МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра информационной безопасности

Составители
Е. В. Прокопенко
И. В. Чичерин

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Методические материалы

Рекомендованы учебно-методической комиссией специальности 10.05.03 Информационная безопасность автоматизированных систем в качестве электронного издания для использования в образовательном процессе

Кемерово 2018

Рецензенты

Стенин Д. В.– кандидат технических наук, доцент директор ИИТМА

Сыркин И. С. – кандидат технических наук, доцент кафедры информационных и автоматизированных производственных систем

Прокопенко Евгения Викторовна
Чичерин Иван Владимирович
Защита электронного документооборота: методические материалы [Электронный ресурс] для обучающихся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. В. Прокопенко, И. В. Чичерин; КузГТУ. – Электрон. издан. – Кемерово, 2018.

© КузГТУ, 2018
© Е.В. Прокопенко,
И. В. Чичерин,
составление, 2018

1. Введение. Понятие «электронный документ», «электронный документооборот».

По мере своего развития любое предприятие сталкивается с необходимостью введения электронного документооборота. Естественно, передаваемые в электронном виде документы имеют различную степень конфиденциальности и могут содержать сведения от полностью открытых до являющихся коммерческой тайной самого предприятия или его партнеров. Кроме того, при введении электронного документооборота возникнет вопрос обеспечения достоверности передаваемых документов, поэтому, помимо защиты конфиденциальных документов от ознакомления, необходимостью будет также использование кодов подтверждения достоверности документов – электронной цифровой подписи.

Наиболее остро вопрос защиты документооборота стоит для предприятий, имеющих территориально-распределенную структуру. Такие предприятия могут иметь несколько локальных вычислительных сетей (ЛВС), расположенных в разных местах, в том числе в различных регионах России, и вынуждены использовать для передачи информации различные глобальные вычислительные сети (ГВС) общего пользования, например, сеть Internet.

В данной статье описаны различные методы защиты передаваемых в ГВС электронных документов. Кроме того, изложенные ниже рекомендации будут полезны и для предприятий, имеющих единственную ЛВС, поскольку применяемые методы защиты не будут являться избыточными и в этом случае.

Угрозы и методы защиты

При электронном документообороте возникают различные угрозы со стороны пользователей ГВС, которые можно разделить на две основные категории:

- угрозы конфиденциальности информации,
- угрозы целостности информации.

Обеспечить конфиденциальность информации можно с помощью шифрования, использование же электронной цифровой подписи (ЭЦП) поможет сохранить целостность информации. ЭЦП позволит также установить авторство посланного документа.

В предлагаемой статье рассматривается комплексный метод защиты передаваемых электронных документов, обеспечивающий как целостность, так и конфиденциальность документов. Кроме того, рассматривается ряд проблем, возникающих при передаче и хранении ключевой информации, а также способы их решения.

Комплексный метод защиты

Естественно, для защиты и конфиденциальности, и целостности информации следует использовать в комплексе шифрование и ЭЦП, что также можно совместить с каким-либо дополнительным сервисом, например, сжатием информации (архивацией). В качестве примера таких систем следует привести специализированный архиватор электронных документов Crypton ArcMail, предлагаемый фирмой «Анкад».

Создаваемый таким образом файл-архив можно передавать по сети без каких-либо опасений. При создании архива исходные файлы подписываются на

секретном ключе ЭЦП (СК) абонента сети, после чего файлы сжимаются и получаемый в результате сжатия архив шифруется на случайном временном ключе. Абоненты, которым предназначается архив, могут расшифровать его с помощью записанного в архив зашифрованного временного ключа. Временный ключ зашифровывается на парно-связном ключе, вычисляемом по алгоритму Диффи-Хеллмана из СК отправителя и открытого ключа ЭЦП (ОК) абонента-адресата. Таким образом, достигаются следующие цели:

- Передаваемые электронные документы снабжаются кодом подтверждения достоверности – ЭЦП, который защищает их от нарушения целостности или подмены.
- Документы передаются в защищенном виде, что обеспечивает их конфиденциальность.
- Абоненты-адресаты могут расшифровать документы, используя свой СК и ОК отправителя.
- Абоненты сети, которым не предназначается данный архив, не могут прочитать его содержимое, поскольку не имеют временного ключа и не могут его вычислить.
- Дополнительный сервис – уменьшение размера, обусловленное архивацией.

Данный метод, а также используемые алгоритмы шифрования (ГОСТ 28147-89) и ЭЦП (ГОСТ Р 34.10-94 и 34.11-94), а также алгоритм вычисления парно-связного ключа (алгоритм Диффи-Хеллмана) наиболее подробно описаны в вышедшей в издательстве «Радио и Связь» книге Ю. В. Романца, П. А.Тимофеева и В. Ф. Шаньгина «Защита информации в компьютерных системах и сетях». Тем, кому наиболее интересна тема предлагаемой статьи, особенно рекомендую прочитать данную книгу.

Проблемы распределения и хранения ключей

При использовании ЭЦП и вышеописанного метода комплексной защиты электронных документов, применяемые в алгоритме ключевые элементы должны распределяться следующим образом: СК должен находиться у его владельца, парный ему ОК должен быть передан владельцем всем абонентам сети, с которыми он хочет обмениваться защищенной информацией.

ОК не являются секретными, но существует возможность их подмены. Например, возможна ситуация, что у злоумышленника есть доступ на компьютер, на котором абонент № 1 хранит открытые ключи. Злоумышленник считывает интересующие его сведения (ФИО, должность, …) из ОК, например, абонента № 2, после чего генерирует где-либо СК и ОК с такими данными и заменяет на компьютере абонента № 1 ОК абонента № 2 на фиктивный. После чего злоумышленник может подписать любой документ своим СК с данными абонента № 2 и переслать его абоненту № 1. При проверке ЭЦП такого документа будет выдано сообщение типа «Подпись лица (ФИО, должность, …) верна», что, мягко говоря, введет в заблуждение абонента № 1. Таким образом, очевидно, что необходима защита и открытых ключей. Такую защиту можно обеспечить несколькими способами.

1. *Использование персональной дискеты.*

Собственный СК и открытые ключи других абонентов могут быть записаны на персональную дискету, доступ к которой должен быть только у ее владельца. Однако, при большом количестве абонентов сети и большом потоке документов такой вариант нецелесообразен, так как замедляется обработка документов.

Смысл данного варианта состоит в использовании ключей-сертификатов. Предположительно, существует некий сертификационный центр (СЦ), в котором на специальном ключе (ключе-сертификате) подписывается открытый ключ абонента сети перед передачей его другим абонентам. Открытый ключ-сертификат должен храниться у всех абонентов сети для проверки целостности всех используемых в сети ОК. При таком варианте рекомендуется при проверке ЭЦП какого-либо документа автоматически проверять подпись соответствующего ОК (что обычно и делается автоматически программными средствами). Таким образом, сами ОК могут храниться в открытом виде, а персональная дискета, помимо СК владельца, должна содержать еще и ключ-сертификат.

