества создаваемых и обрабатываемых документов. Кроме этого, в инструкции ставятся задачи по формированию и контролю упорядоченных документационных потоков, оптимизации управленческих решений. Достижение представленных цели и задач способствует повышению эффективности деятельности организации.

Кроме цели и вытекающих задач, инструкция содержит в себе указания о том, какие документы (группы документов) формируются и обрабатываются службой ДОУ, а какие, соответственно, в отделах организации или структурных подразделениях. Это необходимо для разумного расходования ресурсов и исключения дублирования документов.

Инструкция утверждается приказом руководителя организации. При этом, в приказе необходимо отразить пункты о внедрении и обязательном исполнении инструкции, о появляющихся полномочиях и поручениях службы ДОУ, отделов и подразделений и их руководителей. Инструкция должна быть доведена до каждого работника организации [15].

Подсчет объема документооборота

Формула для подсчета объема документооборота следующая:

$$\text{Общий объем документооборота} = \frac{\text{количество поступивших документов}}{\text{количество копий поступивших документов}} + \frac{\text{количество отправленных документов}}{\text{количество копий отправленных документов}} + \frac{\text{количество внутренних документов}}{\text{количество копий внутренних документов}}$$

В числителе обозначается общее количество документов как единиц учета, то есть объем документооборота, необходимый для анализа процессов документирования и рациональной организации всех бизнес-процессов и делопроизводства, в знаменателе — количество копий документов, необходимое для расчета численности сотрудников, анализа соблюдения норм выработки при работе с документами и разработки новых норм.

Традиционно предлагается нижеприведенная методика расчета численности работников отдела ДОУ. Она определяет оптимальное количество сотрудников в зависимости от объема документооборота и количества исполнителей. Рассчитаем численность персонала ($Ч$) отдела ДОУ в компании по формуле 1:

$$Ч = 0{,}00016 * Д^{0,98} * Р^{0,1}, \quad (1)$$

где 0,00016 — постоянный коэффициент, отражающий средний уровень производительности труда работников делопроизводства, Д— объем документооборота (в числе документов по таблице), Р — количество работников организации.

Допустим, Р = 100, тогда: $0{,}00016 * 13270^{0,98} * 100^{0,1} = 0{,}00016 * 10975 * 1{,}6 = 2{,}8$.

Таким образом, при существующем объеме документооборота количество работников в отделе ДОУ условной компании — три человека.

Вопросы к разделу 1

1. Перечислите актуальные законодательные акты, содержащие информацию о понятии «документооборот».
2. Что такое документооборот?
3. Что такое документоведение?
4. Что такое делопроизводство?
5. Перечислите виды документов по ограничению доступа.
6. Перечислите виды документов по степени подлинности.
7. Какими функциями обладает документ?
8. Перечислите наиболее юридически значимые реквизиты для документов.
9. Чем факсимиле отличается от собственноручной подписи?
10. В каких случаях подпись считается подделанной?
11. В чем разница оригинала и подлинника?
12. Перечислите 7 наиболее важных реквизитов документа.

2. Электронный документооборот

2.1 История и определение

Под электронным документом интуитивно понимается информация в электронной форме, воспроизводимая (читаемая и отображаемая) компьютерной техникой. Другими словами, электронный документ — это документ, который представлен в электронном виде. Электронные документы могут быть ***формализованными*** (с помощью программных средств распознавать их содержимое), и ***неформализованными*** (скан-копия) [16].

Однако существует несколько дополняющих друг друга официальных определений, с формальной точки зрения более точно описывающих понятие «электронный документ».

Первыми носителями информации, воспроизводимой с помощью ЭВМ, являлись *матричные носители*. К ним относятся перфокарты и перфоленты. Например, в начале 20-го века перфокарты применялись для обработки анкет первой Всероссийской переписи населения. Массив из 122 миллионов карт (по числу переписанного населения) обрабатывали 110 электрических счетных агрегатов американской фирмы «Холлерит». Несмотря на «автоматизацию» процесса, результаты переписи были получены спустя 8 лет. В 1920 годы появились первые ручные перфокартотеки: поиск информации в них осуществлялся путем пропускания металлической спицы через отверстие, соответствовавшее нужному понятию, сквозь массив перфокарт; при этом в базе данных хранилась только некоторая поисковая информация, а не полнотекстовый вариант искомого документа.

В 60-е годы происходит дальнейшее развитие матричных носителей информации и, соответственно, поднимается вопрос о возможности и необходимости разработки специальных баз данных, содержащих полные версии хранящихся документов и позволяющие получать доступ напрямую к ним, а не к их поисковым данным.

Для информационных поисков начинают применять *пленочные и оптические носители* информации — микрокарты и рулонную микропленку. Они представляли собой микрофишу или микрофильм, на котором вторичная информация обозначается в виде различных комбинаций черных и белых прямоугольников, уменьшенных путем микрофотокопирования. Для хранения такой пленки требовалось в 200–250 раз меньше объема, чем для хранения перфокартотеки.

Необходимость в хранении большого объема документов различного вида стимулирует развитие области носителей информации. Появляются *магнитные носители* — носители, в которых информация фиксируется намагничиванием специальных дисков, барабанов, магнитных лент, замыканием строго определенных участков системы электроцепей. Появляются также и смешанные типы носителей - к ним относятся киноленты с микрофильмом, микрофильмовые карточки, барабаны и диски с микрофильмами.

История появления самого понятия ***«электронный документ»*** в России начинается в 1970-е годы в СССР с термина *«машиночитаемые документы»*. С конца 1980-х гг. возникла проблема определения правового статуса электронного документа. Некоторыми архивистами было заявлено, что машиночитаемые записи 1960-х — начала 1980-х гг. не обладают юридической силой, так как они не имеют общепринятых атрибутов документов: печатей, подписей или других форм установления подлинности. Вышедший в 1984 г. ГОСТ 6.10.4-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники» закрепил факт наличия в документальной среде документации на новых носителях. Под машиночитаемым документом понимали «документ, пригодный для автоматического считывания содержащейся в нем информации» [17].

ГОСТ 6.10.1-88 «Унифицированные системы документации» содержал четыре определения, относящихся к машиночитаемому документу:

- *машинно-ориентированный документ;*
- *документ на машинном носителе;*
- *документ на машинном магнитном носителе (магнитной ленте, магнитном диске);*
- *машинограмма* [18].

Фактически форма и структура реквизитов таких документов не отличается от бумажных; единственным отличием является возможность создания и редактирования на ЭВМ и, соответственно, пригодность для воспроизведения на ЭВМ. Тогда же впервые поднимался вопрос о возможности воспроизведения документов на ЭВМ с различными операционными системами (вопрос кросс-платформенности электронных документов будет рассмотрен далее).

Несколько другая интерпретация машиночитаемого документа дана в ГСДОУ (Государственная система документационного обеспечения управления в. 2.3.3.1) 1991 года: под ним понимается «документ, пригодный

для автоматического считывания содержащейся в нем информации». По мнению М. В. Ларина, ученого, занимающегося проблемами документоведения, ошибка этого определения заключалась в преувеличении возможностей техники по считыванию информации в автоматическом режиме. В целом даже сегодня, при огромном прогрессе вычислительной техники, это далеко не всегда возможно выполнить без участия человека.

В современном законодательстве есть несколько определений понятия «электронный документ»:

– *электронный документ* — документ на машиночитаемом носителе, для использования которого необходимы средства вычислительной техники (п. 3.1 ГОСТ 7.83-2001 «Система стандартов по информации, библиотечному и издательскому делу Электронные издания. Основные виды и выходные сведения»);

– *электронный документ* — документ, в котором информация представлена в электронной форме (Согласно определению, представленному в п. 3.1 «ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» (утв. Приказом Росстандарта от 17.10.2013 № 1185-ст));

– *электронный документ* — информационный объект, состоящий из двух частей:

1. реквизитной, содержащей идентифицирующие атрибуты (имя, время и место создания, данные об авторе и т.д.) и электронную цифровую подпись и
2. содержательной, включающей в себя текстовую, изобразительную, аудио- или мультимедийную информацию, которая обрабатывается в качестве единого целого. При этом взаимодействие частей электронного документа обеспечивается соответствующими программно-технологическими средствами (ГОСТ Р 7.0.95-2015 Система стандартов по информации, библиотечному и издательскому делу. Электронные документы. Основные виды, выходные сведения, технологические характеристики);

– *электронный документ* — это документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также передачи по информационно-телекоммуникационным сетям или обработки в информационных системах (п. 11.1 ст. 2

Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»);

– *электронный документ* — информация в электронной форме, подписанная квалифицированной электронной подписью, равнозначный документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе. Данное определение содержится в ФЗ от 6.04.2011 г. № 63-ФЗ «Об электронной подписи».

