CNews FORUM 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

ЧатБанк от ПАО "Совкомбанк"

практический опыт создания Интернет-Банка с самым большим в России количеством элементов безопасности

Андрей Бухтияров
Основатель и главный разработчик
ЧатБанк от ПАО "Совкомбанк"

Что защищаем ?

1\ Сессию

2\ Передачу данных

3\ Электронную подпись

СОВКОМБАНК

Сессия

1\ Единый API для всех устройств WEB, iOS, Android;

2\ Blockchain архитектура для быстрых входов на iOS и Android;

3\ Соблюдение owasp.org: https, cookie-token, url-token, xframe-deny, crypto-random и др;

4\ Ограничения: время активности, время непрерывной сессии, один клиент - одна сессия, количество ошибок = блокировка и др;

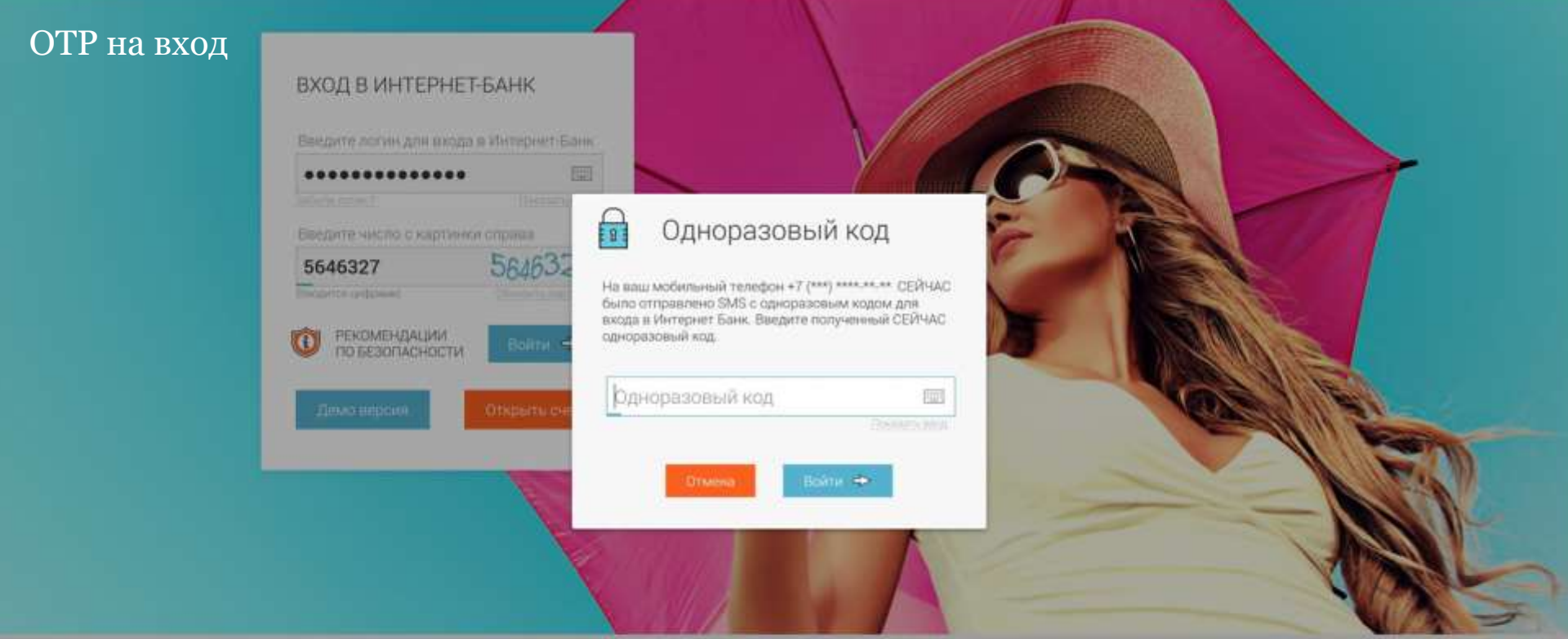
5\ One-touch-session: сессия данных живет до первого прикосновения;

