Федеральное агентство связи

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

Московский технический университет связи и информатики

В.Л. Владимиров, К.Н. Герцев, В.А. Докучаев, В.В. Маклачкова

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Учебное пособие

Часть 1

Москва 2018

Федеральное агентство связи

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

Московский технический университет связи и информатики

В.Л. Владимиров, К.Н. Герцев, В.А. Докучаев, В.В. Маклачкова

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Учебное пособие

Часть 1

для направлений: 05.13.01, 09.03.02, 09.04.02, 11.03.02, 11.04.02

Москва 2018

УДК 651.011.42: 004.6

Владимиров В.Л., Герцев К.Н., Докучаев В.А., Маклачкова В.В. Организационно-технические средства защиты электронного документооборота. Часть 1: учебное пособие/ МТУСИ. – М., 2018. - 38 с.

Учебное пособие по дисциплинам «Практические аспекты применения электронной подписи», «Корпоративные инфокоммуникационные системы и услуги», «Особенности организации электронного документооборота», «Основы использования электронной подписи», «Организационно-технические основы построения современных облачных информационно-коммуникационных систем», «Основы информационно-библиотечной культуры» и «Теория построения инфокоммуникационных сетей и систем»

для направлений подготовки бакалавров:

11.03.02 – Инфокоммуникационные технологии и системы связи (профиль подготовки: Инфокоммуникационные технологии в сервисах и услугах связи);

09.03.02 –Информационные системы и технологии (профиль подготовки: Информационные системы и технологии).

для направлений подготовки магистров:

09.04.01 –Информатика и вычислительная техника (профиль подготовки: Разработка мобильных и интернет приложений);

11.04.02 –Инфокоммуникационные технологии и системы связи (профиль подготовки: Облачные инфокоммуникационные технологии и пакетизация услуг).

для направлений подготовки аспирантов:

05.13.01 –Системный анализ, управление и обработка информации (по отраслям).

Табл. 1, список лит. 18 назв.

Издание утверждено Методическим советом университета в качестве учебного пособия. Протокол №1 от 17.10.2017.

Рецензент: В.Ю. Статьев, к.т.н., с.н.с., начальник отдела (ОАО «РЖД»)

СОДЕРЖАНИЕ

Введение

Предлагаемое вашему вниманию учебное пособие подготовлено коллективом авторов с целью познакомить читателя с практическими аспектами применения электронной подписи и является первой частью из серии учебных пособий, посвящённых электронному документообороту.

В последующих частях учебного пособия авторы планируют рассмотреть основных участников правоотношений в сфере организации работы с электронными документами, особенности регулирования электронного документооборота в различных сферах деятельности, основы организации электронного документооборота, а также архитектуру подсистемы обеспечения юридической значимости электронного документооборота (ПОЮЗД), остановившись на её взаимодействии с прикладными системами.

Основой для написания настоящего учебного пособия послужили лекции и практические занятия проведённые авторами в Московском техническом университете связи и информатики в 2016-2018 годах, на которых студенты узнали современные тенденции электронного документооборота и базовую информацию об электронной подписи как основе современной системы управления органами государственной власти и организациями независимо от формы собственности.

Изучение типов электронной подписи, архитектуры подсистем её реализации в системах электронного документооборота, основных участников правоотношений в сфере организации работы с электронными документами позволит более глубоко понять особенности построения и эксплуатации комплексов средств автоматизации сервисов подсистем обеспечения юридической значимости информационно-коммуникационных систем, используемых для нужд электронного документооборота.

1. Основные понятия электронного документооборота. Регулирование электронного документооборота

1.1. Термины и определения

Документ - материальный носитель с зафиксированной на нём в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения [1].

Каждый официальный документ состоит из ряда составляющих его обязательных элементов, некоторые из которых называются реквизитами.

Реквизиты документа - «обязательный элемент оформления официального документа» [2]. Это могут быть как наименование документа (вид), автор, адресат, текст, дата, подпись, резолюция, так и гриф согласования, утверждения и т.д. — всё это реквизиты документов.

В зависимости от характера документы состоят из разного набора реквизитов. Количество реквизитов, характеризующих документы, определяется целями создания документа, его назначением, требованиями к форме и содержанию данного документа, способом документирования.

Большое количество типов документов имеет строго ограниченное число реквизитов. Отсутствие и (или) неправильное указание хотя бы одного реквизита в служебном документе зачастую делает документ недействительным.

В целях унификации (единообразия) документов в Российской Федерации обязательные реквизиты первичных документов должны соответствовать Государственному стандарту - ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».

На сегодняшний день стандарт ГОСТ Р 6.30-2003 предусматривает 30 реквизитов.

Положения ГОСТа имеют рекомендательный характер, но отдельные элементы являются обязательными для официальных

документов. Разные виды организационно-распорядительных документов обязаны оформляться в соответствии с государственными правилами.

Документ в электронном виде. В настоящее время законодатель не дал точного определения термину «документ в электронном виде», но на конференции в РСПП, посвящённой электронному документообороту, было предложено под термином «документ в электронном виде» понимать электронный файл, содержащий отсканированное с определённой степенью разрешения изображение бумажного документа, удостоверенного надлежащим образом.

Электронный документ. В отличие от термина «документ в электронном виде» толкование термина «электронный документ» встречается в законодательных актах несколько раз. Каждое из предложенных законодателем определений дополняет друг друга и позволяет рассматривать разные аспекты содержания данного термина.

С одной стороны, электронный документ это «Документ, зафиксированный на электронном носителе (в виде набора символов, звукозаписи или изображения) и предназначенный для передачи во времени и пространстве с использованием средств вычислительной техники электросвязи с целью хранения и общественного использования» [3], с другой стороны - это «Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах» [4].

Электронная подпись (ЭП) — реквизит электронного документа. Электронная подпись в некоторых случаях может быть аналогом собственноручной подписи гражданина. В некоторых случаях электронная подпись может быть получена в результате криптографического преобразования информации с использованием закрытого ключа подписи. Это позволяет проверить: отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки - подтвердить факт подписания электронного документа

(неотказуемость). Законодатель определяет электронную подпись так: «информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию» [5].