СЦ можно совместить с центром распределения ключей (ЦРК). В этом случае, это будет выделенное рабочее место, используемое как для генерации ключей абонентов, так и для их сертификации и рассылки абонентам. Даже в случае генерации ключей непосредственно абонентами на местах, СЦ можно использовать для рассылки абонентам заверенных открытых ключей.

Данная схема особенно рекомендуется при организации электронного документооборота между несколькими юридическими лицами.

Порядок распределения ключей состоит в следующем:

- Абонент создает персональную дискету с собственными ключами. Секретный ключ закрывается паролем.
- Для собственного ОК формируется подпись на собственном СК. ОК записывается на дискету для передачи.
- Создается юридический документ на бумаге (например, письмо), в котором указываются: данные о владельце (Ф.И.О., должность, место работы), сам ОК (распечатка в шестнадцатеричном виде), полномочия владельца (перечень документов, которые уполномочен удостоверять владелец открытого ключа). Данный документ должен быть оформлен таким образом, чтобы иметь юридическую силу в случае возникновения спорных вопросов о принадлежности подписи и полномочиях владельца. Если в письме не установлено полномочий, то они определяются по должности и месту работы.
- Данный документ вместе с ОК пересылается в СЦ.
- СЦ проверяет юридическую силу полученного документа, а также идентичность ОК на дискете и в документе.
- В ответ абонент получает:
- сертифицированные ОК всех абонентов (в том числе, и свой),
- сертифицированные файлы с полномочиями владельцев ОК,
- ключ-сертификат, как в виде файла, так и в виде юридического документа.

- Владелец проверяет истинность ключа-сертификата, а также подписи всех полученных им ОК и файлов. При успешной проверке ОК записываются в соответствующий каталог, а ключ-сертификат – на персональную дискету.

При такой организации работ абонент формирует ЭЦП документов и не заботится об обмене открытыми ключами и полномочиями. Однако большая нагрузка по рассылке ОК и полномочий ложится на СЦ. Для пресечения фальсификации ОК сертификационный центр должен использовать организационные меры, о которых будет сказано ниже. В том случае, если у абонента сети остаются какие-либо сомнения относительно конкретного ОК, он может запросить распечатку ОК и полномочия напрямую у его владельца. Можно оставить за СЦ только сертификацию ключей и полномочий, освободив его от рассылки ОК. В этом случае, при первой посылке в любой адрес документов, абоненту необходимо послать по этому адресу также сертифицированные ОК и полномочия. В общем случае, сертификационных центров может быть несколько. Пользователь может сертифицировать свой ОК в разных, не связанных друг с другом, СЦ. Кроме того, СЦ могут быть связаны в сеть с любой необходимой иерархической организацией для обмена либо только ключами-сертификатами, либо дополнительно еще и открытыми ключами. Тогда пользователю достаточно сертифицировать ОК только в одном из таких СЦ для обмена информацией с абонентами всех охватываемых СЦ сетей.

При большом количестве абонентов сети рекомендуется использование баз данных (БД) ОК. В этом случае, вместо отдельных ОК, сертификационный центр пересылает абоненту одинаковый для всех абонентов файл БД, содержащий все используемые ОК.

Согласно сказанному выше, персональная дискета должна содержать следующее:

- СК владельца;
- открытые ключи-сертификаты по числу сертификационных центров.

В качестве ключа сертификационного центра может быть использован собственный СК абонента; в этом случае, при получении ОК другого абонента, его необходимо подписать. При этом на персональную дискету следует записать свой ОК для проверки целостности ОК других абонентов. Вместо персональной дискеты может быть использован другой ключевой носитель, например электронная таблетка Touch Memory (TM) или смарт-карта (SC), что иногда предпочтительнее использованию ключевой дискеты, поскольку, например, с SC ключи шифрования могут быть непосредственно загружены в шифроустройтсво, минуя оперативную память компьютера.

2. *Использование систем защиты от несанкционированного доступа (ЗНСД).*

Нет необходимости в специальных мерах по защите ключей в том случае, если используется система ЗНСД, блокирующая доступ на компьютер неавторизованных пользователей, либо использующая прозрачное шифрование информации на компьютере абонента.

В том случае, если используются персональные дискеты с централизованной генерацией ключей абонентов, использование систем ЗНСД все же необходимо для защиты ЦРК.

Виртуальные частные сети

Другое решение проблемы защиты электронного документооборота – построение виртуальных частных сетей (VPN – Virtual Private Network). VPN представляет собой защищенную корпоративную сеть, использующую любую ГВС (в частности, Internet) для передачи защищенных данных между сегментами VPN. Сегментами VPN могут быть как ЛВС предприятия или его удаленного подразделения, так и мобильные или удаленные пользователи, клиенты или ЛВС предприятий-партнеров.

Защита сегментов VPN происходит, например, с помощью межсетевых экранов. Межсетевой экран представляет собой выделенный компьютер, который производит следующие действия:

- Фильтрует передаваемую через него информацию согласно определенным правилам и таблицам адресов пользователей VPN.
- Обеспечивает шифрование передаваемой информации на определенном ключе. Шифрование информации может происходить и на конкретном рабочем месте абонента сети.
- При получении информации из внешней сети – проверяет ее целостность, расшифровывает и передает конкретному абоненту сети.
- Позволяет изолировать внутреннее адресное пространство путем замены внутренних адресов сети в заголовках передаваемых пакетов.

Защита документооборота с удаленными или мобильными пользователями происходит путем шифрования передаваемой информации, обычно на парносвязном ключе удаленного пользователя и адресата (или отправителя).

Использование VPN имеет следующие преимущества:

- Обмен только защищенной информацией между авторизованными пользователями.
- Изолированность от ГВС внутренней сети и ее топологии.
- Прозрачность для абонентов сети.

К недостаткам использования VPN можно отнести некоторое замедление передачи информации в ГВС.

Использование криптосервера

Шифрование информации в различных системах документооборота производится как программными, так и аппаратными средствами. Аппаратные средства шифрования имеют ряд преимуществ по сравнению с программными (защищенность и неизменность алгоритма шифрования, возможность загрузки ключей шифрования непосредственно в устройство криптографической защиты данных (УКЗД), возможность одновременного использования УКЗД в системе ЗНСД). К недостаткам же аппаратных средств можно отнести несколько более низкую скорость обработки данных и более высокую стоимость.

Использование криптосервера решает ряд проблем, связанных с выбором шифратора. Криптосервер представляет собой отдельный компьютер в ЛВС, ос-

нащенный аппаратным шифратором и используемый для шифрования информации для абонентов сети по их запросам. Зашифрованная информация может впоследствии использоваться абонентом по его усмотрению, в том числе, для передачи по ГВС. Информация абонента может быть также автоматически подписана криптосервером.

