ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНЫЙ ИННОВАЦИОННЫЙ
ВНЕДРЕНЧЕСКИЙ ЦЕНТР
ГНИВЦ

Угрозы информационной безопасности (ИБ) видам электронной подписи (ЭП)

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

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

abaranov@hse.ru, pbaranov@hse.ru

Общая классификация угроз в электронном документообороте (ЭДО)

1. Оперативные или операционные угрозы. Гуманитарные аспекты и обычаи применения ЭДО
2. Юридические последствия нарушений регламентов оборота электронных документов
3. Правоприменительная практика и массовое сознание
4. Технические угрозы для ЭП в основном классифицированы ФСТЭК и ФСБ России. УЦ – гарант принадлежности ЭП объекту.
5. Технологии идентификации заявителя, как биологического, либо юридического объекта.
6. Неприменение ЭП для ЭДО. Фальсификации для АВС вкладов населения

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Угрозы ИБ простой ЭП

ГНИВЦ

1. Идентификация пользователя по двум малонадежным факторам
2. Постоянство и возможность НСД к паре логин – пароль
3. Блокировка доступности владельца с перенаправлением разового пароля злоумышленнику. Подмена sim-карты телефона
4. При рассылке 10^8 разовых паролей в год затраты организации 100 млн. рублей
5. Применение несертифицированного SSL от Microsoft массовым пользователем, как следствие отсутствия удобного отечественного SSL

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Угрозы ИБ усиленной неквалифицированной ЭП (УНЭП)

ГНИВЦ

1. УНЭП сейчас в России это либо американская криптография или ГОСТ с отступлениями при применении от сертификата
2. Сейчас регулятор в области применения УНЭП – регулировщик самой области. Следствие - побеждает информатизация
3. Допустимость применения ключей квалифицированной ЭП (КЭП) в системе УНЭП без отдельного криптопровайдера. Позиция регулятора?
4. В чем угроза применения ПАК УЦ для КЭП в случае выдачи ключей для УНЭП, если последняя на ГОСТе?
5. Применение в Интернете PGP с УНЭП создает предпосылки для вытеснения ГОСТа с рынка России

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГНИВЦ

Угрозы ИБ облачной ЭП

1. В удаленной идентификации объекта позиция правоохранительных органов должна быть определяющей
2. Технические требования ИБ, доступные для реализации в ЦОДе «облака», недоступны массовому (10^7) пользователю
3. Вклинивание нарушителя в работу пользователя с незащищенным компьютером позволяет «правильно» подписать подставной документ, не узнавая ключа подписи
4. Ненадежность оператора облачной ЭП, включая юридический (уголовный) и финансовые аспекты при невозможности исправления затратных операций
5. Недоступность проверки ЭП, включая устойчивость к преднамеренным прерыванию связи с облаком, типа DDOS - атаки
6. Главное! Идентификация только часть проблемы. Доверенная среда!

abaranov@hse.ru, pbaranov@hse.ru

Удаленная идентификация объекта I

1. Описаны ошибки обоих видов $\alpha = P(H_0/H_1)$ и $\beta = P(H_1/H_0)$, H_0 – объект «правильный», H_1 – «неправильный»
2. Обе гипотезы H_0 и H_1 – сложные и описание объекта есть его модели, возможно нечёткие
3. Перехват и фиксация нарушителем элемента h из H_0 позволяет далее использовать h, как простой постоянный пароль.
4. Следствие: h должно зависеть от некого случайного параметра t т.е. h(t). Вариантов h(t) должно быть много, т.е. разовый пароль
5. Отпечаток пальца, идентификация радужной оболочки глаза уже не подходят, фиксированное лицо не подходит, голосовые сообщения в силу имитации не подходят и. т. д.
6. Ужесточение процедуры идентификации, уменьшающие α, как правило ведут к увеличению β

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Удаленная идентификация объекта II примеры проблем

ГНИВЦ

1. Удаленная идентификация на основе рукописной доверенности третьему лицу для УЦ
2. Удаленная идентификация по файлу с содержанием или фото паспорта в недобросовестном УЦ
3. Имитация голосовых сообщений, включая интонации при наличии «обучающей» выборки позволяет сделать неразличимыми цифровые гипотезы $H_0(t)$ и $H_1(t)$
4. Нарушитель не только внешний ,но и внутренний нарушитель. Подделка документов. Подделка изделий и их маркировки, ККТ, и т. д.
5. Различные базы госорганов содержат только косвенные признаки, характеризующие объект. При наличии возможности предварительного обращения к госбазам имитация H_0 будет эффективна
6. Вывод: госбазы защитить от НСД, но какой категории и сколько это будет стоить?

abaranov@hse.ru, pbaranov@hse.ru

Современные угрозы Удостоверяющему Центру, как гаранту применимости КЭП

1. Будет 1000 УЦ и появятся «однодневки» УЦ для криминальных целей
2. Идентификация объекта в УЦ требует специальных знаний и подготовки. Это оценка личности или системы
3. Ликвидация ЭП– ликвидация оцифровки объекта. Объекта нет, а ЭП живет и действует по доверенности до 1 года
4. Массовой КЭП необходима четко и жестко регулируемая система УЦ со строгим регламентом, высокой юридической и финансовой ответственностью
5. Отсутствие законодательной нормы юридически значимого электронного документооборота ставит УЦ в двусмысленное положение. Гарант, а чего? Только КЭП!

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГНИВЦ

СПАСИБО ЗА ВНИМАНИЕ

abaranov@hse.ru
pbaranov@hse.ru