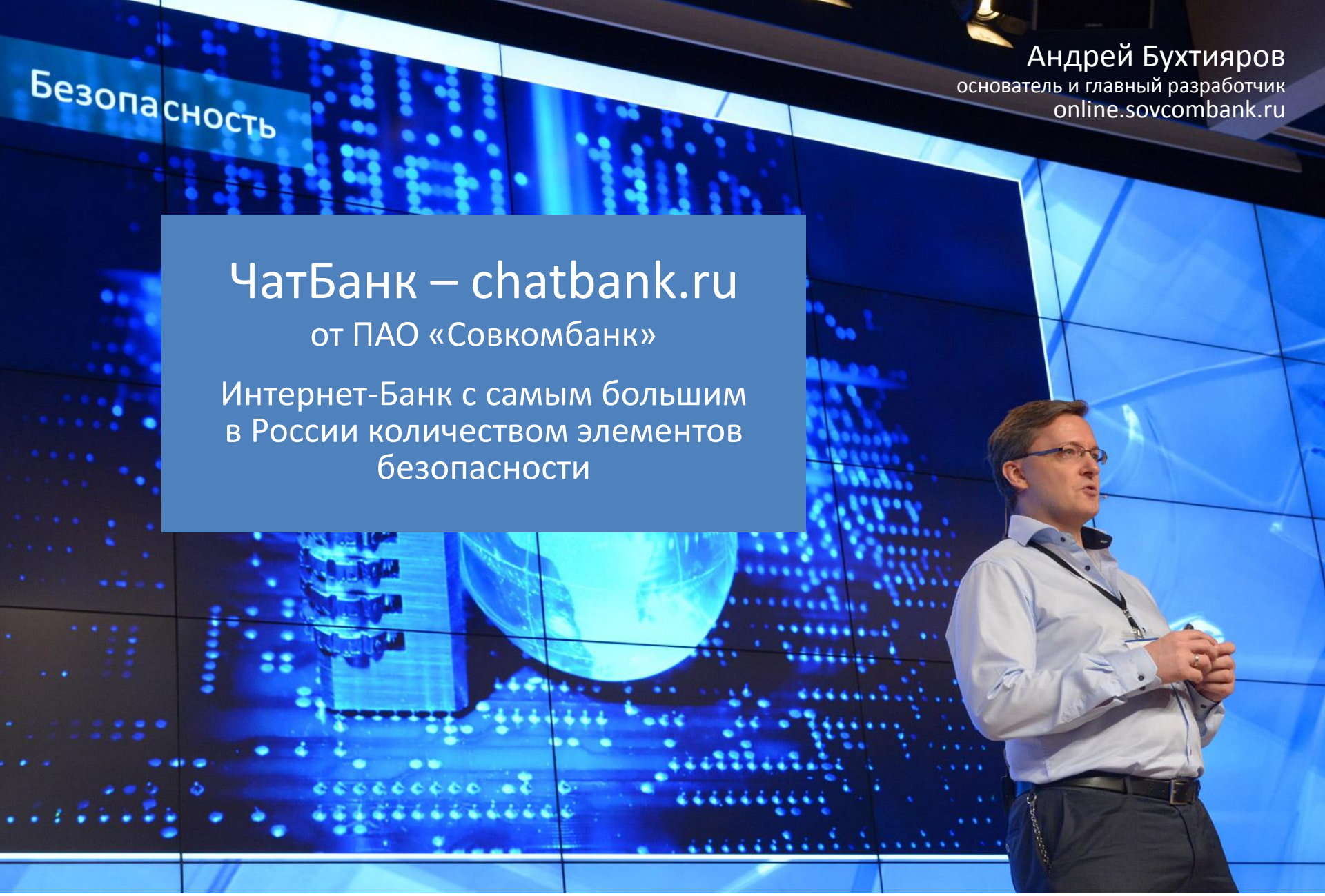
Андрей Бухтияров
основатель и главный разработчик
online.sovcombank.ru



ЧатБанк – chatbank.ru

от ПАО «Совкомбанк»

Интернет-Банк с самым большим в России количеством элементов безопасности

СОВКОМБАНК

ЧАТБАНК

Особенности создания и эксплуатации Интернет-Банка ЧатБанк

Команда разработчиков с опытом создания нескольких банков

(Тиньков, Интерактивный, ЦТБ-Банк)

Собственная платформа, включая среду разработки

(все, язык интерфейса, репозиторий, компилятор, сессии, криптование)

Постановка задач и разработка архитектуры – «от сценария»

Разработка для эксплуатации – «всегда в агрессивной среде»

Своя архитектура: механизм сессий, электронная подпись, архитектура связанных логов и др.