Электронный документооборот (ЭДО) — единый механизм по работе с документами, представленными в электронном виде, с реализацией концепции «безбумажного делопроизводства».

Приведённые выше термины и определения являются базовыми для дальнейшего изучения вопросов создания и использования электронной подписи при организации электронного документооборота.

1.2. Информационные риски при работе с электронными документами

Обработка электронного документа представляет собой сложный технологический процесс, связанный с рядом рисков для безопасности информации, содержащейся в документе. Реализация угроз неправомерного воздействия на информационные потоки, организуемые в результате использования электронного документооборота, может привести к тому, что документ может утратить свою юридическую значимость, а организация понесёт ущерб.

При организации электронного документооборота обычно выделяют следующие информационные риски для электронного документа:

- нарушение конфиденциальности, т.е. неправомочное изменение статуса, предоставленного документу и определяющего требуемую степень его защиты. В общем случае конфиденциальность документа - это свойство информации, содержащейся в документе, быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы (пользователям, процессам, программам). Соответственно для остальных субъектов системы эта информация должна быть неизвестной;

- нарушение целостности документа, т.е. лишение документа свойства, «состоящего в том, что при любой демонстрации документа заданные значения параметров демонстрируемого представления документа соответствуют специфицированным требованиям» [6]:

- доступность документа;
- легитимность документа;
- достоверность документа;
- аутентичность документа.

Рассмотрим информационные риски при работе с электронными документами с позиции оценки вида противоправного воздействия на электронный документ.

Подделка документа (коллизия первого рода)

Злоумышленник может попытаться подобрать документ к данной подписи так, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. Причина в следующем:

- документ представляет собой осмысленный текст;
- текст документа оформлен по установленной форме;
- документы редко оформляют в виде файла открытых данных (Plain Text-файла), чаще всего в формате DOC или HTML. Текстовые данные (также текстовый формат) — представление информации строкового типа (то есть, последовательности печатных символов) в вычислительной системе.

Часто текстовые данные понимаются в более узком смысле — как текст на каких-либо языках (формальных или естественных), который может быть прочитан и понят человеком.

Если у фальшивого набора байт и произойдет коллизия с хэшем исходного документа, то должны выполниться три следующих условия:

- случайный набор байт должен подойти под сложно структурированный формат файла;
- то, что текстовый редактор прочитает в случайном наборе байт, должно образовывать текст, оформленный по установленной форме;
- текст должен быть осмысленным, грамотным и соответствующим теме документа.

Однако, во многих структурированных наборах данных можно вставить произвольные данные в некоторые служебные поля, не изменив вид документа для пользователя. Именно этим пользуются

злоумышленники, подделывая документы. Некоторые форматы подписи даже защищают целостность текста, но не служебных полей.

Вероятность подобного происшествия также ничтожно мала. Можно считать, что на практике такого случиться не может даже с ненадёжными хэш-функциями, так как документы, подписываемые ЭП, обычно имеют большой объём — килобайты.

Получение двух документов с одинаковой подписью (коллизия второго рода)

На практике наиболее вероятна коллизия второго рода. В этом случае злоумышленник создаёт два документа с одинаковой подписью, и в нужный момент подменяет один другим. При использовании надёжной хэш-функции такая атака должна быть также вычислительно сложной. В частности, таким образом можно провести атаку на SSL-сертификаты и алгоритм хэширования.

Социальные атаки

Социальные атаки направлены не на взлом алгоритмов электронной подписи, а на манипуляции с открытым и закрытым ключами.

Возможны следующие ситуации:

- злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа;
- злоумышленник может обманом заставить владельца ключа подписать какой-либо документ, например, используя протокол слепой подписи;
- злоумышленник может подменить открытый ключ владельца на свой собственный, выдавая себя за него.

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

1.3. Нормативно-правовое регулирование электронного документооборота

Учитывая важность электронного документооборота при совершенствовании систем управления государством и экономикой РФ в

рамках реализации Программы «Цифровой экономики», нормативному регулированию электронного документооборота в настоящее время посвящено большое число нормативно-правовых актов (НПА), принятых до момента написания данного учебного пособия и будет принято ещё много в результате дальнейшего развития систем управления.

На сегодняшний день важнейшими НПА, регулирующими электронный документооборот в РФ, являются: Государственная программа Российской Федерации «Информационное общество (2011 - 2020 годы)», Федеральный закон от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации», ГОСТ Р ИСО 15489-1-2007 «Управление документами», Методические рекомендации ЦАДЭНМ по работе с документами на электронных носителях, ГОСТ Р 53898-2010 «Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению», Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», ГОСТ 6.10.4-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемые средствами вычислительной техники».

Особо необходимо выделить НПА, посвящённые криптографической защите электронного документооборота. Это, в первую очередь, государственные стандарты, посвящённые криптографической защите электронного документооборота: ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма»; ГОСТ Р 34.10-2001; ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Последний стандарт описывает алгоритмы формирования и проверки электронной подписи.

Предложенный действующим в настоящее время ГОСТ алгоритм криптографической защиты разработан главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте Российской Федерации при участии Всероссийского научно-исследовательского института стандартизации. Этот алгоритм разрабатывался взамен алгоритма, введённого ГОСТ

Р 34.10-94 для обеспечения более высокой криптографической защищённости обрабатываемой информации.

Алгоритмы, представленные в ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001, основаны на эллиптических кривых. Стойкость этих алгоритмов основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости хэш-функции. Для ГОСТ Р 34.10-2012 используется хэш-функция по ГОСТ Р 34.11-2012.

После подписывания сообщения М к нему дописывается электронная подпись размером 512 или 1024 бит и текстовое поле (см. таблицу 1). В текстовом поле могут содержаться, например, дата и время отправки или различные данные об отправителе.

