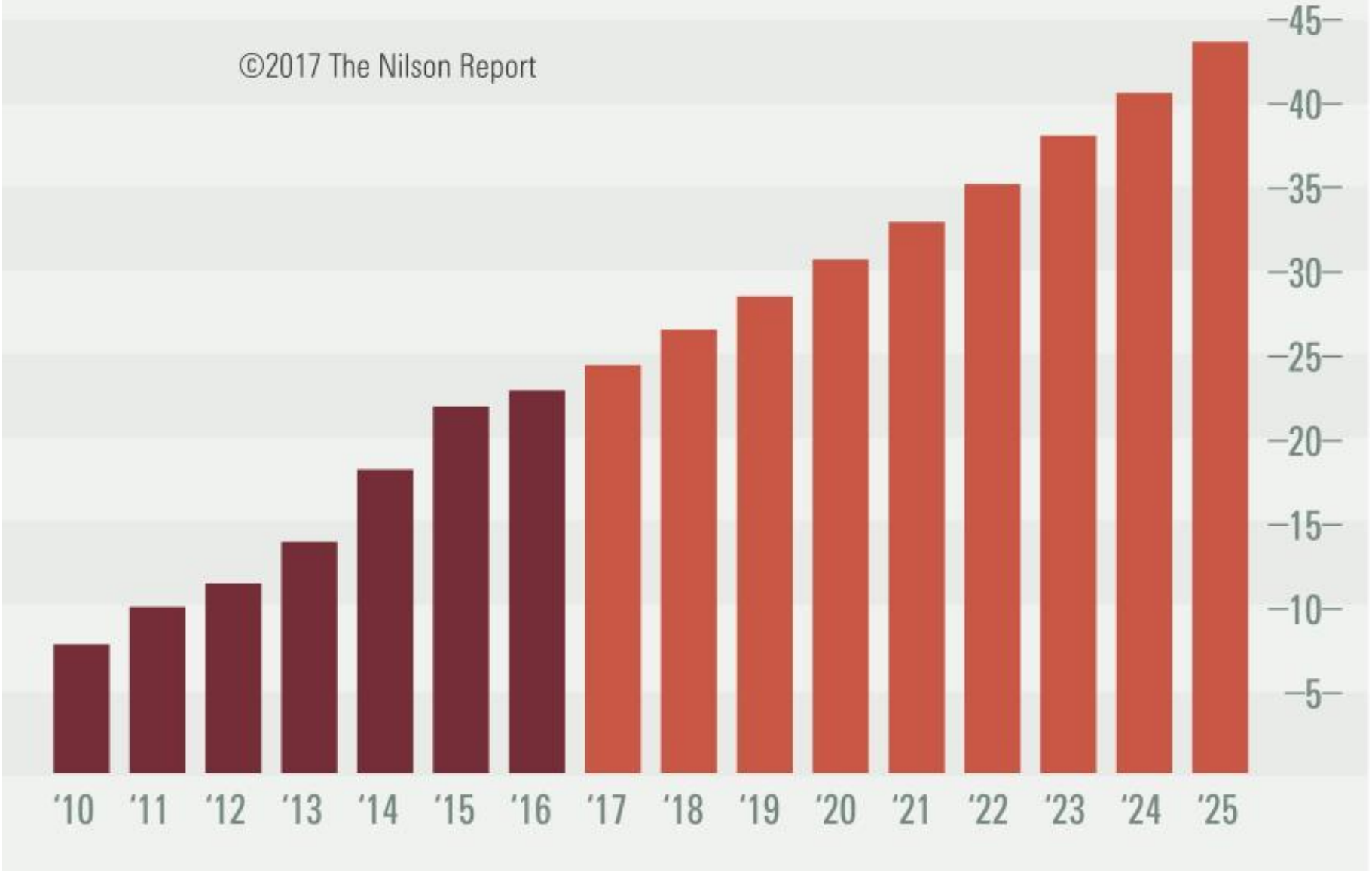
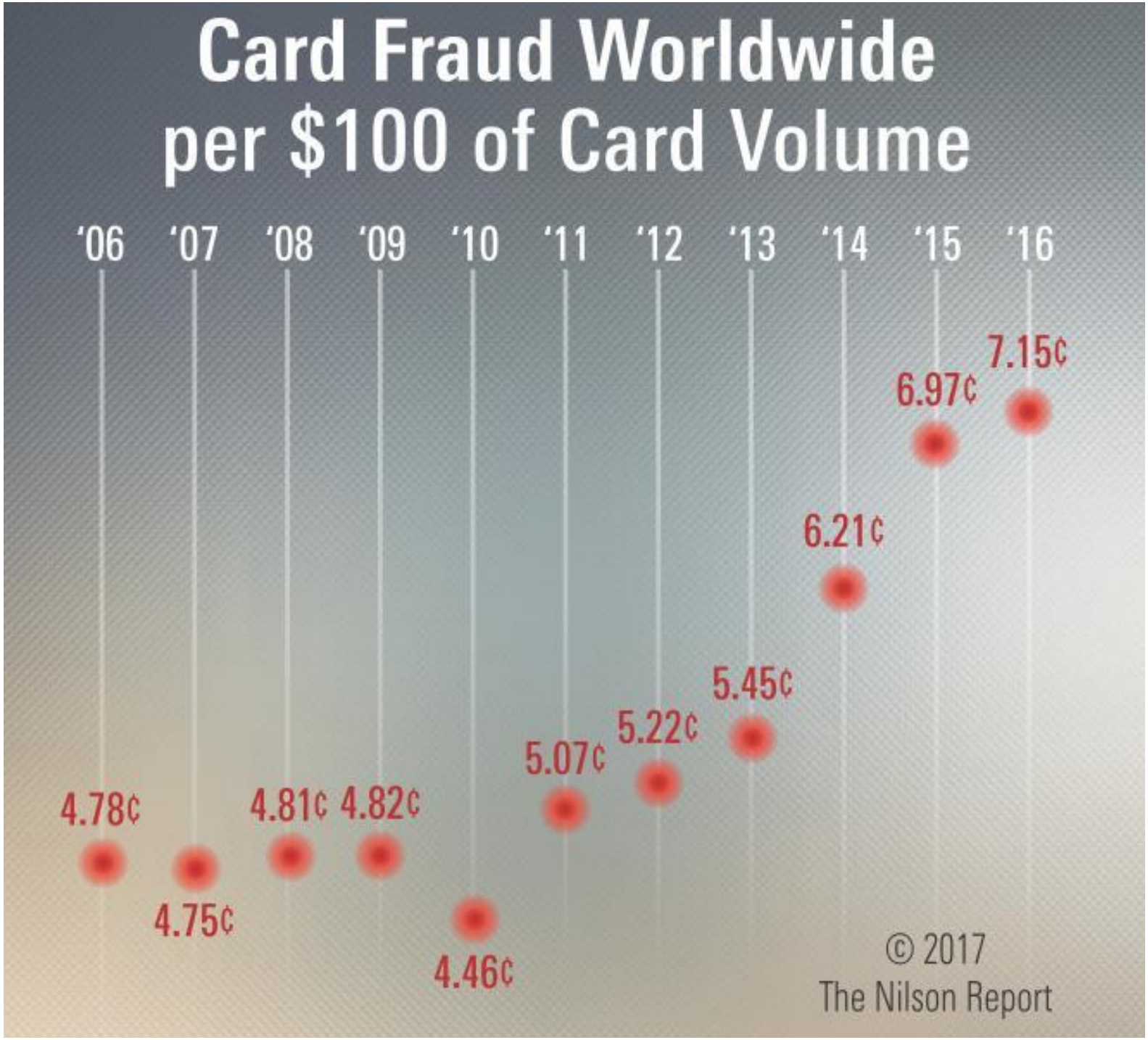
Мошенничество в сфере платежных карт

