Высшая Школа Экономики
Национальный исследовательский университет

Угрозы в актуальных задачах применения ЭЦП (ЭП- 500 УЦ ,ЭЦП-5 УЦ в России)

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

Методология формирования угроз по требованиям регуляторов

1. Постановление Правительства № 555 от 11.05.2017. Аттестация по ИБ обязательна. Наша благодарность Правительству за это
2. Аттестация возможна, если согласована Модель угроз ИБ с регуляторами или согласовано ТЗ. Большинство выбирают Модель угроз. Модели угроз для УЦ не учитывают специфики отраслей применения ЭП, поскольку УЦ универсальны
3. Существует обширная техническая Модель угроз по защите от НСД, разработанная ФСТЭК России
4. Модель угроз по требованиям к уровням безопасности для ЭП, как криптографической функции, построена по принципу роста технических возможностей противника по подделке ЭП. Корректность встраивания в 1000 серверов приложений в ЦОДе
5. Требования на уровне безопасности для ЭП и для устройств шифрования информации весьма близки, хотя сферы применения различны

Совмещение требований ФСБ РФ и ФСТЭК России

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			КА	КВ	КС
			1 (НДВ ОС)	2 (НДВ ПО)	3 (Без НДВ)
ИСПДн – С (специальные)	Нет	> 100 000	УЗ - 1	УЗ - 1	УЗ - 2
	Нет	< 100 000	УЗ - 1	УЗ - 2	УЗ - 3
	Да				
ИСПДн – Б (биометрические)			УЗ - 1	УЗ - 2	УЗ - 3
ИСПДн – И (иные)	Нет	> 100 000	УЗ - 1	УЗ - 2	УЗ - 3
	Нет	< 100 000	УЗ - 2	УЗ - 3	УЗ - 4
	Да				
ИСПДн – О (общедоступные)	Нет	> 100 000	УЗ - 2	УЗ - 2	УЗ- 4
	Нет	< 100 000	УЗ - 2	УЗ – 3 КС	УЗ - 4
	Да				

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Требования к ЭП и ЭЦП

1. ЭЦП по сути сейчас это неквалифицированная ЭП(НКЭП), которая повсеместно используется вместо квалифицированной в массовых системах более 10^5 пользователей
2. До 2011года ЭЦП-«Централизованный» набор УЦ с государственным управлением. Теперь ЭП- «Анархичное» множество УЦ с техническим госрегулированием и самоуправлением в оперативной деятельности
3. Вид противника определяется функционалом системы. Повсеместно внутренний противник порядка применения ЭП игнорируется, а на практике он крайне актуален
4. Для анализа действий нарушителя требуется изучение не столько технических особенностей системы, сколько опыта ее функционирования в прошлом и задач на будущее, включая масштаб применения. Цена редкого события? Следователь по прикладу?

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

В массовых системах работает только ЭЦП

1. Если в системе 100 тысяч пользователей и 1000 бизнес приложений, то даже 1% составляет 1000 внутренних нарушителей
2. Преднамеренный внутренний нарушитель использует разрешенные права доступа, но действует вопреки ожидаемого разработчиками порядка применения системы
3. Нарушитель поневоле, по сути опять внутренний нарушитель и может наносить ущерб, как системе , так и себе, без предумышленной цели. Оценка корректности встраивания ЭП у пользователя массовых систем для какого ППО?
4. Даже в ведомственных системах вместо ЭП работает ЭЦП, так как формальные требования по технической фиксации системы выполнять реально практически невозможно
5. УЦ – по сути, регулярно являются внутренними нарушителями и действуют вопреки регламентов для дополнительного извлечения прибыли

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Новое направление Архивное хранение и ЭП

1. Информация существует только в движении. Хранение это движение информации во времени. В ответственном Архиве ЭП необходима для обеспечения юридической значимости документа и подтверждения его неизменности
2. Ранее созданная ЭП для квалифицированности проверки ее валидности должна проверяться на прежней (старой) технологической платформе, либо новая платформа должна быть аттестована со старой ЭП, с большим сроком действия аттестата и «старым» УЦ
3. Т.е. практически подняться выше уровня КСЗ проблематично из-за несоответствия нового ППО прежним ОС и «старым» ЭП
4. В Архиве документ храниться в виде электронного конверта с подписями Архивистов и под присмотром Администратора
5. Можно ли считать Архивиста и Администратора абсолютно независимыми (или относительно) от обстоятельств жизни? Например, указания руководства на данный момент

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Чья ЭП или аутентификация ее владельца

1. Носитель (токен) с паролем для компьютерной системы и есть личность
2. Выход-компактный и дешевый вариант «PinPad». Подписание и визуализация критически важной информации на борту носителя с фиксированным и надежным ПО
3. Главная угроза удаленной аутентификации личности – повтор признаков настоящего владельца и предъявление их независимо от владельца (отпечатки пальцев, голос, биометрия, ДНК и т.д)
4. Реальная идентификация личности связана с непосредственным ее проявлением в движении (изменении). Автоматическое выявление маски без участия человека-контролера
5. Передача информации от носителя к приемнику по незащищенному каналу требует шифрования на ключе подписи, т.е. ключ подписи опять эквивалентен личности или это другой ключ?

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Предотвращение копирования ключевой и аутентифицирующей информации или ее редактирования

1. Сочетание ЭЦП и электронных водяных знаков (ЭВЗ)-стеганографии повышает устойчивость к несанкционированному применению аутентифицирующей информации
2. Выявление изменений в блоках информации при несанкционированном подписании за счет дополнительной проверки ЭВЗ. Почему ЭВЗ широко не применяется?
3. Применение ЭВЗ в технологиях обмена данными для образования общего ключа в SSL при сервисном предоставлении услуги ЭЦП со стороны облака
4. Квантовые технологии на основе спутанных кубитов, как платформы принципиально не клонируемых элементов ЭЦП
5. Фискальный накопитель, как защита от «неправедного» приказа и несанкционированного применения ЭП. Исторический Архив?

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Особенности ЭЦП в СОПКАх

1. На нижнем уровне СОПКА в организациях или в обществах реально применение только ЭЦП для подтверждения авторства и целостности передаваемой выше информации
2. На среднем уровне для передачи выше реализуема ЭП в целях предотвращения «отвлечения на негодный объект»
3. Подписание ЭП рекомендаций и рассылаемых для использования продуктов, получаемых от верхних уровней нижними
4. Синхронизация и верификация данных о компьютерных атаках (КА), получаемых от различных источников. Насколько целесообразно применение специальных ЭВЗ?
5. Проблема постоянной доступности УЦ, даже в условиях КА. Доступность по Интернету для пострадальца в случаях КА проблематична. При отсутствии контакта с УЦ возможно подсовывание любых обновлений под маркой верхнего уровня

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Выводы

1. Массовой квалифицированной ЭП нет и быть не может при современном уровне развития и эксплуатации компьютерных технологий
2. Повсеместно принимается усиленная неквалифицированная электронная подпись (ЭЦП), юридические особенности применения которой законодательно слабо определены
3. При формировании угроз и выборе уровней защищенности ЭП, необходимо детально изучать область применения и практики нарушений
4. При архивном использовании ЭП необходимо сохранение технологий предыдущего цикла проверки и подтверждения ранее созданных ЭП, ключам предыдущего варианта УЦ
5. Основная угроза владельцу ЭП- неконтролируемое применение аутентифицирующей информации. Актуальна разработка методов выявления клонирования с использованием ЭВЗ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

СПАСИБО ЗА ВНИМАНИЕ

abaranov@hse.ru