# Госключ – успех или катастрофа

Академик АКАДЕМИИ КРИПТОГРАФИИ РФ,
рук.Департамента ИБ Финансового университета
Д.Ф.М.Н.
**А.П. БАРАНОВ**

baranov.ap@yandex.ru
К.Т.Н.

**П.А. БАРАНОВ**

baranov.ap@yandex.ru

# Вопросы содержания предлагаемой системы Noparer

1. Точного описания на техническом уровне не представлено. Имеются лишь приблизительные изложения действий пользователя
2. Утверждается, что ключ вырабатывается «на борту» самого пользователя с помощью псевдослучайного алгоритма
3. Датчиком случайности является сам пользователь
4. Предполагается полная соответствие смартфона владеющей им  физической (юридической) личности
5. Считается абсолютно надежной работа ППР УЭП на смартфоне
6. Отсутствует (нет в описаниях) функции (технологии) проверки принадлежности сертификата личности

baranov.ap@yandex.ru

# Описание (восстановление по рекламе – других нет) алгоритма

1. Входим в систему Госуслуг и предъявляем ранее зафиксированный на Почте России личный пароль
2. Получаем на смартфон код в виде sms от системы Nopaper
3. Видимо после п.2 или п.1 скачиваешь ППО УЭП на свой смартфон
4. Водишь пальцем по экрану и создаешь «случайность», которая видимо в смеси с кодом из sms, на ППО порождает ключ
5. Ключ запоминается в ППО и на смартфоне вырабатывается открытый ключ, который вместе с ОК, sms и твоим паспортом и фото уходит в систему Госуслуг
6. Наверное, потом Вам приходит подписанный КЭП портала Госуслуг сертификат на вашу УЭП

baranov.ap@yandex.ru

# Классификация облачных технологий ЭДО

1. Полуоблачные и облачные технологии получения и Электронной подписи (ЭП). Ключ «на борту» или ключ у провайдера
2. Полуоблачные и облачные технологии ЭДО с использованием подписи. Подписание документа ключом «на борту» или у оператора ЭДО. Возможны 4 комбинации.
3. Тезис: «Там, где ключ, там и главная опасность» не совсем верен. Проблема в удаленной идентификации физического объекта – клиента
4. В Требованиях ФСБ к средствам ЭП нет градации числовой оценки надежности аутентификации для КС1-3,КБ,КА. Предлагаем ввести параметр – вероятность ложной аутентификации. Нормировать ее значение  можно для каждого из уровней защищенности ЭП

baranov.ap@yandex.ru

# Смартфон это не физическая личность

1. Идентификация смартфона по номеру телефона – фикция
2. Идентификация смартфона по Mac–адрес – фикция
3. Аппаратный номер смартфона IMEI – прошит достаточно надежно, но отображается у оператора сотовой связи по Закону Яровой. Хранится некоторое время. У пользователя доступа к нему нет.
4. Цифровой отпечаток (устройства-браузера) может быть сформирован у провайдера
5. Профиль смартфона пользователя по геопозиции
6. Все пять позиций могут быть изменены (подделаны) усилиями квалифицированных нападающих

baranov.ap@yandex.ru

# Внутренний – внешний противник в технологиях ЭП

1. Отказ от ЭП – со ссылкой на хаккера. Возможна предварительная, по сговору, подготовка смартфона для дальнейшего предъявления эксперту
2. Сложность реализации средств защиты смартфона делает массового пользователя внутренним противником
3. Технология идентификации на основе sms-сообщений, предполагает полное доверие к коллективу: оператор сотовой связи – провайдер сайта ЭП
4. Кто принимает на себя юридические, материальные и моральные риски?
5. Например фирма ООО «Акоммерс» предлагающая Nopaper на себя не берет ничего

baranov.ap@yandex.ru

# Уровень цены риска определяет цели сделки

1. Цена риска в пределах убытка до 40 т.₽ не превышает 10 т.₽ и приемлема многими
2. Цена риска при цене потери $10^6$₽ может составлять $10^5 \div 10^4$ руб., что является существенной суммой
3. Цена риска равна (грубо) произведению цены сделки на вероятность обмана. Какова вероятность обмана в УНеКЭП?
4. Для разной цены сделки вероятность обмана различна, т.к. при большой цене сделки затраты на обман могут быть больше
5. При большом количестве больших сделок нападение может разработать дорогую, но массово работающую схему. Например, подделку аутентификации личности

baranov.ap@yandex.ru

# Выводы

1. Необходимо обнародовать и произвести анализ экспертами ИБ алгоритма работы УНеКЭП
2. Необходимо ввести ограничения на объем и цену проводимых сделок с помощью УНеКЭП операций
3. Предлагаем  ввести в Требования ФСБ дифференцированную числовую оценку надежности аутентификации
4. Вероятность подделки УНеКЭП за счет суммирования всех факторов, включая подмену фото-данных порядка 0,1 – 0,01
5. Следует провести оценки вероятностей п.4 путем проведения исследований в авторитетной научной организации, например Академии криптографии РФ
6. Необходимо определить юридическую и материальную ответственность партнеров Госуслуг по реализации платного ЭДО

# Спасибо
# за внимание

baranov.ap@yandex.ru