Содержание:

Введение

Информационные технологии, бурное развитие которых началось в 90-е годы, коренным образом изменили нашу жизнь. Темпы информатизации российского общества одни из самых высоких в мире. Уже сегодня большая часть оборота информации и документов осуществляется в электронном виде. Технология же электронной подписи способна еще более расширить возможности электронного документооборота, распространить его на все сферы общественной жизни. Технологии электронной цифровой подписи постепенно завоевывают признание во всем мире. Вместе с тем развитие возможностей электронной коммерции благоприятным образом скажется в целом на рынке российских информационных технологий, т.к. все проекты электронной коммерции, такие как Интернет-торговля, Интернет-банкинг, Интернет-провайдинг, являются крупными потребителями прикладного программного обеспечения, а его разработка создаст целую отрасль специализированных программно-технологических предприятий в России.

Все сказанное характеризует актуальность темы работы.

Цель работы - изучение электронной цифровой подписи как инструмента для придания юридической силы электронным документам.

Исходя из поставленной цели, можно выделить следующий круг задач:

- Рассмотреть правовое регулирование отношений в области использования электронной цифровой подписи;
- Раскрыть понятие и сущность электронной цифровой подписи как основного реквизита электронного документа. Условия использования электронной цифровой подписи;
- Охарактеризовать электронный документ;
- Рассмотреть особенности использования электронной цифровой подписи.

Основная часть

Электронная подпись 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 цифровой подписи и позволяет идентифицировать владельца сертификата ключа подписи, установить отсутствие искажения информации в электронном документе.

Электронная подпись (ЭП) – это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ

Электронная подпись используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью.

Удостоверяющий центр (Центр сертификации) (англ. Certification authority, CA) — организация, выпускающая сертификаты ключей электронной цифровой подписи.

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.

Электронный документ – это любой документ, созданный при помощи компьютерных технологий и хранящийся на носителях информации, обрабатываемых при помощи компьютерной техники, будь то письмо, контракт или финансовый документ, схема, чертеж, рисунок или фотография.

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 невозможно – 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.

С использованием ЭП работа по схеме "разработка проекта в электронном виде - создание бумажной копии для подписи - пересылка бумажной копии с подписью - рассмотрение бумажной копии - перенос ее в электронном виде на компьютер" уходит в прошлое.

Электронные подписи разделяются законом 2011 г. на три вида.

- Простые подписи создаются с помощью кодов, паролей и других инструментов, которые позволяют идентифицировать автора документа, но не позволяют проверить его на предмет наличия изменений с момента подписания.
- Усиленная неквалифицированная подпись создана с использованием криптографических средств и позволяет определить не только автора документа, но проверить его на наличие изменений. Для создания таких

подписей может использоваться сертификат неаккредитованного центра, можно также вообще обойтись без сертификата, если технические средства позволяют выполнить требования закона.

- Усиленная квалифицированная подпись является разновидностью усиленных, она имеет сертификат от аккредитованного центра и создана с помощью подтвержденных ФСБ средств.

Простые и неквалифицированные подписи заменяют подписанный бумажный документ в случаях, оговоренных законом или по согласию сторон. Например, простые подписи могут использовать граждане для отправки сообщений органам власти. Усиленная подпись также может рассматриваться как аналог документа с печатью.

Квалифицированные подписи заменяют бумажные документы во всех случаях, за исключением тех, когда закон требует наличие исключительно документа на бумаге. Например, с помощью таких подписей граждане могут получать госуслуги в электронном виде, а органы государственной власти могут отправлять сообщения гражданам и взаимодействовать друг с другом через информационные системы. Ранее выданные сертификаты ЭЦП и подписанные с их помощью документы приравниваются к квалифицированным подписям.

Иностранные электронные подписи приравниваются в России к тем видам подписей, которым они соответствуют.

Простая электронная подпись, в отличие от прежней электронно-цифровой подписи, не предназначена для защиты документа от подделки. Она не позволяет обнаружить возможное искажение содержания документа. Единственная ее функция – подтверждение факта формирования электронной подписи (а не самого документа!) определенным лицом.

Целям определения лица, подписавшего электронный документ, а также обнаружения факта внесения изменений в документ после его подписания служит усиленная электронная подпись. Именно эта подпись (в двух видах — неквалифицированная и квалифицированная) является аналогом прежней электронной цифровой подписи.

Поскольку простая электронная подпись требует использования кодов, паролей или иных средств, станет ясно, что можно считать электронной подписью, а что нет. Очевидно, что в случае электронного письма роль электронной подписи не может играть имя отправителя, вручную поставленное после текста, так как оно никак не зависит от пароля, используя который отправитель сформировал и отправил письмо. Информацией, указывающей на лицо, от имени которого был послан документ, может служить, вероятно, идентификатор сообщения в сочетании с IP-адресом компьютера отправителя, свидетельствующие о том, что сообщение было создано в результате доступа к почтовой системе, сопровождавшегося вводом пароля, принадлежащего определенному пользователю. Электронный адрес отправителя и имя отправителя можно считать подписью лишь в том случае, если оператор информационной системы обеспечивает их достоверность, ведь почтовый протокол позволяет указывать любое имя и любой обратный адрес, и некоторые почтовые системы не накладывают здесь никаких ограничений.

