конференция РусКрипто

Переход на аппаратные СКЗИ для массового пользователя

BIFIT

О компании

БИФИТ основан в 1999 году

Основное направление деятельности – разработка и продвижение ДБО «iBank 2»

2015 г. – 38,5% российских банков используют систему «iBank 2»

БИФИТ имеет Лицензии ФСБ РФ (разработка СКЗИ, гостайна)

Угрозы ДБО

Угроза хищений в ДБО носит массовый характер с конца 2007 г.

Анатомия угрозы:

- **заражение рабочего места клиента специализированным вредоносным ПО**
- **создание мошеннического платежа от имени клиента**

Угрозы ДБО: меры противодействия

БИФИТ противостоит угрозе хищений в ДБО по всем направлениям:

- **использование персональных аппаратных криптопровайдеров (поддержка в системе «iBank 2» с 2008 г.)**
- **выявление и противодействие специализированному вредоносному ПО на рабочих местах клиентов**
- **выявление мошеннических платежей**

Угрозы ДБО: текущие тенденции

1. Рост хищений
2. Усложнение вредоносного ПО
3. Усложнение схем мошенничества
4. Угрозы со стороны легитимного ПО
5. Снижение безопасности ради удобства

Вредоносное ПО: статистика по клиентам ДБО

4,45% компьютеров клиентов заражены специализированным вредоносным ПО

Вредоносное ПО для удаленного управления компьютером – **94%** заражений

Рост количества разновидностей за последние 6 месяцев – **40%**

Аппаратные СКЗИ защищают от угрозы удаленного управления

BIFIT

Среда массового клиента - тотально враждебная

Ранее среда работы массового клиента - компьютеры, смартфоны, планшеты - считалась недоверенной

Сегодня среда массового клиента – тотально враждебная

Использование программных СКЗИ массовым клиентом создает неприемлемые риски

Риски хищений по ДБО

Обороты по дебету счетов корпоративных клиентов в 2014 г.	518 994 млрд. руб.
Доля платежей в электронной форме	91%
Объем мошеннических платежей на каждые 1 млн. руб. оборотов	38,63 руб.

Годовой объем угрозы хищений:

18,244 млрд. руб.

Переход к аппаратным СКЗИ на стороне клиента

Решение проблемы:

1. **Полный отказ от программных СКЗИ для массового клиента**

2. **Переход к использованию аппаратных СКЗИ для всех криптографических преобразований**

Аппаратные СКЗИ: требования

1. Неизвлекаемое хранение ключей
2. Выполнение устройством всех криптографических функций:
   - электронная подпись
   - шифрование
   - хэш-функция
3. Наличие сертификата ФСБ РФ
4. Использование карточных чипов как защищенной платформы (CC EAL 5+)

Варианты аппаратных СКЗИ

1. Смарт-карты (ISO, NFC)
2. USB-токены
3. Bluetooth-токены
4. TrustScreen (USB, Bluetooth)

Аппаратные СКЗИ: наши разработки

БИФИТ разработал следующие решения:

1. **Высокопроизводительный USB-токен на базе 32-битного карточного чипа ST33**
2. **Высокопроизводительный TrustScreen**

Работают без программных СКЗИ на хосте

Скорость хэш-функции 1 Мбайт/сек

Аппаратные СКЗИ для пользователей ДБО

1. Отказ от программных компонент (для вычисления хэш-функции на хосте)

2. Расширение спектра аппаратных СКЗИ с функцией отображения документа

3. Поддержка мобильных платформ

Аппаратные СКЗИ для пользователей ДБО

1. Обязательность использования аппаратных СКЗИ массовым клиентом

2. Либерализация дистрибуции СКЗИ для массовых клиентов

конференция РусКрипто

Переход на аппаратные СКЗИ для массового пользователя

Спасибо за внимание!

Вопросы?

Станислав Шилов
shilov@bifit.com

BIFIT