Таблица 1 – Структура подписанного сообщения

<table>
<tr><td rowspan="2">Сообщение М</td><td rowspan="2">+</td><td>Электронная подпись</td><td>Текст</td></tr>
<tr><td colspan="2">Дополнение</td></tr>
</table>

Данный алгоритм не описывает механизм генерации параметров, необходимых для формирования подписи, а только определяет, каким образом, на основании каких параметров получить электронную подпись. Механизм генерации параметров определяется на месте в зависимости от разрабатываемой системы.

Вероятность взлома хэш-функции по ГОСТ 34.11-94 составляет $1{,}73*10^{-77}$ при подборе коллизии на фиксированное сообщение и $2{,}94*10^{-39}$ при подборе любой коллизии. Стойкость алгоритма шифрования основывается на проблеме дискретного логарифмирования в группе точек эллиптической кривой. На данный момент нет метода решения данной проблемы хотя бы с субэкспоненциальной сложностью. Экспоненциальная сложность это сложность задачи в теории сложности алгоритмов, ограниченная экспонентой от полинома от размерности задачи, то есть ограничена функцией exp(P(n)), где P - некоторый многочлен, а n – размер задачи. В этом случае говорят, что сложность задачи растёт экспоненциально. Часто под сложностью подразумевается время выполнения алгоритма. В этом случае говорят, что алгоритм принадлежит к классу EXPTIME. Однако сложность может относиться как к памяти, так и (или) другим ресурсам, необходимым для реализации

алгоритма. Существуют алгоритмы, которые работают более, чем за полиномиальное время («сверхполиномиальное»), но менее, чем за экспоненциальное время («субэкспоненциальное»). Примером такой задачи является разложение целого числа на простые множители (факторизация).

Один из самых быстрых алгоритмов, на данный момент, при правильном выборе параметров — $\boldsymbol{\rho}$-метод и **I**-метод Полларда.

Для оптимизированного $\boldsymbol{\rho}$-метода Полларда вычислительная сложность оценивается как $\boldsymbol{O(\sqrt{q})}$. Таким образом для обеспечения криптостойкости 10^{30} операций необходимо использовать 256-разрядное $\boldsymbol{q}$ [9].

Использование математического аппарата группы точек эллиптической кривой позволяет существенно сократить порядок модуля p без потери криптостойкости.

Контрольные вопросы

1. В чём сходство и отличие понятий «документ» и «электронный документ»?
2. Что такое ЭДО?
3. Какие виды электронной подписи вы знаете?
4. Какие информационные риски возникают при работе с электронными документами?
5. Что такое коллизия второго рода?
6. Назовите основные НПА, регулирующие электронный документооборот.
7. Что такое субэкспоненциальная сложность алгоритма?
8. Что такое алгоритм формирования и алгоритм проверки?
9. Какова длина хэш-кода по ГОСТ Р 34.10-2012?
10. Назовите основные реквизиты документа.

2. Понятие «электронные документы»

2.1. «Электронные документы» и «документы в электронном виде»: общее и различие

Законодатель определяет электронный документ как документ, зафиксированный на электронном носителе (в виде набора символов,

звукозаписи или изображения) и предназначенный для передачи во времени и пространстве с использованием средств вычислительной техники и электросвязи с целью хранения и общественного использования [3].

Наиболее полным является определение электронного документа, предложенное в пункте 11.1 статьи 2 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – «документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах».

Свойство выступать в качестве подтверждения деловой деятельности либо событий личного характера (или как принято говорить – обладать свойством юридической значимости) электронному документу придаёт электронная подпись, которая на территории Российской Федерации равнозначна собственноручной подписи в документе на бумажном носителе [3] при одновременном соблюдении следующих основных условий.

1. Сертификат ключа подписи, относящийся к этой электронной подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа.

2. При наличии доказательств, определяющих момент подписания.

3. Подтверждена подлинность электронной подписи в электронном документе.

4. Электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Под термином «документ в электронном виде» понимается представленная в графическом формате с достаточным разрешением, защищённая от противоправного воздействия и заверенная электронной подписью электронная копия документа.

Электронный документ и документ в электронном виде как носители информации имеют общие признаки и обладают рядом отличий.

Общие признаки: электронный документ и документ в электронном виде - это запись, зафиксированная на магнитном диске, магнитной ленте, лазерном диске и ином электронном материальном носителе. Они могут передаваться по линиям связи и обладают юридической силой при выполнении условий, определённых законодателем.

Отличия: электронный документ, как правило, - это файлы текстового формата, а документ в электронном виде - это исключительно всегда файл графического формата. Законодатель определяет уровень разрешения при сканировании бумажного документа для перевода его в форму документа в электронном виде. Документ в электронном виде всегда является копией исходного документа. Электронный документ (а не его твёрдая копия в форме распечатки) может являться оригиналом документа. Отметим, что здесь может возникнуть коллизия - оригинал в общепринятом смысле этого слова может быть в единственном числе и конечном количестве экземпляров, а для электронного документа количество оригиналов и количество экземпляров определено не всегда.

2.2. «Электронные документы» как отдельная категория информации конфиденциального характера

Понятие «конфиденциальная информация» стало неотъемлемой частью российской юридической лексики. В настоящий момент оно используется в нескольких сотнях нормативных правовых актов Российской Федерации. Не отстают от законодателя и правоприменители: все чаще в различных договорах можно встретить целые разделы или даже отдельные соглашения о конфиденциальности.

Конфиденциальная информация — это сведения независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их правообладателя. Из этого следует, что ряд электронных документов является одной из категорий информации конфиденциального характера.