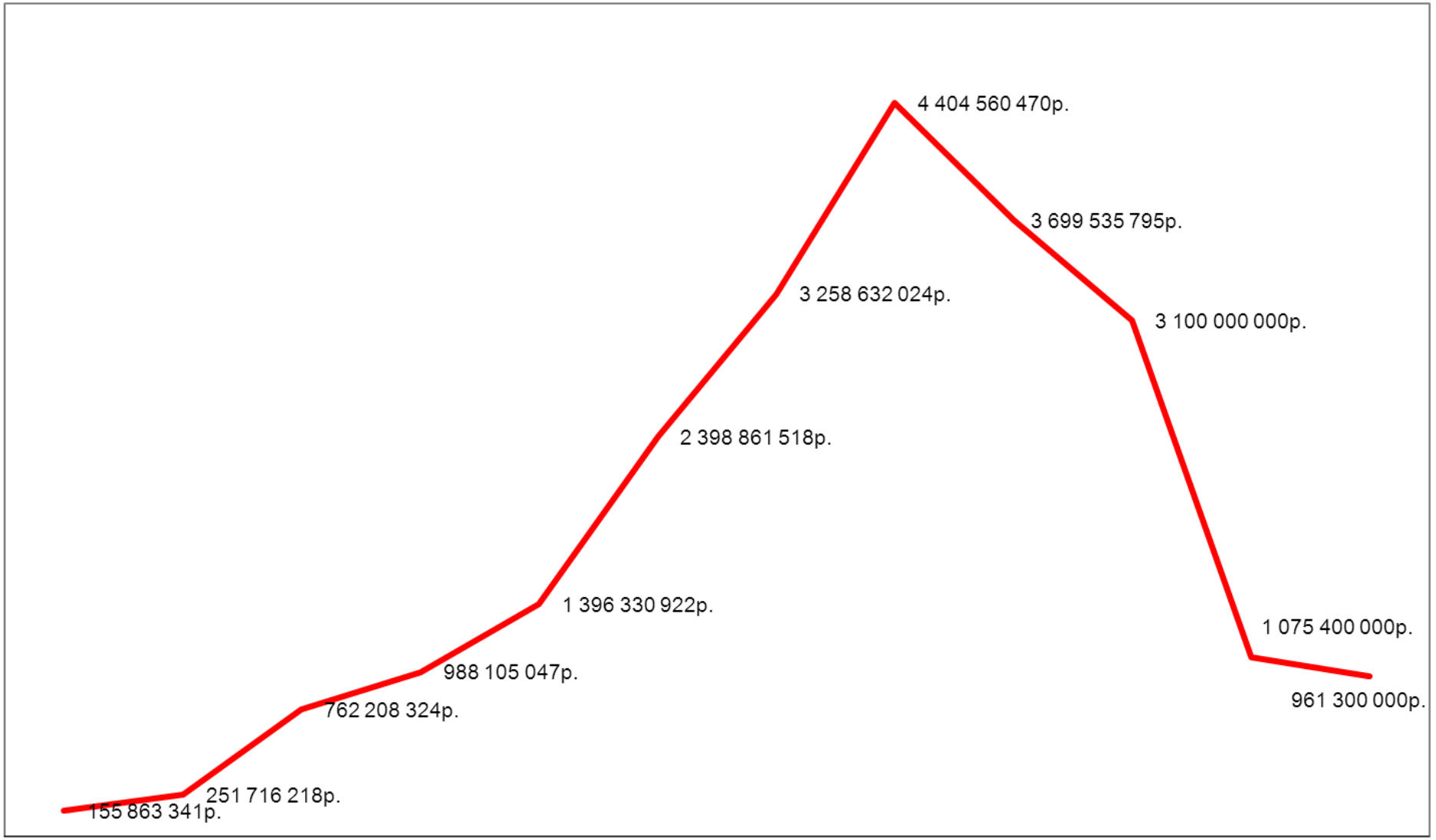
Пятиизбянцев Николай Петрович

Card Fraud Worldwide Projected ($bil.)

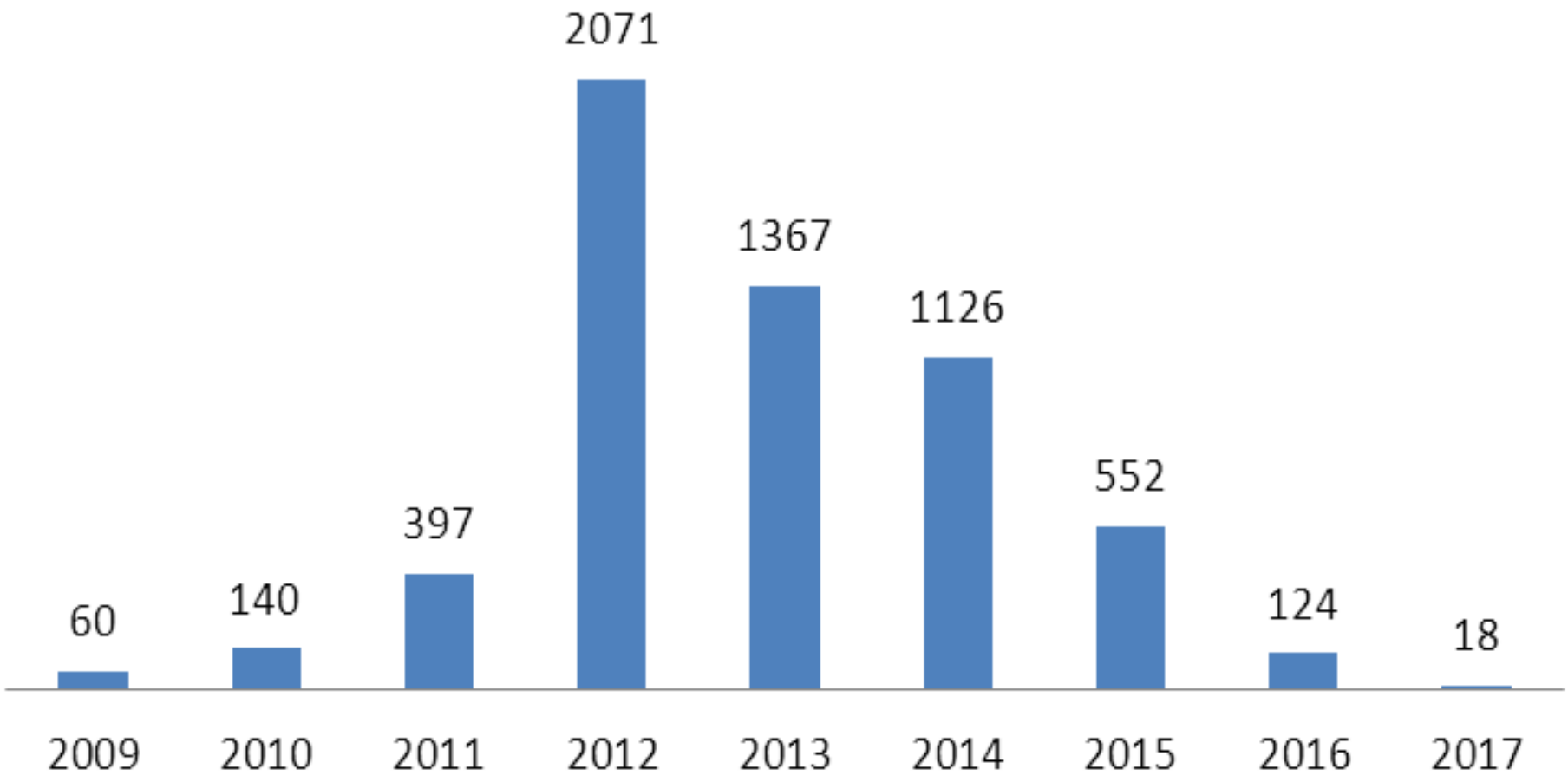


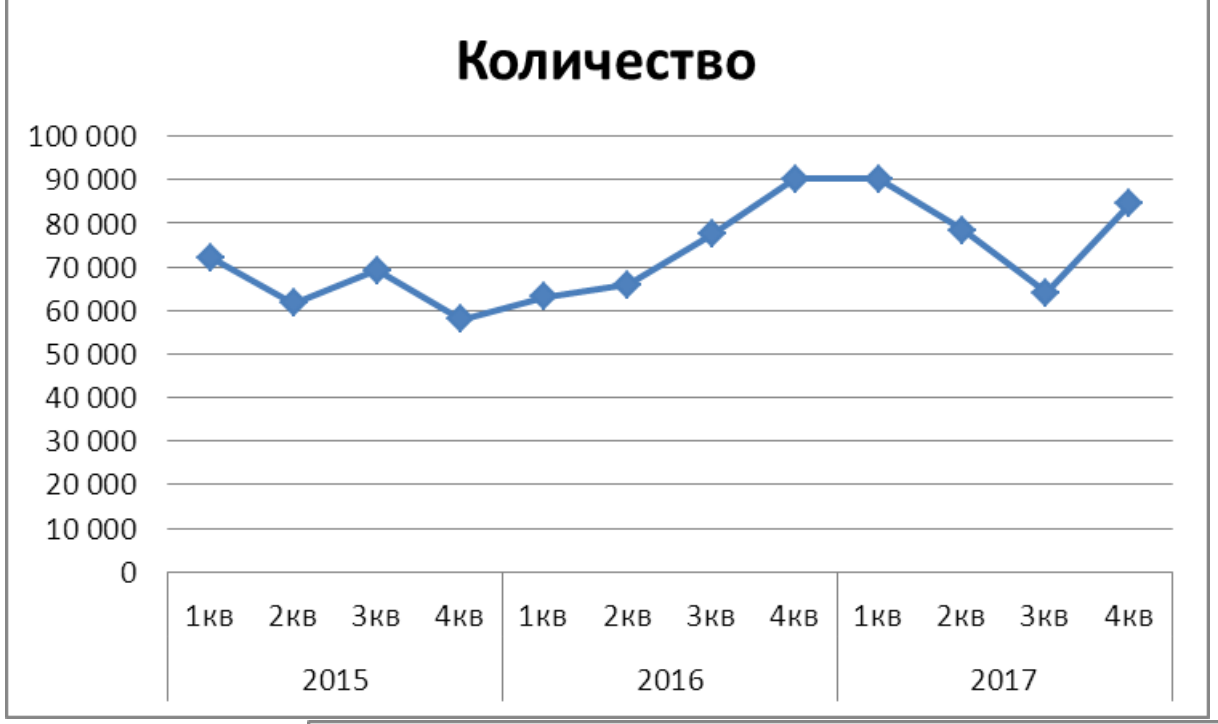

Card Fraud Worldwide
per $100 of Card Volume
'06
'07
'08
'09
'10
'11
'12
'13
'14
'15
'16
4.78¢
4.75¢
4.81¢
4.82¢
4.46¢
5.07¢
5.22¢
5.45¢
6.21¢
6.97¢
7.15¢
© 2017
The Nilson Report

