

Уязвимости безналичных платежей на транспорте

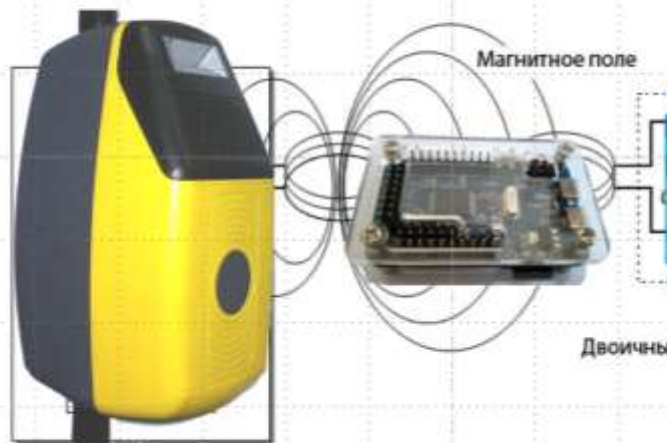
**КАК ИЗБЕЖАТЬ И КАК
ЗАЩИТИТЬСЯ**

ЛЕВ ДЕНИСОВ

Эксперт в сфере АСОП

Flashback из 2015

«Подсматриваем» протокол



Как клонировать
транспортную карту за 3
минуты

Делаем «клон»