В 2005 году Государственная Дума Федерального Собрания РФ предприняла попытку легализовать понятие электронного документа в самостоятельном законе: был создан проект Федерального закона № 159016-4 «Об электронном документе». В нем поднимались и регламентировались вопросы юридической силы электронного документа и правовой режим использования. Кроме этого, проект затрагивал проблемы обеспечения безопасности электронного документа. Законопроект не был поддержан Правительством РФ, потому что некоторые положения дублировали ФЗ от 10.01.2002 г. №1-ФЗ «Об электронной цифровой подписи» (предыдущий вариант действующего закона № 63 «Об электронной подписи») и нуждались в комментариях и уточнениях.

Характерными свойствами электронного документа являются:

–*достоверность* — свойство электронного документа, при котором содержание электронного документа является полным и точным представлением подтверждаемых операций, деятельности или фактов и которому можно доверять в последующих операциях или в последующей деятельности;

–*целостность* — состояние электронного документа, в который после его создания не вносились никакие изменения;

–*аутентичность* — свойство электронного документа, гарантирующее, что электронный документ идентичен заявленному;

–*пригодность для использования* — свойство электронного документа, позволяющее его локализовать и воспроизвести в любой момент времени.

В целом реквизиты ***формы*** электронного документа соответствуют реквизитам бумажного документа — следовательно, если говорить о классическом текстовом документе, то электронный документ оформляется также.

Кроме того, в соответствии с ГОСТ Р 7.0.95-2015, сам электронный документ (как файл) имеет метаданные (описательные, структурные,

административные и идентификационные) и реквизиты (справочные и сервисные). Также электронные документы содержат выходные сведения:

1.титульные данные;

2.сведения об авторе(ах) и других физических и юридических лицах, участвовавших в создании электронного документа;

3.заглавие к тексту или общее заглавие (если заглавие отсутствует, то теоретически его можно сформировать по первой фразе текста/аудио-/видеозаписи или на основании общего анализа содержания);

4.форму содержания электронного документа, которая определяется по природе основной информации (например, текст, звукозапись, аудиовизуальное изображение);

5.название и адрес веб-сайта, на котором хранится электронный документ;

6.дату, место и время создания электронного документа;

7.вид электронного документа (например, электронный каталог, заявка в электронной форме и тому подобное);

8.идентификационный номер (по аналогии с бумажным делопроизводством), который используется для регистрации электронного документа;

9.соотношение с исходным источником (оригинальность);

10.область физического описании, в котором указываются формат, размер, программно-аппаратная среда электронного документа, дата обновления и прочее;

11.физический адрес (IP-адрес, URL-ссылка, место хранения носителя и так далее);

12.минимальные системные требования;

13.библиотечную спецификацию, которая содержит срок хранения, учетный номер документа в библиотечном фонде;

14.знак информационной продукции [19].

Если рассматривать электронный документ с точки зрения универсальности воспроизведения, то представляется возможным выделить платформозависимые электронные документы (доступные для просмотра только на одной аппаратной платформе и/или операционной системе) и платформонезависимые (кроссплатформенные) электронные документы (доступные для просмотра более чем на одной аппаратной платформе и/или операционной системе).

Аналогично бумажному документу:

– *электронные документы могут быть общего доступа и ограниченного доступа;*

– под жизненным циклом электронного документа понимается последовательность событий от создания документа до передачи его на хранение в архив.

2.2 Юридическая сила электронного документа

Электронные документы обладают юридической силой при соблюдении следующих условий:

1. *Соответствие нормативным актам.* К сожалению, не все документы могут обладать юридической силой в электронной форме. Но если в законе или ином нормативном акте нет прямого указания, что документ составляется только на бумаге, значит, его можно публиковать в электронном виде. Вопросы работы с электронными документами также затрагиваются в нормативных правовых актах, посвященных отдельным предметным сферам правового регулирования: гражданскому, административному, уголовному, уголовно-процессуальному, трудовому, налоговому и другому законодательству РФ.

2. *Содержимое и форма.* Если кратко, то содержимое документа не должно противоречить законам Российской Федерации. Требования же к форме электронного документа — фактически такие же, как к форме бумажного документа. Более того, из-за невозможности повсеместного внедрения и не самой высокой надежности современных СЭДО предполагается, что наиболее важные документы (включая документы, регламентирующие финансовые отношения) дублируются на бумажных носителях (распечатываются). В таком случае обязательным требованием является соответствие электронного документа нормам оформления бумажного документа. Более того, унифицированная форма является более простой для обработки как сотрудником службы делопроизводства или контролирующими органами, так и автоматизированными средствами (особенно когда речь идет о распознавании текста на скан-копиях). Однако некоторые формы документирования событий хозяйственной деятельности субъектов не имеют столь строгих требований по оформлению, и зачастую организации сами устанавливают некоторые нормы и форматы оформления внутренней документации.

3. *Формат.* Аналогично бумажному документу, электронный документ представляет собой структурированную с помощью реквизитов информацию. При фиксировании на бумажном носителе информация структурируется в соответствии с нормативно закрепленным формуляром или требованиями по наличию обязательных реквизитов. Электронный

документ точно так же представляет собой информацию, которая должна быть представлена в соответствии с определенной структурой. На основании формата электронного документа можно определить вид документа, длину и расположение полей и прочее. Когда формат универсален и известен всем участникам документооборота, то они без труда с помощью своего программного обеспечения смогут воспроизвести (прочитать) и обработать электронный документ.

4. *Порядок передачи документа* тоже может влиять на юридическую значимость. Для обмена электронными документами используются системы электронного документооборота (СЭДО), речь о которых пойдет далее. В таком случае организации подписывают соглашение об электронном документообороте и выбирают подходящую по параметрам СЭДО. Но существуют и требования для передачи документов определенного вида. Так, например, электронные счета-фактуры (особый вид документов для налоговой службы) обязательно должны быть переданы в определенном порядке (Налоговый Кодекс РФ, ст. 169). Такой порядок был утвержден Приказом Минфина от 25.04.2011 №50Н. Неисполнение данного порядка влечет за собой потерю юридической значимости электронных счетов-фактур. С другой стороны, для документов другого вида, выставляемых в электронном виде контрагенту, может не быть требований к порядку передачи. Порядок обращения с электронными документами внутри организации и между организациями будет рассмотрен далее.

5. *Подписи.* Электронная подпись, согласно Федеральному закону 63-ФЗ «Об электронной подписи», придает электронным документам юридическую значимость (об этом подробнее будет рассказано далее) [20].

2.3 Методы защиты электронного документа

Существует несколько методов защиты электронных документов, появившихся, в принципе, на основе методов защиты бумажных документов:

1.***Маркировка.*** Одним из классических методов защиты, направленных в том числе на обнаружение нарушителя, является маркировка. Данный метод основан на добавлении специальной отметки (дополнительной информации) на электронный документ, которая придает документу особый статус и запрещает копирование (и, соответственно, распространение) и редактирование. В случае, когда необходимо выявить источник утечки конфиденциального документа, маркировку могут оформить незаметной или неочевидной. В качестве простого примера можно привести

аналогичный бумажному делопроизводству вариант, когда перед распространением сотрудникам в нескольких копиях документа ставят специальный символ (точку или прозрачный пробел между словами). При обнаружении такого документа в сети можно определить, кто именно из сотрудников «слил» документ.

Nota bene: более сложный вариант для маркировки бумажных документов — использование специализированных программно-аппаратных комплексов в связке с МФУ, позволяющих менять интервалы и кегль шрифта индивидуально для каждого экземпляра документа. Такой вид защиты позволяет выявить источник утечки уже, к сожалению, после произошедшего инцидента и, соответственно, не позволяет защитить документ от нарушения конфиденциальности.

2.***Пароль.*** Одним из самых простых, известных, доступных и распространенных способов повысить уровень защищенности электронного документа от НСД заключается в установке пароля на документ или электронный архив. Обычно это делается с помощью встроенного программного инструментария, например, в приложениях Microsoft Word или Acrobat можно ограничить возможность редактирования, копирования содержимого документа и даже печать. Однако в данном случае необходимо учитывать, что обеспечение конфиденциальности также находится под угрозой, поскольку если, например, разрешено чтение, то злоумышленнику не составит труда при необходимости сделать несколько снимков экрана и выложить ценную информацию в открытый доступ.