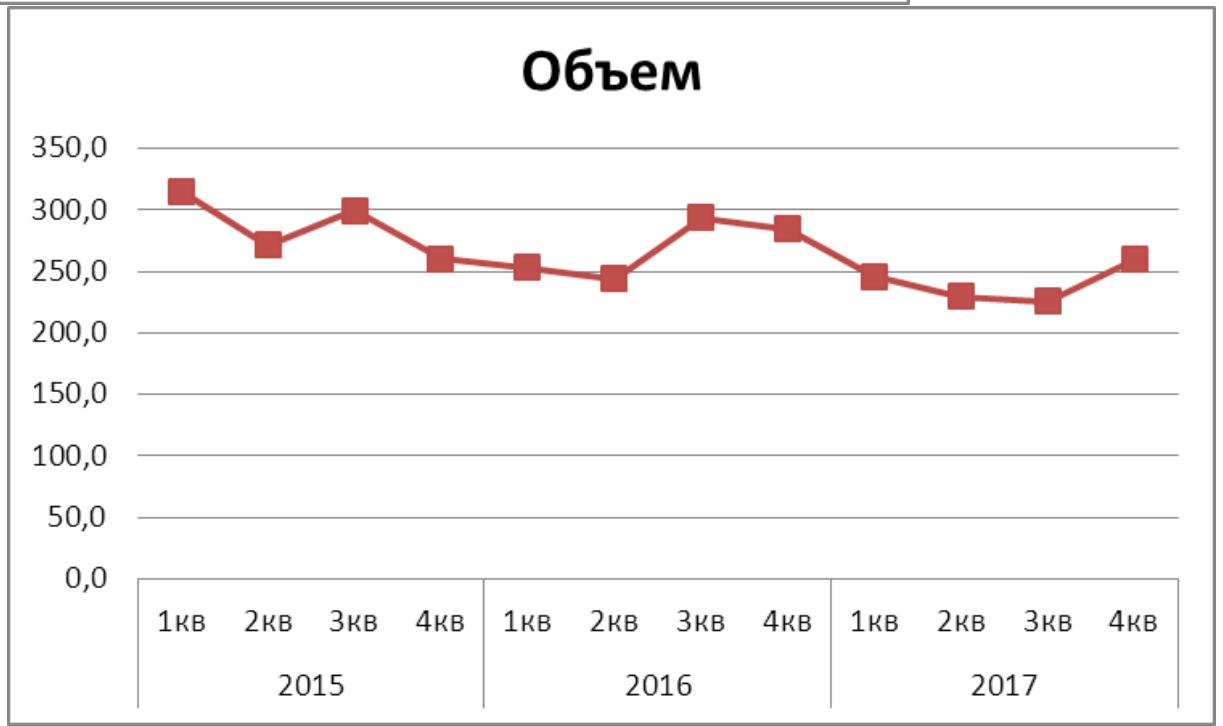
Россия

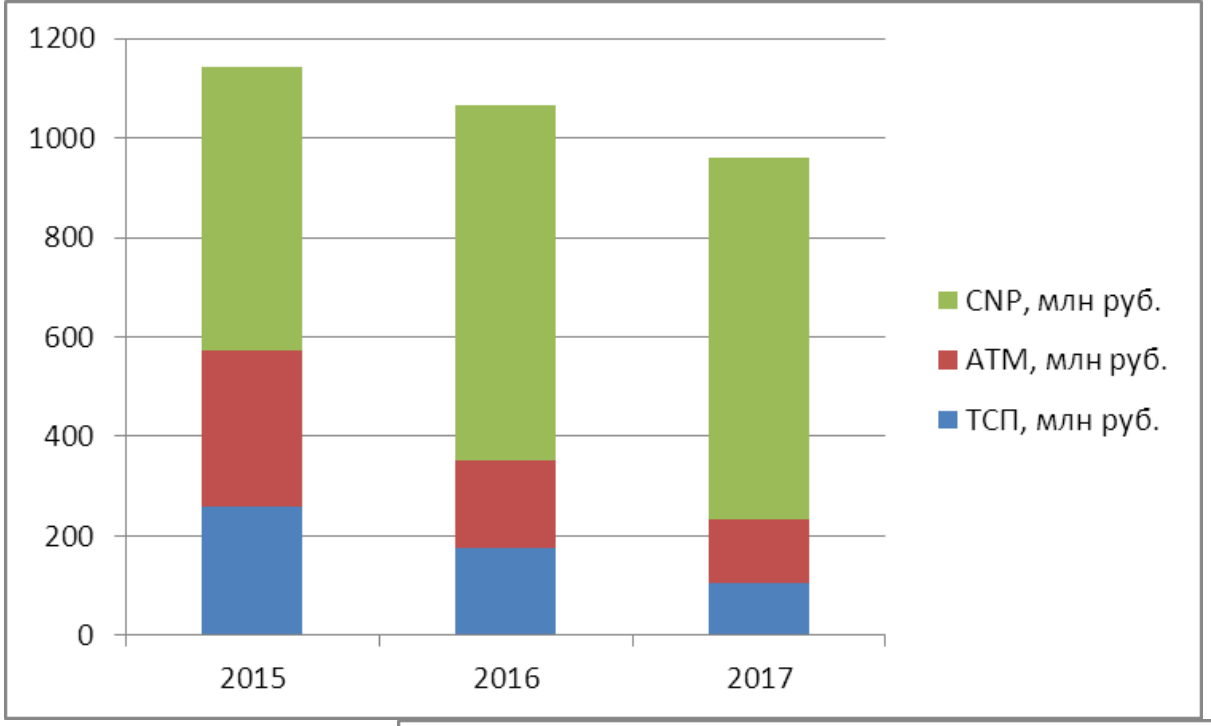

155 863 341р.
251 716 218р.
762 208 324р.
988 105 047р.
1 396 330 922р.
2 398 861 518р.
3 258 632 024р.
4 404 560 470р.
3 699 535 795р.
3 100 000 000р.
1 075 400 000р.
961 300 000р.
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