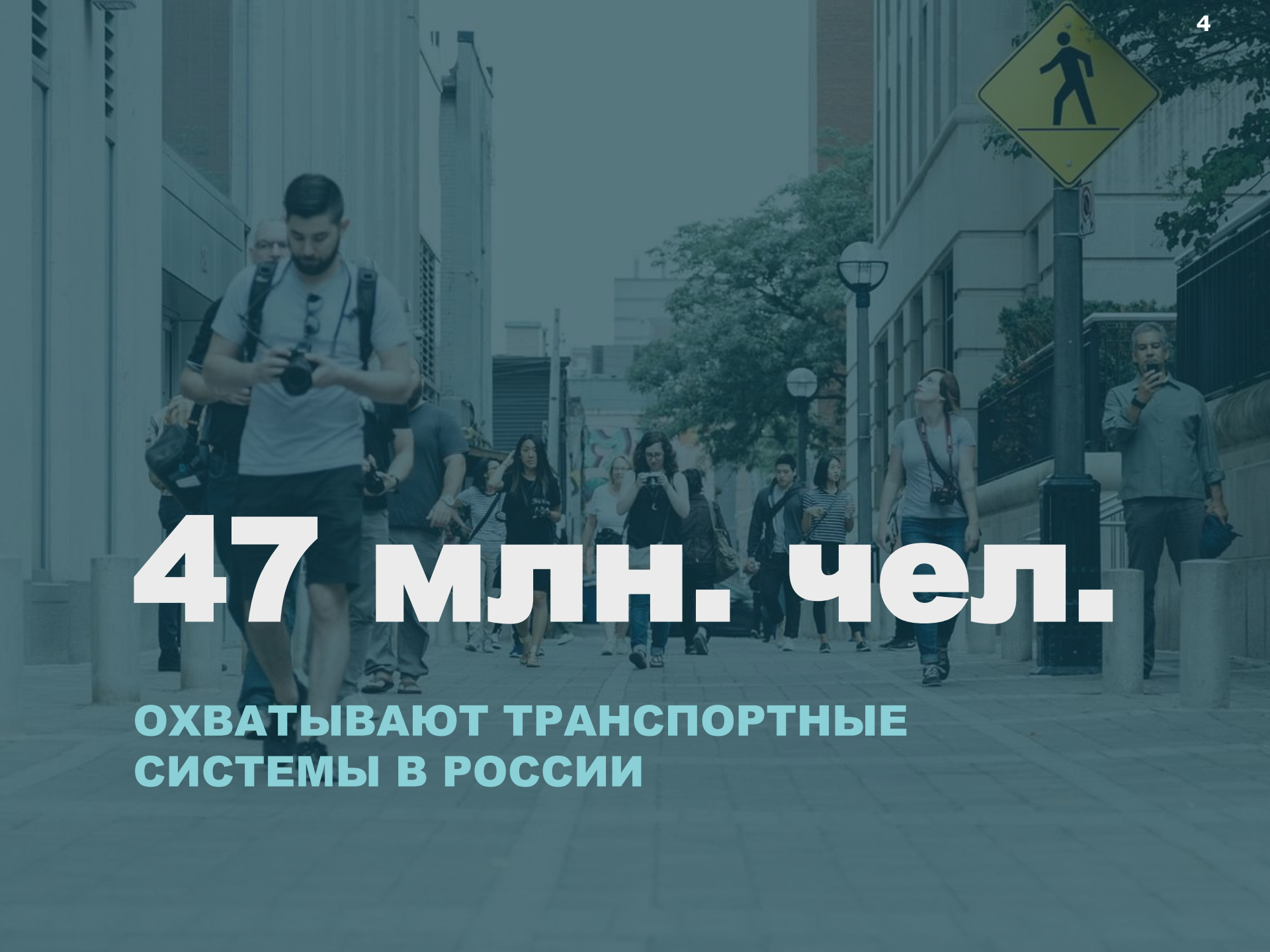


Изменилось ли что-либо за год? Нет

99%

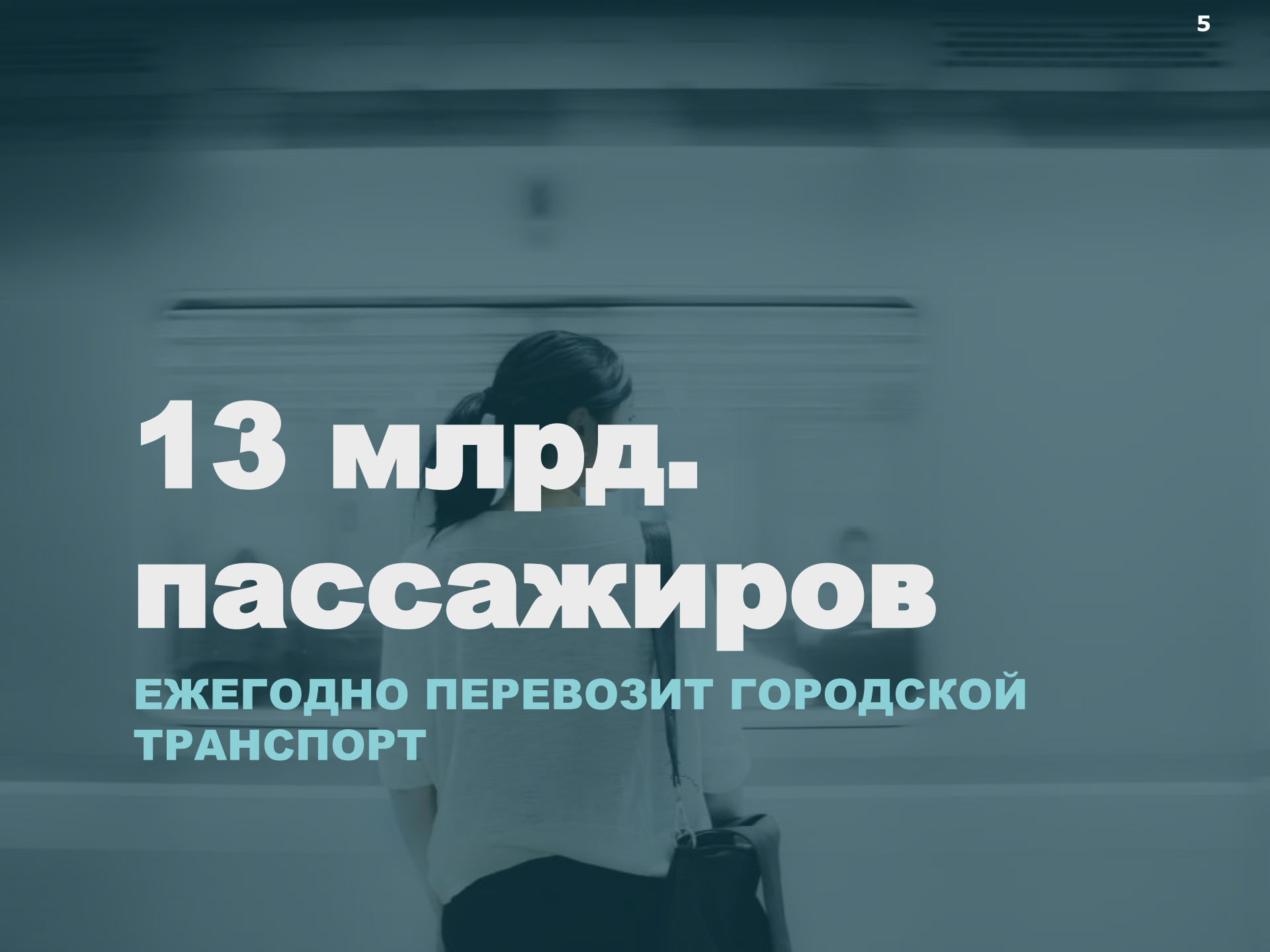


**ТРАНСПОРТНЫХ СИСТЕМ (АСОП) В
РОССИИ УЯЗВИМЫ**



47 млн. чел.

ОХВАТЫВАЮТ ТРАНСПОРТНЫЕ
СИСТЕМЫ В РОССИИ

A woman with dark hair in a ponytail, wearing a white t-shirt and dark pants, stands with her back to the camera, looking towards a blurred train. She is carrying a black bag. The background is a blurred train track with a train passing by.

13 млрд. пассажиров

ЕЖЕГОДНО ПЕРЕВОЗИТ ГОРОДСКОЙ
ТРАНСПОРТ

The background of the slide features a close-up, slightly blurred image of several Russian 500 ruble banknotes. The notes are fanned out, showing their intricate designs, including the word 'КАЗНАЧЕЙСТВО' (Treasury) and the denomination '500'. The overall color palette is a muted teal or blue-green.

260 млрд. рублей

**ЕЖЕГОДНЫЙ ОБЪЕМ ПЛАТЕЖЕЙ НА
ТРАНСПОРТЕ**

Каков % фрода?

Неизвестно, но

Даже при 0,1% это **260 млн. руб.**



В 2009 г. «В Москве вскрыта многомиллионная афера с фальшивыми билетами на проезд в метро. Мошенники действовали с размахом - ущерб от их деятельности оценивается в **150 миллионов рублей.** »

Как взламывают

«Безопасность Mifare Classic равна нулю»



Полный реинжиниринг
криптопротокола

Уязвимость чипа Mifare
Classic: “неслучайный”
датчик случайных
чисел



Mifare Plus – не панацея*

***Если использовать в режиме Mifare Classic**

Mifare Plus – это чип, который для обратной совместимости поддерживает режим Mifare Classic.

Угадайте, в каком режиме большинство использует Mifare Plus?