Много-компонентная система безопасности

СОВКОМБАНК

8 (800) 100-10-20

ВХОД В ИНТЕРНЕТ-БАНК

Введите логин для входа в Интернет-Банк

Логин

Забыли логин ? Показать ввод

Введите число с картинки справа

Код с картинки → 0977674

(Вводится цифрами) Обновить картинку

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

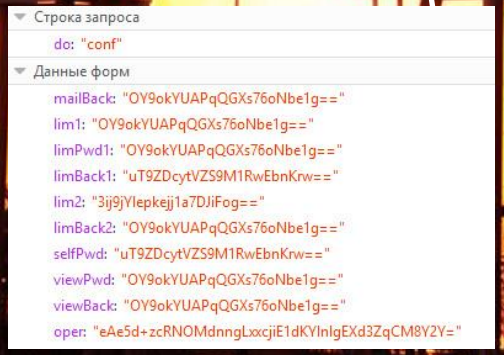
Войти →

Стать клиентом банка, введите только номер мобильного телефона

Попробовать Интернет-Банк без ввода телефона и регистрации

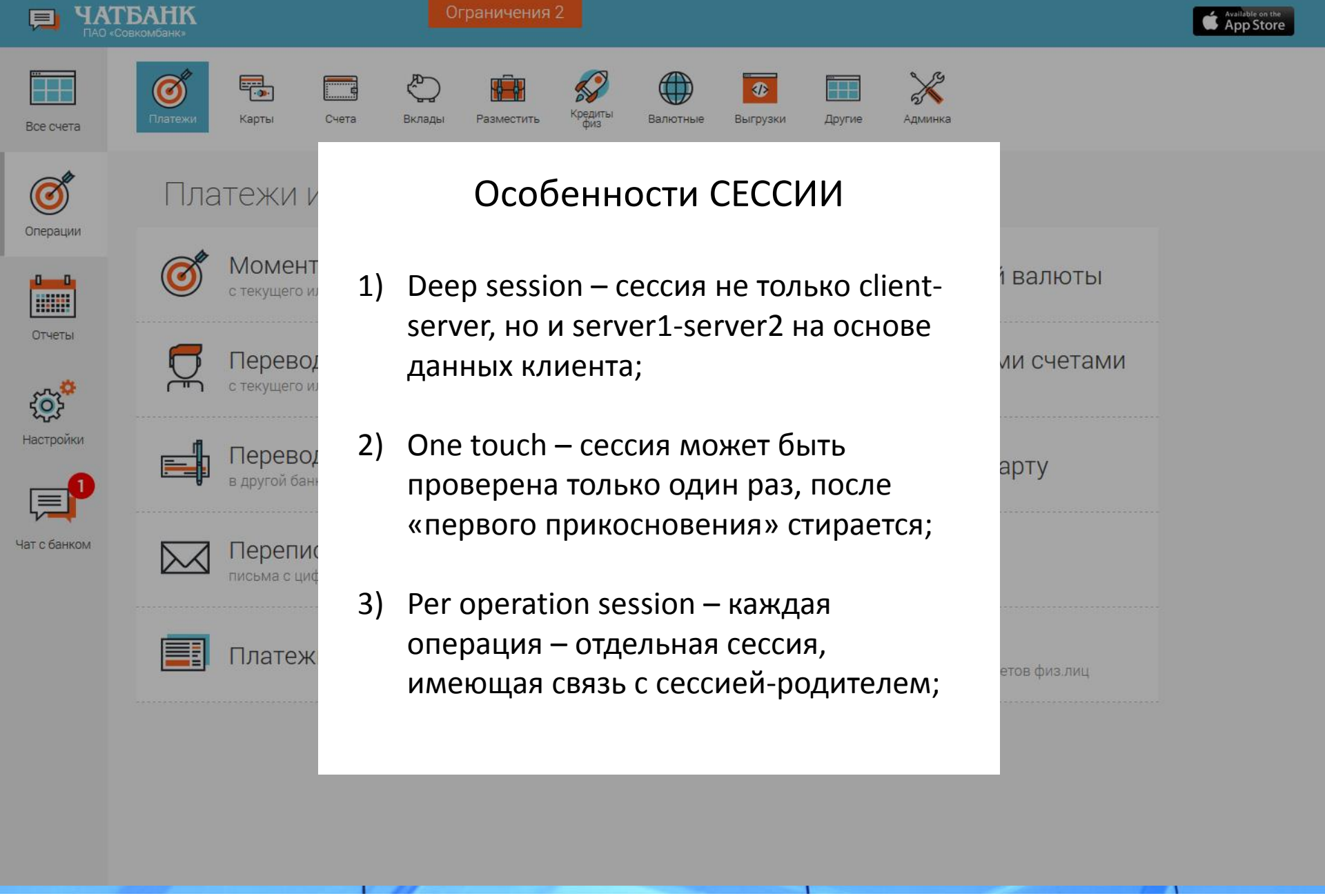
Особенности безопасного ВХОДА

1) Изменяемый логин + СМС на вход;
2) Раздельный токен сессии (owasp.org);
3) Необратимое шифрование SHA-512 при передаче ключей;
4) Шифрование форм криптографией AES-128 без обмена ключами;
5) Прочие рекомендации owasp.org (https, x-frame deny и тд);