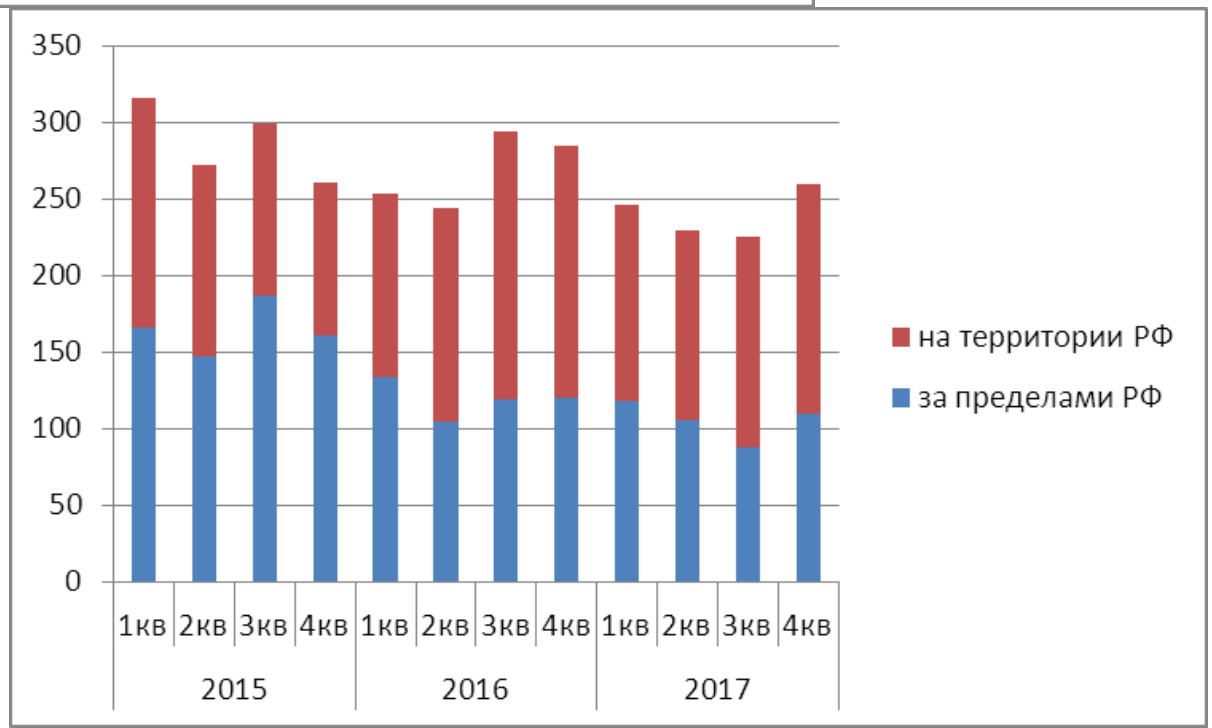
скимминг


2071
1367
1126
552
397
140
124
60
18
2009
2010
2011
2012
2013
2014
2015
2016
2017


Количество
100 000
90 000
80 000
70 000
60 000
50 000
40 000
30 000
20 000
10 000
0
1кв 2кв 3кв 4кв 1кв 2кв 3кв 4кв 1кв 2кв 3кв 4кв
2015
2016
2017


Объем
350,0
300,0
250,0
200,0
150,0
100,0
50,0
0,0
1кв 2кв 3кв 4кв 1кв 2кв 3кв 4кв 1кв 2кв 3кв 4кв
2015
2016
2017


1200
1000
800
600
400
200
0
2015
2016
2017
CNP, млн руб.
АТМ, млн руб.
ТСП, млн руб.


350
300
250
200
150
100
50
0
1кв
2кв
3кв
4кв
1кв
2кв
3кв
4кв
1кв
2кв
3кв
4кв
2015
2016
2017
на территории РФ
за пределами РФ

Основная доля потерь – карта не присутствует

Интернет операции

Компрометация данных карты – социальная инженерия:

Управление поведением человека с использованием социологии и психологии. Может использоваться в противоправных целях, например, с целью получения конфиденциальной информации и хищения денежных средств

Как мошенники выбирают своих жертв?

Воздействие может осуществляться на неопределенную группу лиц, на целевую аудиторию, на конкретного человека

Чем шире целевая аудитория, тем меньше эффективность (процент от общего число), но может компенсироваться количеством

В основном, как правило, жертвами становятся люди финансового и информационно неграмотные, которые не понимают, что их обманывают, не осознают последствий совершаемых действий

Чем больше известно о человеке, группе людей, тем более эффективнее может быть воздействие. Например, если вам по телефону звонит мошенник и обращается по имени отчеству, то уровень недоверия значительно снижается, если к тому же мошенник знает (угадает) клиентом какого банка вы являетесь, то уровень доверия повысится.

В последнее время большую ценность стали представлять данные из социальных сетей (целенаправленное воздействие на основе данных facebook в президентской компании в США или брекзит в Великобритании), а так же интернет объявления, сообщения.

Атаки - Искусственный интеллект.

Почему часто жертва сама отдает мошеннику деньги?

Человек не машина, люди имеют свои слабости, подвержены эмоциям

«На жадину не нужен нож: ему покажешь медный грош – и делай с ним что хошь»

Самым слабым звеном системы безопасности, как правило, является человеческий фактор

Греки не смогли штурмом взять Трою, однако защитники сами втащили коня в город

С точки зрения психологии – ничего нового, появилась киберсфера, человек остался прежним

Как не стать жертвой?

Повышать финансовую, информационную грамотность, как можно меньше раскрывать информации о себе, не совершать поспешных действий, особенно если вы не понимаете их сути и последствий, никому не сообщать конфиденциальной информации (коды, пароли и т.п.)

В школах нужно вводить обучение по кибербезопасности (не только финансовой)

Можно усовершенствовать (сделать безопасными) технологии, нельзя «усовершенствовать» человека, его можно научить

MasterCard® Contact | MasterCard® Contact

nfc.mastercard.ru/#slide-1

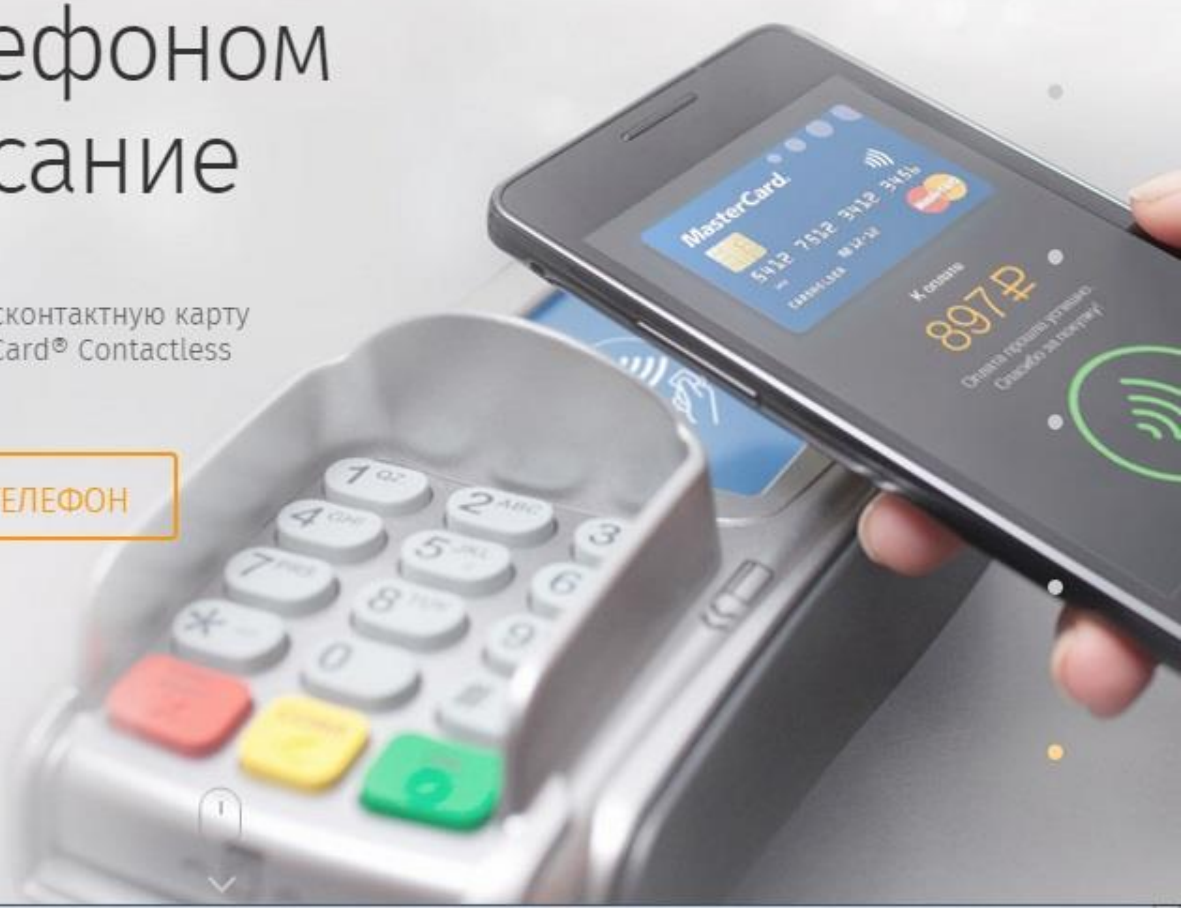
Суды, адвокаты и с | Автокод | Портал госуслуг Мс | «BIS Journal - Инфо | MC compliant PCI | www.visaeurope.con | » Другие закладки

ПОДКЛЮЧИТЬ МОЙ ТЕЛЕФОН

Платите телефоном в одно касание

Превратите ваш смартфон в бесконтактную карту благодаря технологии MasterCard® Contactless

ПОДКЛЮЧИТЬ МОЙ ТЕЛЕФОН



NFC Skimming – NFC скимминг

Можно перехватить информацию между картой и терминалом, которая передается в открытом виде, либо просто считать информацию с карты.

Результат: номер карты, дата действия.

Если карта не подписана эмитентом на технологию 3D Secure, то можно осуществить несанкционированные интернет операции.

