

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В РОССИИ

Стеблецов Борис Алексеевич

Студент ФГБОУ ВО «Армавирский государственный педагогический университет», г. Армавир

Научный руководитель, к.т.н, доцент кафедры информатики и ИТО Андрусенко Е.Ю.

INFORMATION TECHNOLOGIES IN EDUCATION OF CHILDREN

Stebletsov Boris Alekseevich

Student of Armavir state pedagogical University, Armavir

АННОТАЦИЯ

В статье рассмотрено явление электронной цифровой подписи в Российской Федерации и возможности её введения в высших учебных заведениях страны.

ABSTRACT

The article considers the phenomenon of electronic digital signature in the Russian Federation and the possibility of its introduction in higher educational institutions of the country.

Ключевые слова: электронная подпись; информационные технологии; цифровая подпись; документация; нормативные акты.

Keywords: electronic signature; information technology; digital signature; documentation; regulations.

Термины и сокращения

Цифровая подпись или **электронная подпись** - электронная цифровая подпись, а именно метод шифрования текста, позволяющий идентифицировать происхождение текста и защитить его от несанкционированных изменений.

ЭЦП – электронная цифровая подпись.

Введение

С появлением глобальных информационных технологий электронные документы все чаще используются в российской деловой практике. Индивидуальные предприниматели и организации заключают сделки путем обмена электронными письмами, частные пользователи подписываются на услуги в сети интернет по договорам, которые они заключают в электронном виде; в банках работают системы телебанкинга клиентов, а бизнес осуществляет платежи через электронные платежные системы. Этих примеров не хватит, чтобы исчерпать весь перечень возможных видов применения электронной документации. Вследствие этого возникает необходимость определения правового статуса электронных документов в системе российского права.

Нормы права

Гражданский кодекс Российской Федерации (ГК РФ) неоднократно обращается к документам в цифровом формате. Договор считается заключенным в письменной форме, если он совершен путем обмена документами по почте, телеграфу, телефону, электронным или иным средствам связи, позволяющим удостовериться в том, что документ исходит от стороны договора. Ценные бумаги могут выпускаться в бездокументарном виде, то есть с применением электронных и компьютерных технологий. Применение ЭЦП или иных заменителей личных подписей в сделках допускается, если их использование предусмотрено либо законодательством, например Гражданским кодексом, либо иными законами, например Федеральным законом об ЭЦП, Федеральным законом о кредитных историях и иными нормативными правовыми актами, а так же соглашением сторон. Договором банка с клиентом может быть предусмотрено, что полномочия

клиента по контролю за денежными средствами на его счете и любыми электронными деньгами могут быть подтверждены другими документами с использованием заменителей собственноручных подписей клиента, такими как пин-коды, пароли и другие средства предоставления доказательств того, что согласие клиента было дано авторизованным лицом.

Сертификация электронной подписи

Сертификат обязан включать в себя, в частности, срок его действия, наименование центра выдачи, полное имя или псевдоним собственника сертификата, открытую часть ключа, иные сведения, которые может запросить собственник сертификата, а также сведения о сделках, в которых документы, подписанные электронным способом, будут иметь юридическую силу. Последнее положение представляется не совсем ясным. В законе прямо указано, что он применяется к отношениям, возникающим «при совершении сделок по гражданскому праву и в иных случаях, предусмотренных законодательством Российской Федерации». Это положение закона, по-видимому, может применяться к тем видам сделок по гражданскому праву, которые предусмотрены Гражданским кодексом. Но ссылка на «иные дела» открывает широкий круг отношений, включая различные области применения публичного и частного права.

Существенное отличие закона Об электронной подписи от ряда его зарубежных аналогов заключается в попытке разделить все информационные системы на корпоративные и системы общего пользования и установить для каждой системы различный правовой режим.