Порядок работы криптосервера может быть, например, таким:

- Абонент направляет на криптосервер открытые данные.
- Происходит взаимная аутентификация абонента и криптосервера. Для идентификации абонента используется его персональная SC, содержащая используемые для аутентификации СК абонента и ОК криптосервера.
- После успешной аутентификации криптосервер зашифровывает данные на персональном ключе абонента (выбираемом из хранящейся на сервере таблицы ключей абонентов) и подписывает их.
- Абонент получает зашифрованные и подписанные данные.

Преимущества использования криптосервера:

- Использование одного шифратора вместо нескольких (по числу абонентов).
- Хранение всех ключей для предачи документов в ГВС только на криптосервере.
- Упрощение администрирования – все полномочия абонентов определяются администратором и хранятся только на криптосервере.
- Использование микропроцессорной SC в качестве носителя ключей аутентификации – исключает возможность несанкционированного использования хранящихся на криптосервере ключей.

Следует учесть, что, как и у любого другого дешевого решения, у криптосервера есть некоторые недостатки. Прежде всего, это необходимость защиты такой сети от попыток доступа из ГВС, поскольку информация посылается на криптосервер в незащищенном виде. Во-вторых, криптосервер обязательно должен быть защищен системой ЗНСД, поскольку он содержит все ключевые элементы пользователей такой ЛВС.

Организационные мероприятия

Следует учесть, что использование любых систем защиты документооборота будет недостаточным без введения некоторых организационных мер. К ним можно отнести следующее:

- Использование протоколирования всех операций, совершенных с помощью системы защиты. Протоколирование (ведение журналов операций) во многих системах ведется автоматически; оно должно быть обязательным на особо важных рабочих местах, например, ЦРК, СЦ, рабочее место администратора по безопасности.
- Предотвращение получения злоумышленниками ключевых дискет и их тиражирования владельцами. Для этого, помимо простого введения паролей, можно использовать в качестве ключевых носителей микропроцессорные SC.
- Разграничение доступа на рабочие места, как административными мерами (напр., разграничение доступа в помещения), так и с использованием различных систем ЗНСД, что особенно актуально для тех же ЦРК и СЦ.

Электро́нный докуме́нт:

- 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[1].
- Форма представления информации в целях её подготовки, отправления, получения или хранения с помощью электронных технических средств, зафиксированная на магнитном диске, магнитной ленте, лазерном диске и ином электронном материальном носителе[2].
- 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[3].

Юридическую значимость электронному документу придаёт электронная подпись, которая на территории Российской Федерации равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий[4]:

1. сертификат ключа подписи, относящийся к этой электронной цифровой 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 цифровой подписи в электронном документе;
4. электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Электронный документооборот – это обмен электронными документами по телекоммуникационным каналам связи (ТКС) оператора ЭДО.

Сначала поясним понятие «электронный документ». Электронный документ – это файл, заверенный электронной подписью. Его не нужно распечатывать, так как юридически значимым оригиналом он является именно в электронном виде.

Электронный документооборот (ЭДО) происходит через систему оператора ЭДО, включенного в сеть доверия ФНС РФ. Одна организация отправляет другой файл документа. Адресат получает его через несколько секунд на своем ПК. Процесс можно сравнить с электронной почтой. При передаче документа оператор автоматически проверяет легитимность электронной подписи, которой завизирован документ, и соответствие формата документа требованиям законодательства.

Если документ требует двусторонней подписи, получатель также подписывает его электронной подписью или отказывает в подписи и запрашивает корректировку. Движение документа отправитель может отследить благодаря статусам: «Отправлен», «Получен», «Подписан», «Отказано в подписи».

Внедрение ЭДО позволит удобно и просто представлять электронные документы через интернет по требованию налоговых органов. ЭДО подходит как малому и среднему бизнесу, так и крупным предприятиям и холдингам.

Для чего нужен электронный документооборот компаниям:

- уменьшить количество бумажных документов в офисе;
- сократить финансовые и трудозатраты на содержание архива;
- снизить расходы на печать, канцтовары, отправку документов;
- уменьшить трудозатраты за счет исключения ручных действий и автоматизации процесса;
- избавиться от потерь документов и необходимости выставлять их заново.

Электронный документ – 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 (п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

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 – это документ, информация которого представлена в электронной форме.

При этом для электронного документа характерны:

- аутентичность – свойство электронного документа, гарантирующее, что электронный документ идентичен заявленному;
- 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;
- пригодность для использования - свойство электронного документа, позволяющее его локализовать и воспроизвести в любой момент времени.

Исходя из этого, можно сделать вывод, что электронный документ – это любой документ, который представлен в электронном виде, в том числе это может быть скан-образ документа, файл, набранный в текстовом редакторе, и т. п.

При этом электронные документы могут быть формализованными, т.е. составленными в таком виде, который позволяет с помощью программных средств распознавать их содержимое, и неформализованными (например, скан-копия).

В рамках обмена электронными документами стороны могут использовать как формализованные документы, так и неформализованные. Исключение составляют случаи, когда законодательством утвержден обязательный формат для обмена конкретным документом (например, формат счета-фактуры). Но если документ неформализованный, его принятие и распознавание возможно только с участием человека.

Для того, чтобы обмениваться документами в электронном виде без участия человека в распознавании текста этих документов, необходимо все документы со-

ставлять в формализованном виде, т. е. в том формате, который могут использовать программные средства всех участников обмена.

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 другими федеральными законами, регулируются Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Закон № 63-ФЗ).

Электронная подпись (ЭП) – это 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 (пп. 1 ст. 2 Закона № 63-ФЗ).

Именно электронная подпись может сделать электронный документ равнозначным документу на бумажном носителе, подписанному собственноручно, т. е. придать ему юридическую силу.

Согласно ст. 5 Закона № 63-ФЗ различают два вида электронной подписи – простая и усиленная. При этом усиленная электронная подпись может быть неквалифицированной и квалифицированной.

- **Простая ЭП** – это пароли, коды и прочие средства, подтверждающие, что документ подписан определенным лицом. Для того чтобы электронный документ, подписанный этой подписью, признавался равнозначным бумажному документу, подписанному собственноручно, необходимо выполнение определенных условий, предусмотренных Законом об ЭП. Кроме того, условия признания и порядок проверки этой подписи устанавливаются нормативными правовыми актами, принимаемыми в соответствии с федеральными законами, или соглашением между участниками обмена. Документы, требующие печати, не могут быть подписаны простой ЭП.
- **Усиленная неквалифицированная ЭП** создается с помощью специальных программных средств. Данная подпись позволяет определить лицо, подписавшее документ, и защитить его от несанкционированного изменения. Данная подпись также выдается УЦ и признается равнозначной собственноручной подписи в случаях, определенных законодательством или соглашением сторон. Неквалифицированной ЭП можно подписывать документы, которые в бумажном виде заверяются печатью.
- **Усиленная квалифицированная ЭП** отличается от неквалифицированной ЭП тем, что выдается аккредитованным удостоверяющим центром. К ней прилагается квалифицированный сертификат ключа проверки ЭП. Аккредитацию удостоверяющий центр сможет получить в Минкомсвязи России, которое в соответствии с постановлением Правительства РФ от 28.11.2011 № 976 становится уполномоченным органом в области использования электронной подписи.