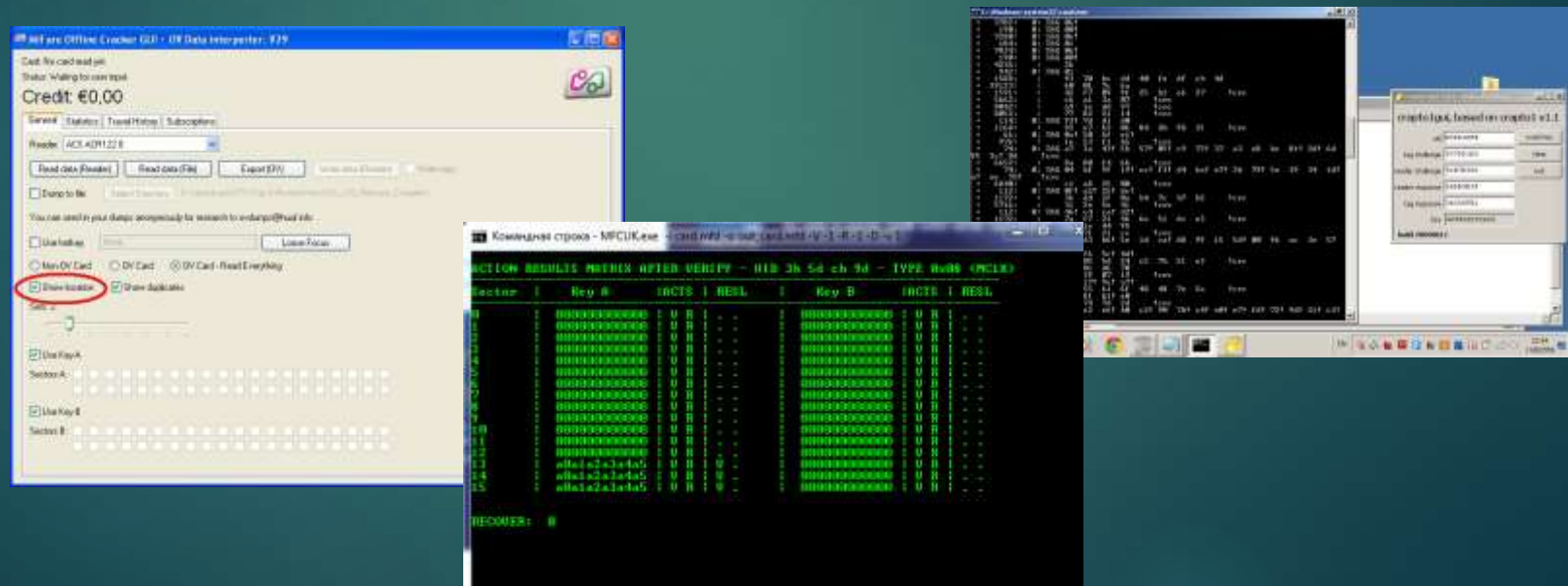
“Забыли” написать, что в режиме Mifare Classic

В Санкт-Петербурге в целях исключения потерь транспортных предприятий от использования поддельных проездных билетов принято решение об оформлении ПБ электронный кошелек «Подорожник» на электронные карты, поддерживающие современную защищенную технологию бесконтактной передачи данных (Mifare Plus).

Новая уязвимость Mifare Plus

Обнаружена в конце 2015 г.

Позволяет использовать card-only-attack для получения ключей

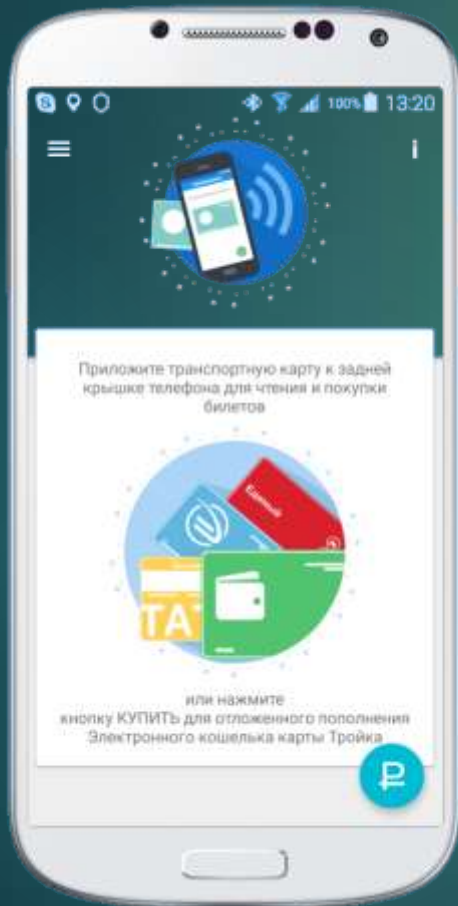


Про взлом «Тройки»