Вне корпоративной информационной системы открытый и закрытый ключи изготавливаются пользователем или центром сертификации по запросу пользователя. Если корпоративная система предоставляет услуги

сертификационного центра для пользователей систем общего пользования, она должна соответствовать предъявленным к ним требованиям. Практическая значимость этого разделения, таким образом, невелика, поскольку закон не предусматривает широкого использования корпоративных систем.

Все операции с применением ЭЦП проводятся с применением специальных аппаратных и программных средств, которые закон определяет как “средства электронной цифровой подписи” (“технология электронной подписи”).

Законодательство придает большое значение обязательной сертификации технологии ЭЦП. Закон гласит, например, что для формирования ключей цифровой подписи должна использоваться только сертифицированная технология. Общегосударственные и муниципальные органы власти не могут использовать в своих корпоративных информационных системах ни несертифицированную технологию, ни ключи, генерируемые такой технологией. Поэтому единственным типом информационных систем, в которых может использоваться технология несертифицированной электронной подписи, являются неофициальные корпоративные системы. С другой стороны, в законе прямо говорится, что электронная подпись может быть признана эквивалентной собственноручной подписи только в том случае, если для ее создания была использована сертифицированная технология.

Сертификация технологии электронной подписи в России является длительным процессом и может потребовать, в частности, декомпиляции сертифицируемого программного обеспечения. В то же время пользователи часто используют технологию ЭЦП иностранного производства, сертификация которой нецелесообразна ни экономически, ни организационно. Поэтому следует признать, что законодательно

требуемая сертификация технологии электронной подписи существенно ограничивает возможности пользователей, предлагаемые агентам электронного документооборота, и является серьезным препятствием для более широкого использования электронных подписей в российской деловой практике.

Хотя лицензирование этой деятельности было отменено, правительство сохранило за собой полномочия по регулированию деятельности в сфере защиты информации. Например, деятельность, связанная с распространением и обслуживанием средств шифрования, шифровальных услуг, технической защиты информации, а также разработка и производство средств защиты информации остаются предметом лицензирования.

Иностранные сертификаты

Зарубежные аналоги ЭЦП могут использоваться на территории Российской Федерации только при соблюдении всех норм установленных законодательством нашего государства. Регулирование таких аналогов осуществляется на государственном уровне, путём внесения и удаления таковых из специализированного реестра. Иностранные сертификаты зачастую имеют временную силу. В конце определенного периода, если не было произведено продление сертификата на территории Российской Федерации, то в соответствии с текущим законодательством с момента прекращения поддержки данных сертификатов перестают иметь юридическую силу все подписанные позже этого срока документы с данной ЭЦП.

Эксплуатация ЭЦП

На практике технические средства, генерирующие цифровые подписи, эксплуатируются не должностными лицами компаний, уполномоченными их уставом подписывать документы, а другими

сотрудниками компаний. При увольнении таких уполномоченных сотрудников необходимо соблюдать всю процедуру получения новых сертификатов электронной цифровой подписи. Существует риск введения в заблуждение корпораций их погашенными подписантами, которые могут рассылать электронные документы, подписанные в электронном виде, после того как они перестали работать в корпорациях.

Кроме того, в отношениях часто возникает следующая практика: собственником цифровой подписи выступает юридическое лицо, а ее пользователями-уполномоченными физические лица. В подобном случае владелец цифровой подписи (руководитель юридического лица) предоставляет контрагенту юридического лица (например, его банку) список уполномоченных цифровых подписей на электронные документы. Эта практика широко распространена, хотя и не разрешена законодательно.

Вывод

Подводя итог, следует отметить, что действующее в России законодательство предусматривает возможность использования электронных документов и возможность использования цифровой подписи в качестве необходимого идентификатора. С другой стороны, существуют определенные недостатки, которые затрудняют использование электронного документооборота в деловой практике. К таким недостаткам относятся, в частности, требование использования только сертифицированной технологии электронной подписи, невозможность использования цифровых подписей для идентификации юридических лиц, требование использования бумажных копий в процедурах выдачи сертификатов ключей электронной подписи, а также отсутствие положений об ответственности удостоверяющих центров".