Также можно провести атаку с подбором CVV/CVC на магнитной полосе.

Уровень угрозы низкий.

Рост числа инцидентов с кражей с помощью RFID-ридеров.

В России растет количество инцидентов с новым видом мошенничества — кража денег с карт, оснащенных технологиями бесконтактной оплаты товаров (карта прикладывается к PoS-терминалу, сумма покупки списывается с «пластика»).

Мошенническое ТСП

Выявляется программами платежных систем

Уровень угрозы низкий

Мошенническое ТСП

Можно модернизировать ПО терминала таким образом, чтобы осуществлять операции по небольшим суммам в офф-лайн.

На карту для формирования криптограммы (ТС) направляется не большая сумма (1$/1€/1р.), а в расчеты уходит другая (большая) сумма.

Это возможно, если эмитент не сравнивает сумму из криптограммы и из расчетов.

ТСП выявляется программами платежных систем.

Уровень угрозы низкий.

NFC Transaction Relay

Возможно инициировать транзакцию без ведома держателя.

Один телефон выступает в качестве NFC терминала и инициирует транзакцию, направляя запросы карте, другой выступает в качестве NFC карты.

Ответы на запросы полученные от карты передаются от одного телефона другому, далее на NFC терминал. Ответы (запросы) терминала также транслируются через два мобильных телефона на карту.

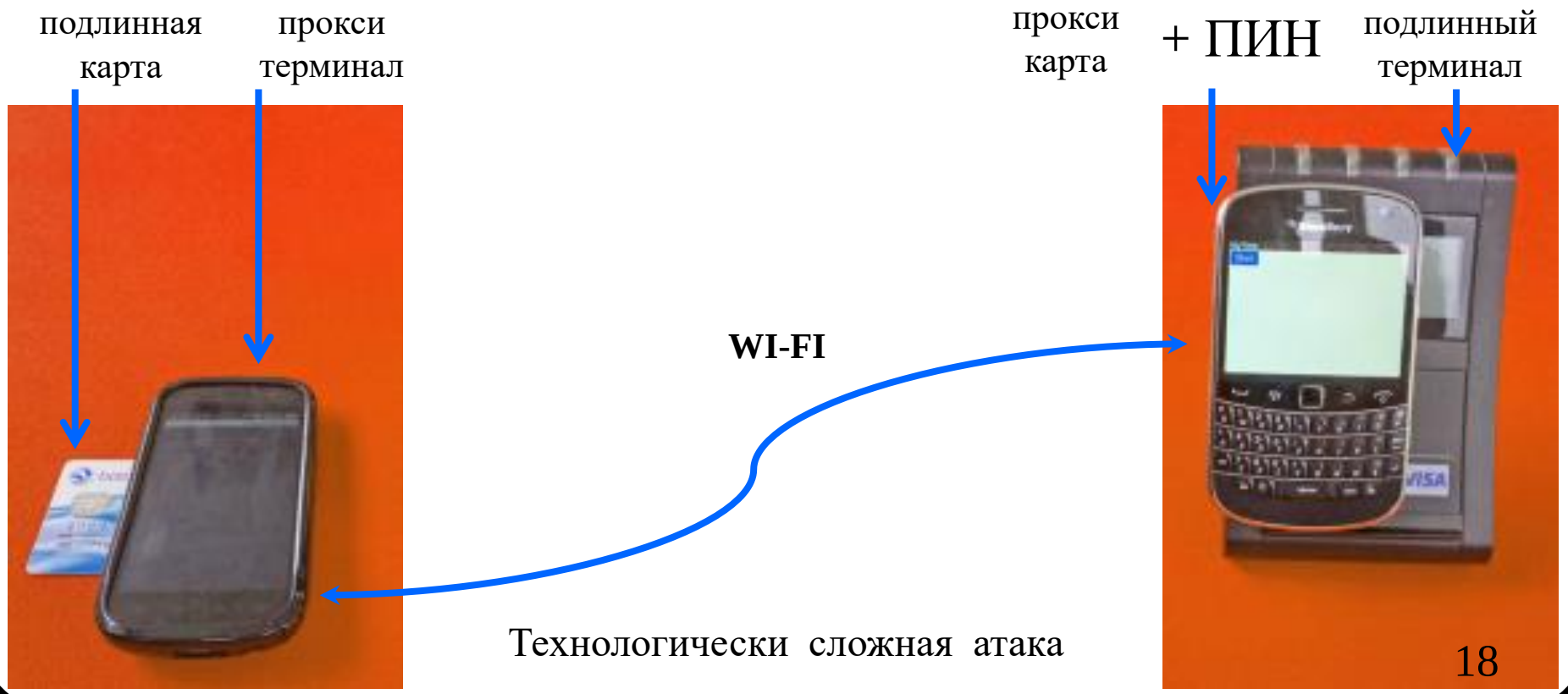
До 1000 р. ПИН код не запрашивается.

В данной атаке может быть реализована составляющая «человек по середине»: некоторые данные при передачи от карты к терминалу можно изменить, например, метод верификации держателя Cardholder Verification Methods (CVMs).

NFC Transaction Relay + PIN

Компрометация ПИН (подглядывание, видео, др.) + relay attack.

Транзакция на большую сумму может быть осуществлена, если предварительно каким-то образом был получен ПИН-код, например, подсмотрен.



NFC Relay Attacks with Android

https://blog.kaspersky.ru/contactless-payments-security/8608/

Испанские хакеры Рикардо Родригес и Хосе Вилла (конференция Hack In The Box) создали вредоносное ПО для Android системы, который превращает смартфон жертвы в ретранслятор NFC-сигнала.

Как только зараженный телефон оказывается возле бесконтактной карты, он отправляет через Интернет злоумышленникам сигнал о доступности транзакции. Мошенники активируют обычный платежный терминал, подносят к нему свой NFC-смартфон. Таким образом создается «мост» через Интернет между NFC-карточкой и NFC-терминалом, удаленными друг от друга на любое расстояние.

Троянец может распространяться стандартным способом

Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited

Cards Will Not Need to Be Re-read for Consecutive Contactless ATM Transactions

AP, Canada, CEMEA, LAC, U.S. | *Acquirers, Issuers, Processors, Merchants*

Overview: Effective 16 April 2016, Visa will remove the requirement for a card to be re-read in contactless ATM transaction chaining.

Transaction chaining provides cardholders with the convenience of performing multiple ATM transactions in a single session (e.g., a balance inquiry followed by a cash withdrawal).

Effective 16 April 2016, in instances of contactless transaction chaining, Visa will facilitate quicker transactions by removing the requirement to re-read the card for each new ATM transaction. However, the requirement will remain in effect for contact chip transactions. PIN entry will continue to be required for each ATM transaction in a chain.

Background

Chip cards generate unique data for each transaction. Contact chip ATMs re-read the card to generate a fresh set of data for each new transaction in a chain. Re-reading provides limited security benefits, because the card's authenticity was established using the data created in the first read. For contact chip transactions, the cardholder is unaware that the card is being read multiple times because the card remains inserted in the ATM for the duration of the session. For contactless transactions, multiple card reads may inconvenience the cardholder because the card may need to be represented to the reader after having been put away in a wallet or bag.

Not need to be re-read

Если при бесконтактных операциях на АТМ считывание карты происходит один раз, а транзакций может быть выполнено несколько, следовательно не происходит генерации картой уникальной криптограммы на каждую транзакцию.

Можно дублировать операции по снятию наличных в банкомате.

Держатель получил деньги и ушел, а вредоносное ПО продолжает выдавать наличные.

Потери несет эмитент (держатель), эквайрер не нарушает правил МПС.

Токенизация

MDES

MasterCard Digital Enablement Service- Implementation Quick Reference Guide. May 2015

MDES - сервис, который позволяет держателю привязать свои карты к мобильному устройству и затем осуществлять платежи непосредственно с устройства.

Физический номер карты (PAN) заменяется на «суррогатный» номер (токен)

Токенизация

Digitization Process

1. Cardholder requests digitization

Держатель карты привязывает свою карту к мобильному устройству (запрашивает токен) путем направления запроса, содержащего: физический номер карты, срок действия и CVC2.

4. MasterCard sends Card Eligibility Request

Unless the issuer has declined the TER or ASI eligibility check (see Step 2), MasterCard sends a

Tokenization Authorization Request (TAR) or Account Status Inquiry (ASI) to the issuer asking them

to authorize the cardholder’s digitization request.

В зависимости от выбора эмитента MasterCard направляет ему Tokenization Authorization Request (TAR) or Account Status Inquiry (ASI) для авторизации (разрешения выдавать токены).

Токенизация

Digitization Process

Account Status Inquiry (ASI) - стандартный тип сообщения, эмитент проверяет срок действия карты и CVC.

Tokenization Eligibility Request (TER) – запрос дополнительной информации для верификации держателя.