С 30.01.2016 в соответствии с п. 5 ч. 4 ст. 8 Закона № 63-ФЗ (в ред. Федерального закона от 30.12.2015 № 445-ФЗ) на Минкомсвязь России возложены пол-

номочия по установлению формата электронной подписи, обязательного для реализации всеми средствами электронной подписи, по согласованию с ФСБ России.

Сертификат ключа проверки ЭП – электронный или бумажный документ, который подтверждает принадлежность этой подписи конкретному лицу.

Удостоверяющий центр (УЦ) – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Законом № 63-ФЗ. Эта организация должна получить аккредитацию в Минкомсвязи России, которое уполномочено на выдачу в соответствии с постановлением Правительства РФ от 28.11.2011 № 976.

Напомним, что до 01.07.2013 аналогичные отношения регулировались Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

Юридическая сила документов, подписанных электронной подписью

В соответствии с нормами Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» электронные документы, подписанные квалифицированной электронной подписью, всегда признаются равнозначными документам, подписанным собственноручно и могут применяться в любых правоотношениях в соответствии с законодательством Российской Федерации. Исключение составляют случаи, когда законодательство допускает составление документа только на бумажном носителе.

Электронные документы, подписанные простой электронной подписью или неквалифицированной электронной подписью, признаются равнозначными документам на бумажном носителе, подписанным собственноручно, если это установлено законодательством или соглашением между сторонами.

В соглашении или нормативном правовом акте, которые признают документы, подписанные простой или неквалифицированной электронной подписью, равнозначными собственноручно подписанным документам, должны быть прописаны:

1) порядок проверки электронной подписи;

2) правила определения лица, подписывающего электронный документ, по его подписи (только для простой электронной подписи);

3) обязанность лица, создающего или использующего ключ простой электронной подписи, соблюдать его конфиденциальность (только для простой электронной подписи).

Таким образом, Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» признает юридическую силу тех электронных документов, которые подписаны усиленной квалифицированной электронной подписью. Для того, чтобы документы, подписанные усиленной неквалифицированной подписью имели юридическую силу, необходимо заключать дополнительное соглашение, где прописывать дополнительные условия признания таких документов равнозначными, подписанным собственноручно.

Гражданский кодекс РФ и Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете» (далее - Закон № 402-ФЗ) не уточняют, какой именно вид электронной подписи необходимо использовать в бухгалтерских документах,

чтобы они признавались юридически значимыми (ч. 5 ст. 9 Закона № 402-ФЗ, п. 2 ст. 160 ГК РФ). В то же время согласно п. 4 ч. 3 ст. 21 Закона № 402-ФЗ виды электронных подписей, используемых для подписания документов бухгалтерского учета, должны быть установлены соответствующим федеральным стандартом, который на настоящий момент отсутствует.

Налоговый кодекс РФ, напротив, признает только те электронные документы, которые подписаны усиленной квалифицированной электронной подписью (п. 7 ст. 23, п.п. 4,6 ст. 78, п. 2 ст. 79, п. 1 ст. 80, п. 6 ст. 169, п. 6 ст. 176 НК РФ). Исключение составляет только передача налогоплательщиками – физическими лицами документов в электронной форме через личный кабинет, где допускается применение усиленной неквалифицированной электронной подписи, сформированной в соответствии с приказом ФНС России от 20.08.2015 № СА-7-6/364@ (п. 2 ст. 11.2 НК РФ).

2. Нормативная правовая база в сфере электронного документооборота.

1. Гражданский кодекс Российской Федерации

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).

2. Арбитражный процессуальный кодекс Российской Федерации

Закон регулирует отношения в сфере предпринимательской и экономической деятельности. В частности, разрешает использовать документы, подписанные электронной подписью в качестве письменных доказательств в арбитражных спорах (п. 3 ст. 75).

3. Налоговый кодекс Российской Федерации

Регулирует вопросы уплаты налогов и представления отчетов в контролирующие органы – прежде всего в ФНС. Кодекс содержит понятие «электронный счет-фактура» и устанавливает порядок его использования (ст. 169).

4. Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»

Закон устанавливает единые требования к бухгалтерскому учету. В статье 9 обозначены обязательные реквизиты первичного учетного документа, а также общие процедуры, связанные с ним, такие как подписание и исправление. Кроме того, пункт 5 статьи 9 разрешает составлять первичный учетный документ в электронном виде с электронной подписью.

5. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также при совершении иных юридически значимых действий.

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Регулирует отношения, возникающие при обеспечении защиты информации, применении информационных технологий, осуществлении права на поиск,

получение, передачу, производство и распространение информации. В статье 2 содержится понятие «электронный документ».

3. Классификация систем электронного документооборота.

Классификация систем электронного документооборота (СЭД) Современные предприятия все чаще переходят от бумажной документации к электронной, что позволяет упростить рабочие процессы и добиться повышения их результативности.

Классификация систем электронного документооборота является достаточно обширной, поэтому для выбора нужного принципа работы понадобится тщательно в них разобраться.

Все системы электронного документооборота классифицируются сразу по нескольким принципам.

Все виды СЭД в этом случае делятся на российские, зарубежные и российские, но сконструированные на основе платформ Domino и Lotus. Классификация появилась не случайно – она имеет определенные обоснования. Зарубежные разработчики начали создавать виды систем электронного документооборота намного раньше всех остальных. За многие годы разработок они сумели создать качественное ПО и проработали пути решения всех возможных ошибок.

Отечественные системы обладают целым рядом технических несовершенств, поскольку создавались в сжатые сроки. Однако отечественные виды систем электронного документооборота обычно учитывают российскую специфику: ввод имени и отчества, специальные параметры ввода адреса и т. д.

Таким образом, происхождение системы напрямую влияет на ее потребительские свойства, и пользователю нужно делать определенный выбор. Те системы, что были возведены с помощью платформ Domino и Lotus, следует рассматривать как самостоятельный класс СЭД. Они созданы на основе отечественных подходов к организации рабочего процесса, но механизмы в них используются зарубежные. Таким образом, получается удачное сочетание двух разновидностей.

Все системы, имеющие дело с электронным документооборотом, обладают определенной функциональностью, о которой пользователь также должен знать. Главные свойства той или иной СЭД обычно подчеркиваются производителями.

Согласно им можно выделить следующие классы данных систем:

- регистрационные;
- создающие электронные документы;
- автоматизирующие работу с архивной информацией;
- управляющие архивами;
- извлекающие информацию из архивных файлов и прочих источников;
- управляющие обработкой документов;
- контролирующие работу устройств для хранения данных.

Такая классификация СЭД создается по функциональному признаку, но это лишь видимость. Классы в данном случае выделяются по совершенно разным признакам. Кроме того, они способны пересекаться, и два пользователя могут вести работу по одному и тому же файлу одновременно.