3.***Доступ по цифровому (электронному) ключу.*** Метод основывается на наличии у пользователя физического ключа (флеш-накопителя или SD-карты) для расшифровки документа. Фактически электронный ключ не является средством защиты информации от распространения, но даже если злоумышленнику удалось скопировать защищенный цифровым ключом документ, то открыть и отредактировать он его, скорее всего, при отсутствии необходимого ключа не сможет. Однако данный метод защиты также обладает рядом недостатков:

− ответственность за сохранность и правомерное использование лежит на владельце электронного ключа;

− необходимо обеспечить безопасную передачу такого ключа между лицами, у которых есть доступ к данному документу. При этом чем больше копий цифрового ключа, тем выше вероятность компрометации. Особенное значение данный недостаток приобретает в случае, когда необходимо оперативное редактирование документа разными сотрудниками;

− сам по себе носитель электронного ключа имеет свою стоимость. Более того, существуют определённые требования ФСТЭК и ФСБ по отсутствию недекларированных возможностей в ПО, установленном на носителе;

− носитель электронного ключа может выйти из строя. В некоторых случаях производители могут предоставить новый, если такое развитие событий предусмотрено гарантией, однако даже этот процесс может занять какое-то время, а значит, нарушить доступность электронного документа.

4.***Система управления правами доступа.*** В основном этот метод защиты документов используется для корпоративных пользователей на базе службы управления правами Active Directory (AD RMS). Документы, защищенные AD RMS, шифруются, а автор может устанавливать разрешения для тех, кто получит доступ к файлам. Список возможных ограничений прав:

–Чтение, изменение, печать.

–Срок действия документа.

–Запрет пересылки электронного письма.

–Запрет печати электронного письма.

5. ***Комбинированные методы защиты документов.*** Все представленные методы имеют достоинства и недостатки. Производители систем защиты электронных документов постоянно работают над тем, чтобы соединить преимущества всех методов в одном универсальном решении. Представленные ниже идеи также могут составлять эффективную комбинацию:

–предоставление доступа к документу по паролю, который может быть отправлен на электронную почту или мессенджер, привязанный к мобильному устройству и номеру телефона;

–привязка к уникальному материальному носителю (например, уже используемому мобильному устройству, фитнес-трекеру или подобному устройству);

–управление правами доступа через интернет в режиме реального времени (отличным примером данной опции в целом является гугл-документ);

–отображение на документе специальных меток для обозначения особого режима распространения [21].

2.4 Электронная подпись

Под электронной подписью (ЭП) в классическом виде понимают дополняющие электронный документ реквизиты (разумеется, в электронном виде), позволяющие однозначно определить автора документа, время его создания и факт обеспечения целостности. При этом речи об обеспечении конфиденциальности не идет: ЭП не обеспечивает конфиденциальность документов при передаче, однако может использоваться со стандартными методами шифрования.

В соответствии с федеральным законом «Об электронной подписи» от 06.04.2011 N 63-ФЗ, различаются несколько видов ЭП:

– **простая**;

– **усиленная**:

  – *неквалифицированная;*

  – *квалифицированная.*

Простая ЭП является фактически совокупностью логина и пароля для входа в информационную систему, в которой создается документ. При этом юридическую силу простая ЭП имеет только в корпоративных информационных системах — специализированных системах, для регистрации в которых используются документы, удостоверяющие личность пользователя и, соответственно, позволяющих однозначно идентифицировать человека. Примером корпоративной информационной системы является ИСУ Университета ИТМО: любое действие или созданный документ, в том числе электронное письмо, имеет автора, дату и имеет контроль версий (если говорить, например, о различных заявках).

В то же время другие открытые информационные системы, требующие регистрации, но не ограничивающие круг лиц, использующих данные системы, привязанные к личному адресу электронной почты или мобильному телефону, теоретически могут обеспечивать юридическую силу для простой электронной подписи, но вряд ли могут использоваться при, например, судебных разбирательствах, разве что в случаях, когда на основании дополнительных сведений можно утверждать, что указанный номер мобильного телефона или адрес электронной почты принадлежит определенному человеку.

Целостность документа после подписания простая электронная подпись также не гарантирует.

Усиленная электронная подпись создается с помощью криптографических преобразований и хэш-функций, позволяет определить автора и факт внесения изменений в электронный документ. В классическом варианте используются асимметричные алгоритмы шифрования. В целом

процесс подписания и проверки усиленной ЭП можно свести к следующей последовательности шагов:

1) Генерация ключевой пары. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается закрытый ключ, вычисляется соответствующий ему открытый ключ.

2) Формирование подписи. Для заданного электронного документа с помощью закрытого ключа вычисляется подпись. Данный шаг можно разбить на два этапа:

1. вычисление хэш-суммы от документа;
2. шифрование полученной хэш-суммы закрытым (приватным) ключом пользователя (полученная в результате преобразования информация фактически и является ЭП документа);

3) Передача документа и ЭП.

4) Проверка (верификация) подписи. Для данных документа и подписи с помощью открытого ключа определяется действительность подписи. Этот шаг также можно представить следующим образом:

1. вычисление хэш-суммы от полученного документа с помощью такой же функции;
2. расшифровка ЭП с помощью открытого (публичного) ключа пользователя;
3. сравнение полученных в п.4 и п.5 хэш-сумм.

В результате сравнения можно выявить, обеспечена ли целостность документа или нет. Если да, то, соответственно, подтверждается авторство и время подписания документа. Если же полученные хэш-суммы не совпадают, то целостность документа была нарушена. В данном случае либо запрашивается повторная передача документа, либо выбирается другой канал переда данных.

Для того, чтобы использование цифровой подписи имело смысл, необходимо выполнение двух условий:

–Верификация подписи должна производиться открытым ключом, соответствующим именно тому закрытому ключу, который использовался при подписании.

–Без обладания закрытым ключом должно быть вычислительно сложно создать легитимную цифровую подпись.

Поскольку усиленная ЭП направлена на подтверждение целостности документа, хэш-сумма в подписи шифруется уникальным закрытым ключом автора, а проверить целостность документа может любой субъект,

каким-либо образом получивший открытый ключ автора. При этом обеспечение конфиденциальности передаваемых документов - отдельная задача защиты информации, не отличающаяся от защиты любой другой информации ограниченного доступа.

Квалифицированная электронная подпись — самая широко применяемая и регулируемая из всех видов ЭП. Для получения квалифицированной ЭП подается заявление и оплачивается государственная пошлина. В результате владелец квалифицированной ЭП получает в распоряжение от аккредитованного удостоверяющего центра ключи ЭП, специальное ПО, сертификат электронной подписи, в котором указаны следующие сведения:

1) уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата;

2) фамилия, имя и отчество (если имеется) — для физических лиц, наименование и место нахождения — для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;

3) уникальный ключ проверки электронной подписи;

4) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;

5) наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи;

6) иная информация (в соответствии с ФЗ «Об электронной подписи»).

Аккредитованные удостоверяющие центры выдают электронную подпись на токенах с USB-разъемом или смарт-картах. Эти цифровые носители защищены паролями и сертифицированы в соответствии с требованиями ФСТЭК и ФСБ РФ. И, в соответствии с постановлением правительства РФ от 28.11.2011 № 976, уполномоченным органом проверки ЭП может стать любой удостоверяющий центр, получивший аккредитацию у Минкомсвязи России.

В данном случае закрытый или приватный ключ ЭП называется ключом ЭП, а открытый (публичный) ключ называется ключом проверки ЭП. Чаще всего оба ключа генерируются и выдаются удостоверяющим центром. Документ, подписанный с помощью сертификата квалифицированной ЭП, приравнивается к документу, который собственноручно подписан физическим лицом или уполномоченным представителем юридического лица. Для проверки авторства и целостности документа получатель (или оппонент автора) может запросить у УЦ

сертификат ЭП и, таким образом, проверить принадлежность ключа проверки ЭП автору и, соответственно, проверить целостность электронного документа. Проверить сертификат ЭП можно также, например, на портале Госуслуг.

Сертификат ключа подписи выдается на 1 год, однако действие поставленных с его помощью подписей не ограниченно; по истечении данного срока сертификат становится недействительным. Для того чтобы продолжить работать в системе электронной документации, следует продлить сертификат.

Более подробная информация о формировании документов и функциях удостоверяющих центров представлена в ФЗ №63 «Об электронной подписи».

Именно квалифицированная ЭП открывает владельцу максимум возможностей для работы на электронных торговых площадках и информационных ресурсах. Она подходит для работы на государственных электронных порталах и получения финансовых услуг, для организации закупок в соответствии с 223-ФЗ, участия в коммерческих торгах и торгах по реализации имущества банкротов, даже для организации международного электронного документооборота (информация об этом подробнее представлена далее).

Неквалифицированная электронная подпись позволяет определить автора документа и проверить, были ли внесены в файл какие-либо изменения после его отправки. Подписанный с его помощью документ заменяет бумажный документ только в случаях, оговоренных законом, или по согласию сторон. Процесс формирования неквалифицированной ЭП в целом не отличается от формирования квалифицированной ЭП; однако выпуск ключей неквалифицированной ЭП возможен внутри организации или даже на устройстве пользователя, и сертификат подписи не является необходимым условием ее существования, а ключ проверки может распространяться любым удобным автору и пользователям системы способом.