СОВКОМБАНК

ЧАТБАНК

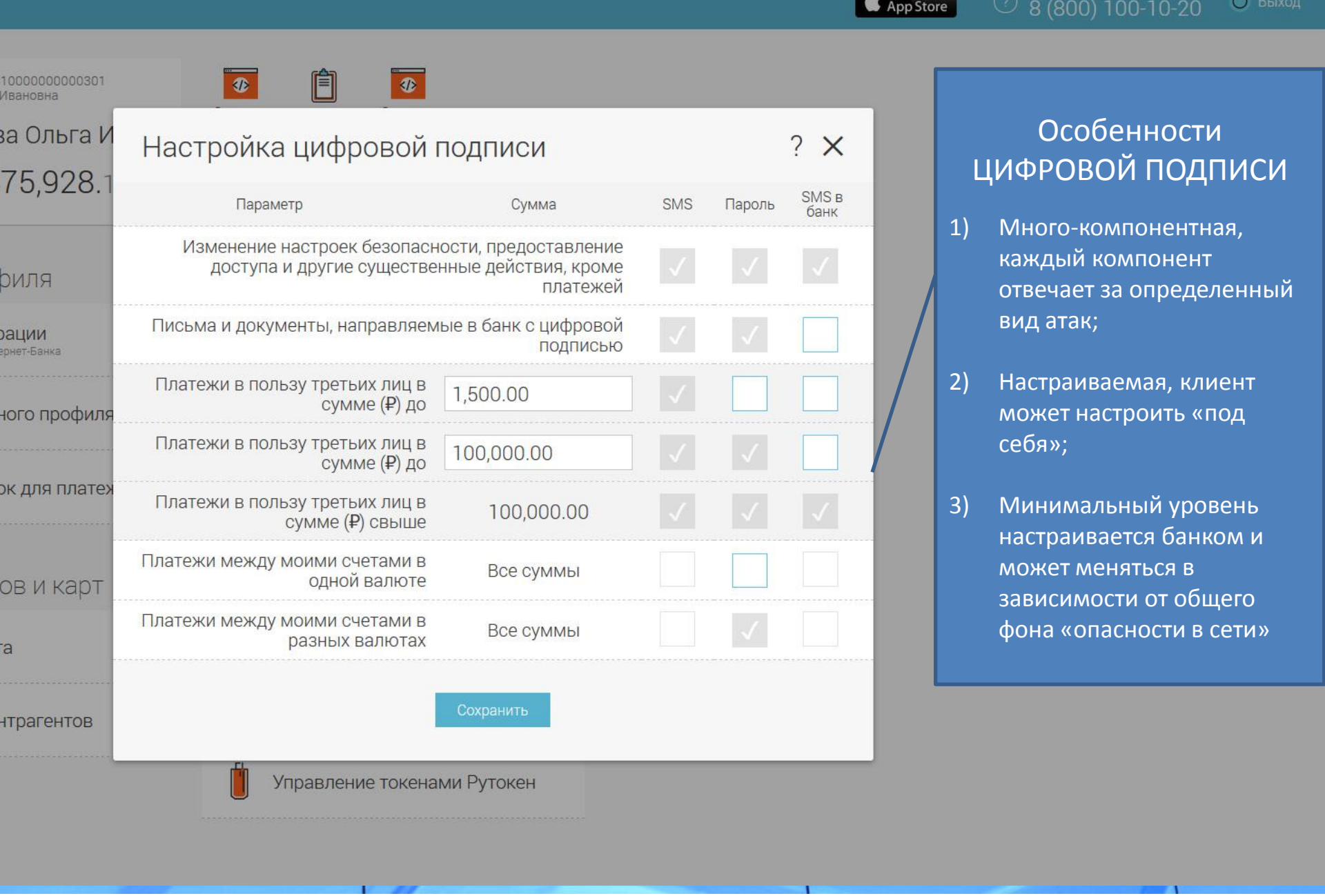


Особенности СЕССИИ

1) Deep session – сессия не только client-server, но и server1-server2 на основе данных клиента;

2) One touch – сессия может быть проверена только один раз, после «первого прикосновения» стирается;

3) Per operation session – каждая операция – отдельная сессия, имеющая связь с сессией-родителем;