Главный плюс подобной классификации – высокая информативность. Функционал всех материалов описан достаточно подробно, при желании пользователь сможет легко разобраться, к какому именно классу можно отнести те или иные данные. Однако эту классификацию нельзя назвать корректной, она нуждается в серьезной доработке.

Специалисты считают, что к СЭД необходимо относить системы, контролирующие общий корпоративный контент.

В данном случае виды СЭД будут следующими:

– для управления документами и обеспечения их связи с бизнес-процессами;
– для обработки документации и ее ввода в постоянное использование;
– для контроля за всеми записями, как актуальными, так и архивными;
– для поиска и анализа имеющихся материалов;
– для управления контентом на интернет-порталах;
– для автоматизации бизнес-процессов;
– для формирования коллективного сотрудничества;
– для создания информационного сайта внутри организации.

Информативность данной классификации достаточно высока, но здесь также возможно активное пересечение видов друг с другом. В этом случае придется дополнительно разбираться с каждым материалом, что может вызвать дополнительные временные затраты.

Быстрота и удобство – основные принципы качественной системы электронного документооборота, и их классификация может быть осуществлена и по компонентам и общему функционалу. Согласно этой классификации, существует 17 групп компонентов, которые внутри могут подразделяться на почти 90 типов. Среди групп СЭД выделяют те, что отвечают за: ввод данных, их распознавание, регистрацию (по правилам), поиск, индексацию, лингвоанализ, обработку материалов, прием и передачу файлов. Некоторые из них занимаются репликацией, хранением файлов, работой в интернете, защитой от взлома, выводом документации, их используют для управления данными и разработки дополнительных приложений.

Такая классификация очень продуктивна. Ее использование помогает описывать системы электронного документооборота вместе с их достоинствами и недостатками, а также формировать требования к системам, которые только будут разработаны. Общий функционал описывается очень подробно, на их основе можно создать грамотные и содержательные требования. Есть у этой классификации и недостаток – таким образом можно будет сформировать технические требования. Прикладные требования, имеющие отношение к реалиям предметной области, нужно будет формировать отдельно. Речь идет о типах материалов, с которыми придется работать внутри системы, а также об алгоритмах работы с ними. Важно понять, как именно файлы нужно обрабатывать и выводить из системы, но на это может уйти очень много времени.

Классификация систем электронного документооборота

1. Универсальные «коробочные» СЭДО:

- стандартный набор функций;
- невозможность полного соответствия потребностям конкретной организации;
- низкие временные затраты на приобретение и установку;
- относительно низкая стоимость;
- необходимость приобретения лицензии на каждое внедряемое рабочее место.

2. Индивидуально разрабатываемые СЭДО:

- максимально персонифицированная система;
- большие временные затраты;
- высокая стоимость разработки;
- сопутствующие расходы: затраты на обучение сотрудников, покупку нового оборудования и программного обеспечения.

3. Комбинированные СЭДО:

- базовая платформа, к которой разрабатываются необходимые дополнительные модули;
- полное соответствие нуждам предприятия;
- небольшие временные затраты на разработку и внедрение;
- стоимость включает: цену базовой платформы и стоимость индивидуальной доработки, зависящей от сложности заказа;
- передача заказчику прав на продукт;
- простота освоения и использования;
- полная локализация;
- удобный интерфейс;
- взаимодействие с существующими офисными приложениями.

4. Основные функции систем электронного документооборота.

Основными функциями системы электронного документооборота являются:

- регистрация документов;
- контроль исполнения документов;
- создание справочников и работа с ними;
- контроль движения бумажного и электронного документа, ведение истории работы с документами;
- создание и редактирование реквизитов документов;
- формирование отчетов по документообороту предприятия;
- импорт документов из файловой системы и Интернета;
- создание документа прямо из системы на основе шаблона (прямая интеграция);
- работа с версиями документа, сложными многокомпонентными и многоформатными документами, вложениями;
- электронное распространение документов;
- работа с документами в папках;
- получение документов посредством сканирования и распознавания.
- уменьшением затрат на доступ к информации и обработку документов.

5. Идентификация, аутентификация, авторизация в системе электронного документооборота.

В защищенной ОС любой пользователь (субъект доступа), перед тем как начать работу с системой, должен пройти идентификацию, аутентификацию и авторизацию. *Субъектом доступа* (или просто *субъектом)*называют любую сущность, способную инициировать выполнение операций над элементами ОС. В частности, пользователи являются субъектами доступа.

Идентификация субъекта доступа заключается в том, что субъект сообщает ОС *идентифицирующую информацию* о себе (имя, учетный номер и т. д.) и таким образом идентифицирует себя.

Для того чтобы установить, что пользователь именно тот, за кого себя выдает, в информационных системах предусмотрена процедура *аутентификации*, задача которой – предотвращение доступа к системе нежелательных лиц.

Аутентификация субъекта доступа заключается в том, что субъект предоставляет ОС помимо идентифицирующей информации еще и *аутентифицирующую информацию,* подтверждающую, что он действительно является тем субъектом доступа, к которому относится идентифицирующая информация (см. гл. 7).

Авторизация субъекта доступа происходит после успешной идентификации и аутентификации. При авторизации субъекта ОС выполняет действия, необходимые для того, чтобы субъект мог начать работу в системе. Например, авторизация пользователя в операционной системе 1Ж1Х включает в себя порождение процесса, являющегося операционной оболочкой, с которой в дальнейшем будет работать пользователь. В ОС Vindows N7 авторизация пользователя включает в себя создание маркера доступа пользователя, создание рабочего стола и запуск на нем от имени авторизуемого пользователя процесса Е^еппк, инициализирующего индивидуальную программную среду пользователя. Авторизация субъекта не относится напрямую к подсистеме защиты ОС. В процессе авторизации решаются технические задачи, связанные с организацией начала работы в системе уже идентифицированного и аутентифицированного субъекта доступа.

Взаимосвязь идентификации, аутентификации и авторизации

Наверное, вы уже догадались, что все три процедуры взаимосвязаны:

1) Сначала определяют имя (логин или номер) – идентификация
2) Затем проверяют пароль (ключ или отпечаток пальца) – аутентификация
3) И в конце предоставляют доступ – авторизация

6. Разграничение прав пользователей в системе электронного документооборота. Матрица доступа.

Модель безопасности, специфицированная в предыдущем разделе, имеет вид матрицы, которая называется ***матрицей доступа***. Какова может быть эффективная реализация *матрицы доступа*? В общем случае она будет разреженной, то есть большинство ее клеток будут пустыми. Хотя существуют структуры данных для представления *разреженной матрицы*, они не слишком полезны для приложений, использующих возможности защиты. Поэтому на практике *матрица дос-*

тупа применяется редко. Эту матрицу можно разложить по столбцам, в результате чего получаются **списки прав доступа** (access control list – ACL). В результате разложения по строкам получаются *мандаты* возможностей (capability list или capability *tickets*).

Безопасный доступ к данным внутри СЭД обеспечивается аутентификацией и разграничением прав доступа к объектам.