В любом случае сохранность ключей ЭП ложится на плечи владельцев. Необходимо учитывать, что с помощью квалифицированной ЭП могут быть подписаны практически любые документы, в том числе напрямую связанные с благосостоянием владельца, поэтому при утере ключа электронной подписи или появлении подозрений о компрометации необходимо сразу же сообщить об этом в УЦ.

Для закрепления знаний о разных видах электронной подписи в приложении к данному пособию приведены кейсы для решения и самостоятельной проверки [22].

2.5 Юридическая сила ЭП

ЭП стала инструментом, без которого в настоящее время невозможно совершить определенные действия, имеющие юридическую значимость, например:

–Осуществлять документооборот с государственными структурами и контрагентами-организациями.

–Дистанционно подписывать договоры и крупные контракты.

–Подтверждать свое авторство.

–Подавать налоговые декларации, бухгалтерские отчеты.

–Получать информацию с сайта государственных услуг и др.

В соответствии с ФЗ №63 документы, которые подписаны электронной подписью, имеют такое же юридически важное значение, как и бумаги, подписанные от руки человеком. То есть ЭП является аналогом собственноручной подписи лица, подписывающего дистанционно документ, поэтому юридическая сила ЭП неоспорима.

Электронный документ, подтвержденный ЭП, будет иметь силу совершенно в любых правоотношениях, будь то коммерческая, банковская, бухгалтерская, финансовая, налоговая и иная сфера. Электронная подпись и юридическая сила — связь, которая неразрывна, ведь она установлена действующим законодательством Российской Федерации [23].

Области использования ЭП:

1) ***Электронный документооборот***. Технология ЭП широко используется в системах электронного документооборота различного назначения: внешнего и внутреннего обмена, организационно-распорядительного, кадрового, законотворческого, торгово-промышленного и прочего. Это продиктовано главным свойством электронной подписи - она может быть использована в качестве аналога собственноручной подписи и/или печати на бумажном документе и, соответственно, отражать юридическую значимость электронного документа и представленных в нем положений.

2) ***Документооборот с физическими лицами.*** На данном этапе развития сферы электронный документооборот между физическими лицами не особо распространен. Однако, поскольку любое физическое лицо может получить электронную подпись, становится возможным заключение договоров с сотрудниками на дистанционном режиме работы

и получение от них всех отчетных материалов без использования услуг почты или курьерских служб для передачи и подписания бумажных документов.

3) Во внутреннем документообороте ЭП используется как ***средство визирования и утверждения электронных документов в рамках внутренних процессов***. Например, во время согласования договора руководитель организации подписывает его ЭП, что значит, что договор утвержден и может быть передан в исполнение.

4) При построении ***межкорпоративного документооборота*** наличие ЭП является критически важным условием обмена, поскольку является гарантом юридической силы. Только в этом случае электронный документ может быть признан подлинным и использоваться в качестве доказательства в судебных разбирательствах. Подписанный усиленной электронной подписью документ также может длительное время храниться в цифровом архиве, сохраняя при этом свою легитимность.

5) ***Электронная отчетность для контролирующих органов***. Современный подход к сдаче отчетности через Интернет состоит в том, что клиент может выбрать любой удобный для себя способ: отдельное ПО, продукты семейства 1С, порталы Госуслуг, Федеральной налоговой службы (ФНС) или Фонда социального страхования (ФСС). В основе осуществления передачи подписанных ЭП документов лежит доказательство легитимности электронной подписи с помощью сертификата ЭП, подписанного аккредитованным удостоверяющим центром, по умолчанию считающимся надежной третьей стороной и в достаточной мере обеспечивающим безопасность формирования и хранения ключей ЭП. В таком случае ЭП считается усиленной квалифицированной, а канал и метод передачи данных уже не имеют особого значения. Например, сайт nalog.ru генерирует сертификат ЭП в течение получаса, а подписать соответствующие документы можно, зная пароль от личного кабинета налогоплательщика и пароль от сертификата. При этом, если пользователь забывает пароль от сертификата, то восстановить его нельзя. Процедура отзыва и получения нового сертификата происходит в том же разделе и также занимает очень короткий промежуток времени.

6) ***Органы исполнительной власти***. Пользователь имеет возможность подписать электронной подписью заявление, отправляемое в орган исполнительной власти (при готовности органа исполнительной власти принимать заявления, подписанные электронной подписью). При реализации этого механизма используются отечественные стандарты ЭП (ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001) и применяются сертифицированные

в системе сертификации ФСБ России средства криптографической защиты информации, такие как «Aladdin e-Token ГОСТ» и «КриптоПро CSP», что дает основания считать данную подпись усиленной квалифицированной электронной подписью.

7) ***Электронные торги***. Электронные торги проходят на специальных интернет-площадках (сайтах), как государственных, так и коммерческих. ЭП поставщиков и заказчиков гарантируют участникам, что они имеют дело с реальными предложениями. Кроме того, заключенные контракты приобретают юридическую силу только при подписании обеими сторонами.

8) ***Арбитражный суд***. При возникновении каких-либо споров между организациями в качестве доказательства в суде могут использоваться электронные документы. Согласно Арбитражному процессуальному кодексу РФ, документы, полученные посредством факсимильной, электронной или иной связи, подписанные электронной подписью или другим аналогом собственноручной подписи, относятся к письменным доказательствам [24].

2.6 Атаки на ЭП

Поскольку ЭП формируются с помощью криптографических преобразований и, в частности, с использованием хэш-функций, на них возможны атаки с использованием открытого ключа:

– *Атака на основе известных сообщений.* Противник обладает допустимыми подписями набора электронных документов, которые ему известны.

– *Адаптивная атака на основе выбранных сообщений*. Криптоаналитик может получить подписи электронных документов, которые он выбирает сам.

При безошибочной реализации современных алгоритмов ЭП получение закрытого ключа алгоритма является практически невозможной задачей (из-за вычислительной сложности вычислительных задач, на базе которых построена электронная подпись). Гораздо более вероятен поиск криптоаналитиком коллизий первого и второго рода.

Коллизией первого рода является такая возможность подбора злоумышленником документа к данной подписи, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. Причина в том, что документ представляет из себя осмысленный текст, и подобрать какой-то другой подходящий текст почти невозможно. Злоумышленники, подделывая документы подбирают под

текст произвольный набор данных и вставляют его в служебные поля. Это позволяет повысить вероятность подбора документа под ЭЦП, хотя она и остается очень малой.

Коллизией второго рода называется получение двух документов с одинаковой подписью. При этом вычислительно сложная атака возможна из-за ошибок реализации алгоритмов или слабостей алгоритмов хэширования. В этом случае злоумышленник фабрикует два документа с одинаковой подписью и в нужный момент подменяет один другим. В частности, таким образом можно провести атаку на SSL-сертификаты и алгоритм хеширования MD5.

Другой вид атак на ЭП — социальные атаки, которые направлены не на взлом алгоритмов цифровой подписи, а на получение хитростью от владельца его ключей и манипуляции с открытым и закрытым ключами:

– *Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа.*

– *Злоумышленник может обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи.*

– *Злоумышленник может подменить открытый ключ владельца на свой собственный, выдавая себя за него.*

Использование протоколов безопасного обмена ключами и защита закрытого ключа от несанкционированного доступа позволяет снизить опасность социальных атак.

Возможные результаты атак на ЭП:

– *Полный взлом ЭП. Получение закрытого ключа, что означает полный взлом алгоритма.*

– *Универсальная подделка ЭП* —нахождение алгоритма, аналогичного алгоритму подписи, что позволяет подделывать подписи для любого электронного документа.

– *Выборочная подделка ЭП* — возможность подделывать подписи для документов, выбранных криптоаналитиком.

– *Экзистенциальная подделка ЭП* — возможность получения допустимой подписи для какого-то документа, не выбираемого криптоаналитиком.

– *Адаптивная атака на основе выбранных сообщений* является одной из самых «опасных» атак, и при анализе алгоритмов ЭП на криптостойкость нужно рассматривать именно ее (если нет каких-либо особых условий).

Одними из главных условий защищенности электронных документов с использованием ЭП – это использование криптостойких закрытых ключей, их надежная сохранность, проверка ЭП на подлинность, подписание проверенных документов, снижение вероятности влияния человеческого фактора [25].

2.7 Электронный документооборот (ЭДО)

Электронный документооборот представляет собой систему процессов по обработке документов в электронном виде, так называемый «безбумажный документооборот».

По логике ЭДО в целом совпадает с бумажным документооборотом. Фактически это тот же путь документа от создания до перемещения в архив; разница лишь в том, что при создании, обработке, передаче и хранении электронных документов используются компьютерные информационные системы, свойственные каналы передачи информации и электронные архивы, расположенные на специально выделенных машинах или серверах.

