РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ НЕФТИ И ГАЗА
ИМЕНИ И.М.ГУБКИНА

ВЫСШАЯ ШКОЛА ЭКОНИМИКИ
НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

КЭП в массовых системах

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ РОССИИ
А.П. БАРАНОВ
baranov.ap@yandex.ru

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

baranov@gnivc.ru pbaranov@hse.ru

Современные характеристики массовых систем

1. Порядка 10^7 пользователей
2. Мобильные пользовательские устройства: смартфоны, компьютеры с sim-картами, Wi–Fi –доступ. Не доверенный центральный процессор и ОС
3. Низкий уровень знаний и навыков пользователя гаджета
4. Существенная вероятность возможной утраты гаджета и требование возможности его удаленной блокировки владельцем
5. Легкая авторизация в нем, при недостаточной надежности идентификации
6. В облачном решении предполагается, что ЦОД может **всё**, как и телеком с опорой на Интернет (скорость)
7. Однократная явка пользователя для личной идентификации

baranov@gnivc.ru pbaranov@hse.ru

Парадигма массовых технологий в применении к КЭП

1. Заготовки, шаблоны документов должны быть представлены из облака. Желательно доверенные
2. Разнообразие центров для доступа работы с документами из разных ЭДО с различными УЦ
3. Разные технологии работы с документами — **это плохо. Массовый пользователь пытается придерживаться уже освоенных приемов**
4. Учитывая возможность широкого показа или распространения контента нужна защита от несанкционированного копирования и сохранения авторства. Электронные «водяные знаки» как дополнение к КЭП
5. Ключ или личный идентификатор должны быть дополнительно защищены от посторонней активации

baranov@gnivc.ru pbaranov@hse.ru

Центральная часть системы массового применения КЭП. Система УЦ

1. Система взаимодействующих Удостоверяющих Центров. Количество отдельных узлов, связанных по КБ порядка нескольких десятков
2. Точек физического контакта и проверки личности или заявлений ЮЛ, ФЛ порядка нескольких тысяч. Связаны с узлами по КБ
3. Нужна эффективная балансировка нагрузки в этом географически распределенном вычислительном кластере. Заявка в одном месте, получение в другом
4. Время обслуживания на точке выдачи и авторизации не более 15 минут при явке без предварительного заказа. При предварительном заказе – 5 минут
5. Связи узлов и взаимодействие с другими ведомствами по проверке личности заявителей. СМЭВ и другие виды телекоммуникаций. КС-2 и выше

baranov@gnivc.ru pbaranov@hse.ru

Облачный УЦ для выдачи ключа КЭП на «борт»

1. Доверенный элемент (ДЭ) на «борту» для идентификации пользователя
2. Требования к ДЭ, как к паспорту личности с удаленным предъявлением
3. Система выдачи ДЭ, как выдача КЭП в УЦ. Те же проверки и требование однократной явки
4. Длительность использованных ДЭ - несколько десятков лет?
5. Система «заначки» ключа КЭП в «доверенные» хранилища на гаджете-смартфоне
6. Шифрование при передаче ключа КЭП на борт пользователю по КСЗ. Альтернатива- генерация ключа на борту с направлением открытого ключа в УЦ на формирование сертификата

baranov@gnivc.ru pbaranov@hse.ru

«Облачный» ЭДО

1. Главная проблема - ДЭ, идентифицирующей пользователя и не допускающий модификацию или воспроизведение (подделку) как хакером, так и самим пользователем
2. Пример такого элемента есть: sim-карта или токен с соответствующей аттестацией по уровню КС-3
3. Для пользовательского ДЭ в гаджете он должен работать на уровне L-1 или L-2, обеспечивая независимость от ОС и ПО борта
4. Фактически элемент ДЭ это дополнительный компьютер в гаджете на связи гаджет – облако
5. Облако должно иметь возможность разделять и идентифицировать ДЭ в потоке запросов, соотнося пользователя с обслуживающим его УЦ

baranov@gnivc.ru pbaranov@hse.ru

Принципы облачного доверенного ЭДО

1. ДЭ создает имитозащищенную «трубу» по уровням L1, L2 и в нее втекают «ручьи» из возможно разных ЭДО
2. ДЭ есть составляющая часть ЭДО. Может быть несколько ДЭ одного пользователя даже в рамках одного ЭДО
3. ИБ для массового удаленного пользователя заключается не столько в обеспечении конфиденциальности, сколько в обеспечении целостности и доступности. Аналогия с АСУ ТП
4. Идентификация пользователя при массовой выдаче ДЭ есть одна из главных задач в массовом ДЭО.
5. Необходим регулятор, который бы утвердил правила и степени – надежности процедур при идентификации ФЛ в общегражданском сегменте доверенного ЭДО

baranov@gnivc.ru pbaranov@hse.ru

Проблемы массового пользователя с доверием к ХЕШу

1. Все общее в ЭДО должно быть максимально шаблонизировано. Действия пользователей желательно возможны только на смартфоне или только на планшете
2. Вычисление хеш на не доверенном процессоре гаджета порождает проблему доверенности системы в целом. Идеально вычислять хеш только в облаке, но это порождает вопрос о доверенной передаче конкретных данных в шаблон
3. Общая оценка защищенности в системе определяется самым слабым звеном. В ЭДО это теперь похоже вычисление хеш на борту
4. Веб –доступ плохое решение, возможное только на начальном этапе. ЭДО нужно для пользователя в виде приложения под различные ОС и для различных ЭДО это будут разные программы

baranov@gnivc.ru pbaranov@hse.ru

Проблемы массового пользователя с CRL

1. Процедура общения с облачным ЭДО должна иметь эффективную структуру в виде круглосуточного Call-центра
2. Проверка чужой ЭП на «борту» и доступ к CRL УЦ в значительной степени зависит от решения по времени скачиваемого зашифрованного массива CRL узла УЦ. При 10 узлах и 10 млн. пользователей время скачивания 3 минуты. Скорость 300 CRL/сек.
3. Критично: браузер гаджета работает с узлом УЦ, как с любым сайтом. Узел УЦ должен обеспечивать время полного скачивания, как для любого сайта , т.е. 0,5 минуты. Иначе тормозится работа с другими сайтами
4. Пример с CRL иллюстрирует разницу между корпоративными и массовыми системами

Спасибо за внимание

baranov@gnivc.ru