ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

ограниченность функционального предназначения единого пространства доверия

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ
А.П. БАРАНОВ

ФУНКЦИИ ЭЛЕКТРОННОЙ ПОДПИСИ (ЭП) В СИСТЕМАХ УСЛУГ «ГРАЖДАНИН – ВЕДОМСТВО» И «ВЕДОМСТВО – ВЕДОМСТВО»

- Аутентификация пользователей со стороны системы. Как правило нет аутентификации системы для пользователя. Это две разные задачи
- Подтверждение целостности электронного документа (ЭД). Ничего не изменено
- Обеспечение гарантированности подписания тем, кем заявлено
- Обеспечение неотказуемости от подписания документа тем, кем заявлено
- 1 – 4 – обеспечивают юридическую значимость ЭДО на основе Закона №63 или частных договоров
  Идентификация – login
  Аутентификация - password

РАЗНОКАЛИБЕРНОСТЬ ЭД ОБУСЛАВЛИВАЕТ РАЗЛИЧНОСТЬ ТРЕБОВАНИЙ КИБ И ЭП

- Различная цена рисков неправильного (неправомерного) применения ЭП порождает разнокалиберность ЭДО
- Разнокатегорийность по конфиденциальности не эквивалентна разнокалиберности
- Юридическая и ценовая разница применения ЭП в ЭДО
  По классике:
- **цена риска =**
  (цена ущерба от реализации угрозы) Х
  (вероятность реализации угрозы) Х
  (вероятность возникновения угрозы)

- Приказ ФСБ РФ от 27.12.11 №756 по Требованиям к средствам ЭП и требованиям к средствам УЦ фактически только описывает 6 классов угроз
- Сравнение: требования ФСБ или оценка рисков
- Требования применять проще и надежней с юридической, формальной точки зрения

РАЗЛИЧНЫЕ КЛАССЫ ГУ СООТВЕТСТВУЮТ РАЗЛИЧНЫМ ВИДАМ ЭП

- В правильном направлении разрабатываются новые рекомендации Минкомсвязи по применению простой ЭП в системе ГУ в случаях малых юридических и финансовых последствий
- Нет задекларированной области применения усиленной (неквалифицированной подписи). Например подписи от Microsoft или разовая подпись Сбербанка
- Область применения квалифицированной и простой подписей определены Постановлением Правительства РФ от 25.06.12 № 634. В ГУ применение квалифицированной ЭП - предписано в области высоких ценовых и репутационных рисков
- Главный недостаток простой ЭП – воспроизводимость после ее демонстрации и отсутствие связанности с документом. Варианты усиления: разовые пароли, системы «свой – чужой»

• ПРОБЛЕМЫ РАЗЛИЧНОЙ РЕАЛИЗАЦИИ ЭП В ЗАВИСИМОСТИ ОТ ОЦЕНКИ РИСКОВ

- Системы «свой – чужой». Оценка цены риска сверхвысокая. Система ЭП - имитоприставка. Это не простая ЭП связанная с документом и не квалифицированная - нет СКП. УЦ – есть, но нет ключа проверки подписи.
  Видимо имитоприставка – усиленная неквалифицированная подпись

- Логин – пароль – простая ЭП
  Проблемы удаленного банкинга и платежных систем.
  Риски высокие – подпись слабая. Потери крупные.

- СМЭВ (ведомственные системы), - квалифицированная ЭП. Не решает проблемы некорректного использования ЭЦП (передача другому лицу, использование отозванного СКП)

- Перспектива в ГУ передача личной, конфиденциальной информации, SSL на основе ЭЦП. Стыковка различных производителей ЭЦП и отечественного варианта SSL

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИБ ДЛЯ РАЗЛИЧНЫХ ВИДОВ ЭП

- ИБ для квалифицированной ЭП регулируется Приказом ФСБ РФ №796. Разделение по классам угроз
- ИБ для усиленной и простой ЭП?
- ИБ для различных по массовости применения ЭП систем:
  - требования к АИС;
  - требования к клиентским приложениям
- ИБ систем off – line и on – line применения ЭП например: системы мониторинга - фиксации событий (фото с регистраторов ГАИ, видео с регистраторов граждан, видео камер наблюдения. Цена рисков может быть значительна.

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ЕПД

- ЕПД для всех сфер применения ЭП без корректировки закона №63 затруднительно. Вариативный характер СКП. Запрет ведомственных вариантов?

- ЕПД для простой и усиленной (неквалифицированной) ЭП вообще не проработан

- Технологические проблемы формирования ЕПД
  - большое количество УЦ второго эшелона. Слабая законодательная основа контроля за деятельностью ДУЦ;
  - контроль ИБ со стороны регуляторов практически отсутствует, у них нет юридических оснований. ДУЦ - орган оперативного взаимодействия
  - единая, общедоступная, ежедневно обновляемая база отозванных сертификатов ЕПД не поддерживается

- Разделение юридической ответственности ГУЦ и ДУЦ перед участниками ЕПД, пользователями и АИС ведомств

ЧТО ЛОГИЧНО СДЕЛАТЬ ДО 07.01.2014 ?

- Выпустить стандарт для СКП Госпортала не противоречащий Приказу ФСБ РФ № 795. Тогда в феврале 2014 года можно говорить о ЕПД
- Сорентировать стандарт на отдельные виды Госуслуг ?
- Запустить поддержку списка отозванных сертификатов на площадке ГУЦ и обеспечить широкополосный постоянный доступ к нему
- Ведомствам – максимально перевыпустить СКП под стандарт
- Ведомствам работающим, через портал ГУ доработать приемную часть АИС под стандарт СКП или Госпортала
- Определить, кто со стороны ГУЦ будет идти в суды для разбора кризисных ситуаций


СПАСИБО ЗА
ВНИМАНИЕ