Высшая Школа Экономики
Национальный исследовательский университет

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИМЕНИ И.М. ГУБКИНА)

Криптографические системы и внутренний нарушитель

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

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

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Нарушители

ФСТЭК РОССИИ

Внешние нарушители – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозу безопасности информации из за границ информационной системы (ИС)

Внутренние нарушители – лица имеющие право постоянного или разового доступа к ИС, ее отдельным компонентам

(Приказ ФСТЭК №27 от 15.02.2017)

ФСБ РОССИИ

Внешние нарушители это КС1. Формально уже КС2 и даже возможно проведение атак внутри К3, но, например, для КС2 без физического доступа к аппаратным средствам, на которых реализованы СКЗИ, следовательно уже все требования ≥ КС2 ФСБ РФ относятся к внутреннему нарушителю

(Приказ ФСБ РФ № 378 от 10.07.14)

abaranov@hse.ru, pbaranov@hse.ru

Внутренний нарушитель (ВтН) в корпоративных и массовых компьютерных с

1. Нацеленный ВтН
   а) $ВтН_1$ – использование КС для личной, нештатной выгоды
   б) нанесение ущерба КС или ее средствам
2. Случайный (необученный) $ВтН_2$ – ИБ по направлениям К,Ц,Д
3. $ВтН_3$ – жертва внешнего нападения
4. ВтН – в корпоративных и массовых общественных системах похожи
5. $ВтН_{1,2}$ – в корпоративных системах может быть нейтрализован административными и техническими дополнительными СЗИ мерами
6. $ВтН_3$ в массовых системах может наносить существенный ущерб по всем сервисам

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Криптографические функции шифрования и сущности, требующие защиты от ВтН до уровня КС3 включительно

1. Контролируемые сущности в канале передаче

   а) исходное сообщение
   б) ключевая информация – «слабые - договорные» ключи
   в) включение шифрования – отсутствие «байпаса»
   г) удаленное управление ключами
   д) «маскирование» исходного сообщения
   е) для SSL – встреча посередине

2. Контролируемые сущности в аппаратуре реализации шифрования

   а) доступность для ВтН ключевой информации при вводе - выводе
   б) возможность влияния (изменения) на криптографическую схему, реализованную в аппаратуре

3. Идеи 1а), 1б), 1г), 2а), 2б) присутствуют в Требованиях регулятора, а 1в), 1д), 1е) присутствуют в жизни

4. Защищенность информации и ПО по ФСТЭК России, означает защищенность ключевой информации или ПО шифрования?

abaranov@hse.ru, pbaranov@hse.ru

Криптографические сущности ЭП и вопросы защиты от ВтН до уровня КС3 включительно

1. Работающий в соответствии с аттестацией УЦ и свободный доступ к реестру отозванных сертификатов
2. Надежность работы пользовательского комплекта ЭП и ее проверки в условиях многофункциональности Рабочего места массового пользователя, нестабильности его ПО, и непосредственного подключения к Интернету. Стыковка ключей и разных криптопровайдеров при выработке ЭП
3. Класс защиты и соответствие надежности удаленной аутентификации в облачном варианте ЭП. Классы надежности удаленной аутентификации физической сущности клиента?
4. Взаимодействие ПО для ЭП и систем удаленного ЭДО, включая смартфоны и другие мобильные устройства
5. ЭП в Архивном хранении с Доверенной третьей стороной (15 лет действия сертификата на проверку ЭП нет в требованиях ФСБ России, как нет до сих пор самих требований)
6. Количество подписей на одно лицо не ограничено в ФЗ №63

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Оценка рисков и эгоизм банков

1. Банки вернули только 1/7 часть средств, похищенных у клиентов через электронное взаимодействие
2. Оценка риска это оценка средней величины потери по статистическим данным – мнениям экспертов
3. Оценки должны быть получены по двум направлениям: оценка вероятности – частота событий и оценка ущерба
4. Стандартный подход, как взвешенная сумма оценок, работает только при достаточном количестве независимых оценок. Все коммерческие эксперты базируются на малом поле доступных их наблюдениям событий
5. Оценки может собрать только Регулятор. Оценки рисков нельзя выставлять в номинации по анализу защищенности
6. Риски может адекватно оценить только мегарегулятор. Цена ущерба для банков и для госструктур принципиально различны, см п 1. Для госрегуляторов цены ущерба в 100 раз большие

abaranov@hse.ru, pbaranov@hse.ru

Обеспечение КС3 в массовых системах

1. Центральная часть не имеет проблем, как корпоративная система, если делается с нуля. Известны сложности перехода с КС2 на КС3 с помощью только дополнительных средств, часто требуется доработка ППО

2. РМ массового пользователя и есть $ВтН_{1,2,3}$!

   а) доверенность Сим-карты или токена с ответственной аутентификацией при продаже: Сим-карта ⇔ клиент
   б) противоречие не извлекаемости ключа и отдельных информационных технологий, требующие реализации ЭП на скоростях 100 Гбит/с
   в) сертификация Сим-карты по КС3 обеспечивает реальную защиту только в режиме «пробки»
   г) ключевая структура Сим-карты для шифрования и для ЭП различны, даже для SSL

3. Для смартфона актуальна выдача подтверждения в условиях возможной работы с фальшивой сотой

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Обеспечение КСЗ в массовых системах. Симбиоз прикладных и защитных функций ППО

1. Аппаратный элемент (АЭ) должен быть максимально индифферентен к ППО. Пробка-идеальна, но в одиночку не решает всех проблем
2. Главный вопрос ИБ в защищаемой ЭДО – подсовывание в АЭ поддельного документа взамен истинного
3. Следовательно, АЭ должен быть сразу (пробка) за устройством ввода документа и перед микросхемой физического уровня. Пробка два раза!
4. Т.е. нарушается стандартная схема ПЭВМ в виде: ЛВС – все аппаратные части на общей шине. Это не есть нарушение архитектуры Фон-Неймана
5. Схема: документ – внесение защитных элементов в $АЭ_1$-обработка – ЭП в $АЭ_2$ – отправка
6. Возможно $АЭ_1$ располагается на внешнем носителе или в разрыве клавиатуры

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Задачи разработки и внедрения новых технологий защиты в массовых системах

1. Обеспечение доступности, т.е. устойчивости на уровне L1, т.е. создание и применение на физическом уровне доверенный ASIC
2. Выполнение всеми облачными сервисами требований Закона в части защиты ПД т.е. шифрования трафика между ЦОДами отечественными криптографическими средствами.
3. Интеграция средств выработки ЭП уровня КС 3 для документооборота на мобильных пользовательских устройствах с надежностью аутентификации сопоставимой с КС 3
4. Исключение рискового подхода из требований Регулятора, как невозможного для реализации или выработка требований к экспертам и их оценкам
5. Единообразное определение срока эксплуатации сертификатов ЭП для проверки правильности ЭП, по аналогии с ключом подписи 1 год
6. Формирование требований к «доверенной третьей стороне»
7. Разработка аналога защищенной Сим-карты для Wi-Fi – протокола, т.е. домашних массовых рабочих мест

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

СПАСИБО ЗА ВНИМАНИЕ

abaranov@hse.ru