Основные правовые новеллы в актах ФСБ России, принятые во исполнение федеральных законов от 30.12.2015 № 445 -ФЗ и от 27.12.2019 № 476 -ФЗ

Логачев А.С., к ф.-м. н.
Дробаденко К.В.
Игнатенкова О.А.

Основные изменения Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (с учетом изменений, внесенных федеральными законами от 30.12.2015 № 445-ФЗ и 27.12.2019 № 476-ФЗ) с точки зрения обеспечения информационной безопасности

- Расширены полномочия ФСБ России в части установки ряда требований.
- Определены методы идентификации заявителя при подаче заявления на создание сертификата:
  1) При личном присутствии;
  2) Без личного присутствия с применением:
     - Квалифицированной электронной подписи при наличии действующего квалифицированного сертификата;
     - Предоставления информации, содержащейся в заграничном паспорте нового образца;
     - Предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы;
     - В отношении усиленных неквалифицированных электронных подписей - с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи.
- Квалифицированный сертификат должен содержать идентификатор, однозначно указывающий на то, что идентификация заявителя при выдаче сертификата ключа проверки электронной подписи проводилась либо при его личном присутствии, либо без его личного присутствия.
- Введено понятие доверенной третьей стороны, являющейся юридическим лицом, осуществляющим деятельность по проверке электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ, для обеспечения доверия при обмене данными и электронными документами.

Приказы ФСБ России, утвержденные в соответствии с доработанным Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

1. Приказ ФСБ России от 4 декабря 2020 г. № 554 «Об утверждении Порядка уничтожения ключей электронной подписи, хранимых аккредитованным удостоверяющим центром по поручению владельцев квалифицированных сертификатов электронной подписи».
2. Приказ ФСБ России от 4 декабря 2020 г. № 555 «О внесении изменений в приложения № 1 и 2 к приказу ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».
3. Приказ ФСБ России от 4 декабря 2020 г. № 556 «Об утверждении Требований к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи».
4. Приказ ФСБ России от 29 января 2021 г. № 31 «О внесении изменений в приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».
5. Приказ ФСБ России 20 апреля 2021 г. № 154 «Об утверждении Правил подтверждения владения ключом электронной подписи».
6. Приказ ФСБ России от 1 мая 2021 г. № 171 «Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц».

Основные положения Приказа ФСБ России от 4 декабря 2020 г. № 554 «Об утверждении Порядка уничтожения ключей электронной подписи, хранимых аккредитованным удостоверяющим центром по поручению владельцев квалифицированных сертификатов электронной подписи»:

1. Ключ электронной подписи и резервные копии, содержащие его, уничтожаются удостоверяющим центром не позднее 1-го рабочего дня после истечения срока действия ключа.
2. Уничтожение осуществляется комиссией, назначаемой актом удостоверяющего центра, с применением встроенной функции используемого средства электронной подписи. Факт уничтожения фиксируется в акте.
3. При поступлении от владельца квалифицированного сертификата уведомления об обнаружении неуничтоженного ключа электронной подписи удостоверяющий центр в течение 1-го рабочего дня проверяет его обоснованность. По результатам проверки удостоверяющий центр уничтожает ключ электронной подписи и информирует об этом владельца квалифицированного сертификата, либо сообщает ему о том, что ключ электронной подписи был уничтожен ранее.

Приказом ФСБ России от 20 апреля 2021 г. № 154 «Об утверждении Правил подтверждения владения ключом электронной подписи» определены:

1. Порядок подтверждения лицом, обратившимся за получением сертификата, факта владения ключом электронной подписи, который соответствует ключу проверки, указанному заявителем для получения сертификата.
2. Функции удостоверяющего в ходе указанного подтверждения, в том числе в случае представления заявления на выдачу сертификата с использованием информационно-телекоммуникационных сетей общего пользования, в том числе сети «Интернет».

Приказом ФСБ России от 1 мая 2021 г. № 171 «Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц» определены:

- Организационно-технические требования в области информационной безопасности к доверенным лицам. В соответствии с указанными требованиями должностное лицо должно:

  1) Обеспечить контролируемую зону, а также осуществлять контроль за нахождением и действиями лиц и (или) транспортных средств в зданиях и помещениях, предназначенных для размещения технических средств, обеспечивающих выполнение доверенным лицом своих функций;
  2) Организовать и вести учет машинных носителей информации, используемых средств криптографической защиты информации, включая средства электронной подписи, а также обеспечить их защиту от несанкционированного доступа;
  3) Обеспечить защиту подключения к информационно-телекоммуникационным сетям общего пользования, в том числе к сети «Интернет», технических средств, обеспечивающих выполнение доверенным лицом своих функций;
  4) Применять для выполнения возложенных на доверенное лицо функций информационные системы, аттестованные на соответствие Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17.
  5) Разработать и утвердить перечень локальных актов, регламентирующих меры реализации требований по обеспечению информационной безопасности.

- Типовая схема доставки заявлений о получении квалифицированного сертификата юридического лица в удостоверяющий центр (необходимость утверждения была определена Постановлением Правительства Российской Федерации от 31 декабря 2020 г. № 2409), а также распределение между отдельными работниками доверенного лица раздельных групп обязанностей в целях исключения возможного доступа работников доверенного лица к ключам электронной подписи заявителей при реализации полномочий по их созданию.

Основные положения Приказа ФСБ России от 4 декабря 2020 г. № 556 «Об утверждении Требований к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи»

- Средства доверенной третьей стороны должны содержать следующие компоненты:
  - ✓ Подтверждения действительности электронной подписи, используемых при подписании электронного документа, в том числе установлении фактов того, что соответствующие квалифицированные сертификаты действительны на определенный момент времени, созданы и выданы аккредитованными удостоверяющими центрами, аккредитация которых действительна на день выдачи этих сертификатов;
  - ✓ Проверки соответствия квалифицированных сертификатов требованиям, установленным Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», и иным принимаемым в соответствии с ним нормативным правовым актам, а также проверки полномочий участников электронного взаимодействия;
  - ✓ Создания и подписания квалифицированной электронной подписью доверенной третьей стороны квитанции с результатом проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания (компонент квитирования);
  - ✓ Создания и проверки метки доверенного времени;
  - ✓ Документирования операций, выполняемых средствами доверенной третьей стороны;
  - ✓ Предоставления информации об операциях, выполненных средствами доверенной третьей, по запросам участников электронного взаимодействия.

- Средства электронной подписи, используемые средством доверенной третьей стороны, должны обеспечивать возможность их функционирования в режимах создания электронной подписи и ее автоматической проверки.

Благодарю за внимание!