Законодательные акты РФ, затрагивающие вопросы электронного документооборота

В соответствии с действующим федеральным законодательством основополагающим законодательным актом, который регулирует отношения, возникающие при использовании информационных технологий (в том числе систем электронного документооборота), а также обеспечении защиты информации, является Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. №149-ФЗ. В ст.11 говорится, что электронное сообщение, подписанное электронной подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью. Также устанавливается, что 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, то есть является официальным документооборотом.

Следующим не менее важным законодательным актом в области электронного документооборота является рассмотренный выше ФЗ «Об электронной подписи» от 06.04.2011 г. №63-ФЗ, который обеспечивает правовые условия использования электронной подписи в электронных документах в качестве аналога собственноручной подписи в документе на

бумажном носителе. Иными словами, ЭП как реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, идентификации владельца сертификата ключа подписи, применяется для удостоверения электронных документов, в том числе при использовании систем электронного документооборота (СЭДО).

Гражданский кодекс РФ (ГК РФ) сообщает, что документ является основой гражданских правоотношений и содержит основополагающие понятия, такие как «сделка» и «договор». Закреплена возможность подписания документов электронной подписью (п.2 ст. 160) и обмена документами с помощью электронной связи (п.2 ст. 434).

Кодекс РФ об административных правонарушениях в п. 2 ст. 26.7 содержит положение о том, какие документы могут содержать сведения, зафиксированные как в письменной, так и в иной форме. К документам могут быть отнесены материалы фото- и киносъемки, звуко- и видеозаписи, информационных баз и банков данных и иные носители информации.

Уголовный кодекс РФ предусматривает в ст. 272-274 ответственность за неправомерный доступ к информации; создание, использование и распространение вредоносных программ для персональных компьютеров; нарушение правил эксплуатации техники, систем ЭВМ или их сетей.

Арбитражный процессуальный кодекс РФ (в ст. 75), Уголовно-процессуальный кодекс РФ (в ст. 74), Гражданский процессуальный кодекс РФ (в ст. 71) содержат положения, позволяющие рассматривать электронные документы в качестве вещественных доказательств, при этом обязательным условием удостоверения таких документов является наличие ЭП.

Отраслевые кодексы также содержат положения, касающиеся работы с электронными документами в соответствующих сферах деятельности. В частности, Налоговый кодекс РФ в ст. 80 содержит разрешение представлять налоговую отчетность в электронном виде. Таможенный кодекс РФ в п. 8 ст.63 также закрепляет, что документы, необходимые для таможенного оформления, могут быть представлены в электронной форме. Трудовым кодексом РФ в главе 49.1 предусмотрено взаимодействие дистанционного работника или лица, поступающего на дистанционную работу, и работодателя путем обмена электронными документами, используются усиленные квалифицированные электронные подписи дистанционного работника (данные изменения в ТК РФ были внесены введением в силу ФЗ № 60 от 05.04.2013 г. «О внесении изменений в отдельные законодательные акты Российской Федерации») [27].

Нормативно-методические документы, регулирующие современную организацию электронного документооборота

Государственная система документационного обеспечения управления (ДОУ) содержит рекомендации по оформлению управленческих документов, организации работы с документами, в том числе отдельный пункт посвящен автоматизации работы с документами. В п. 4.3 закреплено, что автоматизированная технология работы с документами осуществляется путем создания и внедрения автоматизированной подготовки документов, автоматизированных информационно-поисковых систем и решения других задач с использованием персональных ЭВМ и автоматизированных рабочих мест. При этом должна обеспечиваться информационно-техническая совместимость средств вычислительной техники между собой.

Для федеральных органов исполнительной власти при организации внутренней деятельности разработаны рекомендации Росархива по подготовке перечней документов работа, с которыми должна осуществляться в электронной форме (утверждены приказом Росархива от 23.12.2009 № 76). Эти рекомендации могут быть опорными для любых организаций.

Кроме того, полезными будут рекомендации по комплектованию, учету и организации хранения электронных архивных документов в архивах организаций и другие рекомендации, разработанные Росархивом.

2.8 Система электронного документооборота

Система электронного документооборота (СЭДО) — это компьютерная программа (программное обеспечение, информационная система), которая позволяет организовать работу с электронными документами в полном жизненном цикле документа (создание, редактирование, утверждение, подписание, контроль версий, поиск), а также взаимодействие между сотрудниками (передача документов, выдача заданий, отправка уведомлений и тому подобное).

На английском СЭДО называется Electronic Document Management Systems (EDMS) и переводится буквально как «система управления электронными документами». Однако в зарубежном представлении существуют более сложные, комплексные системы электронного документооборота — системы «управления корпоративными информационными ресурсами (содержанием, наполнением, контентом)» — Enterprise Content Management (ECM). Это понятие несколько шире, чем классическое понимание СЭДО. Под ECM-системой понимают набор технологий, инструментов и методов, используемых для сбора, управления,

накопления, хранения и доставки информации (контента) всем потребителям внутри организации. Например, для того чтобы стать ECM-системой, СЭДО должна содержать средства сканирования документов, гарантировать сохранность документов, поддерживать правила хранения документов и так далее.

Функционал СЭДО

В соответствии с положениями, выдвигаемыми исследовательской компанией Gartner касательно функционала СЭДО, чтобы называться комплексной СЭДО, система должна предоставлять более трех из перечисленных функций:

–управление документами (создание, контроль версий, выписка/возврат, безопасность, группировка документов и так далее);

–совместная работа над документами общего доступа;

–сканирование документов и управление образами бумажных документов;

–управление записями для долгосрочного архивного хранения, автоматизации правил и нормативов хранения, гарантирование соответствия записей законодательству и регулирующим правилам;

–workflow для поддержки бизнес-процессов, маршрутизации контента, назначение рабочих задач, изменение состояний бизнес-процесса и контроль исполнения поставленных заданий;

–управление веб-контентом для автоматизации публикаций, управление динамическим контентом и взаимодействием пользователей для этих задач.

Соглашение сторон

Как упоминалось ранее, использование неквалифицированной электронной подписи возможно даже за пределами одной организации с сохранением юридической силы, если составлено соглашение сторон. Однако для появления возможности в принципе организовать электронный документооборот между организациями необходимо составлять соглашения о переходе на электронный документооборот.

Переход на ЭДО — дело добровольное. Стороны могут выразить свое согласие или отказ работать с электронными документами. Согласие может быть выражено в различной форме — например, в конклюдентной, то есть когда участники своими действиями подтверждают согласие. Содержание соглашения участники определяют самостоятельно.

В случае, если у компаний есть потребность детально прописать особенности взаимодействия с контрагентом (например, установить

конкретные обязательства и ответственность сторон, возможные форматы входящих и исходящих электронных документов, процесс редактирования и визирования документов и так далее), лучше составить соглашение о порядке работы с электронными документами.

Логично предположить, что система электронного документооборота должна поддерживать весь жизненный цикл документов, включая организацию архивного хранения документов с доступом к электронным архивам. В свою очередь, отношения, возникающие в сфере организации хранения, комплектования, учета и использования архивных документов, регулирует Федеральный закон «Об архивном деле в РФ» от 22.10.2004 № 125-ФЗ. В ст. 5 закона говорится, что в состав Архивного фонда входят находящиеся на территории РФ архивные документы независимо от источника их происхождения, времени и способа создания, вида носителя, формы собственности и места хранения, в том числе электронные и телеметрические документы.

При использовании СЭД и ЭД появляется острая необходимость в обеспечении информационной безопасности и защиты обрабатываемой и хранящейся информации. Кроме ФЗ «Об информации, информационных технологиях и защите информации», в этой связи необходимо знать положения Федерального закона «О государственной тайне» от 21.07.1993 г. № 5485-1 и Федерального закона «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ (если в деятельности организации создается информация, составляющая данные виды тайн) [28].

2.9 **Виды СЭДО**

В соответствии с количеством реализуемых функций СЭДО делятся на:

Системы делопроизводства

Организационные системы делопроизводства подразделяются на централизованные, децентрализованные и смешанные.

Централизованные системы делопроизводства создаются на крупных, территориально распространенных предприятиях, имеющих удаленные отделения и филиалы. В таких условиях отдельная служба делопроизводства, обеспеченная современными автоматизированными системами электронного документооборота, необходимой техникой и квалифицированными специалистами, выполняет множество функций и полностью обеспечивает обмен информацией как внутри головного офиса, так и за его пределами. В задачи централизованной системы делопроизводства входит не только обработка и распределение входящей и исходящей документации, но и ведение номенклатуры дел, организация

архивного хранения документов и даже контроль над своевременностью их исполнения.

Децентрализованная система делопроизводства предприятий оптимальна для внедрения в крупных обособленных организациях, в структуру которых входит большое число подразделений. При такой организационной системе служба делопроизводства также выполняет все основные функции, связанные с документооборотом и хранением.

