ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

ОПЫТ МАССОВОГО ПРИМЕНЕНИЯ РАЗЛИЧНЫХ ТИПОВ ЭЛЕКТРОННОЙ ПОДПИСИ (ЭП)

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ
А.П. БАРАНОВ
abaranov@hse.ru

ДОЦЕНТ НИУ ВШЭ
П.А. БАРАНОВ
pbaranov@hse.ru

abaranov@hse.ru

Целевое предназначение ЭП

1. Подтверждение авторства или принадлежности информации и обеспечение неотказуемости

2. Обеспечение целостности и выявление изменений

3. В Законе №63 акцент на 1. и 2. в совокупности, либо только на 1. (простая ЭП)

4. CRC, контрольные суммы, имитоприставка обеспечивают только 2.

abaranov@hse.ru

Области применения типов ЭП

- Простая ЭП по договору сторон:
  - пароль – блокировка гаджета;
  - "логин – пароль" – системы взаимодействия с населением;
  - "двухфакторная аутентификация" - пароль - составная часть оцифровки личности
- Усиленная неквалифицированная подпись, в ограниченной Законом юридической значимости:
  - торговые площадки
  - международный доступ;
  - таможенные процедуры – заявки из-за рубежа;
  - ЛК физлица – налоговые процедуры
- Квалифицированная подпись, как повсеместная юридически значимая сущность:
  - открытие и закрытие бизнеса;
  - нотариальные процедуры

abaranov@hse.ru

Простая ЭП

- Отсутствует методологический и административный регулятор по техническим деталям применения
- Слабость пары Л – П в ее постоянстве при предявлении. Брешь для хакеров. Базы скомпрометированных Л – П
- Усиление системы Л – П путем смены пароля по SMS – затратно, громоздко и мало защищенно
- Желательно на основе Л – П усилить простую ЭП, связав ее с сихропосылкой, как в системе "свой - чужой"
- Шутка: передавать пароль в зашифрованном виде с использованием SSL

abaranov@hse.ru

Усиленная неквалифицированная подпись (УНП)

- По определению это криптографический примитив. Следовательно, подлежит регулированию ФСБ РФ. В Законе об ЭП этого нет. Нет и регулятора, т.е. их много
- По практике это либо SSL с иностранным крипторовайдером, либо сертифицированный отечественный примитив с отступлениями от требований ФСБ РФ
- Требует отдельного УЦ, даже если все ПО УЦ сертифицировано в ФСБ РФ
- Для десятков миллионов пользователей стала возможна реализация "облачного" или локального варианта УНП, за счет упрощения процедуры выдачи, противоречащей регламенту регулятора для квалифицированной подписи

abaranov@hse.ru

Квалифицированная подпись ЭП (КЭП)

- Физические и юридические лица заменяются (КЭП) и цифирь существует отдельно от субъекта. Нет возможности отзыва КЭП без заявления владельца, даже по инициативе правоохранительных органов
- 300 УЦ в РФ:
  - выдачи КЭП без проверки паспортных данных;
  - ничтожный контроль за деятельностью УЦ;
  - отсутствие регулярно обновляемой общей базы отозванных СКЭП;
  - дороговизна услуги КЭП с учетом смены ключей один раз в год
- Реализация КЭП в сложных прикладных продуктах сопровождается длительной и дорогостоящей экспертизой корректности встраивания

abaranov@hse.ru

Госулуги и госфункции с КЭП

- Несимметричность ответственности и электронной нагрузки в паре: гражданин – государственный орган (ГО). Заказ услуги от гражданина с КЭП, и получения результата – личная явка в ГО
- Отсутствие в обороте электронных справок с КЭП от госорганов (справка о судимости, справка о собственности, справка от наркодиспансера и т.д.),для которых не нужен биологический объект
- Спектр решений для применения КЭП в Web-технологиях без экспертизы встраивания узок. Нет заказчика на задачу
- Единый агент ПГУ пользователя упростил бы решение задач мультибраузерности, мультиоперационности и защиты массового рабочего места

СПАСИБО
ЗА ВНИМАНИЕ

abaranov@hse.ru