Токенизация

https://threatpost.ru/moshenniki-aktivno-osvaivayut-apple-pay/6633/

… количество случаев использования платежной системы от Apple для махинаций растет, как заявляют представители крупных американских банков. На освоение новой платежной системы у преступников ушло полгода — за это время оборот от их деятельности значительно вырос: 6% транзакций в Apple Pay приходится на долю мошенников, в то время как для кредитных карт показатель мошеннических транзакций не превышает 0,1%. Уязвимость в большей мере связана не с самой технологией платежной системы, а скорее с политикой некоторых банков, которые выдают карты, привязываемые к аккаунту в Apple Pay. Злоумышленники используют «мулов», чтобы привязать краденую кредитку к аккаунту.

Комментарий: в настоящий момент Apple Pay использует усиленную верификацию при привязке карты.

Samsung Pay:

Tokenized Numbers, Flaws and Issues

Salvador Mendoza July 14, 2016

%4012300001234567^21041010 82000 0 232 646?

%4012300001234567^21041010 82000 0 233 969?

%4012300001234567^21041010 82000 0 234 196?

%4012300001234567^21041010 82001 0 235 585?

Сервис код:

101 – технология карт с магнитной полосой

Счетчик транзакций:

232-235

Динамический CVV/CVC:

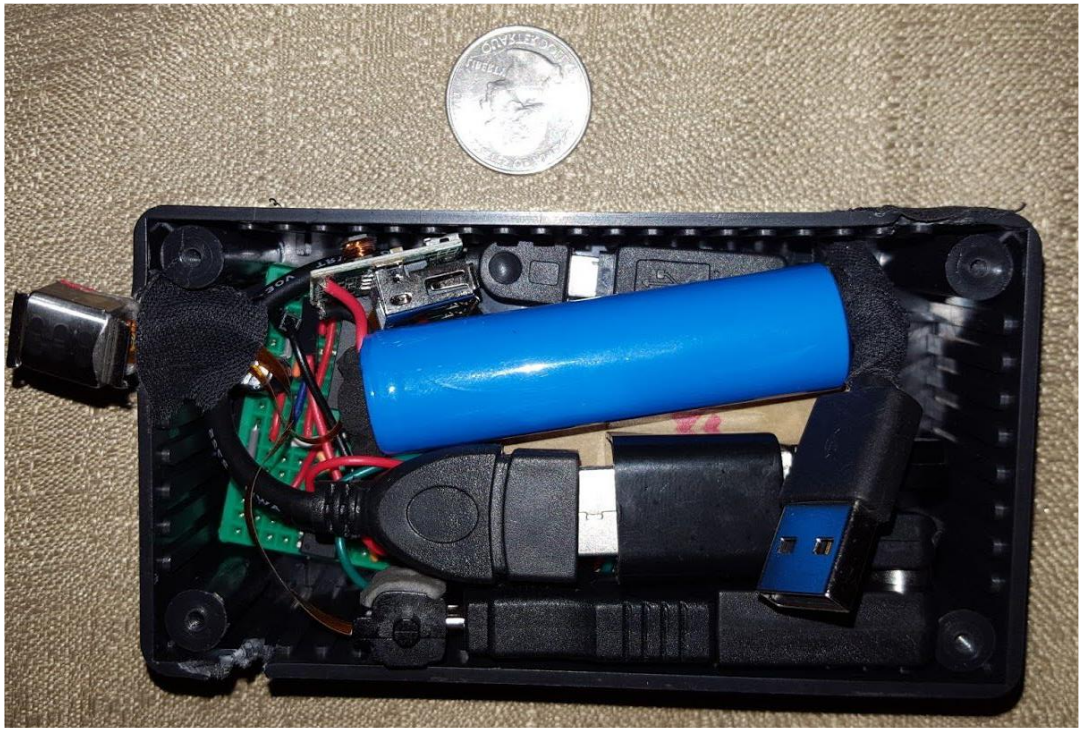
646-585

JamPay – перехват платежа

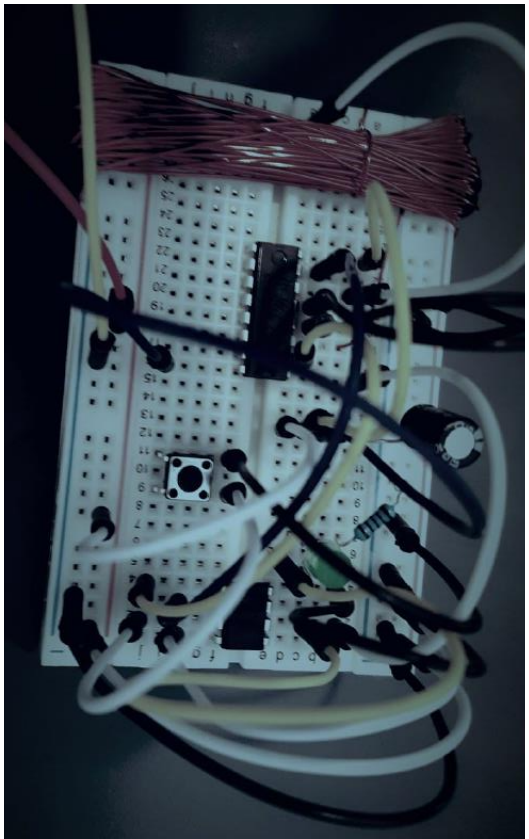
https://www.youtube.com/watch?v=rZwvOZJGCro

Специальное электронное устройство (MagSpoof) интегрированное с микрокомпьтером (Raspberry) при оплате Samsung Pay подавляют платежный терминала, перехватывают с телефона сформированный трек и передают его злоумышленнику.

MagSpoof (http://samy.pl/magspoof/)



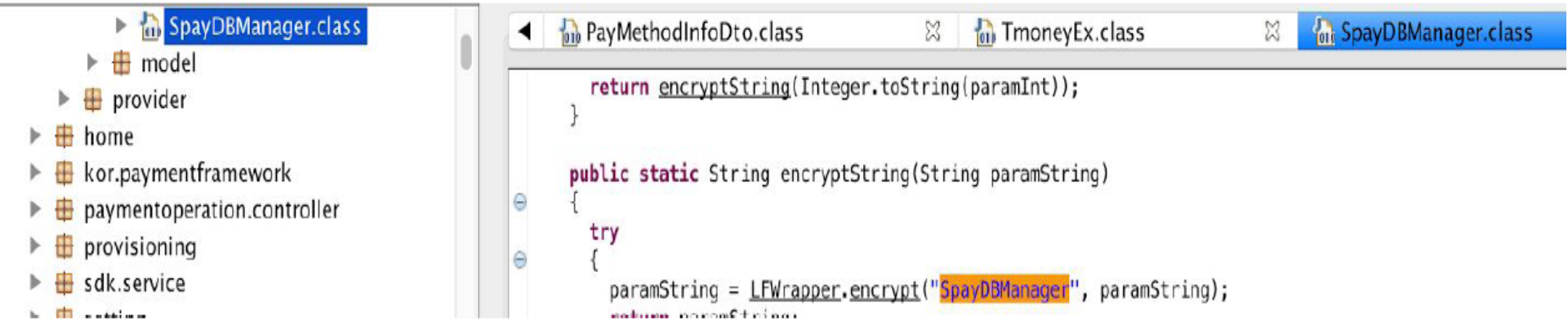
MagSpoof integrated with Raspberry zero



Приложение Samsung Pay

Токены хранящиеся в приложении на телефоне «зашифрованы» на статическом ключе прописанном в коде программы.

Могут быть расшифрованы и перехвачены вредоносным ПО.



Samsung Pay: Tokenized Numbers, Flaws and Issues
Salvador Mendoza, July 14, 2016

Relay Attack on Google Wallet

- Relay app
  - Android app
  - Unlock/lock Google Wallet on-card component
  - Forward APDUs to secure element
- Card emulator
  - Python application
  - ACR 122U
  - Notebook computer
- POS terminal
  - Hypercom Artema Hybrid
    ViVOtech ViVOpay 5000

Relayed payment transaction **successful**


H-Ä-N-D-L-E-R-B-E-L-E-G

Testterminal
OPP B50

Terminal-ID 54183583
TA-Nr 000219 BNr 0062

Kartenzahlung
MasterCard

EUR 1,00

PAN 5430[redacted]0[redacted]7[redacted]
EMV-AID A0000000041010
VU-Nr 158632721
AIDPara 0100000002
Genehmigungs-Nr 735259
Datum 20.02.12 17:18 Uhr

Zahlung erfolgt

==========
AS-Proc-Code = 00 914
00
Capt.-Ref.= 0010
AID59: 714487
==========

BITTE [redacted]N

Europol

Зарегистрированы сообщения об атаках на платежные NFC карты.