Электронные архивы

Электронный архив является системой структурированного хранения электронных документов, обеспечивающей надежность хранения, конфиденциальность и разграничение прав доступа, отслеживание истории использования документа, быстрый и удобный поиск. Электронный архив также является подвидом систем электронного документооборота относится к классу систем управления корпоративным контентом. Он представляет собой информационную систему, специальное программное обеспечение, призванное автоматизировать процедуры управления архивным фондом документов организации в соответствии с требованиями государственного нормативного регулирования и спецификой внутренних процессов компании. Основная задача электронного архива — обеспечить сохранность и доступность данных. Аналогично бумажному архиву, в электронном архиве создается картотека дел, в которой логируются все действия с переданным в архив документом: когда и куда документ передан на хранение, кем и когда был запрошен, на какой срок. Кроме того, в электронном архиве предусматривается возможность выборки файлов по указанным параметрам, например, по сроку хранения, чтобы вовремя удалять документы, более не требующие хранения. В простейшем случае система электронного архива должна поддерживать следующую функциональность, соответствующую требованиям к архивному делопроизводству:

– Прием на хранение и сопутствующее формирование архивных дел в СЭДО осуществляется на основе передачи документации из других информационных систем, а также оцифровки и ввода в систему архивной документации.

– Управление документацией, хранящейся как в электронном виде, так и на бумажном носителе.

– Удобный и быстрый поиск по номенклатурам, атрибутам и по тексту документов и дел.

– Учет выдачи оригиналов документов и дел.

– Предоставление доступа к архивным материалам в электронном виде.

Также некоторые источники выделяют дополнительные возможности электронного архива:

– Управление web-контентом.

– Наличие систем сообщений, позволяющих пользователям обмениваться сообщениями, а также назначать задачи и отслеживать статус их выполнения.

Workflow-системы

Workflow-система — это система электронного документооборота, цель которой заключается в обеспечения выполнения исполнителем бизнес-задач в контексте разноуровневого управления. Другими словами, WF-система координирует выполнение и контроль появляющихся в организации задач. Задания назначаются индивидуально ответственным исполнителям в соответствии с принципом о том, что сотруднику может быть доступна только та документация, которая необходима для выполнения должностных функций.

Все взаимодействие между руководителем и исполнителями, а также выполнение заданий, передача информации, подписание и передача на хранение происходит в среде информационной системы или приложении. Организации имеют множество бизнес-процессов, которые могут быть автоматизированы в рамках системы workflow. На каждой функции в выполнении поставленной задачи принимают участие различные исполнители или рабочие группы. Иногда выполнение задачи занимает достаточно длительное время, и в ней участвует несколько организаций. Для упрощения выполнения совокупности задач процессов применяются информационные системы класса workflow [29].

Комплексные или ECM-системы

Управление корпоративным информационным контентом — это управление различными документами и другими типами контента, а также их хранение, обработка и доставка в масштабах предприятия. ECM-системы автоматизируют и упрощают этот процесс. Системы электронного документооборота также относятся к ECM-системам.

Корпоративная информация обычно достаточно не имеет чёткой и единой для всех организаций структуры — это могут быть файлы различных форматов, электронные документы с различными наборами полей, а также прочие материалы, которые используются в работе

компании. Таким образом, перед ECM системами стоит задача управления и обеспечения доступности этой разнородной информации.

Еще один важный аспект работы ECM — это разграничение доступа к информации, некоторые материалы могут быть конфиденциальны или содержать коммерчески значимую информацию, которая не должна попасть «не в те руки». Классический путь организации хранения информации и доступа к ней не позволяет в достаточной мере разграничить права — как правило, если разграничение доступа и присутствует, то на уровне достаточно больших групп пользователей [30].

2.10 **Роуминг**

Роуминг в ЭДО работает аналогично роумингу между операторами сотовой связи, который обеспечивает возможность общения абонентам разных операторов мобильной связи. Таким же образом роуминг в электронном документообороте позволяет обмениваться документами участникам ЭДО, подключённым к разным операторам.

Прошло время, когда компании приходилось подключаться к системе, используемой контрагентом, с которым планировался документооборот. Подходящей альтернативы не было - применение нескольких систем ЭДО неудобно и невыгодно при большом объёме документов.

Роуминг как технология, воплощённая в опытном виде, появился в ЭДО в 2013 году. Первые вариации роуминга были результатом договорённости между конкретными участниками рынка для решения задач, связанных с необходимостью обеспечить взаимодействие крупных организаций через взаимодействие их операторов ЭДО.

Согласно требованиям, утверждённым Приказом ФНС России от 04.04.2016 № ММВ-7-6/176, роуминг может быть реализован двумя способами: через роумингового оператора или напрямую с каждым оператором электронного документооборота.

В основе роуминга ЭДО лежит технология обмена юридически значимыми электронными документами между операторами электронного документооборота, созданная Ассоциацией РОСЭУ.

Благодаря роумингу электронное взаимодействие стало свободнее — можно выбрать оператора, подходящего вам по ключевым параметрам, большинство систем электронного документооборота уже поддерживают межоператорский роуминг. Главное преимущество роуминга заключается в том, что он позволяет выбирать систему ЭДО независимо от количества компаний, подключённых к ней.

Как происходит взаимодействие в роуминге

В настоящее время механизмы настройки возможностей роуминга для конкретных абонентов ЭДО ещё не достигли уровня полной автоматизации и максимального удобства, поэтому взаимодействие начинается с создания «роуминговой пары» абонентов — логической цепочки.

У всех операторов эта процедура реализована по-разному, но в целом она похожа на подключение одной из услуг. Абонент заполняет заявку с нужными параметрами либо передаёт данные контрагента своему оператору вместе с просьбой подключить роуминг для пары абонентов. Операторы производят настройки технологического характера, обеспечивая саму возможность отправить документ от одного абонента другому.

После настройки процесс обмена, точнее то, как его видит пользователь, выглядит как процесс передачи документов в рамках одной системы ЭДО. Абонент одного оператора направляет документы, выбрав как получателя абонента другого оператора в своей системе ЭДО. Чаще всего для этого абонент загружает готовый документ с указанием получателя в систему либо находит документ вручную по основным реквизитам своего контрагента — ИНН и КПП. Получатель видит новый документ от отправителя уже в своей системе. Процесс выглядит очень быстрым и простым, если не мгновенным [31].

2.11 Угрозы информационной безопасности СЭДО

Угрозы СЭДО классически можно разделить на угрозы конфиденциальности, целостности и доступности. И, как в других информационных системах, угрозам подвержены такие элементы СЭДО, как рабочие места, каналы связи и базы данных (серверы).

К угрозам конфиденциальности относятся угрозы получения несанкционированного доступа (НСД) к информации внутри СЭДО в обход существующих правил:

– *НСД к рабочим местам (в том числе удаленным)* представляет собой физический доступ к компьютерам сотрудников, когда злоумышленник/нарушитель уже имеет данные для идентификации и аутентификации в системе документооборота (логин и пароль, электронный ключ или, например, сертификат защищенного протокола HTTPS) легального, зарегистрированного пользователя или администратора СЭДО. В результате реализации данной угрозы злоумышленник получает доступ к документам пользователя, чьи данные были использованы для идентификации и аутентификации. Если же злоумышленнику удается получить данные администратора СЭДО, то он

получит доступ ко всем документам, обрабатывающимся и хранящимся в СЭДО, а также к настройкам прав системы разграничения доступа.

– *НСД к серверу операционной системы, серверу СЭДО и серверу, на котором хранится база данных СЭДО,* позволит получить частичный или полный контроль над системой документооборота, а также обеспечит доступ к обрабатываемым и хранящимся в СЭДО электронным документам.

– *НСД через канал связи между элементами системы* позволяет злоумышленнику перехватывать пакеты между рабочими местами и основными серверами системы. Классический вариант с применением HTTPS позволяет повысить уровень сложности перехвата и расшифровки информации.

Угрозам нарушения целостности в СЭДО подвержены:

– *электронные документы, их резервные копии;*

– *серверы операционной системы и оболочки (интерфейсной части) системы документооборота.* В данном случае под угрозой находятся как сами сервера, так и рабочие места сотрудников. В целом с точки зрения необходимости обеспечения целостности информации нарушения, связанные с этими элементами, не являются критичными: при восстановлении системы целостность данных, в том числе и данных конфиденциального характера, не нарушается.

– *серверы БД — среда хранения электронных документов — является наиболее важным компонентом СЭДО, однако при своевременном использовании резервирования и зеркалирования целостность данных также нарушена не будет.*

Угрозы нарушения доступности в СЭДО чаще всего связаны с ошибками в настройках системы разграничения доступа, ошибками штатных пользователей или системных администраторов и других лиц, обслуживающих компоненты СЭДО. Нарушение доступности к любому элементу СЭДО приводит к снижению скорости электронного документооборота и может привести к остановке бизнес-процесса всей организации.