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.

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.
- Быстрый обмен документами позволяет ускорить бизнес-процессы компаний.
- 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.

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.

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

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи,
- подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе,
- создание закрытых и открытых ключей электронных цифровых подписей.

В основе электронной подписи лежит криптография открытого ключа. С ее помощью формируется специальный сертификат пользователя. Он содержит данные о пользователе, открытый ключ и электронную подпись сертификата, ее

можно проверить с помощью открытого ключа удостоверяющего центра. Алгоритм гарантирует, что произвести генерацию подписи может только удостоверяющий центр, который имеет секретный ключ шифрования и доверие, к которому является основой для работы всей системы ЭЦП.

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, 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 ЭЦП, но и валидность всей цепочки сертификатов, задействованных при изготовлении сертификата подписанта, на момент подписания им конкретного электронного документа.

В России сейчас создается система PKI, которая доступна практически всем желающим. Изначально она была создана агентством Росинформтехнологии на базе Общероссийского государственного информационного центра (ОГИЦ). Однако сейчас федеральный удостоверяющий центр передан в ведение «Ростелекома». Этот телекоммуникационный оператор активно предлагает развивать различные проекты с использованием PKI.

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Область применения ЭЦП определяется идентификатором, называемым OID. У каждой области действия свой OID. Например, область применения, которая позволяет подписывать документы для постановки объектов на ГКН, имеет OID 1.2.643.5.1.24.2.1.3.1 «Формирование кадастровым инженером документов для получения услуг со стороны заявителя». ЭЦП с таким OID выдается только кадастровым инженерам, которые для получения предъявляют Аттестат кадастрового инженера.

Область применения, которая позволяет органу кадастрового учёта подтверждать документы – результаты кадастрового учета имеет OID - 1.2.643.5.1.24.2.1.2 «Формирование документов как результата оказания услуги со стороны органов кадастрового учета». ЭЦП с такими OID нами не выдается. И не может быть выдан без специальной аккредитации.

Особенности использования электронной цифровой подписи:

- Никто, кроме владельца секретного ключа, не сможет создать такой шифротекст.
- Общая схема электронной подписи Схема электронной подписи обычно включает в себя: 1 Алгоритм генерации ключевых пар пользователя; 2 Функцию вычисления подписи; 3 Функцию проверки подписи.
- Законодатель не говорит и о том, какая категория документов может подтверждаться ЭЦП, а следовательно, полагаем, что речь может идти о любых документах, хранимых, обрабатываемых и передаваемых с помощью информационных и телекоммуникационных систем, за исключением тех, которые в соответствии с законодательством могут существовать только в бумажном виде.
- Применение электронной цифровой подписи.
- При этом Федеральный закон не касается вопросов заключения и действительности договоров, которые относятся к предмету регулирования Гражданского кодекса.
- Федеральное агентство по информационным технологиям осуществляет данную деятельность в соответствии с правилами, установленными в отношении деятельности удостоверяющих центров Использование электронного документооборота, в том числе и электронной цифровой подписи, в отношениях между двумя или несколькими договорившимися хозяйствующими субъектами имело свое место значительно раньше принятия данного Федерального закона.

Заключение

Итак, развитие и широкое применение информационных и коммуникационных технологий является глобальной тенденцией мирового развития и научно-технической революции последних десятилетий.

Сегодня субъекты предпринимательской деятельности взаимодействуют посредством электронного документооборота как между собой, так и с конечными потребителями и органами власти.

Принципиально важным для стабилизации и безопасности электронного документооборота является, с одной стороны, прямое закрепление в нормах права презумпции авторства, в соответствии с которой электронная цифровая подпись в электронном документе признается созданной владельцем сертификата ее открытого ключа, если владелец сертификата ключа подписи не докажет обратное, с другой стороны, установление обязанности удостоверяющих центров непосредственно проверить соответствие данных, изложенных в заявлении на изготовление сертификата ключа электронной цифровой подписи, предоставленным документам.

Особое внимание в работе уделено исследованию правового регулирования использования такого электронного аналога собственноручной подписи, как электронная цифровая подпись (ЭЦП). Это объясняется предпринятой в действующих нормах права попыткой законодательного закрепления равенства собственноручной и электронной цифровой подписи при условии соблюдения требований закона

ЭЦП позволяет подтвердить ее принадлежность зарегистрированному владельцу. ЭЦП является неотъемлемой частью электронного документа.

Используемая литература

1. «Электронный документ» А. Марченко.
2. «Законодательное регулирование правового статуса ЭЦП. Основные положения» Ткачев А.В
3. «Юридический справочник руководителя»2008 г.

Интернет-источники:

1. /wiki/ЭЦП
2. /cer-ecp.html
3. /sed/eds.php
4. /about.html
5. /nashi-usl0/elektronn21/