В СЭД могут использоваться различные методы аутентификации. Самый распространенный из них – применение многоразовых паролей. Шифрованные значения паролей обычно хранятся на сервере в специальной базе данных пользователей. Однако надежность данного метода сильно снижает человеческий фактор. Даже если пользователь использует правильно сгенерированный пароль, иногда его можно обнаружить записанным на листке бумаги в столе или под клавиатурой.

Часто полномочия пользователя подтверждаются специальным носителем информации. Существует множество решений для имущественной аутентификации пользователя: это USB-ключи, смарт-карты, магнитные карты, дискеты и компакт-диски. Здесь также не исключено влияние человеческого фактора, но злоумышленнику необходимо не только получить сам ключ, но и узнать PIN-код.

Надежным для проведения идентификации и последующей аутентификации является биометрический метод, при котором пользователь идентифицируется по своим биометрическим данным (это может быть отпечаток пальца, сканирование сетчатки глаза). Однако стоимость решения в этом случае выше, а современные биометрические технологии еще не настолько совершенны, чтобы избежать ложных срабатываний или отказов.

Важным параметром аутентификации является количество учитываемых факторов. Процесс аутентификации может быть однофакторным, двухфакторным и т. д. Возможно также комбинирование различных методов: парольного, имущественного и биометрического. Например, аутентификация может проходить при помощи пароля и отпечатка пальца (двухфакторный способ).

Разграничение прав доступа к объектам. Разграничение прав доступа к объектам системы электронного документооборота, может быть реализовано исходя из различных принципов:

– задание пользователей и групп, имеющих право чтения, редактирования или удаления всего документа, включая присоединенные файлы и реквизиты;

– мандатный доступ по группам, когда доступ к данным, предоставляется в соответствии с фиксированными уровнями полномочий групп пользователей;

– разграничение доступа к различным частям документов, например к разным присоединенным файлам, группам реквизитов, полям регистрационных карточек, поручениям по документу.

Среди методов разграничения доступа можно выделить:

– задание доступа на уровне серверной базы данных;

– ограничение доступа на интерфейсном уровне, когда ряд действий не может быть выполнен через пользовательский интерфейс, но доступен в случае написания отдельной программы.

7. Электронные подписи.

Электронная подпись (ЭП) – это особый реквизит документа, который позволяет установить отсутствие искажения информации в электронном документе с момента формирования ЭП и подтвердить принадлежность ЭП владельцу. Значение реквизита получается в результате криптографического преобразования информации.

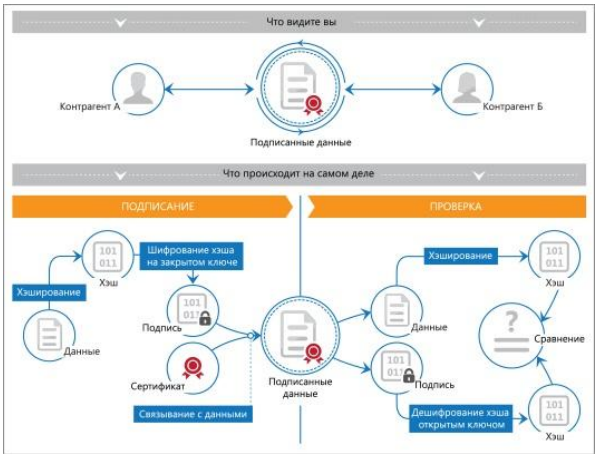
Сертификат электронной подписи – документ, который подтверждает принадлежность открытого ключа (ключа проверки) ЭП владельцу сертификата. Выдаются сертификаты удостоверяющими центрами (УЦ) или их доверенными представителями.

Владелец сертификата ЭП – физическое лицо, на чье имя выдан сертификат ЭП в удостоверяющем центре. У каждого владельца сертификата на руках два ключа ЭП: закрытый и открытый.

Закрытый ключ электронной подписи (ключ ЭП) позволяет генерировать электронную подпись и подписывать электронный документ. Владелец сертификат обязан в тайне хранить свой закрытый ключ.

Открытый ключ электронной подписи (ключ проверки ЭП) однозначно связан с закрытым ключом ЭП и предназначен для проверки подлинности ЭП.

Ниже представлены схема подписания электронного документа и схема проверки его неизменности.



Согласно Федеральному закону №63-ФЗ «Об электронной подписи», имеет место деление на:

- простую электронную подпись;
- усиленную неквалифицированную электронную подпись;
- усиленную квалифицированную электронную подпись.

Простая электронная подпись посредством использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом.

Усиленную неквалифицированную электронную подпись получают в результате криптографического преобразования информации с использованием закрытого ключа подписи. Данная ЭП позволяет определить лицо, подписавшее электронный документ, и обнаружить факт внесения изменений после подписания электронных документов.

Усиленная квалифицированная электронная подпись соответствует всем признакам неквалифицированной электронной подписи, но для создания и проверки ЭП используются средства криптозащиты, которые сертифицированы ФСБ РФ. Кроме того, сертификаты квалифицированной ЭП выдаются исключительно аккредитованными удостоверяющими центрами (Перечень аккредитованных УЦ).

Согласно ФЗ № 63 «Об электронной подписи» электронный документ, подписанный простой или усиленной неквалифицированной ЭП, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью. При этом обязательным является соблюдение следующего условия: между участниками электронного взаимодействия должно быть заключено соответствующее соглашение.

Усиленная квалифицированная подпись на электронном документе является аналогом собственноручной подписи и печати на бумажном документе. Контролирующие органы, такие как ФНС, ПФР, ФСС, признают юридическую силу только тех документов, которые подписаны квалифицированной ЭП.

Область применения электронной подписи

Мы собрали все возможные сферы применения ЭП в одной таблице.

	Простая	Неквалифицированная	Квалифицированная
Внутренний и внешний документооборот	✔	✔	✔
Арбитражный суд	✔	✔	✔
Документооборот с физическими лицами	✔	✔	✔
Госуслуги	✔		✔
Контролирующие органы (ФНС, ФСС,ПФР)			✔
Электронные торги			✔

Начнем рассматривать с самых распространенных на данный момент.

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

При построении межкорпоративного документооборота (B2B) наличие ЭП является критически важным условием обмена, поскольку является гарантом юридической силы. Только в этом случае электронный документ может быть при-

знан 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.

2. Электронная отчетность для контролирующих органов. Многие компании, наверняка, уже оценили удобство сдачи отчетности в электронном виде. 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 ФНС, ФСС. Основа этой услуги – сертификат электронной подписи, который должен быть выпущен надежным удостоверяющим центром, метод же отправки не имеет решающего значения. Такая подпись нужна для придания документам юридической значимости.

3. Государственные услуги. Каждый гражданин Российской Федерации может получить электронную подпись для получения госуслуг. С помощью ЭП гражданин может заверять документы и заявления, отправляемые в ведомства в электронном виде, а так же получать подписанные письма и уведомления о том, что обращение принято на рассмотрение от соответствующих органов 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 (Источник: портал Госуслуги).