Для того чтобы определить, относится электронный документ к данной категории или нет, следует обратиться к Перечню сведений конфиденциального характера, который содержится в соответствующем

НПА [7]. Согласно действующему законодательству к сведениям конфиденциального характера относятся:

- персональные данные;
- сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и НПА Российской Федерации;
- служебная тайна;
- врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений;
- коммерческая тайна;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Следует обратить внимание на то обстоятельство, что данный перечень не может рассматриваться как закрытый. Действующее законодательство [4] не требует принятия нормативных актов Президента или Правительства для дальнейшего развития понятия «конфиденциальная информация». Более того, закон позволяет обладателю информации самостоятельно решать вопрос о наделении ее статусом конфиденциальной. Поэтому перечень следует рассматривать как примерный.

Данный вывод имеет очень важное практическое значение. Возможность самостоятельного определения статуса информации позволяет ее обладателю вырабатывать способы ее защиты от несанкционированного доступа, использования и распространения, а также предусматривать меры гражданско-правовой ответственности в случае совершения указанных действий.

Учитывая, что электронные документы обрабатываются на средствах автоматизации и часто передаются по открытым каналам электросвязи, а также циркулируют в различных системах электронного

документооборота, на них накладываются определённые ограничения на разграничение доступа к ним.

Использование систем электронного документооборота учитывает свойство конфиденциальности электронных документов и обеспечивает его соблюдение путём организации разделения доступа и применения электронной подписи.

2.3. Применение понятия «электронные документы» в государственных и коммерческих организациях

Практика применения электронных документов в органах государственной власти начинается со второй половины восьмидесятых годов прошлого века. Первоначально в СССР электронный документооборот создавался в министерствах и институциональных организациях. На этом этапе электронный документооборот носил фрагментарный характер. Значительным шагом в развитии электронного документооборота стало создание правовых информационных систем, которые объединили системы законодательной власти и коммерческие базы знаний в единую сеть на основе электронного документооборота («Консультант+», «Гарант» и др.). При разработке информационных правовых систем были выработаны общие подходы к созданию единых систем электронного документооборота в органах государственной власти и организациях независимо от формы собственности.

Следующим этапом развития автоматизированной системы управления государством и экономикой стала разработка и реализация программы «Цифровая экономика Российской Федерации», утверждённая Распоряжением от 28 июля 2017 г. № 1632-р Председателем Правительства Российской Федерации Д.А. Медведевым.

Основа «цифровой экономики» - это защищённый обмен данными, который может осуществляться в основном в виде электронных документов.

Электронный документооборот (ЭДО) в России занимает все более основательные позиции: с каждым днем растет число вовлеченных в него предприятий. В судебной практике все чаще встречаются процессы, объектом которых являются документы с электронной подписью.

Вне зависимости от формы собственности системы ЭДО можно разделить на два класса:

корпоративные, в которых факт подлинности ЭП на электронном документе с юридической точки зрения недоказуем;

глобальные, предусматривающие возможность юридической доказуемости факта постановки ЭП.

Считается, что первый тип систем является вырожденным и не представляет большого интереса, второй - в последнее время является предметом множества дискуссий и целого ряда научных работ. Однако отметим, что в настоящее время всё большее число крупных коммерческих предприятий вводят в свою структуру подразделения с правами удостоверяющих центров, что кардинально меняет отношение к корпоративному документообороту.

2.4. «Электронные документы» в российском и международном законодательствах

Нормативное регулирование электронного документооборота в РФ осуществляется рядом законодательных актов. 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 обеспечение защиты информации, является ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ. В ст.11 данного ФЗ говорится, что электронное сообщение, подписанное электронной подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью. Также в этой статье устанавливается, что обмен электронными сообщениями, каждое из которых подписано ЭП или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными НПА или соглашением сторон, рассматривается как обмен документами.

ФЗ «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ, обеспечивает правовые условия использования электронной подписи в качестве аналога собственноручной подписи в документе на бумажном носителе. В этом законе ЭП определяется как реквизит электронного документа, предназначенный для его защиты от подделки и

идентификации владельца сертификата ключа подписи. В этом законе также дается понятие «электронного документа» как документа, в котором информация представлена в электронной форме.

ФЗ «О персональных данных» от 27.07.2006 г. № 152-ФЗ регулирует отношения, возникающие при обработке персональных данных, в том числе с использованием средств автоматизации. Руководствоваться положениями этого закона в организации необходимо, прежде всего, при работе с документами по личному составу.

Вопросы работы с электронными документами также затрагиваются в НПА, посвященным отдельным предметным сферам правового регулирования: гражданскому, административному, уголовному, уголовно процессуальному, трудовому, налоговому и другому законодательству РФ. Рассмотрим некоторые из них.

Приказ ФСБ РФ «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи» от 27.12.2011 г. № 795 устанавливает требования к совокупности и порядку расположения полей квалифицированного сертификата электронной подписи.

Приказ Министерства финансов РФ от 25.04.2011 № 50н «Об утверждении Порядка выставления и получения счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной цифровой подписи» устанавливает процедуры взаимодействия участников электронного документооборота в рамках выставления и получения счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной подписи.

Гражданский кодекс РФ (ГК РФ) предусматривает, что документ является основой гражданских правоотношений и содержит основополагающие понятия, такие как «сделка» и «договор». В нём 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, что 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 (УК 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. 1 А), 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.

Налоговый кодекс РФ в ст. 80 содержит разрешение представлять налоговую отчетность в электронном виде.

Таможенный кодекс РФ в п. 8 ст.63 определяет, что документы, необходимые для таможенного оформления, могут быть представлены в электронной форме.

Трудовой кодекс РФ в главе 49.1 предусматривает взаимодействие дистанционного работника или лица, поступающего на дистанционную работу, и работодателя путем обмена электронными документами. При этом 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»).

Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ устанавливает единые требования к бухгалтерскому учету. В ст. 9 обозначены обязательные реквизиты первичного учетного документа. Там же приведены общие процедуры, связанные с ним, такие как подписание и исправление. Кроме того, п. 5 ст. 9 разрешает составлять первичный учетный документ в электронном виде с электронной подписью.

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 ЭДО 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).

