

Использование электронной подписи в ежедневной деятельности организации

Левиев Дмитрий Олегович

эксперт

НОУ «Академия Информационных Систем»

Законодательство

1. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» (принят ГД ФС РФ 25.03.2011) Начало действия 08.05.2011. Окончание переходного периода 01.07.2012
2. «Требования к форме квалифицированного сертификата ключа проверки электронной подписи" Приказ ФСБ РФ от 27.12.2011 N 795 (Зарегистрировано в Минюсте РФ 27.01.2012 N 23041)
3. «Требования к средствам электронной подписи и Требованиям к средствам удостоверяющего центра" Приказ ФСБ РФ от 27.12.2011 N 796 (Зарегистрировано в Минюсте РФ 09.02.2012 N 23191)

Системы организации связанные с ЭП

- Система сдачи обязательной отчетности в ФНС, ПФР, ФСС, ФФОМС
- Система обмена первичными бухгалтерскими документами
- Система юридически значимого внутреннего документооборота
- Система юридически значимого документооборота для партнеров и клиентов
- Система обеспечения управления ключевой информации

Выбор типа ЭП

электронная подпись - 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

Выбор типа ЭП

- Простая подпись
- Усиленная неквалифицированная подпись (неквалифицированная подпись)
- Усиленная квалифицированная подпись (квалифицированная подпись)

Средства ЭП

средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи

Требования к средствам ЭП

- К средствам ЭП в части их разработки, производства, реализации и эксплуатации предъявляются требования, закрепленные Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. N 66, для шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
- Требования к технологиям создания (формирования) и проверки ЭП с помощью средства ЭП указываются в тактико-техническом задании или техническом задании на проведение опытно-конструкторской работы или составной части опытно-конструкторской работы по разработке (модернизации) средства ЭП

Требования к средствам ЭП

- При создании ЭП средства ЭП должны:
 - показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
 - создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;
 - однозначно показывать, что ЭП создана.

Требования к средствам ЭП

- При проверке ЭП средства ЭП должны:
 - показывать содержание электронного документа, подписанного ЭП;
 - показывать информацию о внесении изменений в подписанный ЭП электронный документ;
 - указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

Требования к средствам ЭП

- Необходима разработка модели нарушителя на рабочее место согласно нормативно-методических документов ФСБ России и ФСТЭК России
- Необходима разработка модели угроз и атак согласно нормативно-методических документов ФСБ России и ФСТЭК России
- При разработке средств ЭП должны использоваться криптографические алгоритмы, утвержденные в качестве государственных стандартов или имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований
- В средстве ЭП должен быть реализован механизм (процедура) контроля целостности средства ЭП и СФ

Требования к средствам ЭП

- Срок действия ключа проверки ЭП не должен превышать срок действия ключа ЭП более чем на 15 лет
- Криптографические протоколы, обеспечивающие операции с ключевой информацией средства ЭП, должны быть реализованы непосредственно в средстве ЭП
- Исследования средств ЭП с целью оценки соответствия средств ЭП Требованиям (приказ 796) должны проводиться с использованием разрабатываемых ФСБ России числовых значений параметров и характеристик реализуемых в средствах ЭП механизмов защиты и аппаратных и программных компонентов СФ

Система управления ключевой информации

- Центр сертификации ОС Windows (CA сервер)
- Система управления ключевой информации, встроенная в конечную информационную систему
- Специализированная выделенная система управления ключевой информации - Удостоверяющий центр.

Средства управления ключевой информацией

- средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра
- удостоверяющий центр (далее - УЦ) - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные 63-ФЗ

Требования к средствам УЦ

- Требования (приказ 796) распространяются на средства УЦ, предназначенные для использования на территории Российской Федерации
- К средствам УЦ в части их разработки, производства, реализации и эксплуатации предъявляются требования, закрепленные Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. N 66 (с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 г. N 173), для шифровальных (криптографических) средств защиты информации (далее - СКЗИ) с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

Требований к средствам УЦ

- Необходима разработка модели нарушителя для УЦ согласно нормативно-методических документов ФСБ России и ФСТЭК России
- Необходима разработка модели угроз и атак согласно нормативно-методических документов ФСБ России и ФСТЭК России
- Необходимо проведение классификации УЦ как ИСПДн

Применение ЭП

- Только квалифицированная усиленная ЭП:
 - Система сдачи обязательной отчетности в ФНС, ПФР, ФСС, ФФОМС
 - Система обмена первичными бухгалтерскими документами
- Возможно применение неквалифицированной усиленной ЭП:
 - Система юридически значимого внутреннего документооборота
 - Система юридически значимого документооборота для партнеров и клиентов
- Система обеспечения управления ключевой информации
 - Только на базе ПО Удостоверяющий центр

Организационные изменения

- Необходимость разворачивания новой версии УЦ (квалифицированная подпись)
- Необходимость проведения новой классификации ИСПДн УЦ
- Необходимость письменного уведомления каждого получателя сертификата об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки
- Необходимость проверки документа удостоверяющего личность владельца для каждого сертификата (требование ФСБ России к УЦ класса КС2 и выше)
- Необходимость получение от физического лица - владельца сертификата ключа проверки подписи СНИЛС (для квалифицированной подписи)

Состояние

- Ответственность за выполнение требований по ЭП перекладывается на юридический отдел
- Необходимость проведение большого количества судебных экспертиз по проверке квалифицированной подписи
- Отсутствие сертифицированных версий средств УЦ, соответствующих требованиям для квалифицированной подписи
- Отсутствие сертифицированных средств ЭП, выполняющих требование по подписанию и проверки ЭП
- Отсутствие требований по аккредитации УЦ
- Отсутствие головного УЦ
- В мае 2012 года выходят новые 5 Постановлений Правительства и более 5 нормативно-методических документов по защите ПДн

Состояние

- Имеющиеся средства ЭП для генерации ключей имеют не реализуемые требования по эксплуатации в понимании юристов
- Контроль встраивания в большинстве систем, защищенных с использованием ЭП, не проходил контроль встраивания
- Осталось 94 дня!

План действий для организаций

- Выявление систем использующих ЭЦП (ЭП), где применение квалифицированной электронной подписи обязательно
- Направление запроса организации-администратору системы или органу требующему применение квалифицированной подписи для разъяснения порядка использования ЭП после 01 июля 2012 года
- Для систем, использующих ЭП, где возможно применение неквалифицированной подписи:
 - Изменение или разработка договора с учетом требований 63-ФЗ
 - Разработка регламента разбора конфликтных ситуаций в соответствии 63-ФЗ понятного юристам
 - Перевод системы управления ключевой информации на УЦ
 - Внесение изменений в регламент работы УЦ в соответствии с требованиями 63-ФЗ

Что делать?

- Принятие ФЗ о переносе сроков отмены 1-ФЗ от ЭЦП на 1 или 2 года
- Создание прозрачной для юристов схемы оценки соответствия средств ЭП и УЦ
- Приведение правил использования сертифицированных средств ЭП в соответствие со сложившейся практикой применения средств ЭП

Контакты

Левиев Дмитрий Олегович

Эксперт

Академия Информационных Систем

Тел./факс +7 495 231-3049

E-mail dleviev@infosystem.ru

<http://www.infosystems.ru>