4. Электронные торги. Электронные торги проходят на специальных площадках (сайтах). Электронная подпись необходима поставщикам на государственных и коммерческих площадках. ЭП поставщиков и заказчиков гарантируют участникам, что они имеют дело с реальными предложениями. Кроме того, заключенные контракты приобретают юридическую силу только при его подписании обеими сторонами.

5. Арбитражный суд. При возникновении каких-либо споров между организациями в качестве доказательства в суде могут использоваться электронные документы. Согласно Арбитражному процессуальному кодексу РФ, полученные посредством факсимильной, электронной или иной связи, подписанные электронной подписью или другим аналогом собственноручной подписи, относятся к письменным доказательствам. Об этом подробнее ниже.

6. Документооборот с физическими лицами. Надо признать, данная сфера применения ЭП весьма специфична и пока редко используема, тем не менее, возможна. С помощью ЭП заверять различные документы могут физические лица. Благодаря этой возможности удаленные работники на основании договоров оказания услуг, например, могут выставлять акты приемки-сдачи работ в электронном виде.

Начинаем использовать ЭП

Выбор сертификата ЭП

Во-первых, как уже говорилось, существуют различные типы электронной подписи. Участники электронного взаимодействия вправе использовать электронную подпись любого вида по своему усмотрению, если законодательство РФ не закрепляет использование конкретного вида подписи в зависимости от целей ее использования.

Во-вторых, выбор типа электронной подписи зависит от задач, которые необходимо решать с ее помощью. Так, например, выдвигаются требования к выбору электронной подписи при работе с бухгалтерскими первичными документами: электронный счет-фактура является документом основанием для вычета сумм НДС только в том случае, если он подписан квалифицированной электронной подписью. Для сдачи отчетности в государственные органы также потребуется использование усиленной квалифицированной электронной подписи.

Для решения задач межкорпоративного электронного документооборота можно использовать усиленную квалифицированную электронную подпись. Получить сертификат квалифицированной электронной подписи можно в любом аккредитованном Минкомсвязи РФ Удостоверяющем центре (Перечень аккредитованных УЦ).

Квалифицированная электронная подпись позволяет осуществить доказательное подтверждение авторства документа, защиту от изменений и контроль целостности документа.

Для внутреннего электронного документооборота при наличии соответствующих локальных НПА вы всегда можете самостоятельно создать и использовать как простую электронную подпись, так и неквалифицированную.

Сколько сертификатов ЭП нужно?

Усиленная квалифицированная электронная подпись решает достаточно широкий спектр задач. С ее помощью вы сможете сдавать отчетность в налоговые органы, обмениваться электронными документами с контрагентами и другое.

Приобретая сертификат, вы должны четко понимать, где он будет использоваться, так как, во-первых, цена сертификата напрямую зависит от количества функций, которые он может выполнять, во-вторых, чтобы быть уверенным, что сертификат будет пригоден для достижения ваших целей. Обычно цели использования электронной подписи указываются при заказе сертификата.

На практике бывают ситуации, когда применение сертификата зависит от стороны, принимающей документ. Например, некоторые операторы электронного документооборота принимают сертификаты, выданные только их удостоверяющим центром. Всегда важно убедиться, что нет никаких ограничений на использование вашего сертификата в той или иной информационной системе.

Обмен электронными документами с ЭП

Межкорпоративный документооборот – обмен электронными документами между компаниями (B2B). Уже сейчас организации и компании могут наладить обмен юридически значимыми электронными документами (ЮЗЭД). Такой обмен имеет существенные преимущества перед бумажной формой:

- Быстрый срок доставки документов (вне зависимости от адреса контрагента): в десятки раз меньше, чем срок доставки бумажных документов.
- Сокращение издержек, связанных с подготовкой и последующей передачей электронных документов между контрагентами: подготовка и передача юридически значимых документов в электронной форме по стоимости меньше передачи документов в бумажной форме.
- Из данных преимуществ следуют реальные экономические выгоды:
- Быстрый обмен документами позволяет ускорить бизнес-процессы компаний (например, по заключению и актированию сделок), что в свою очередь увеличивает скорость оборота денежных средств, т. е. позволяет больше заработать за тот же самый период времени.
- Сокращение издержек на подготовку и передачу документов экономит денежные средства, которые можно направить на решение других задач.
- Быстрый обмен электронными документами и гарантия их доставки позволяют вовремя подавать отчетность в налоговые органы и НДС к вычету, что также позволяет оставлять денежные средства в обороте.
- Электронная форма документов облегчает процедуру обработки документов и позволяет ее существенно автоматизировать, что положительно влияет на скорость обработки документов в целом.
- Эти преимущества особенно актуальны для компаний с большим объемом внешнего документооборота.

Для межкорпоративного обмена, согласно действующему законодательству, например, можно использовать следующие виды документов:

- письма (требующие юридической значимости);
- договоры;
- счета;
- товарные накладные;
- товарно-транспортные накладные;
- акты выполненных работ и оказания услуг;
- акты сверки взаиморасчетов;
- счета-фактуры.

Что нужно для обмена ЮЗЭД

Чтобы наладить межкорпоративный документооборот юридически сильными (или юридически значимыми) электронными документами необходимо решить задачи:

1. Подписание ЭП и отправка электронных документов контрагентам.
2. Приём и проверка подписи на электронных документах от контрагентов.
3. Создание, хранение (в том числе архивное), поиск и обработка подписанных электронных документов.
4. Обеспечение юридической значимости документов в процессе архивного хранения.

Первые две задачи отлично решают **сервисы межкорпоративного обмена** под управлением операторов электронного документооборота. При выборе сервиса необходимо обратить внимание на следующие факторы:

- наличие необходимых лицензий у оператора сервиса обмена;
- возможности интеграции сервиса обмена с вашими корпоративными информационными системами;
- предлагаемые варианты тарификации передачи электронных документов.

Для решения двух других задач идеально подходят системы электронного документооборота, т.к. там уже есть необходимый функционал проверенный временем, например, система DIRECTUM. В случае, если документы изначально создаются и обрабатываются в учётной системе, то системы электронного документооборота могут быть интегрированы с ними для приёма-передачи необходимых данных.

При отсутствии СЭД вышеуказанные задачи могут быть отчасти решены либо решениями от оператора сервиса обмена и интегрироваться с бухгалтерскими программами или ERP-системами с выполнением дополнительных условий. Следует обратить внимание на следующие факторы:

- используемые на текущий момент в компании корпоративные информационные системы (далее – КИС) и их функциональные возможности применительно к решению задач межкорпоративного документооборота;
- возможности интеграции КИС и сервиса обмена;
- стоимость проекта подключения ваших КИС к сервису обмена;
- комплексное решение всех необходимых задач на базе КИС.

Обязателен ли сервис ЭДО?