«Хакер научился бесплатно ездить на метро, взломав «Тройку» » (из СМИ)



Что произошло на самом деле



Взломали приложение «Банка Москвы»

Ключи передавались по SSL в открытом (!) виде

Классическая MITM-атака - и ключи известны



К чему все это ведет

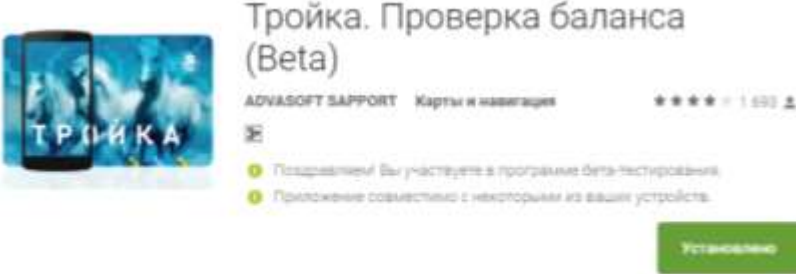


«"Тройка" и "Стрелка" теперь доступны в одной карте» (из СМИ)

«Ура»! Теперь стали известны и ключи от «Стрелки»

Кто следующий? С кем будем объединяться? Чьи ключи еще не известны хакерам?

Есть ли от этого польза?



Тройка. Проверка баланса (Beta)
ADVASOFT SUPPORT Карты и навигация ★★★★★ 1 690

Поздравляем! Вы участвуете в программе бета-тестирования.
Приложение совместимо с некоторыми из ваших устройств.

Установлено

Проверка баланса электронного кошелька "Тройка"

Примоките карту к обратной стороне Вашего смартфона

Проверка баланса электронного кошелька "Тройка"

№ 0000 882 142

Ваш баланс
20 руб.

Дата последней оплаты:
26.12.2014 г.

Хватит ли средств на карте "Тройка" для оплаты проезда? Узнайте мгновенно в любое удобное для Вас время, в любом удобном месте.
Для проверки баланса доступ в интернет НЕ требуется.

Самое долгожданное приложение теперь в Вашем смартфоне!

Можно мгновенно проверять баланс карты с помощью неофициальных приложений

Как защититься

Как делают сейчас

Меняют формат данных на карте

Меняют способ генерации ЭП

От клонирования это
НЕ СПАСАЕТ







FAIL

MAXIMUM SECURITY ENTRANCE



Почему никого это не волнует

Заказчики – не знают

Что-то слышали

**Поэтому покупают самые дорогие карты и
используют самым небезопасным образом**

Поставщики – не знают/не хотят



Взлом Mifare Classic (SL1)

По мнению
разработчиков АСОП



На самом деле



Что реально можно (было бы) сделать

В существующих проектах – постепенная миграция

Диверсификация ключей

Доработка валидаторов

Не так сложно, как кажется

В новых проектах – изначально делать на более защищенных протоколах

Делать соответствующую **независимую** экспертизу

Не использовать **устаревшие** ТЗ

Нужна ли шапочка из фольги?



Пока еще нет – но для карты лишним не будет



Лайфхак: если нет специального RFID-кошелька, то кладите в обычный кошелек хотя бы 2 бесконтактные карты (это убережет от возможного «сниффинга»)

Спасибо за внимание

Лев Денисов

ask@afc.guru

+7 903 231 8296

