# Безопасный интернет-банк: мифы и реальность.

*Павел Есаков*

*Компания CompuTel*

*Заместитель директора по продажам в финансовом секторе*

# Содержание

- Мифы о методах обеспечения безопасности интернет-банка
- Реальное положение дел с безопасностью интернет-банка
- Какие решения могут реально обеспечить безопасность
- Заключение

# Краеугольные камни системы безопасности

- Аутентификация и авторизация (кто Вы и каковы Ваши права)
- Целостность и неизменность информации
- Безотзывность отправленной информации
- Конфиденциальность

# Мифы о информационной безопасности

- ЭЦП  по ГОСТ - единственный законный метод подтверждения платежа (ФЗ-1)
- ЭЦП  – самое защищенное решение
- Только ЭЦП обеспечивает неизменность и безотзывность
- ЭЦП с неизвлекаемым ключом исключает возможность хищения средств клиента
- При использовании ЭЦП я вижу, что подписываю

# Мифы об информационной безопасности
(продолжение)

- Для подтверждения банковской операции необходима квалифицированная электронная подпись
- Одноразовый пароль по SMS –простое и  надежное средство как аутентификации клиента, так и подтверждения платежа
- Перехватить или изменить SMS невозможно
- SMS OTP –  система строгой (двухфакторной) аутентификации!
- Однокнопочные генераторы пароля всех вендоров работают одинаково

# Реальное положение дел с безопасностью

***Хакеры снимали деньги со счетов абонентов «большой тройки»***

*Киберпреступники заставляли чужие телефоны отправлять SMS на платный «короткий номер». Ущерб составил около 3 млн рублей*

*Крупный скандал на рынке сотовой связи — абоненты «МегаФона», «Билайна» и МТС стали жертвами киберпреступников, подключившихся к мобильникам десятков тысяч человек. Собрав из контрабандных запчастей базовую станцию сотовой связи — такие раньше использовались лишь спецслужбами для отслеживания переговоров, — хакеры отправляли на счет своей подставной фирмы SMS-сообщения, за которые абоненты платили от 30 до 80 рублей. Мошенников ловили около года — за это время ущерб сотовых компаний составил около 3 млн рублей.*

*Уникальную аферу на рынке операторов сотовой связи раскрыли оперативники управления «К» МВД и следователи Главного следственного управления столичной полиции. Сенсация в том, что раньше службы безопасности сотовиков утверждали, что злоумышленники не могут управлять чужими сотовыми. Однако 31-летний студент-недоучка Леонид Сидоров, ранее судимый за мошенничество, доказал, что это возможно.*

*— **Когда включенный мобильный телефон попадал в зону действия псевдостанции, злоумышленники могли делать с ним фактически что угодно, — говорит старший следователь по особо важным делам Главного следственного управления ГУ МВД по Москве Александр Попов**.*

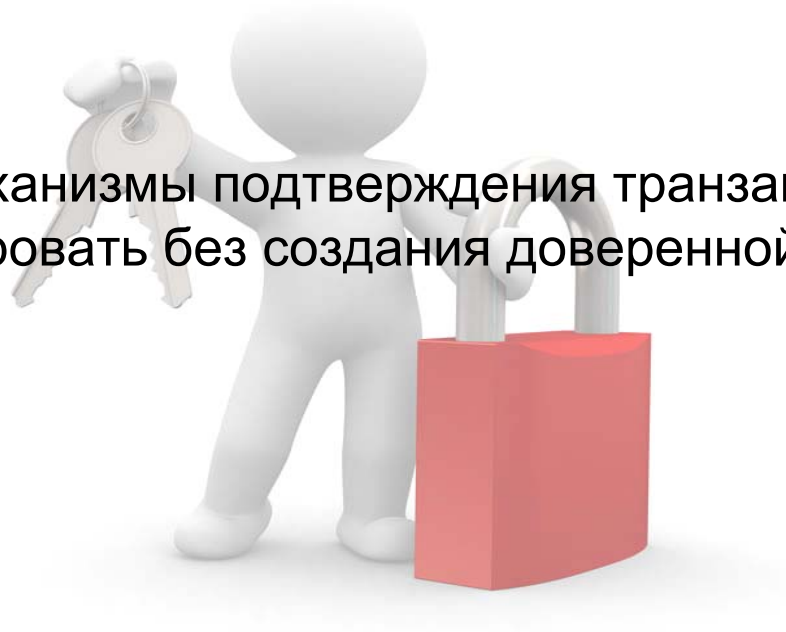
*Хакеры подключались к мобильным телефонам обычных абонентов и без их ведома отправляли SMS на «короткий номер». Принадлежал этот номер подставной фирме, специально созданной организаторами аферы. Как правило, стоимость одной SMS составляла от 28 до 80 рублей. Поступавшие на счета деньги обналичивались.*

*По словам Попова, «Соболь» останавливался для «захвата» мобильных телефонов у станций метро, ресторанов и других людных мест. Сначала не более чем на 5–10 минут. При этом при общении между собой они соблюдали все меры конспирации — называли друг друга вымышленными именами, общались преимущественно через Skype.*

# Безопасные решения – где они?

Есть два различных подхода к обеспечению безопасности:

- Создать доверенную среду на клиентском компьютере (это достаточно затратный и неудобный вариант)



- Использовать механизмы подтверждения транзакций, которые могут функционировать без создания доверенной среды

# Средства аутентификации на базе симметричных алгоритмов:

## Преимущества:

- Не требуют какого-либо ПО на стороне клиента – тонкий клиент
- Могут быть использованы по любым каналам ДБО
- Обеспечивают защиту транзакций и безотзывность транзакций
- Полностью соответствуют требованиям 63-ФЗ к средствам усиленной электронной подписи
- Достаточно портативны и сравнительно недороги

## Недостатки:

- Требуют повышенного внимания к защите ключей на стороне банка
- Для защиты транзакций необходим ввод (как правило, ручной) информации о транзакции

## На стороне клиента

- Автономные токены на базе симметричных криптоалгоритмов с PIN клавиатурой (желательно на основе time-based решений)

- Персональные EMV CAP ридеры (автономные и подключаемые)



# Требования к серверу аутентификации

**Сервер должен обеспечивать**

- Поддержку всех имеющихся технологий: (PKI, EMV CAP, автономные токены, биометрия)
- Работу со средствами аутентификации различных вендоров
- Использование специализированных криптографических модулей для надежного хранения ключей
- Ведение защищенных журналов аутентификационных событий

# Заключение

**Современные аутентификационные решения позволяют:**

- Создать безопасный интернет-банк, работающий в любом месте даже при отсутствии доверенной среды
- Найти правильный компромисс между удобством использования, безопасностью и общей стоимостью владения
- Провести сегментацию клиентов в зависимости от их потребностей
- Использовать средства аутентификации для новых каналов ДБО

**Спасибо за внимание!**

**Вопросы?**