Чтобы наладить обмен электронными документами, подключаться к услугам оператора электронного документооборота совсем не обязательно. Выбор решения зависит от соглашения между контрагентами (можно использовать обычную электронную почту), которые приступают к внешнему электронному взаимодействию. При самостоятельной организации межкорпоративного электронного документооборота придется столкнуться с рядом трудностей.

Для подписания документов электронной подписью можно использовать программный продукт КриптоАРМ, который потребуется установить и настроить своими силами. С каждым из ваших контрагентов придется заключить отдельное соглашение о начале электронного взаимодействия с описанием принимаемых правил обмена. После настройки рабочих мест сотрудников и подписания всех необходимых документов, возникнет вопрос хранения электронных документов. И это далеко не все задачи, которые вам придется решать при самостоятельной организации межкорпоративного электронного обмена, также останутся открытыми вопросы безопасности и конфиденциальности передаваемых данных.

К тому же согласно требованиям Приказа Минфина от 20.04.2011 № 50н выставление и получение счетов-фактур в электронном виде по телекоммуникационным каналам связи осуществляется через организации, обеспечивающие обмен открытой и конфиденциальной информацией по телекоммуникационным каналам связи, т. е. через оператора электронного документооборота. Сдача отчетности в государственные органы происходит только с использованием услуг специализированного оператора связи.

Все эти вопросы можно легко и быстро решить, воспользовавшись *услугами оператора электронного документооборота*. Решать вам, какой способ для вас будет более эффективным при организации обмена электронными документами с контрагентами.

Юридическая сила электронного документа

Государственный стандарт РФ ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения» даёт следующее определение юридической силы документа (юридической значимости документа): *«юридическая сила документа: Свойство официального документа, сообщаемое ему действующим законодательством, компетенцией издавшего его органа и установленным порядком оформления»*.

Юридическую силу электронному документу, равно как и бумажному, придает обязательное наличие определенных реквизитов:

- название вида документа (за исключением писем);
- номер документа;
- название организации или имя автора документа;
- дата документа;
- место разработки, издания, принятия или подписания;
- подпись.

Конечно, когда мы говорим о подписи, имеем в виду электронную подпись. Именно она является гарантом целостности и подлинности документа. Кроме того, существуют нюансы обеспечения юридической силы формализованных и неформализованных документов. Так, неформализованные документы, подписанные квалифицированной ЭП, уже являются легитимными. Формализованные электронные документы приобретают легитимность в том случае, если они подписаны квалифицированной ЭП и вы, как налогоплательщик, присоединены к регламенту обмена.

Кроме того, другим важным фактором в обеспечении юридической силы документа является право автора создавать и подписывать документы.

Хранение электронных документов

Срок действия сертификата электронной подписи составляет один год, а, например, бухгалтерские документы, необходимо хранить пять лет. Но даже после истечения срока действия сертификата, документ не потеряет юридической силы, так как в момент подписания ставится штамп времени.

Штамп времени – это аналог даты на подписываемом документе. Он подтверждает, что сертификат электронной подписи был действителен на момент подписания документа. Так, в момент подписания документа проставляется штамп времени и результат проверки сертификата.

Подтвердить тот факт, что на момент подписания сертификат был действующим, можно также, обратившись к списку отозванных сертификатов на сайте удостоверяющего центра.

Непосредственно хранение электронных документов можно организовать, по крайней мере, двумя способами:

- локальное хранение (документы хранятся на локальных серверах вашей компании, например, в СЭД);
- хранение в облаке (документы хранятся на серверах компании, услугами которой вы воспользовались).

Услуги электронного архивирования, например, предлагают операторы ЭДО.

Использование документов в судебной практике

Согласно п. 3 ст. 75 Арбитражного процессуального кодекса РФ (АПК РФ), документы, полученные с использованием информационно-телекоммуникационной сети Интернет и подписанные электронной подписью, допускаются в качестве письменных доказательств в арбитражных спорах.

На сегодняшний день суд принимает в электронном виде заявления, ходатайства и отзывы. Подать исковое заявление можно через единую систему «Мой арбитр», на официальном сайте арбитражного суда, где будет рассматриваться дело, или на сайте Высшего Арбитражного Суда РФ. При этом отправлять какие-либо документы на рассмотрение в суд могут только те лица, которые зарегистрированы в системе «Электронный страж», где у каждого пользователя свой личный кабинет.

Важно соблюдать технические требования к отправляемым документам: черно-белое изображение, формат .PDF, не менее 200 точек на дюйм, наличие графической подписи ответственного лица, печати и других реквизитов. Один документ – один файл, в названии которого отражено содержание и количество страниц.

В электронном виде не принимаются такие документы, как заявление об обеспечении иска, об обеспечении имущественных интересов, ходатайство о приостановлении исполнения судебных актов.

Источник: Электронное правосудие: новые стандарты открытости и доступности правосудия на примере Федерального арбитражного суда Поволжского округа

Если технические средства суда не позволяют использовать в качестве доказательств электронные документы, достаточно будет сделать их копии в бумажном виде. Распечатанный документ следует заверить печатью организации и подписью уполномоченного лица (или руководителя организации).

Пожалуй, самым известным примером того, что суды признают легитимность электронных документов, является постановление суда Волго-Вятского округа по делу № А43-5226/2010. Истец настаивал на взыскании задолженности с ответчика за неоплаченный товар. Ответчик же считал недействительными электронные документы, подписанные ЭП. Однако между сторонами было заключено дополнительное соглашение к договору, в котором явно прописана возможность применения электронного документооборота с использованием ЭП. Суд установил, что первичные документы составлены в соответствии с нормами и подписаны уполномоченным лицом. Нужно ли уточнять, кто выиграл дело?

Нормативно-правовое поле использования электронной подписи

Основные нормативно-правовые акты (далее – НПА), регулирующие межкорпоративный обмен электронными документами:

1. Гражданский кодекс РФ регулирует использование электронных документов и электронной подписи при совершении сделок и заключении договоров (ст. 160, 434, 847 ГК РФ).

2. Федеральный закон № 63-ФЗ «Об электронной подписи» от 06.04.2011 регулирует 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.

3. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 дает понятие электронного документа и смежных с ним областей, а также регулирует отношения, возникающие при обеспечении защиты информации, применении информационных технологий, осуществлении права на поиск, получение, передачу, производство и распространение информации.

4. Федеральный закон № 402-ФЗ «О бухгалтерском учете» от 06.12.2011 устанавливает единые требования к бухгалтерскому учету, а также разрешает составление первичных учетных документов в электронном виде и регулирует их использование.

5. Налоговый кодекс РФ определяет возможность использования электронных счетов-фактур (ст. 169, счёт-фактура).

6. Приказ Минфина 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» определяет порядок обмена электронными юридически значимыми счетами-фактурами.

Представленное выше законодательство составляет основу обмена электронными документами между организациями. Для того чтобы начать обмен необходимо подключиться к оператору электронного документооборота или заключить с контрагентами соглашения об обмене электронными документами напрямую.

Подробнее: https://ecm-journal.ru/e-sign