ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная безопасность электронного взаимодействия с использованием квалифицированных сертификатов ключей проверки ЭП

Кузьмин Алексей Сергеевич

Федеральный закон «Об электронной подписи»

Сертифицировано 19 средств УЦ

Сертифицировано более 25 средств ЭП

Государственные органы (Федеральное Казначейство, ФНС, ФТС и др.), государственные внебюджетные фонды (ПФР, ФСС и др.), а так же коммерческие организации обеспечены сертифицированными средствами

Задачи ФСБ России по введению в действие Федерального закона «Об электронной подписи» выполнены в полном объеме

Обеспечение криптографической защиты электронных взаимодействий

Дискредитация какого-либо компонента инфраструктуры аккредитованных УЦ может иметь негативные последствия в части утраты доверия к федеральным информационным системам, участвующим в предоставлении государственных услуг и других сервисов

Инфраструктура аккредитованных УЦ

Федеральный орган исполнительной власти, осуществляет функции ГУЦ для инфраструктуры аккредитованных УЦ

Реализуется естественный механизм установления доверия ключу аккредитованного УЦ и контроля статуса аккредитации УЦ в момент проверки квалифицированной ЭП

ГУЦ достаточно отозвать соответствующий квалифицированный сертификат и возможность признания электронной подписи пользователя действительной квалифицированной будет исключена

Использование самоподписанных сертификатов аккредитованных УЦ

Либо требует использование дополнительных технологий (например, TSL)

Либо создает предпосылки для:

- Признания подписи квалифицированной в условиях отозванной (приостановленной) аккредитации УЦ
- Появления «ложных» квалифицированных сертификатов пользователей, созданных УЦ, не имеющих аккредитации

Приказ ФСБ России от 27 декабря 2011 года № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»

Классы средств:
КС1, КС2, КС3, КВ1, КВ2, КА1

Иерархия уровней криптографической защиты информации

Приказ ФСБ России от 27 декабря 2011 года № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»

Механизм включения сведений

Дополнение certificatePolicies (алгоритм обработки описан в RFC 5280)

Уровень криптографической защиты информационного взаимодействия при обмене электронными документами, подписанными КЭП, не превышает класс средств ГУЦ

Приказ ФСБ России № 796 от 27 декабря 2011 г. Требования к средствам удостоверяющего центра

Пункт 35

«При подключении средств УЦ к информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц, указанные средства должны соответствовать требованиям к средствам УЦ класса КВ2 или КА1»

Средства УЦ, входящие в состав подсистемы ГУЦ и используемых для создания и выдачи квалифицированных сертификатов аккредитованным УЦ

класс КВ2 или КА1

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

СПАСИБО ЗА ВНИМАНИЕ