6\ Deep-session: глубокая сессия = единая цепочка сессий client-fe & fe-be на клиентских данных;

7\ Раздельный лог по составляющим действия: начало, отправка SMS, получение SMS и тд;

8\ OTP на вход;

OTP на вход



TOP10 BUSINESS INTERNET BANKING RANK 2017

4-е место

Business Internet Banking Rank 2017

Самый эффективный Интернет Банк для малого бизнеса

TOP10 INTERNET BANKING RANK 2017

10-е место

Internet Banking Rank 2017

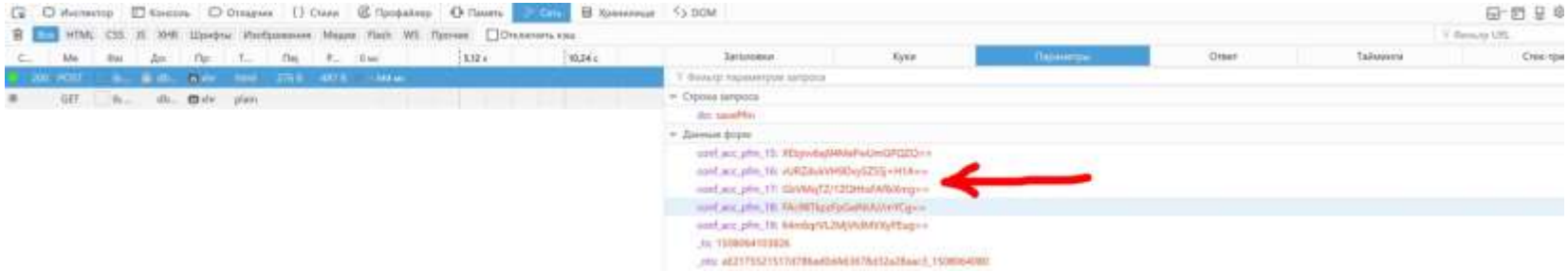
Самый эффективный Интернет Банк для частных лиц

СОВКОМБАНК

Передача данных

1\ Отдельная двухшаговая сессия на каждое подписание, подписание данных которые уже на сервере, а не передача подписи с данными;

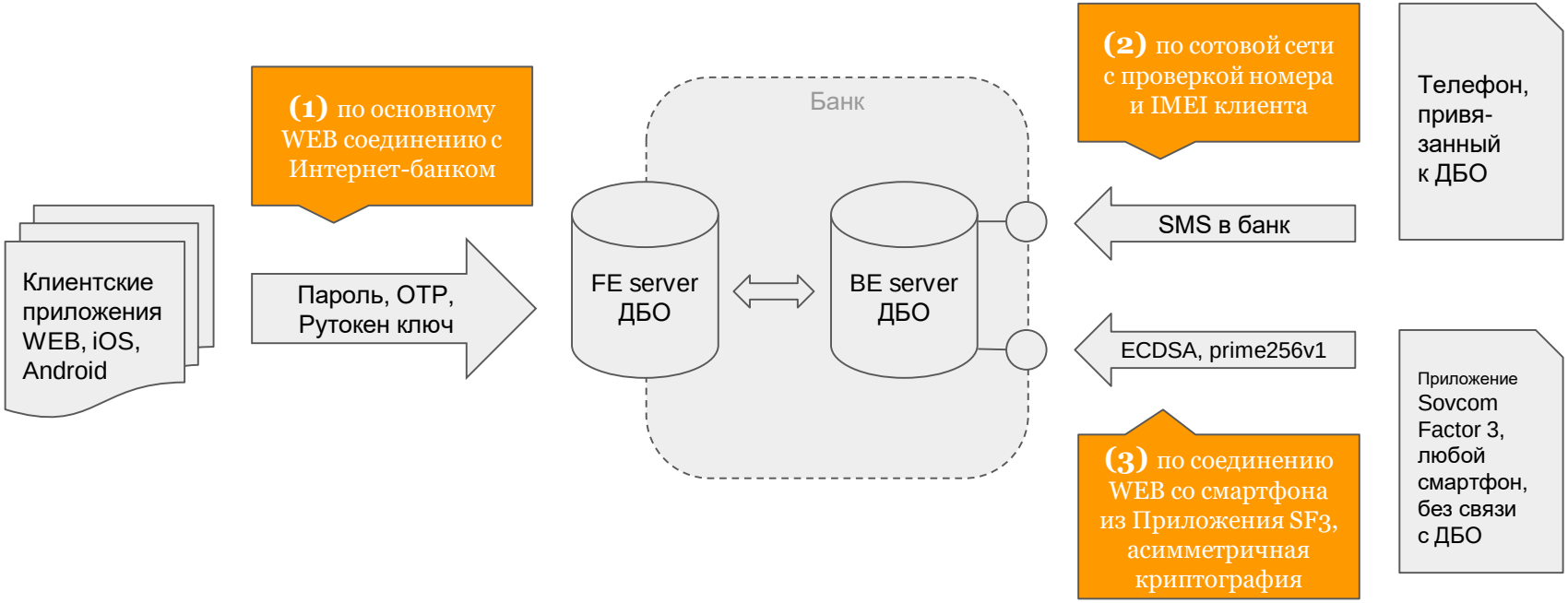
2\ Encrypted POST: дополнительное автоматическое шифрование форм AES криптографией, без обмена ключом по сети;



