

Безопасность

Андрей Бухтияров  
основатель и главный разработчик  
[online.sovcombank.ru](http://online.sovcombank.ru)

ЧатБанк – [chatbank.ru](http://chatbank.ru)

от ПАО «Совкомбанк»

Интернет-Банк с самым большим  
в России количеством элементов  
безопасности



# 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

## 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);

```
Строка запроса
do: "conf"

Данные форм
mailBack: "OY9okYUAPqQGxs76oNbe1g=="
lim1: "OY9okYUAPqQGxs76oNbe1g=="
limPwd1: "OY9okYUAPqQGxs76oNbe1g=="
limBack1: "uT9ZDcytVZS9M1RwEbnKrw=="
lim2: "3ij9YIepkejj1a7DJIIFog=="
limBack2: "OY9okYUAPqQGxs76oNbe1g=="
selfPwd: "uT9ZDcytVZS9M1RwEbnKrw=="
viewPwd: "OY9okYUAPqQGxs76oNbe1g=="
viewBack: "OY9okYUAPqQGxs76oNbe1g=="
oper: "eAe5d+zcRNOMdnngLxxcjiE1dKYInlgEXd3ZqCM8Y2Y="
```



## 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;

## Настройка цифровой подписи



Параметр	Сумма	SMS	Пароль	SMS в банк
Изменение настроек безопасности, предоставление доступа и другие существенные действия, кроме платежей		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Письма и документы, направляемые в банк с цифровой подписью		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Платежи в пользу третьих лиц в сумме (₽) до	<input type="text" value="1,500.00"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Платежи в пользу третьих лиц в сумме (₽) до	<input type="text" value="100,000.00"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Платежи в пользу третьих лиц в сумме (₽) свыше	100,000.00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Платежи между моими счетами в одной валюте	Все суммы	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Платежи между моими счетами в разных валютах	Все суммы	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Сохранить"/>				



Управление токенами Рутокен

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»

×

Подписать документ и отправить его в банк?

Осталось время: 176 сек.

×

Введите ваш пароль  
для платежей

Пароль для платежей был отправлен вам в SMS-сообщении при регистрации

Курс конвертации **62.05** RUR/EUR

Осталось время: 161 сек.

×

-- Шаг 1

Отправте СМС с кодом →  
на номер ПАО «Совкомбанк»  
+7 (903) 767-22-57

3267

→ Шаг 2

Введите ваш пароль  
для платежей

Пароль для платежей был отправлен вам в SMS-сообщении при регистрации

-- Шаг 3

На ваш телефон СЕЙЧАС отправлено SMS-сообщение с одноразовым паролем для проведения ТОЛЬКО этой операции. Внимательно прочитайте и проверьте данные в сообщении.

Введите полученный СЕЙЧАС  
одноразовый пароль из SMS

Осталось время: 176 сек.

×

Mar 1

Отправьте СМС с кодом →  
на номер ПАО «Совкомбанк»  
**+7 (903) 767-22-57**

5429

-- Mar 2

Введите ваш пароль  
для платежей

Пароль для платежей был отправлен вам в SMS-сообщении при регистрации

- - Шаг 3

На ваш телефон СЕЙЧАС отправлено SMS-сообщение с одноразовым паролем для проведения ТОЛЬКО этой операции. Внимательно прочитайте и проверьте данные в сообщении.

Введите полученный СЕЙЧАС  
одноразовый пароль из SMS

-- War 4

Вставьте Рутокен в USB разъем компьютера и выберите ключ (?)

Ожидание токе

Id токена

Осталось время: 176 сек.

# Собственная архитектура логирования: «связанные логи»

Детализация операций за 26 Мая 2017

Показано с 1 по 10 из 43

На странице: 5 | 10 | 20 | 50 | 100

Страница: 1 | 2 | 3 | 4 | 5

Окружение

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Детализация лога #7072

Операция	POST	GET	COOKIE	SERVER	Связанные 4	С тем же входом 32
uid	23					
ptime	26 Мая 2017 17:06:51					
action	Подписать письмо в банк					
step	Начать подписание					
result	Успешно					
ip						
signing_hash	LPHgeow6nWH5CQkRzhcv81MnYKw7w1EHPWz6_1495807519					
ibtim	6a9930800a2c407cf9dc7391520bd5a529594f63c9690b2e970ffc4c9ef84e0bc01b1d5748735					
ibext	8f312873afef675814aabea82c4fbd43948f9b36d3ce25e0fe67e10623e6304cf5f9c2bfa32b382					

Викторовна 17:02:59

банк

подписание

Отправлено SMS с одноразовым паролем

Закреть

Успешно

Подписать письмо в банк

26 Мая 2017 17:01:25

# Собственная архитектура логирования: «связанные логи»

Детализация операций за 26 Мая 2017

Показано с 1 по 10 из 43

На странице: 5 | 10 | 20 | 50 | 100

Страница: 1 | 2 | 3 | 4 | 5

Окружение

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Детализация лог #7072

Операция POST GET COOKIE SERVER Связанные 4 С тем же входом 32

uid 23

банк

Детализация лог #7072

Дата	Счет	Операция	Шаг	Результат	IP	Окружение
26 Мая 2017 17:07:24		Подписать письмо в банк	Операция завершена	Успешно		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
26 Мая 2017 17:07:24		Подписать письмо в банк	Завершить подписание	Успешно		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
26 Мая 2017 17:06:51		Подписать письмо в банк	Отправлено SMS с одноразовым паролем	Успешно		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
26 Мая 2017 17:06:51		Подписать письмо в банк	Начать подписание	Успешно		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Детализация лог #7072

Операция	POST	GET	COOKIE	SERVER	Связанные 4	С тем же входом 32
26 Мая 2017 17:02:59			Подписать письмо в банк	SMS с одноразовым паролем	Успешно	AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
26 Мая 2017 17:02:59			Подписать письмо в банк	Начать подписание	Успешно	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
26 Мая 2017 17:02:04			Подписать письмо в банк	Операция завершена	Ошибка	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
26 Мая 2017 17:02:04			Подписать письмо в банк	Завершить подписание	Ошибка	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
26 Мая 2017 17:01:25			Подписать письмо в банк	Отправлено SMS с одноразовым паролем	Успешно	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

# 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](http://online.sovcombank.ru)

