А. М. Грецкая[1]
Российский государственный
профессионально-педагогический университет

УДК [005.92:004.056.5:004.738.5]:340.13

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ И ОБЛАЧНЫЕ ТЕХНОЛОГИИ: ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ

Аннотация. В статье рассмотрены особенности облачной электронной подписи и вытекающие из них проблемы использования. Проанализирована нормативная регламентация электронной подписи в России.

Ключевые слова: электронная цифровая подпись, облачный сервис, удостоверяющий центр, ключ защиты информации.

Тенденция нескольких последних лет говорит о том, что многие сервисы переходят из традиционных установок к облачным. Не стало исключением и электронная цифровая подпись (далее – ЭЦП). Однако миграция ЭЦП в «облака» воспринимается пользователями и экспертами пока неоднозначно. Так как стоит вопрос об обеспечении информационной безопасности новых облачных технологий. Однако, ни технологии, ни законодательство не стоят на месте, и вскоре можно ожидать нового витка развития электронной подписи с участием облачных вычислений.

Проблема развития облачной подписи в России заключается в отсутствии чёткой нормативно-правовой базы, регулирующей этот вопрос. На уровне федерального законодательства существует ряд понятий, определяющих электронную цифровую подпись и электронный документооборот, а также оборот данных и защиту информации. Отдельно рассмотрен регламент использования ЭЦП в статьях Гражданского кодекса РФ.

Основной закон об электронной подписи – ФЗ № 63 «Об электронной подписи» от 06.04.2011. А в ФЗ № 149 «Об информации, информационных технологиях и о защите информации» от 27.07.2006 конкретизируется термин электронного документа и связанных с ним сегментов.

Так, подпись на облачном носителе – это вычислительная система, предоставляющая через сеть доступ к возможностям создания, проверки электронной подписи и интеграции этих функций в бизнес-процессы других систем [ФЗ № 63 от 06.04.2011].

Кроме этого, дополнительно разработаны правовые акты, регулирующие работу электронного документооборота и предусматривающие требования к документам. Также при работе со стандартной электронной подписью учитывают и требования Арбитражного процессуального кодекса РФ, который определяет юридическую силу квалифицированной подписи и приравнивает её к собственноручной. Однако нет единого

[1] Научный руководитель: М. Б. Ларионова, кандидат исторических наук, доцент РГППУ.

стандарта, где были бы описаны процессы и правила использования облачных технологий для хранения данных об электронной цифровой подписи.

Таким образом, пока нормативная база по применению облачных технологий в области применения электронной подписи в России не сформирована, то с 01.01.2022 г. в силу вступили поправки к ФЗ № 63 «Об электронной подписи» от 06.04.2011, которыми вводятся новые правила получения и работы с электронной подписью в организациях, у индивидуальных предпринимателей и нотариусов. Именно эти поправки запрещают всем организациям, удостоверяющим центрам (далее – УЦ) выпускать электронные подписи на облачном носителе. Теперь подпись можно получить только на физическом носителе лично в налоговой, либо в некоторых УЦ, получивших аккредитацию и лицензию на право выпуска электронных подписей [Казаков, 2021].

В открытых источниках нет информации о причинах изменений в законодательстве. Поэтому, чтобы понять, в чём заключаются причины, следует разобраться в проблемах использования облачной ЭЦП.

Итак, подпись в «облаке» – это молодая технология, которая совсем недавно появилась в России. Все операции с электронными подписями выполняются на удалённом сервере, и ключи сертификатов тоже хранятся удалённо. При этом облачные подписи никак не упоминалась в законах, в частности, в ФЗ № 63 «Об электронной подписи» от 06.04.2011 [ФЗ № 63 от 06.04.2011]. На практике она приравнивалась к обычной электронной подписи, которая хранится на ключевом носителе, однако юридический статус облачных подписей не был закреплен.

Основной проблемой при переводе любой IT-системы «в облако» становится информационная безопасность, связанная с передачей в облачный сервис информации для обработки или хранения. Если раньше эта информация не покидала некоторого защищённого периметра, а именно физического носителя, флеш-накопителя, на которой хранилась информация о подписи, то можно было сравнительно легко обеспечить её конфиденциальность. В «облаке» же само понятие периметра отсутствует. При этом ответственность за обеспечение конфиденциальности информации в каком-то смысле «размывается» между её владельцем и поставщиком облачных услуг.

ЭЦП защищает электронный документ от подделки и копирования, а также содержит ключевую информацию о сертификате электронной цифровой подписи, реквизиты владельца сертификата и УЦ. То есть это ключ электронной подписи, который содержит конфиденциальную информацию, позволяющую идентифицировать её пользователя и защитить подпись [Соловяненко, 2020, с. 173–176].