Развитие систем ЭП нашло продолжение в международном или трансграничном документообороте (ТЭДО) [8]. ЭДО в рамках РФ регламентирован законодательством, носящим отчасти формальный характер. Но, выходя за рамки государства, документ, юридически значимый на территории РФ, теряет свои свойства на территории других государств.

На сегодняшний день правовая база, регламентирующая ТЭДО, находится на начальной стадии формирования. Очевидно, что это должны быть международные нормативные документы, описывающие весь процесс документооборота, - от понятия «электронный документ» и при каких условиях он становится международным до определения доверенного механизма удостоверяющих центров.

В российском законодательстве отсутствуют требования к системам электронного документооборота, которыми можно было бы руководствоваться при выборе системы. При этом во многих странах уже давно созданы и действуют данные стандарты, содержащие в себе требования к подобным системам. Например, в США это стандарт DoD 5015.2-STD (Design Criteria Standard for Electronic Records Management Software Applications), в Евросоюзе стандарт MoReq и др. Мы рассмотрим европейский стандарт MoReq (Model requirements for the

management of electronic records), который наиболее подходит для отечественного документооборота. Именно его можно рекомендовать при выборе системы ЭДО организации.

Система ЭДО может быть представлена как в виде единого специализированного пакета программ, так и в виде нескольких отдельных интегрированных пакетов или заказной разработки, учитывающей специфику организации. Что выбрать, решает каждая организация самостоятельно. В стандарте не указываются конкретные требования к характеру системы.

Стандарт может использоваться:

- разработчиками систем ЭДО при разработке программного продукта и его совершенствовании;
- текущими клиентами системы в качестве основы для проведения аудита использования системы;
- потенциальными заказчиками для написания технического задания;
- специализированными учебными заведениями в качестве методического материала для написания учебных курсов по электронному делопроизводству.

В настоящее время на рынке представлено множество различных систем ЭДО, отличающихся по функциональным возможностям, но близких по описанию. Это усложняет процесс выбора оптимальной для конкретно взятой организации системы ЭДО. Облегчить этот выбор при составлении списка требований к системе ЭДО позволяет следование рекомендациям MoReq [10].

Применение международных стандартов в РФ не является обязательным, тем не менее, необходимо учитывать, что в настоящее время стандартизация работы с документами переходит на международный уровень. Поэтому при использовании СЭД и ЭД в нашей стране желательно ориентироваться на положения международных стандартов в области электронного документооборота.

Российский стандарт ИСО 15489-1-2007 (аутентичный перевод международного стандарта ISO 15489) «Информация и документация. Управление документами» разработан подкомитетом № 11 «Управление

архивами (документами)», действующим в структуре технического комитета № 46 «Информация и документация» Международной организации по стандартизации. Это «первый международный стандарт по организации делопроизводства и документооборота, содержащий общие требования и методологию управления документами на всех видах носителей и во всех форматах, а также процедуры разработки и внедрения систем документооборота». Более того, «стандарт ISO 15489 использует современный функциональный подход к организации документооборота, позволяющий связывать нормативные требования (например, статус «документа», сроки хранения и т.п.) с деловыми функциями, в результате выполнения которых возникает данный информационный материал» [11].

Международный стандарт ИСО 23081 «Информация и документация. Процессы управления записями. Метаданные для записей» посвящён делопроизводственным метаданным в управленческой деятельности, их типам, функциям по обеспечению управленческих и делопроизводственных процессов, а также управлению метаданными.

Требования к хранению документов в архивах и библиотеках устанавливает ИСО 11799:2003 «Информация и документация. Требования к хранению архивных и библиотечных документальных материалов».

Рассмотрим особенности организации документооборота за рубежом.

Особенности нормативного регулирования ЭДО в США

Система управления документацией в США - это результат длительного исторического развития, на ход которого оказывали влияние различные факторы.

Первым из таких факторов являлось влияние европейских традиций документооборота.

Вторым фактором являлся постоянный рост количества документов и затрат на их обработку. Эта тенденция сохраняется до настоящего времени. По данным ВНИИДАД [12], только на начало 90-х годов федеральное правительство США ежегодно рассылало около 1 млрд. писем.

Определенное влияние на развитие процессов работы с документами оказало и то, что в США позднее, чем в других странах, была создана архивная служба.

Под документами в США понимаются записи на любых носителях независимо от физической формы и содержания, созданные или полученные любым ведомством США в порядке исполнения федерального закона или в связи с совершенствованием деловых операций и передаваемые на хранение ведомством или его юридическим законным преемником в качестве свидетельства организационной структуры, функций, политики, процессов работы или в силу информационной ценности, заключающейся в них.

Закон «О федеральных документах» 1950 года обязал ведомства США разрабатывать специальные программы управления документацией.

Основными элементами таких систем являются:

- создание документов (составление форм документов и их обработка, создание информационных систем и применение современных информационных технологий);

- хранение и использование информации (формирование дел, создание систем поиска документов, управление файлами и телекоммуникациями, выбор копировальной техники, развитие программ работы с ценными документами);

- передача документов в архив;

- управление архивами.

США в настоящее время являются одной из стран, которые наиболее активно трансформируют свою систему для управления современным цифровым информационным обществом и экономикой.

Согласно Закону «О ликвидации бумажного документооборота в государственных органах» 1998 года, федеральные органы США должны перейти на электронный документооборот и обеспечить доступ граждан к электронным документам. На основе Закона были разработаны правила, которые помогают государственным органам перестроить работу с документами. Для этого государственные органы США должны проанализировать документацию с позиций требований, предъявляемых

к ней законодательством, решить вопрос о возможности замены бумажных документов электронными. В ряде случаев допускается, что отдельные виды документов могут быть только на бумажных носителях. Этот Закон также определил правила регистрации и хранения электронных документов.