Разграничение прав доступа в СЭДО

Важным звеном в системе защиты конфиденциальных документов, обрабатываемых в СЭДО, является организация санкционированного доступа к ней. Это достигается путем внедрения механизмов аутентификации пользователей и разрешительного управления доступом.

Разрешительная система управления доступом основывается на предоставлении пользователю такого объема конфиденциальной информации, который необходим для выполнения служебных обязанностей. В основе организации разграничения доступа в СЭДО лежат классические модели.

При внедрении разрешительной системы доступа необходимо обеспечить выполнение следующих требований:

– *передаваемая работнику конфиденциальная информация полностью соответствует его функциональным обязанностям;*

– *единственным критерием доступа к конфиденциальной информации является служебная или производственная необходимость;*

– *система исключает возможности несанкционированного доступа посторонних лиц к конфиденциальным документам при любых условиях;*

– *система охватывает все категории пользователей и конфиденциальной информации;*

– *решения системы понятны и однозначны;*

– *состав лиц, управляющих доступом пользователей, четко определен и задокументирован;*

– *система исключает возможность несанкционированного управления доступом третьими лицами;*

– *имеются необходимые условия в помещениях, предназначенные для работы с конфиденциальной информацией;*

– *сформированы необходимые нормативно-методические документы и положения по режиму конфиденциальности информации, защите и доступу к ней;*

– *организована и регламентирована работа всех категорий пользователей с конфиденциальной информацией.*

Другим значимым компонентом системы защиты информации в СЭДО является механизм аутентификации. Самый распространенный метод аутентификации – это использование многоразовых паролей. Их хешированные значения хранятся в специальной базе данных на сервере, однако надежность этого метода сильно зависит от человеческого фактора. Даже если для пользователя сгенерирован правильный и безопасный пароль, иногда его можно встретить записанным на листе бумаги или под клавиатурой.

Зачастую уровень доступа пользователей подтверждается специальными физическими носителями информации (смарт-картами, USB-ключами). В этом случае тоже не исключено влияние человеческого

фактора, однако злоумышленнику придется заполучить не только ключ, но и PIN-код для него.

Одним из самых надежных способов идентификации и аутентификации является биометрический метод, основанный на измерении уникальных признаков, например сетчатки глаза или отпечатка пальца. Однако стоимость такого инструмента выше, чем у привычных методов, а современные биометрические технологии все еще несовершенны и приводят к большому проценту ложных срабатываний.

Повышение безопасности процесса аутентификации может быть осуществлено при помощи комбинирования перечисленных выше методов (то есть повышения количества учитываемых факторов) – например, путем двухфакторной аутентификации с отпечатком пальца и паролем [32].

Вопросы к разделу 2

1. Что такое электронный документ?
2. Какие свойства характерны для электронного документа?
3. В чем юридическая сила электронного документа?
4. Перечислите методы защиты электронного документа.
5. Перечислите варианты атак с использованием открытого ключа.
6. На что направлены социальные атаки?
7. Что может снизить опасность социальных атак на СЭДО?
8. Как можно организовать контроль количества копий защищенного документа?
9. Какие существуют виды ЭП?
10. В чем заключается особенность работы с ЭП?
11. Как происходит процесс создания ЭП?
12. Какие действия невозможно совершить без ЭП?
13. Какие существуют виды носителей ЭП?
14. В каких системах простая ЭП имеет юридическую силу?
15. Какие виды СЭДО вы можете назвать?

3. Литература и ссылки

1. Александрова А. Я. и др. Документ в российской истории. – федеральное государственное бюджетное образовательное учреждение высшего образования" Нижегородский государственный технический университет им. РЕ Алексеева", 2012.
2. ГОСТ 16487-70. Делопроизводство и архивное дело. Термины и определения [Электронный ресурс] // URL: https://internet-law.ru/gosts/gost/44980/
3. ГОСТ 16487-83. Делопроизводство и архивное дело [Электронный ресурс] // URL: https://files.stroyinf.ru/Data2/1/4294835/4294835961.pdf
4. ГОСТ Р 7.0.8-2013. Делопроизводство и архивное дело. Термины и определения [Электронный ресурс] https://docs.cntd.ru/document/1200108447
5. ГОСТ Р 51141-98 Делопроизводство и архивное дело [Электронный ресурс] // URL: https://docs.cntd.ru/document/1200003829
6. ГОСТ Р 6.30-2003. Унифицированная система организационно-распорядительной документации [Электронный ресурс] // URL: https://docs.cntd.ru/document/1200031361
7. Ларьков Н. С. Документоведение. – 2016.
8. Плешкевич Е. А. Определение функций документа //Научные и технические библиотеки. – 2006. – №. 6. – С. 5-5.
9. ГОСТ Р 7.0.97-2016 Система стандартов по информации, библиотечному и издательскому делу (СИБИД). Организационно-распорядительная документация [Электронный ресурс] // URL: https://docs.cntd.ru/document/1200142871
10. Иванова Е. В. Официальный документ в электронной форме как предмет преступления, предусмотренного ст. 327 УК РФ //Уголовное право. – 2012. – №. 3. – С. 29-31.
11. Средства защиты документов [Электронный ресурс] // URL: https://www.sekretariat.ru/article/211017-qqq-17-m7-sredstva-zashchity-dokumentov
12. Способы защиты документа [Электронный ресурс] // URL: http://www.bnti.ru/showart.asp?aid=940&lvl=01.03.05.
13. Куняев Н. Н., Дёмушкин А. С., Фабричнов А. Г. Конфиденциальное делопроизводство и защищенный электронный документооборот. Учебник. – 2011.
14. Мазурова В. В., Фадеева Н. В. Роль службы документационного обеспечения управления в организации //Проблемы сертификации, управления качеством и документационного обеспечения управления. – 2018. – С. 65-68.
15. Рогожин М. Ю. Документационное обеспечение управления. – Directmedia, 2014.

16. Системы электронного документооборота. История развития систем электронного документооборота [Электронный ресурс] // URL: https://www.sites.google.com/site/upravlenieznaniami/tehnologii-upravlenia-znaniami/sistemy-elektronnogo-dokumentooborota?tmpl=%2Fsystem%2Fapp%2Ftemplates%2Fprint%2F&showPrintDialog=1%23TOC--2
17. ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники [Электронный ресурс] // URL: https://docs.cntd.ru/document/9010879
18. ГОСТ 6.10.1-88. Унифицированные системы документации [Электронный ресурс] // URL: https://internet-law.ru/gosts/gost/46345/
19. Текущее законодательство в сфере электронного документооборота и СЭД/ECM [Электронный ресурс] // URL: https://ecm-journal.ru/post/Tekushhee-zakonodatelstvo-v-sfere-ehlektronnogo-dokumentooborota-i-SEhDECM.aspx
20. Юридическая сила электронной подписи [Электронный ресурс] // URL: http://elektronnayapodpis.ru/wiki/yuridicheskaya-sila
21. Методы защиты электронных документов от копирования и редактирования [Электронный ресурс] // URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D1%8B_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%BE%D0%B2_%D0%BE%D1%82_%D0%BA%D0%BE%D0%BF%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F_%D0%B8_%D1%80%D0%B5%D0%B4%D0%B0%D0%BA%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F
22. Понятие электронной подписи и ее виды [Электронный ресурс] // URL: https://its.1c.ru/db/eldocs#content:4:hdoc
23. Что такое электронный документ и какова его юридическая сила? [Электронный ресурс] // URL: https://kontur.ru/articles/823
24. Малофеев С. С. О применении электронной цифровой подписи в электронном документообороте //Делопроизводство. – 2009. – №. 2. – С. 38-43.
25. Анализ угроз информации систем электронного документооборота [Электронный ресурс] // URL: https://cyberleninka.ru/article/v/analiz-ugroz-informatsii-sistem-elektronnogo-dokumentooborota
26. Особенности защищаемой информации [Электронный ресурс] // URL: https://studopedia.ru/7_65653_osobennosti-zashchishchaemoy-informatsii.html

27. Текущее законодательство в сфере электронного документооборота и СЭД/ECM [Электронный ресурс] // URL: https://ecm-journal.ru/docs/Chast-2-Tekushhee-zakonodatelstvo-v-sfere-ehlektronnogo-dokumentooborota-i-SEhDECM.aspx
28. Мокрый В. Ю. Системы электронного документооборота. – 2018.
29. Workflow [Электронный ресурс] // URL: https://piter-soft.ru/knowledge/glossary/process/workflow.html
30. Системы управления корпоративной информацией (ECM-системы) и системы электронного документооборота (СЭД) [Электронный ресурс] // URL: https://web-creator.ru/articles/ecm
31. Роуминг в электронном документообороте [Электронный ресурс] // URL: https://iitrust.ru/articles/article/rouming-v-elektronnom-dokumentooborote/
32. Сухотерин А. И. РЕКОМЕНДАЦИИ ПО ВНЕДРЕНИЮ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА НА ПРЕДПРИЯТИИ //Р43 Ресурсам области-эффективное использование [Текст]. – 2015. – С. 175.