Но здесь нужно понимать, что в случае облачной электронной подписи закрытая часть ключа, которая является конфиденциальной и должна принадлежать только пользователю, будет находиться на сервере УЦ. Поэтому всё зависит от требований компании к безопасности и от политики, связанной с подписанием документов. Если важно, чтобы документы подписывали сами

владельцы закрытых ключей, то облачная электронная подпись не подойдет. И в данной ситуации нужно решать вопрос о доверии к УЦ и серверам, на которых хранятся закрытые ключи.

Также можно использовать облачную подпись только в тех сервисах, с которыми есть интеграция программного обеспечения УЦ. Это связано с тем, что в случае облачной подписи закрытый ключ хранится на сервере УЦ. Для того, чтобы нужный сервис мог использовать такой закрытый ключ подписи для подписания, то нужно уметь отправлять запрос на формирование электронной подписи на сервер УЦ. На данный момент сервисов много, и все они не смогут предусмотреть интеграцию с программным обеспечением УЦ [Смирнов, 2020, с. 79–82]. Получается, что облачную подпись придётся использовать только с определенными сервисами. Для работы с другими сервисами придется покупать другой сертификат электронной подписи, и нет гарантий, что эти сервисы будут поддерживать какую-либо облачную электронную подпись.

Например, в банках есть множество сервисов, где применялись разные облачные электронные подписи. Для сервиса по отправке отчётности, деклараций в налоговую применяется одна подпись, выпущенная, например, в УЦ «Астрал». А для подачи документов в налоговую на регистрацию или регистрацию ликвидации организации, нужна другая подпись, которая подходит именно для этого сервиса [Дарькина, 2020, с. 30–33].

Таким образом, есть следующие риски в использовании облачной электронной подписи:

– риск взлома удаленного сервера и последующей кражи закрытых ключей ЭЦП;

– удаленный сервер, на котором будут храниться ЭЦП, может оказаться недоступным по техническим причинам. Владелец электронной подписи воспользоваться ею при этом не сможет. А это может привести, к примеру, к потере выгодного контракта или к штрафу за несвоевременную подачу финансовой отчетности со стороны ФНС;

– с юридической точки зрения владельцем закрытого ключа ЭЦП будет являться удостоверяющий центр, а не сам получатель сертификата [Клименко, 2019, с. 188–191].

Так как облачные технологии представляют собой перспективы в развитии электронного документооборота и имеют также и свои преимущества, например, затраты времени и денег на выпуск подписи, то при всех проблемах использования сертификата электронной подписи, ясно, что нормативную регламентацию по использованию облачных технологий в области электронной подписи нужно дорабатывать.

Список источников и литературы:

Дарькина М. М. Практика использования электронной цифровой подписи в предпринимательской деятельности // Право и цифровая экономика. 2020. № 3 (9). С. 28–35.

Клименко К. В., Власенко А. В., Егорихин Ю. Е. Проблемы использования облачных технологий в процессе выпуска электронных подписей удостоверяющим центром // Каспий в эпоху цифровой экономики: материалы Международного научно-практического форума, Астрахань, 24–25 мая 2019 г. Астрахань: Астрахан. ун-т, 2019. С. 188–191.

Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ (последняя редакция) // Российская газета. 2011. 8 апр. (№ 75).

Смирнов П. В., Смышляев С. В. Обеспечение безопасности систем дистанционного формирования электронной подписи в условиях слабодоверенного окружения // International Journal of Open Information Technologies. 2020. Vol. 8, iss. 12. P. 77–84. URL: https://cyberleninka.ru/article/n/obespechenie-bezopasnosti-sistem-distantsionnogo-formirovaniya-elektronnoy-podpisi-v-usloviyah-slabodoverennogo-okruzheniya (дата обращения: 20.01.2022).

Соловяненко Н. И. Юридическое значение электронной подписи в правовых отношениях электронного бизнеса // Colloquium-journal. 2020. № 8 (60), ч. 7. С. 55–58.

Казаков С. Электронная подпись: что изменится с 1 июля 2021 г. и позже // Контур: электронный журнал. 2021. 19 апр. URL: https://kontur.ru/articles/5728 (дата обращения: 20.01.2022).

А. К. Гуторова[1]
Российский государственный
профессионально-педагогический университет

УДК 005.92:004.056.55

ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Аннотация. В статье рассматривается сущность электронной подписи, проблемы применения электронной подписи и защиты информации, а также разбирается возможность использования электронной подписи для придания документу целостности и аутентичности.

Ключевые слова: электронная подпись, электронный документ, конфиденциальность, персональные данные, средства защиты, информационные технологии, идентификация, целостность и аутентичность документа.

Любой документ, издаваемый в организации, должен быть подписан уполномоченным на это лицом, чтобы придать ему юридическую силу и обеспечить правовую значимость. Современные информационные технологии, которые тесно вошли в нашу жизнь, поспособствовали переходу документооборота из бумажного в электронный формат, что в свою очередь привело к упрощению обмена документами, как внутри организации, так и за ее пределами. В итоге появились

[1] Научный руководитель: М. Б. Ларионова, кандидат исторических наук, доцент РГППУ.