В 2000 году в США был принят Федеральный закон «Об электронных подписях в международной и внутренней торговле». Он посвящен общим принципам регулирования электронной торговли, в том числе, правовому признанию электронных сделок. Он также включает большое число норм, регламентирующих применение электронных документов и электронных подписей. Отметим, что Федеральный закон США отвечает тем же основным принципам, что и законодательство ЕС в области ЭДО. Закон применяется, когда электронные подписи используются для совершения коммерческих операций. Он закрепляет правило, в соответствии с которым электронные документы и подписи приравниваются к документам и подписям в письменной форме. Исключением является ограниченное число случаев. Например, федеральные органы власти США могут потребовать предъявить документ в письменной форме в случаях, диктуемых службой национальной безопасности.

Особенности нормативного регулирования электронного документооборота во Франции

В 2000 году французское правительство приняло Закон, вносящий изменения в главу VI Гражданского кодекса Франции, которая касалась формы и доказательственной силы договоров. Основной упор сделанных изменений направлен на создание общих правил, которые позволяют уравнять юридическую силу электронных документов и подписей с собственноручной формой во всех сферах правоотношений. Рассмотрим основные особенности этих изменений.

Для большей определенности статья 1316-1 ГК Франции определяет условия допустимости доказательств в электронной форме - можно с достаточной долей уверенности определить лицо, от которого исходят данные, и способ их создания гарантирует целостность.

Статья 1316-2 указывает, что в случае возникновения расхождений между электронной и бумажной копией, суд определяет, какая из них

имеет большую доказательственную силу, основываясь на тщательном изучении всех обстоятельств и на непредвзятом отношении к используемому носителю.

Данная глава ГК Франции гарантирует, что электронные документы имеют юридическую силу и возможна оценка их надежности судом без обращения к технологической природе самого документа и связанной с ним электронной подписи.

Таким образом, внесённые изменения в законодательство Франции позволили повысить степень безопасности и надежности ЭДО до уровня, который соответствует технологии электронной подписи. Отметим, что законодательство Франции либерально относится к факту признания юридической силы электронных документов без привязки к конкретным технологическим средствам. Несмотря на то, что в настоящее время правилам, выдвигаемым к электронным подписям, соответствует только технология цифровой подписи, они (правила) не ограничиваются только данным видом аутентификации. В настоящее время нет готовых к использованию технологически нейтральных средств аутентификации, однако возможно принятие таковых в будущем, если они будут соответствовать требованиям законодательства Франции и будут использовать квалифицированные сертификаты.

Законодательство Франции устанавливает, что сертифицирующие организации государств не членов ЕС признаются законом, если они выполняют требования Директивы об электронных подписях 1999/93/ЕС [13]. Это означает, что они должны соответствовать требованиям французского закона и должны пройти аккредитацию, как того требует Директива, или что за их сертификаты поручается аккредитованный сертифицирующий орган государства-члена ЕС, или что они действуют в соответствии с международным договором.

Особенности нормативного регулирования электронного документооборота в Германии

В Германии правовой режим электронных документов, подписанных электронными подписями, установлен Законом «О подписях» 2001 года [13] и некоторыми другими нормативными актами.

Упомянутый Закон обеспечивает правовое признание электронных подписей, а также юридическую силу и допустимость электронных записей в качестве судебных доказательств.

Кроме специального закона, юридическое признание электронных подписей прописано и в общем законодательстве Германии (например, Германском гражданском уложении и процессуальном законодательстве). В общих законах также прописаны и исключения из правил. Например, не могут быть представлены в электронном виде и, соответственно, подписаны электронными подписями завещания, векселя и т.д.

Немецкий подход к приданию юридической силы договорам в электронной форме в части требования собственноручной подписи строго регламентируется. Дополнительные технические требования закреплены в Постановлении «О цифровой подписи» [13]. Данные нормативные акты совместно сформировали правовую основу для создания и подтверждения электронных подписей сертифицирующими органами, которые имеют государственную лицензию.

В соответствии с требованиями законодательства ЕС, законодательство Германии предусматривает использование как ЭП, так и электронных подписей в других формах, включая биометрию (принцип технологической нейтральности).

В Законе «О подписях» устанавливаются различные виды электронных подписей: простая, усовершенствованная и квалифицированная. Квалифицированная является полным юридическим эквивалентом физической подписи, хотя первые две также могут применяться в судебных процедурах. В Германии обязательная аккредитация удостоверяющих центров не предусмотрена. Тем не менее, центры могут пройти добровольную аккредитацию в качестве так называемых квалифицированных поставщиков сертификационных услуг, или центров доверия. Только те сертификаты, которые выпущены аккредитованными удостоверяющими центрами, признаются квалифицированными.

Законодательство Германии признаёт иностранные сертификаты ЭП при условии, что выдавшие их сертифицирующие органы прошли

аккредитацию в Германии и могут обеспечить соответствующий уровень безопасности.

Контрольные вопросы

1. Назовите основные риски при работе с электронными документами.
2. Что такое «информация конфиденциального характера»?
3. Какая информация может быть отнесена к персональным данным?
4. Как осуществляется разграничение доступа к электронным документам?
5. Что составляет основу «цифровой экономики»?
6. Дайте определение термину «электронный документооборот».
7. Какие плюсы и минусы электронного документооборота вы знаете?
8. Как организован трансграничный электронный документооборот в рамках одной организации?
9. Какие особенности электронного документооборота в США вы знаете?
10. Какие особенности электронного документооборота во Франции вы знаете?
11. Какие особенности электронного документооборота в Германии вы знаете?
12. Какие особенности регулирования электронного документооборота в РФ вы знаете?

3. Электронная подпись

3.1. Виды электронной подписи

ЭП предназначена для защиты электронного документа, передаваемого посредством различных сред или хранящегося в цифровом виде, от подделки и является атрибутом электронного документа. Она получается в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Отметим, что в общем случае термин «электронная подпись» является синонимом устаревшего термина «электронная цифровая подпись».

ЭП - это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;

- конфиденциальность документов;

- установление лица, отправившего документ.

Использование ЭП позволяет:

- значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;

- усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;

- гарантировать достоверность документации;

- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;

- построить корпоративную систему обмена документами.