Особенности ЦИФРОВОЙ ПОДПИСИ

1) Много-компонентная, каждый компонент отвечает за определенный вид атак;

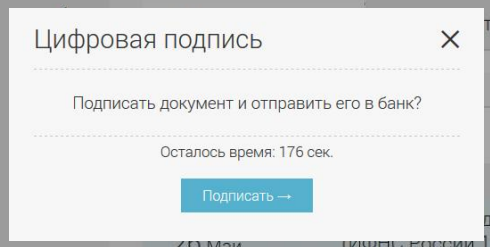
2) Настраиваемая, клиент может настроить «под себя»;

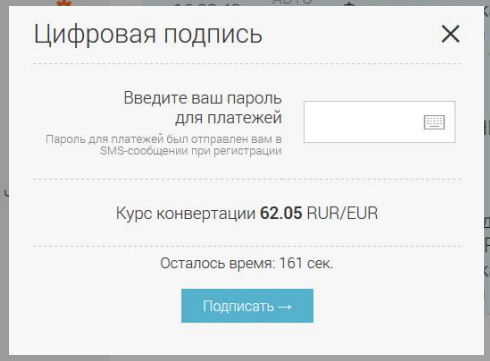
3) Минимальный уровень настраивается банком и может меняться в зависимости от общего фона «опасности в сети»