В результате этих недостатков практика использования технологии цифровой подписи негосударственными корпоративными структурами редко основывается на соблюдении требований закона Об электронной подписи. В этом случае агентам электронного документооборота отказано в государственной поддержке в применении и защите их электронных документов, в частности, они рискуют получить отказ со стороны государственных органов и судов в признании действительности их электронных документов. Таким образом, можно сделать вывод, что закон Об электронной подписи не полностью защищает интересы пользователей негосударственных корпоративных информационных систем.

Однако, все более важную роль технологии цифровой подписи в отношениях, регулируемых публичным правом. Приняты новые законы, в которых законодатели используют понятия электронного документа и электронной подписи. Например, Федеральный закон "О кредитных историях" отводит значительную роль электронному документообороту в функциях кредитных бюро. Информация предоставляется кредитным бюро, субъектам кредитной истории и пользователям кредитной информации в форме электронного документа, юридическая сила которого удостоверяется электронными цифровыми подписями в соответствии с законодательством Российской Федерации или различными заменителями собственноручных подписей. Кроме того, с начала 2005 года российскими таможенными органами реализуется программа внедрения электронного декларирования.

Таким образом, следует отметить, что в области регулирования, где государство может поручить соблюдение положений Закона Об электронной подписи, в частности соблюдение требования об использовании сертифицированной технологии цифровой подписи,

существуют хорошие перспективы для дальнейшего использования и развития инструментов цифровой подписи.

С другой стороны, государственное регулирование не лишено странных несоответствий. Известно, что были приняты типовые правила внутренней структурной организации федеральных органов исполнительной власти, а также типовая политика взаимодействия федеральных органов исполнительной власти. Эти модели устанавливали порядок рассмотрения заявлений от представителей широкой общественности только в печатном виде. Таким образом, было создано еще одно досадное препятствие для ограничения внедрения безбумажного документооборота в деятельность органов государственной власти, которое, как мы надеемся, будет преодолено в ближайшее время.

Список литературы:

1. А.С. Кузьмин, В.Г. Антипкин, С.В. Гребнев, Д.В. Матюхин, Н.Н. Мурашов, А.Ю. Нестеренко, А.В. Уривский, А.В. Лунин, И.А. СериковГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»// [Электронный ресурс] - URL:<https://tc26.ru/standarts/mezhgosudarstvennye-dokumenty-po-standartizatsii/gost-34-10-.html>(дата обращения: декабрь 2020).
2. Б. А. Фороузан. Схема цифровой подписи Эль-Гамала // Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин. — Курс лекций.[Электронный ресурс]- URL: <https://intuit.ru/>(дата обращения: ноябрь 2020).
3. СЭД: перспективы развития отрасли: электронная статья [Электронный ресурс]

URL:<https://www.bbsoftware.ru/articles.php?id=92&idCat=4>(дата обращения: декабрь 2020).

4. Анучин М. Электронные документы как альтернатива «бумажному» документообороту // Юрист компании. – 2008. – № 10.

5. Наталья Козлова Как цифровая подпись может оставить собственников без жилья // Российская газета - Федеральный выпуск № 113(7871) [Электронный ресурс] - URL: <https://rg.ru/2019/05/27/kak-cifrovaia-podpis-mozhet-ostavit-sobstvennikov-bez-zhilia.html>(дата обращения: декабрь 2020).

6. Нысанбаева С.Е., Капалова Н.А. Моделирование схемы электронной цифровой подписи в непозиционной полиномиальной системе счисления // Образовательные ресурсы и технологии. – 2014. – № 1 (4). – С. 156-161.

7. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации // Электронная подпись(последнее обновление: 6 марта 2019)

8. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ (последняя редакция)