Подделать ЭП очень сложно, т.к. это требует огромного количества вычислений, которые не могут быть реализованы при современном уровне математики и вычислительной техники за приемлемое время, то есть, пока информация, содержащаяся в подписанном документе, сохраняет актуальность. Дополнительная защита от подделки обеспечивается сертификацией Удостоверяющим центром открытого ключа подписи.

По сути, ЭП является официальным реквизитом, предназначенным для подтверждения целостности и аутентичности подписываемого документа. В отличие от обычной подписи некоторые виды ЭП не только подтверждают ее авторство, но и позволяют проследить изменения, внесенные в документ с момента его подписания. ЭП в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

- подтверждена подлинность электронной подписи в электронном документе;

- электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Чтобы разъяснить последний тезис, стоит подробнее рассмотреть современные виды электронных подписей.

Своим появлением электронная подпись обязана работам математиков Уитфилда Диффи и Мартина Хеллмана, которые в 1976 году в работе, посвящённой открытому кодированию, впервые предложили понятие «электронная цифровая подпись», выдвинув гипотезу о возможности существования схемы такой подписи.

Средствами ЭП являются аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи;

- подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи в электронном документе;

- создание закрытых и открытых ключей электронных подписей.

В основе ЭП лежит криптография открытого ключа. С ее помощью формируется специальный сертификат пользователя. Он содержит данные о пользователе, открытый ключ и электронную подпись сертификата, которую можно проверить с помощью открытого ключа удостоверяющего центра. Произвести генерацию ЭП может только удостоверяющий центр, который имеет секретный ключ шифрования и доверие к которому является основой для работы всей системы ЭП.

Доверие к удостоверяющим центрам основано на иерархическом принципе: сертификат удостоверяющего центра нижнего уровня заверяется электронной подписью удостоверяющего центра более высокого уровня. Высочайшим уровнем удостоверяющих центров является федеральный, который находится под управлением государственных органов. Вся система доверия, построенная на сертификатах, образует так называемую инфраструктуру открытых ключей (Public Key Infrastructure, или PKI). При такой инфраструктуре

требуется проверка не только легитимности ключа удостоверяющего центра, выдавшего сертификат, но и всех вышестоящих удостоверяющих центров. В частности, при формировании электронной транзакции необходимо проверить не только математическую корректность ЭП, но и валидность всей цепочки сертификатов, задействованных при изготовлении сертификата подписанта, на момент подписания им конкретного электронного документа.

Отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных Федеральным законом «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 г. № 210-ФЗ, регулируются ФЗ «Об электронной подписи» № 63-ФЗ от 06.04.2011 г. Этот закон вводит единообразное понимание следующих терминов:

1) электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (хотя справедливо и следующее определение ЭП: это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий установить отсутствие искажения информации в электронном документе с момента формирования подписи и проверить принадлежность подписи владельцу сертификата ключа подписи);

2) сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

3) квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным

удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

4) владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном Федеральным законом № 63-ФЗ порядке выдан сертификат ключа проверки электронной подписи;

5) ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

8) аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона;

9) средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

10) средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

11) участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

12) корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

13) информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано [3].

Законодатель выделяет три вида электронных подписей – простой электронной подписи, усиленной электронной подписи и квалифицированной электронной подписи [3].

Простая ЭП позволяет успешно установить авторство документа, но не позволяет проследить изменения, внесенные после его подписания. Следовательно, сфера использования простой ЭП сводится к обращениям в госструктуру, органы местного самоуправления или к частному лицу.

Для создания и выдачи такой ЭП удостоверяющий центр использует коды, пароли и подобные средства подтверждения личности владельца, обычно согласно схеме «логин-пароль», реже с использованием одноразового пароля.

Усиленная ЭП позволяет отследить изменения в подписанном документе и дает своему владельцу право принимать участие в значительно более широком спектре деловых отношений. Особенностью усиленной ЭП является то, что она может быть квалифицированной или неквалифицированной. Отметим, что сфера использования последнего вида ЭП резко сокращается.

Оба подвида усиленной ЭП равносильно используются при работе на коммерческих торговых площадках, для сдачи официальных отчетов в Национальный Союз Страховщиков, предприятиям сферы ЖКХ и подобным организациям.

Усиленная ЭП создаётся путем криптографического преобразования информации. Она в равной степени защищена двумя ключами – закрытым, как правило, хранящемся на носителе (токен) и открытым, необходимым для проверки ЭП. Ключевое различие между квалифицированной и неквалифицированной электронной подписью

заключается в уровне аккредитации, которую получил данный удостоверяющий центр по выдачи электронной подписи.

3.2. Удостоверяющие центры

Сертификаты ЭП выдают организации, которые называются Удостоверяющие центры (УЦ). В их функции входят:

- генерация закрытых ключей;

- предоставление открытых ключей (сертификатов) ЭП любым заинтересованным лицам;

- приостановка действия сертификатов ЭП в случае их компрометации;

- удостоверение действительности подписи электронных документов;

- разбор конфликтных ситуаций.

Для получения сертификата ЭП необходимо обратиться в УЦ или его представительство. Список УЦ, имеющих право выдавать сертификаты ЭП, принимаемые той или иной организацией, публикуется на сайте этой организации.

Процедура получения сертификата ЭП зависит от вида ЭП. Простая ЭП получается путём задания пользователем оригинальной пары логин-пароль, удовлетворяющей внутренним требованиям сервиса по длине кодовой комбинации и набору используемых символов.

Усиленная ЭП в простейшем случае может быть сгенерирована самим пользователем с использованием криптографических средств, распространяемых за плату или на безвозмездной основе.

Квалифицированные сертификаты ЭП выдаются на возмездной основе только Удостоверяющими центрами, получившими государственную аккредитацию (аккредитованными УЦ, АУЦ). Список АУЦ публикуется на официальном сайте федерального органа исполнительной власти, ответственного в области ЭП (Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации). Пользователь, желающий получить квалифицированный сертификат ЭП, может заполнить анкету-заявление на сайте выбранного им АУЦ либо, позвонив по указанному на сайте АУЦ телефону,

связаться со специалистом, который составит анкету-заявление и сообщит пользователю перечень необходимых для выдачи сертификата ЭП документов.