СОВКОМБАНК

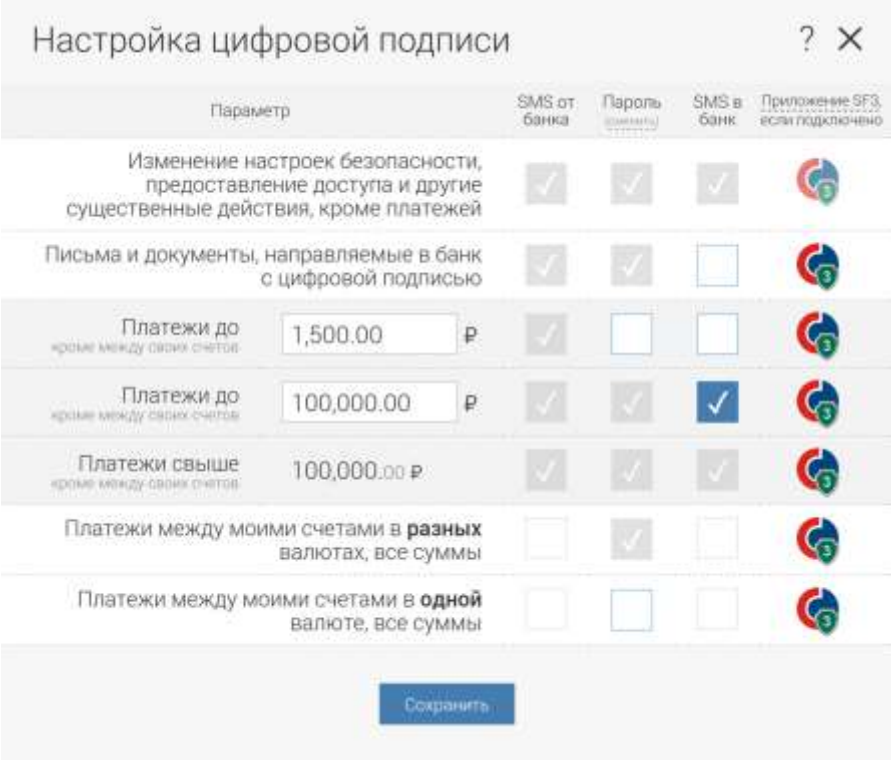
Электронная подпись: 3 фактора безопасности

Фактор = независимый канал доставки подтверждения подписи в банк



СОВКОМБАНК

Электронная подпись: настройки



СОВКОМБАНК

Французский сценарий

или для чего нужен пароль для платежей

СЦЕНАРИЙ ЗЛОУМЫШЛЕННИКА:

1\ Отследить человека который зашел в ИБ с телефона, обычно в кафе или ТЦ;