В Darknet (темный интернет) предлагают программное обеспечение, которое загружает скомпрометированные данные карт на телефон Android, чтобы осуществить платежные операции в магазинах, оборудованные NFC терминалами.

В случае несанкционированного использования карты (утрата, подделка), эмитент имеет возможность направить команду на её изъятие.

Использование NFC телефона для мошеннических платежных операций не дает возможность сотруднику ТСП изъять такую карту (телефон).

IOCTA 2016 Europol

Атака – подмена хоста

Злоумышленник подключает банкомат к компьютеру, который представляется банкомату хостом процессинга. Подключение происходит либо по проводному каналу, либо по радиоканалу.

На запрос выдачи наличных ложный хост выдает положительный ответ.

Атака возможна из-за отсутствия MAC и VPN (можно отключить).

Атака – black box

Установка мини-компьютера внутри сервисной зоны банкомата, благодаря чему появляется возможность посылать прямые команды о выдаче наличных денежных средств на диспенсер.

1) мини-компьютер может подключаться после открытия крышки сервисной зоны.

2) путем проникновения в сервисную зону через вырезанное рядом с ПИН-клавиатурой отверстие. Отверстие может вырезаться горелкой/паяльником, как следствие - отсутствует вибрация и не срабатывают датчики типа "шорох". Обходится система контроля доступа и усиленный (индивидуальный) замок верхнего кабинета. Подключение осуществляется к разъему SDC-шины EPP или в USB порт.

Атака на функцию приема наличных

Вредоносное ПО получает контроль над COM-портом, к которому подключен купюроприемник, и имитирует внесение наличных.

Атака на платежные терминалы

Атака осуществлялась удаленно (к терминалу никто не подходил)

Было выявлено вредоносное ПО и radmin

Атака снятие холдов

Снятие холдов (hold) - операция выполняется эмитентом, т.е., например, в банкомате «злодей» снял деньги, а вредоносное ПО у эмитента сняло холд, деньги на карте оказались опять доступны, эмитент эквайреру обязан возместить сумму операции, ущерб эмитенту.

Атака отмена операции

Отмена операции (reversal) - выполняется эквайрером, т.е., например, в банкомате «злодей» снял деньги, а вредоносное ПО у эквайрера сформировало отмену операции и отправила её эмитенту, деньги на карте оказались опять доступны, эмитент эквайреру не обязан возмещать сумму операции, ущерб эквайреру.

Атака cash-out

В процессинге по контролируемым картам поднимаются доступные балансы (кредитные лимиты), лимиты по снятию наличных снимаются.

В течении короткого промежутка времени осуществляется максимально возможное количество операций по снятию наличных в банкоматах.

Если контролируемые карты без микропроцессора (зарубежные банки, предоплаченные карты), изготавливаются дубликаты карт с магнитной полосой.

Атака – вредоносное ПО

На банкомат устанавливается вредоносное ПО:

1) локально – USB, CD, DVD;

2) дистанционно – используя штатно установленные средства удаленного доступа (R-admin) и/или доступа (login/password).

Сценарий:

1) Вредоносное ПО на уровне XFS направляет команды на диспенсер на выдачу наличных.

2) Вредоносное ПО перехватывает запросы на выдачу наличных и возвращает положительные ответы.

3) Вредоносное ПО перехватывает трек и ПИН (ПИН не перехватывался с 2009 г.).

ПОЛОЖЕНИЕ ЦБ РФ № 382-П

О ТРЕБОВАНИЯХ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ И О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ БАНКОМ РОССИИ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ.

2.6.3. При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 настоящего пункта, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают:

выполнение процедур идентификации, аутентификации, авторизации лиц, осуществляющих доступ к программному обеспечению банкоматов и платежных терминалов;

выполнение процедур идентификации и контроль деятельности лиц, осуществляющих техническое обслуживание банкоматов и платежных терминалов;

«РЕШЕНИЕ» ЗАДАЧИ

Установка на банкоматы нештатного (нерекомендованного производителями) программного обеспечения удаленного администрирования.

Radmin (Remote Administrator), RDC (Remote Desktop Connection), TSC (Terminal Services Client), Ammyy Admin, TeamViewer, VNC и т.п.

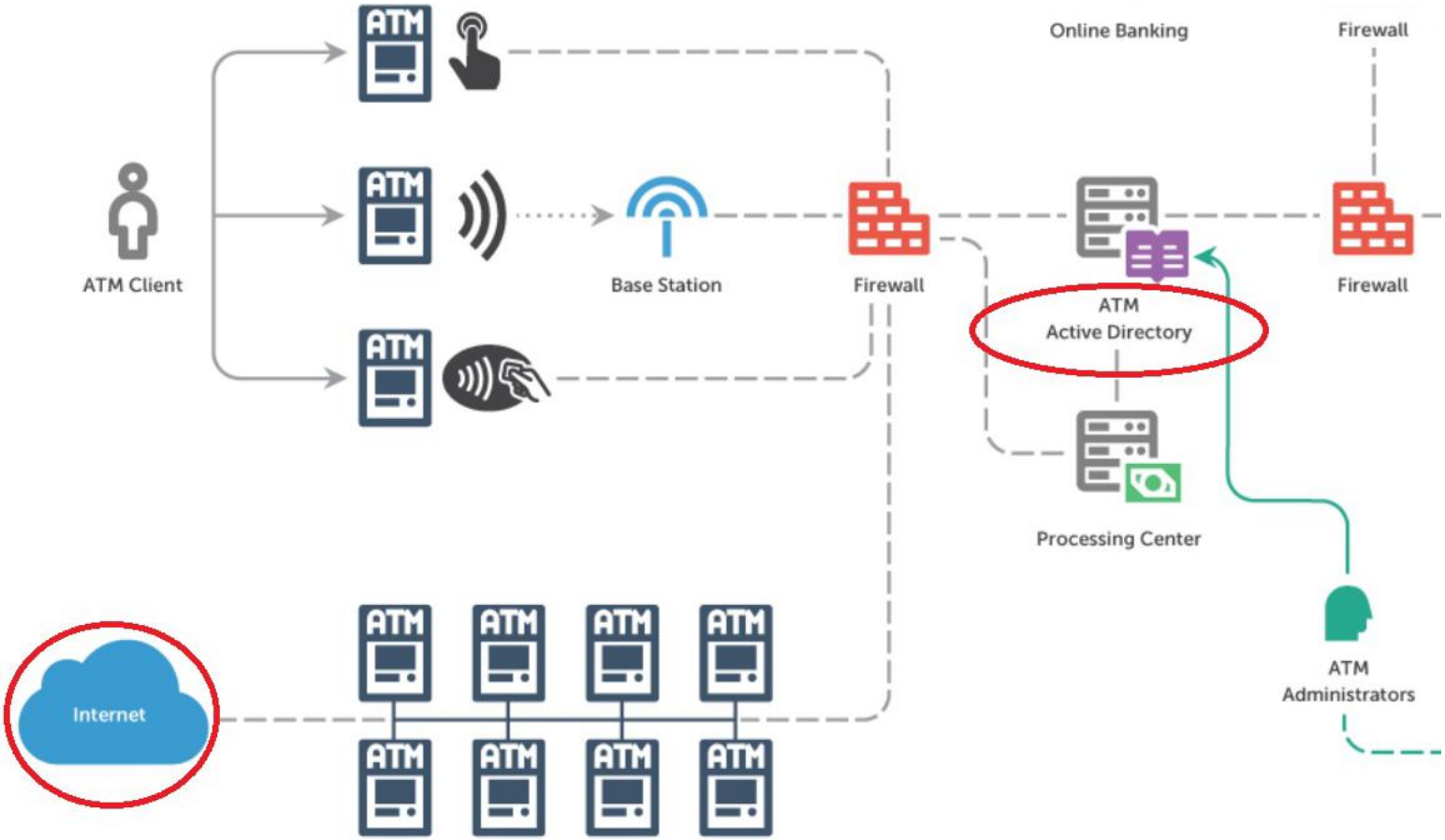
Включение банкоматов в Active Directory Domain Services.

Легко управлять, загружать, скачивать файлы, делать настройки, не нужен выезд технического персонала.

Предоставление удаленного доступа к банкоматам (логин/пароль) из Интернет.

KASPERSKY

https://securelist.com/files/2016/09/Future_ATM_attacks_report_eng.pdf?bcsi_scan_79476223f705d7a8=0&bcsi_scan_filename=Future_ATM_attacks_report_eng.pdf



Cobalt snatch 2016

Анализ журналов системы защиты подтвердил перемещения в сети со скомпрометированных компьютеров, в том числе подтвердились факты подключений к банкоматам с помощью RAdmin. В инфраструктуре атакованного банка это ПО активно используется администраторами для удаленного управления, среди прочего, и банкоматами. Поэтому подобная активность не вызвала подозрений.