Собрав все необходимые для выдачи сертификата ЭП документы, отправив их копии в АУЦ и оплатив стоимость подготовки ЭП, пользователь через 3-5 дней при предъявлении оригиналов документов получает от АУЦ сертификат ЭП.

АУЦ на основании заполненной анкеты-заявления и комплекта документов готовит на своём программно-аппаратном комплексе сертификат ЭП.

Контрольные вопросы

1. Отличия электронной и электронной подписей.
2. Для чего предназначена ЭП?
3. Что обеспечивает ЭП при электронном документообороте?
4. Что такое сертификат ключа ЭП?
5. В каком виде может быть представлен ключ проверки электронной подписи?
6. Какое значение имеет ЭП в системе электронного документооборота?
7. Какова криптографическая основа ЭП?
8. Чем отличаются квалифицированная и неквалифицированная ЭП?
9. Какие удостоверяющие центры вы знаете?
10. Какая архитектура PKI (инфраструктура открытых ключей) действует в России?
11. Опишите процедуру получения сертификата электронной подписи.
12. Что лучше - шифровать или подписывать?
13. Как можно узнать статус сертификата ключа проверки ЭП?
14. Какая организация является регулятором в области электронной подписи?
15. При каких условиях сертификат считается недействительным?
16. Чем отличается защищенный носитель от «обычного» флеш-накопителя?

Список литературы

основная

1. Федеральный закон от 29.12.1994 № 77-ФЗ (ред. от 03.07.2016) «Об обязательном экземпляре документов» [Электронный ресурс]/Сайт Президента РФ. – Режим доступа http://www.kremlin.ru/acts/bank/7384 (дата обращения 23.05.2018).
2. ГОСТ Р 7.0.8-2013 Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения [Электронный ресурс]/Сайт Российский архив государственных стандартов. – Режим доступа http://www.rags.ru/gosts/gost/56742/ (дата обращения 23.05.2018).
3. Федеральный закон от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи» [Электронный ресурс]/Сайт Президента РФ. – Режим доступа http://www.kremlin.ru/acts/bank/17720 (дата обращения 24.05.2018).
4. Федеральный закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]/Сайт Президента РФ. – Режим доступа http://www.kremlin.ru/acts/bank/24157 (дата обращения 24.05.2018).
5. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» [Электронный ресурс]/Сайт Президента РФ. – Режим доступа http://www.kremlin.ru/acts/bank/32938 (дата обращения 24.05.2018).
6. ГОСТ Р 52292-2004 Информационная технология. Электронный обмен информацией. Термины и определения [Электронный ресурс]/Сайт Российский архив государственных стандартов. – Режим доступа http://www.rags.ru/gosts/gost/5028/ (дата обращения 24.05.2018).
7. Указ Президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера» [Электронный ресурс]/Сайт Президента РФ. – Режим доступа http://www.kremlin.ru/acts/bank/10638 (дата обращения 24.05.2018).
8. Конвенция ООН об использовании электронных сообщений в международных договорах (принята Резолюцией ООН N A/Res/60/21 от 9 декабря 2005 г.) [Электронный ресурс]/Сайт Организации Объединённых Наций.

http://www.un.org/ru/documents/decl_conv/conventions/elect_com.shtml (дата обращения 24.05.2018).
9. Бабенко Л.К., Курилкина А.М. Алгоритмы «распределенных согласований» для оценки вычислительной стойкости криптоалгоритмов / URSS — М., 2008.
10. «MoReq2010® Унифицированные требования к системам управления записями» [Электронный ресурс]/Сайт DLM Forum Foundation (Сайт государственных архивов и заинтересованных сторон Европейской комиссии) http://www.dlmforum.eu (дата обращения 24.05.2018).
11. ГОСТ Р ИСО 15489-1-2007 Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования [Электронный ресурс]/Сайт Российский архив государственных стандартов. – Режим доступа http://www.rags.ru/gosts/gost/461/ (дата обращения 24.05.2018).
12. Сокова А.Н. Документоведение: теория и практика С59 / предисл. проф. М.В. Ларина. М., 2009.
13. Арндт А.Ю. Электронная торговля: имплементация директив ЕС в национальное законодательство Германии, Франции и Великобритании / А.Ю. Арндт, О.А. Романов // [Электронный ресурс]/ Сайт «Право и Интернет»- http://www.russianlaw.net (дата обращения 23.05.2018)

дополнительная

1. Бачило И.Л., Семилетов С.И. Комментарий к Федеральному закону «Об электронной цифровой подписи» от 10.01.2002 г. №1-ФЗ // База данных Консультант плюс. - М, 2002.
2. Ларин М.В. Управление документацией в организациях / Научная книга. — М., 2002
3. Малофеев С. О применении электронной цифровой подписи в электронном документообороте / С. Малофеев // Секретарское дело. — 2009. — №7. — С. 24−28.
4. Романов Д., Ильина Т., Логинова А. Правда об электронном документообороте. — СПб.: Питер, 2008. — 244 с.
5. Семилетов С.И. Бумажный и электронный документ как результат документирования информации. Сб. Административное и информационное право // ИГП РАН, М., 2003.

План УМД на 2018/2019 уч.г.
С. 11, п. 53

Владимир Львович Владимиров,

Константин Николаевич Герцев,

Владимир Анатольевич Докучаев,

Виктория Валентиновна Маклачкова.

Организационно-технические средства защиты электронного документооборота

Часть 1

Учебное пособие

Подписано в печать 28.05.18. Формат 60x90 1/16.

Объем 2,4 усл. п. л. Тираж 50 экз. Изд. №58. Заказ

ООО «ТР-принт». Москва, ул. Правды, д. 24, стр. 5.

www.tirazhy.ru +7(499)519-01-24