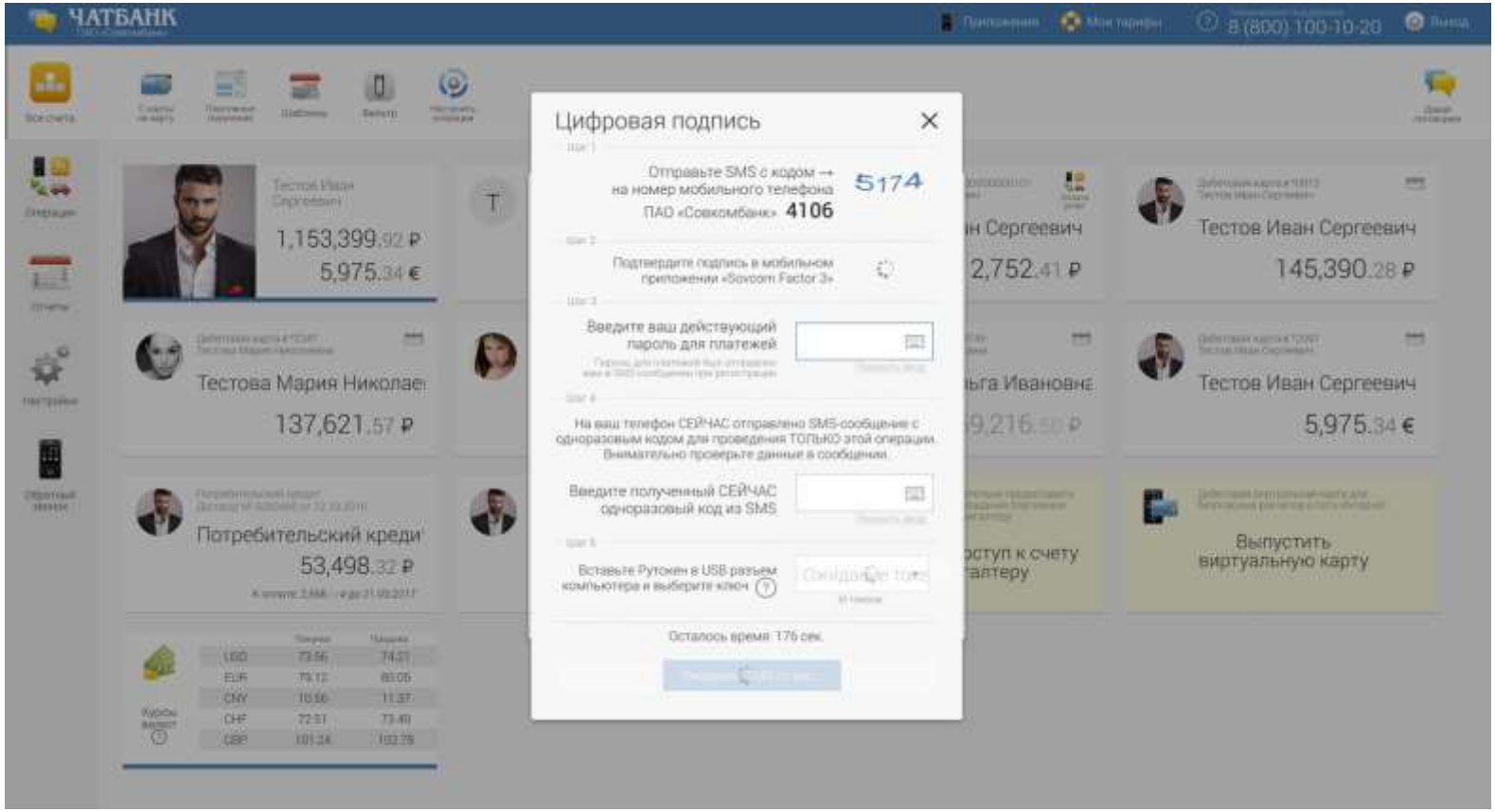
2\ Вырвать из рук телефон и убежать;

3\ Произвести платеж, который подтверждается через Да-Нет, SMS или Push;

4\ Вернуть телефон жертве, извиниться, пообещать прислать деньги позже;

КТО УЯЗВИМ: клиенты банков, где платеж в мобильном банке подтверждается через Да-Нет, SMS или Push

Электронная подпись: все элементы включены



СОВКОМБАНК