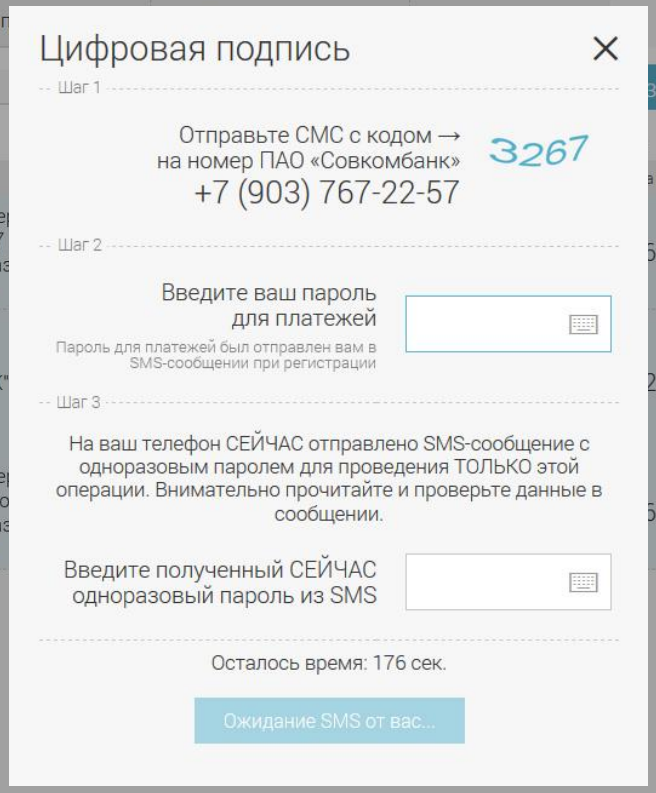
СОВКОМБАНК

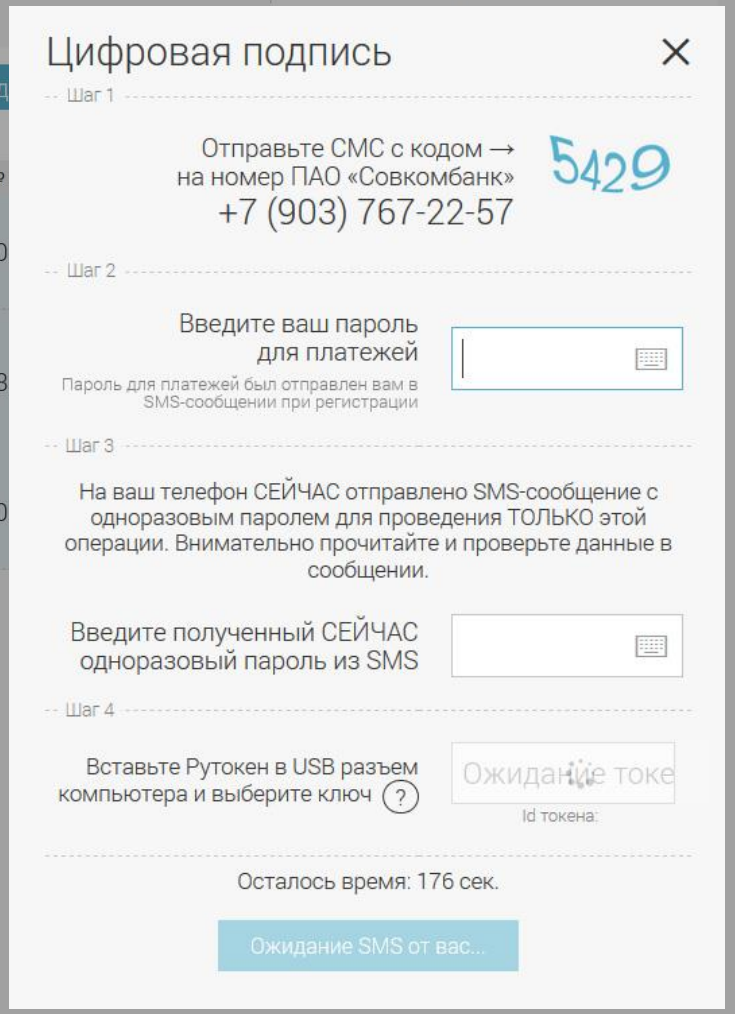
ЧАТБАНК

Простая → Сложная → Максимальная





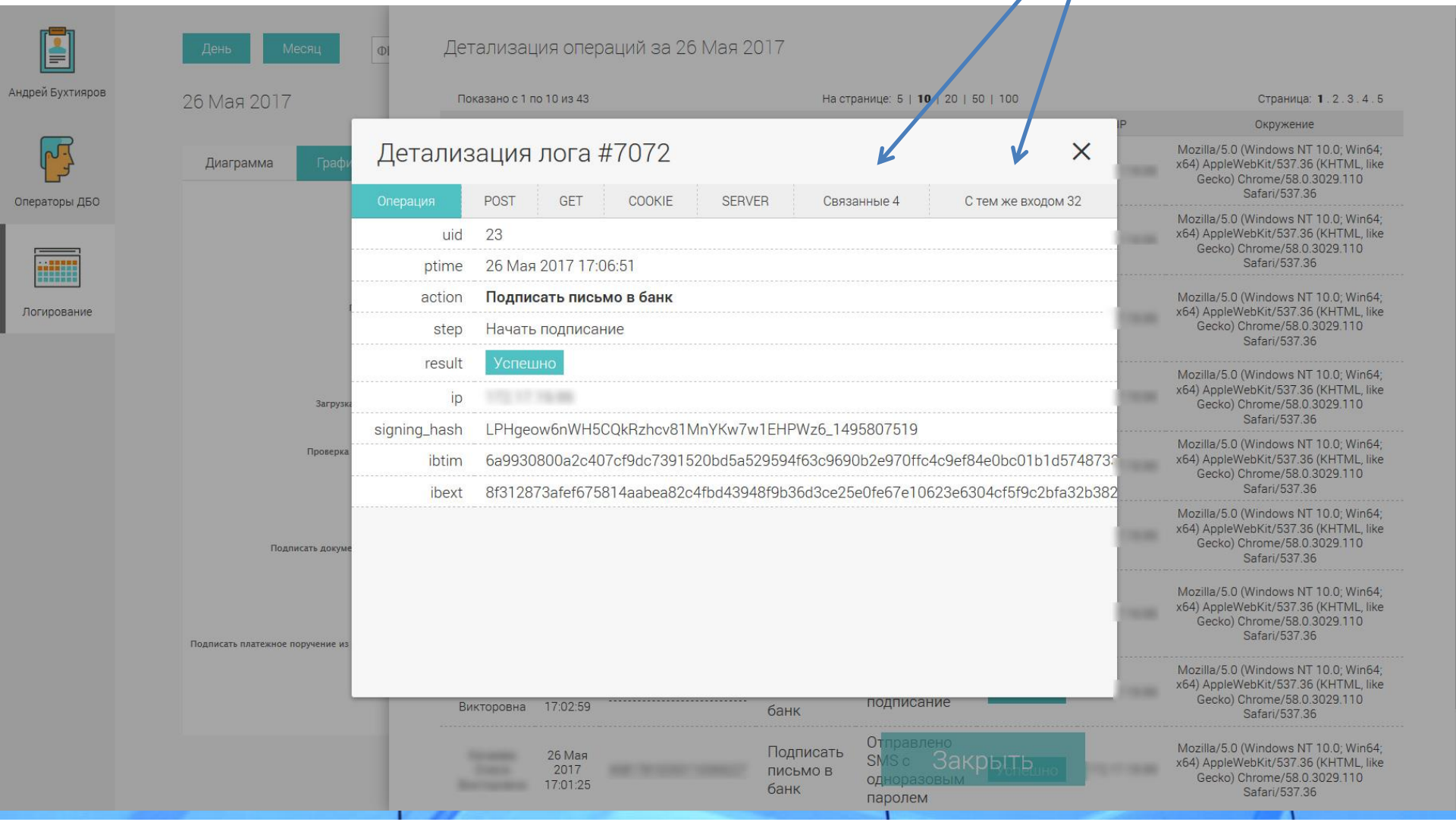




СОВКОМБАНК

ЧАТБАНК

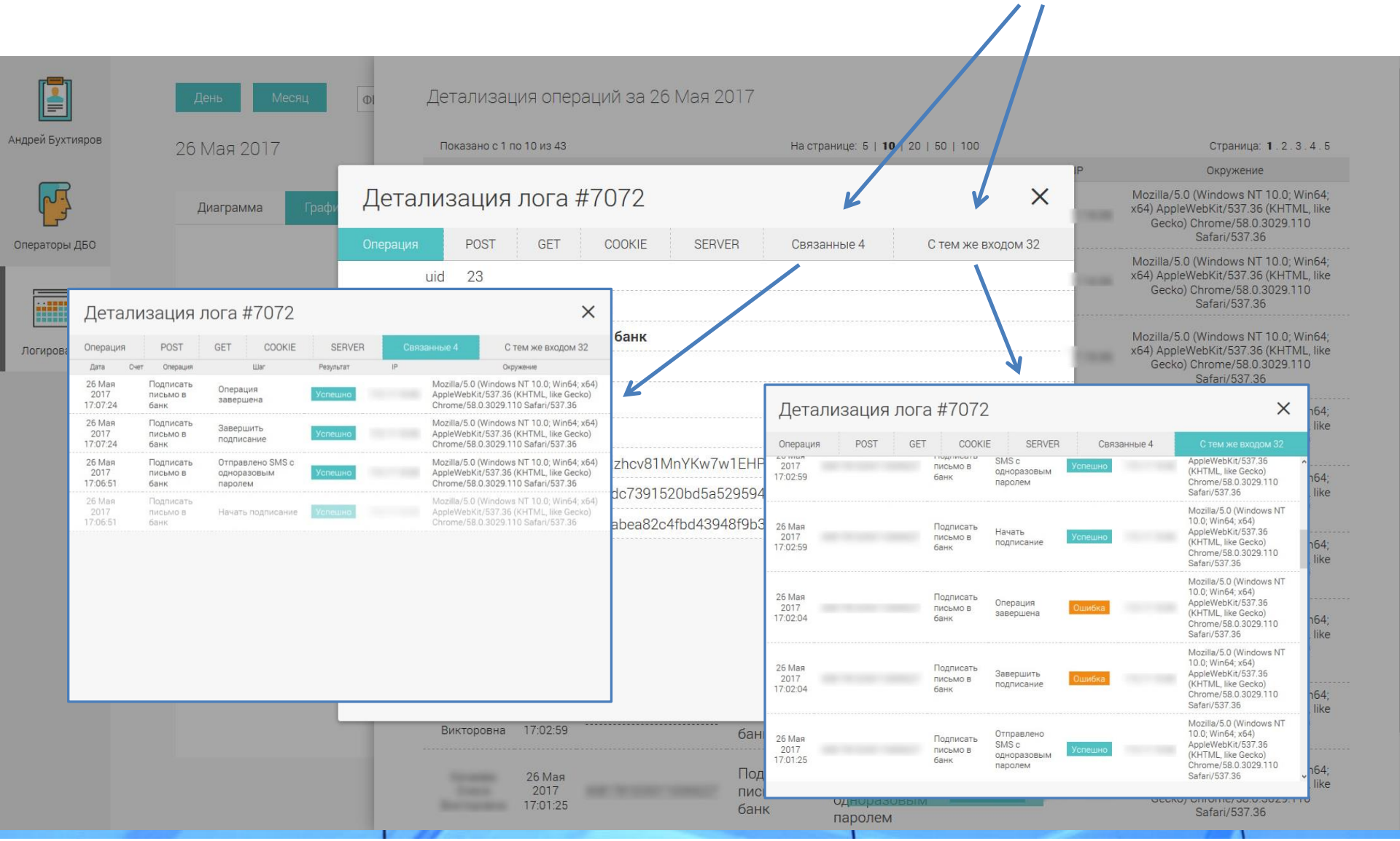
Собственная архитектура логирования: «связанные логи»



СОВКОМБАНК

ЧАТБАНК

Собственная архитектура логирования: «связанные логи»



СОВКОМБАНК

ЧАТБАНК

Удобство ← ? → Безопасность

1) Цель хакеров – деньги, а не PR. Выбирая между банком, где платежи проводятся с одним SMS и банком где 40 степеней защиты, хакеры выбирают где проще, где один SMS.

2) Распространенная иллюзия банкиров: «Разумный баланс удобства и безопасности». Такого баланса не существует. Банк либо защищен либо уязвим. Для хакера такой баланс означает «незащищенный банк».

3) Аргументы для маркетинга:
   - ожидания бедного клиента от банка: безопасность, ценовая составляющая, наличие сервисов, удобность;
   - ожидания богатого клиента от банка: безопасность, наличие сервисов, удобность;
   Обе категории боятся потерять деньги, одна так как их мало, вторая так как их много :)

4) Вывод: безопасность Интернет-Банка всегда будет на первом месте.

Андрей Бухтияров

основатель и главный разработчик

online.sovcombank.ru

СОВКОМБАНК

ЧАТБАНК