Приложение

Кейсы по теме «Электронная подпись и электронный документооборот»

1. Писатель на сайте издательства хочет внести правки в свою еще не изданную книгу, которая доступна для редактирования еще несколько недель. После того, как правки будут внесены для их сохранения, писатель должен воспользоваться *ЭП данного вида*.

2. Обязательно ли использование сертифицированных носителей (токенов) для ключа электронной подписи и какой закон регулирует данный вопрос? Какие сертификаты может иметь сертифицированный токен?

3. Женщина обратилась к нотариусу онлайн и заказала доверенность. Нотариус выполнил свою работу и в конце поставил на электронный документ перед его отправкой *эту электронную подпись*.

4. В новой компании «Х» реализовали систему электронного документооборота. На предприятии есть разные уровни доступа к документам, зависящие от должности сотрудников, поэтому должна быть обеспечена целостность документов в СЭДО (то есть необходимо обеспечить возможность обнаружения внесения изменений в документ). Какой вид ЭП стоит использовать для работы в организованной СЭДО?

5. В цифровом городе М, где все предприятия и госучреждения переведены на системы электронного документооборота, Типография №1 имеет соглашение с налоговой инспекцией, в котором описываются условия по предоставлению услуг печати налоговых бланков типографией. Для того, чтобы можно было свободно обмениваться теми или иными документами между сторонами (например отчетностью), необходимо наличие *этого*. Какой вид ЭП следует использовать для организации электронного документооборота между типографией и налоговой инспекцией?

6. Новый сотрудник пришел в компанию, где весь документооборот электронный. Этот сотрудник пришел на замену сотрудницы, ушедшей в декретный отпуск. Может ли новый сотрудник использовать ЭП сотрудницы, чью должность он занял? Какие действия следует предпринять?

7. При увольнении сотрудника, на которого оформлена квалифицированная электронная подпись, возникла необходимость

аннулирования ключа электронной подписи. Куда именно необходимо обратиться и какие документы подать для аннулирования ЭП?

8. В результате повреждения токена его функционал стал ограничен лишь одним компьютером. Возможно ли создать новый токен без обращения в УЦ, и чем необходимо воспользоваться, если подобное возможно?

9. Почему не следует записывать ЭП на диск или флешку?

10. В компании три человека сдают отчетность. Может ли один сотрудик получить одну квалифицированную ЭП на всех?

11. Сотрудник компании забыл пароль от ключа электронной подписи. Как он может восстановить ключ ЭП?

12. Специалист по информационной безопасности решил для упрощения работы записать ЭП на флешку: быстро считывается и всегда под рукой и другие нужные файлы в одном месте. Какую ошибку допустил специалист?

13. Директор ООО «Очень Важная Компания» полчаса ругался с сотрудником удостоверяющего центра по телефону, требуя доставить ему сертификат ключа проверки электронной подписи на дом, так как он очень занят переговорами с инвесторами в банном комплексе. Но сотрудник стоял на своем: это невозможно. Кто прав и почему?

14. У ИП Иванова Ивана Ивановича закончился срок действия сертификата ЭП. Иван Иванович, будучи человеком образованным, знал, что некоторые виды сертификатов электронной подписи можно продлить удаленно через личный кабинет пользователя, не обращаясь в удостоверяющий центр. Его сертификат подходил под эти условия, но продлить его он все же не смог. Почему?

15. «…Мой начальник, когда брал меня на работу, помог мне получить электронную подпись. Потом я уволилась, но начальник приказал вернуть подпись, так как это собственность фирмы. Должна ли я возвращать ее?…»

Ответы на кейсы для самопроверки

1. В данном случае можно использовать простую электронную подпись (логин и пароль), так как нужно только доказать авторство, однако

не требуется наличие возможности узнать о наличии изменений в тексте книги (поскольку редактировать ее могут все, у кого есть доступ — это могут быть (кроме писателя) редакторы и корректоры издательства.

2. В ФЗ-63 «Об электронной подписи» прямого указания на обязательность использования сертифицированных носителей для ключа электронной подписи нет. Токен может иметь как один сертификат ФСБ (позволяет использовать токен как средство криптографической информации) или ФСТЭК (подтверждающий, что ПО токена не имеет недекларированных возможностей защищает хранимую информацию от НСД), который позволит ему решать одну задачу, так и оба.

3. Нотариус поставил усиленную квалифицированную ЭП, так как именно такая ЭП обеспечивает юридическую силу документа.

4. В данном случае при наличии корпоративной информационной системы возможно использование простой ЭП. Кроме того, возможно использование усиленной неквалифицированной ЭП для внутреннего документооборота и обмена с организациями-партнерами (при наличии соглашения), так как необходимо подтверждение целостности документов. Усиленная квалифицированная ЭП будет использоваться для того, чтобы можно было осуществлять обмен документами с государственными учреждениями, например налоговой службой или проверяющим гос. органом.

5. В данной кейсе речь идет о роуминге и о усиленной квалифицированной электронной подписи.

6. Нет, ЭП является индивидуальной и не подлежит передаче (за исключением условий, оговоренных в ФЗ №63). Новому сотруднику необходимо получить свою электронную подпись.

7. Уволившийся сотрудник сам обращается в удостоверяющий центр, указанный в сертификате ЭП, и пишет заявление об аннулировании ЭП. Если бывший сотрудник не хочет ничего предпринимать, сделать это вправе его руководитель, обратившись в УЦ и написав заявление об отзыве, указав ИНН и СНИЛС.

8. Это не запрещается и возможно; при этом для копирования электронной подписи (контейнер) необходимо применить специальную программу (Crypto Pro или другой аналогичный крипто-провайдер).

9. При создании электронной подписи ее пароль генерируется владельцем ключа в специальной программе. В отличие от простого кода,

получается длинная и сложная цепочка чисел и символов объемом до 256 бит. Запомнить или набрать электронный ключ невозможно, поэтому он сохраняется на цифровом носителе. Используемые в повседневной жизни флеш-карты или лазерные диски не обеспечивают защиту от считывания ключа и подвергают электронную подпись высокой вероятности компрометации.

10. Технология создания электронной подписи подразумевает привязку каждого сертификата к конкретному физическому лицу (приказ ФНС от 17.12.2008 № ММ-3-6/665). Теоретически сотрудники могут передавать токен друг другу, но тот, на кого выпущен сертификат, компрометирует свою электронную подпись. Ею могут воспользоваться для мошеннических целей, и владельцу будет сложно доказать свою непричастность.

11. Если ключи хранились на сертифицированных носителях, то необходимо посмотреть в документации, прилагаемой к этим носителям о возможности разблокировки. В остальных случаях необходимо получать новые в Удостоверяющем центре.

12. Используемые в повседневной жизни флеш-карты не обеспечивают защиту от считывания ключа и подвергают электронную подпись высокой вероятности компрометации. Аккредитованные удостоверяющие центры выдают электронную подпись на токенах с USB-разъемом или смарт-картах. Эти цифровые носители защищены паролями и сертифицированы в соответствии с требованиями ФСТЭК и ФСБ РФ.)

13. Прав сотрудник УЦ, так как Закон № 63-ФЗ, ст. 18, требует от аккредитованных удостоверяющих центров установления личности владельца электронной подписи. Для этого владельцу необходимо лично явиться в офис удостоверяющего центра с оригиналами или официально заверенными копиями необходимых документов. Выдача сертификата ключа проверки электронной подписи по почте или через курьера законом не предусмотрена.

14. Подать заявку на продление сертификата на сайте нужно до истечения срока действия сертификата.

15. Согласно части 3 статьи 14 Федерального закона от 06.04.2011 №63 «Об электронной подписи», в случае выдачи сертификата ключа проверки электронной подписи юридическому лицу в качестве владельца сертификата наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица

на основании учредительных документов юридического лица или доверенности. Таким образом, как женщина, так и начальник – владельцы ЭП. Поэтому ответственность за использование несут оба и должны всегда быть в курсе манипуляций с ЭП. Поэтому наиболее целесообразным для сотрудницы будет обращение в УЦ, выпустивший сертификат, для его аннулирования, после чего она смогла бы сдать указанный ключевой носитель бывшему работодателю с документальным подтверждением такой сдачи.

Коржук Виктория Михайловна
Попов Илья Юрьевич
Воробьева Алиса Андреевна

Защищенный документооборот. Часть 1

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49, литер А