Таблица 1 – Основные меры противодействия атакам (на АТМ)

№	Мера противодействия	Разъяснение
1	Смена пароля BIOS	Смена пароля для входа в BIOS с предустановленного производителем
2	Уточнить возможность установки двухфакторной аутентификации для входа в BIOS.	Свяжитесь с производителем банкомата для выяснения подобной возможности, при необходимости обновите BIOS
3	Установка сигнализации на открытие верхнего кабинета банкомата, использование уникальных ключей для сервис-блоков, установка дополнительных замков, затрудняющих вскрытие банкомата	-
5	Активировать технологию Intel AMT	Активация технологии позволит управлять изменениями паролей BIOS, контролировать вход в BIOS
6	Обновить ПО банкомата	Следует отслеживать, чтобы ПО банкомата было в актуальном состоянии
7	Установка защищенного протокола обмена	Проверить, что используются протоколы SPEAR / FMPP для обмена командами с диспенсером, установить максимальный уровень безопасности
9	Обновить BIOS	Обновить BIOS до версии, в которой поддерживается двухфакторная аутентификация, после чего активировать ее
10	Убедиться (по возможности), что используются последние версии протоколов	Убедиться, что используется протокол версии SPEAR II при использовании SPEAR
11	Установка специализированного ПО для мониторинга состояния банкомата, в т.ч. и для отслеживания вскрытия верхнего кабинета и(или) несанкционированного отключения питания, ПО контроля целостности	-

Комментарий

Intel AMT (Active Management Technology) - (аппаратная технология, позволяющая удаленно управлять компьютером).

Удаленный запрос информации о состоянии, восстановление работоспособности, обновление и обеспечение защиты устройств.

Внеполосный доступ к системе – благодаря встроенным средствам управления ИТ-персонал получает возможность обнаружения ресурсов даже при отключенном питании.

Изолирует зараженные программные клиенты, блокируя их доступ в сеть, оповещает об удалении критичных программных агентов.

Поддерживает в актуальном состоянии ПО и антивирусную защиту.

Возможность дистанционной настройки.

Комментарий

1 мая 2017 корпорация Intel опубликовала инструкцию по устранению проблем безопасности в связи с возникновением критичной уязвимости встроенного ПО в определенных системах, использующих технологию Intel® Active Management (AMT), Intel® Standard Manageability (ISM) или Intel® Small Business (SBT). Из-за этой уязвимости взломщик компьютерных сетей может получить удаленный доступ к корпоративным компьютерам или другим устройствам, оснащенным этими технологиями. https://www.intel.ru/content/www/ru/ru/architecture-and-technology/intel-amt-vulnerability-announcement.html

Комментарий

14 июня 2017 Исследователям из компании Microsoft удалось обнаружить вредоносное программное обеспечение, использующее в качестве «моста» для передачи информации Intel Serial-over-LAN (SOL), являющуюся частью инструментария Active Management Technology (AMT). Технология SOL работает таким образом, что трафик поступает в обход сетевого стека локального компьютера, поэтому его «не видят» и не блокируют файерволы и антивирусное ПО. Это позволяет беспрепятственно извлекать данные с зараженных хостов. https://habrahabr.ru/company/it-grad/blog/330572/

Кибератака

В случае неблагоприятной политической обстановки возможна ситуация, когда в широковещательных стандартных пакетах TCP/UDP может быть направлена команда на блокирование чипсетов Intel.

Технология Anti-Thefr (AT). Intel может послать команду kill, которая блокирует компьютер с vPro, если его украли.

Банкомат в стандартной конфигурации имеет программный firewall и VPN, которые не могут контролировать или блокировать Intel AMT.

Таким образом, существует возможность заблокировать (вывести из работоспособного состояния) практически весь парк банкоматов российских банков.

Иностранные спецслужбы готовят кибератаки,

направленные на дестабилизацию финансовой системы России

02.12.2016

ФСБ России получена информация о подготовке иностранными спецслужбами в период с 5 декабря 2016 года масштабных кибератак с целью дестабилизации финансовой системы Российской Федерации, в том числе деятельности ряда крупнейших российских банков.

http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10438041%40fsbMessage.html

Отключение банкоматов

04-12-2016

Уважаемые клиенты!

Руководством Генбанка принято решение о временном отключении сети банкоматов банка. Отключение будет с 21.00 04/12/16 по 9.00 05/12/16 года.

Причина - готовящаяся по информации Спецслужб России Ddos-атака **(кибер атака) на банковскую систему РФ**. Блокировка устройств будет осуществлена в целях предотвращения несанкционированных транзакций и утраты клиентами своих средств.

https://www.genbank.ru/allnews/otklyuchenie-bankomatov

Штатные решения

NCR

для дистанционного управления программным обеспечением банкоматов использует программное обеспечение

Gasper Exchange и CAITClientManager.

Diebold

для дистанционного управления программным обеспечением банкоматов использует программное обеспечение

Agilis SW Distribution и Phoenix Commander.

Рекомендация: Если не используется штатное решение, то лучше не использовать ничего, удаленной доступ к банкоматам отсутствует (382-П ЦБ РФ).

Применение биометрии для аутентификации и идентификации клиентов

115-ФЗ редакции: с 30.06.2018 (N 482-ФЗ от 31.12.2017)

идентификация - совокупность мероприятий по **установлению** определенных настоящим Федеральным законом **сведений о клиентах**, их представителях, выгодоприобретателях, бенефициарных владельцах и **подтверждению достоверности** этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий и (или) государственных и иных информационных систем

Применение биометрии для аутентификации и идентификации клиентов

115-ФЗ редакции: с 30.06.2018 (N 482-ФЗ от 31.12.2017)

5.8. Банки, соответствующие критериям, установленным абзацами вторым - четвертым пункта 5.7 настоящей статьи, **вправе открывать и вести счета** (вклады) клиентов - физических лиц, **предоставлять кредиты** клиентам - физическим лицам, а также осуществлять переводы денежных средств по таким счетам по их поручению без их личного присутствия после проведения идентификации клиентов - физических лиц путем установления и подтверждения достоверности сведений о них, определенных настоящим Федеральным законом, **с использованием единой системы идентификации и аутентификации и единой биометрической системы** в порядке, установленном Федеральным законом от 27 июля 2006 года N149-ФЗ

ГОСТ Р 57580.1-2017

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ (БАНКОВСКИХ) ОПЕРАЦИЙ. ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. БАЗОВЫЙ СОСТАВ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

3.16 идентификация: **Присвоение** для осуществления логического доступа субъекту (объекту) доступа уникального признака (**идентификатора**); сравнение при осуществлении логического доступа предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов.

3.17 аутентификация: Проверка при осуществлении логического доступа принадлежности субъекту (объекту) доступа предъявленного им идентификатора (**подтверждение подлинности**).

Стенограммы по законопроекту №157752-7

ВОДОЛАЦКИЙ В. П., фракция "ЕДИНАЯ РОССИЯ".

… всё-таки как будет защищён данный инструментарий в единой системе? Какие будут гарантии, что у людей не станут воровать их данные и потом брать кредиты?

АКСАКОВ А. Г. Вопрос, можно сказать, риторический. Я уже подчеркнул, что мы этот вопрос очень детально обсуждали, в том числе с Федеральной службой безопасности, и очевидно, по крайней мере в моём представлении, что тема защиты будет в том числе особой статьей работы наших силовых структур. Ну и правительство, Центральный банк нас также заверяют, что их технологии позволяют эту информацию защитить, то есть именно информация, связанная с биометрическими данными, будет защищаться наиболее серьёзно.

Стенограммы по законопроекту №157752-7

СКОРОБОГАТОВА О. Н., первый заместитель председателя Центрального банка Российской Федерации.

Предполагается, что система будет работать следующим образом: человек, обращаясь в банк первый раз, регистрируется как клиент, представляет свои документы; в банке снимают его биометрические данные - мы с коллегами из силовых структур, из министерств и ведомств определили, что это лицо и голос; эти данные попадают, что важно, в государственную систему единой аутентификации и идентификации и в базу биометрической платформы; когда клиент обращается во второй банк, он уже может себя удалённо идентифицировать по параметрам, которые с его согласия в эту единую систему были зашиты.

… решаем на государственном уровне вопрос о единой системе защиты информации. https://lexfeed.ru/law/157752-7

Атаки на биометрические данные

Нейросеть Baidu уже умеет имитировать ваш голос

Baidu Research занимается разработкой нейросети Deep Voice, она имитирует голоса людей. Для работы достаточно очень короткой записи оригинального голоса.

В ноябре 2016 года Adobe представил свой проект VoCo. На презентации показали, что инструмент может читать указанный текст и звучит довольно реалистично.

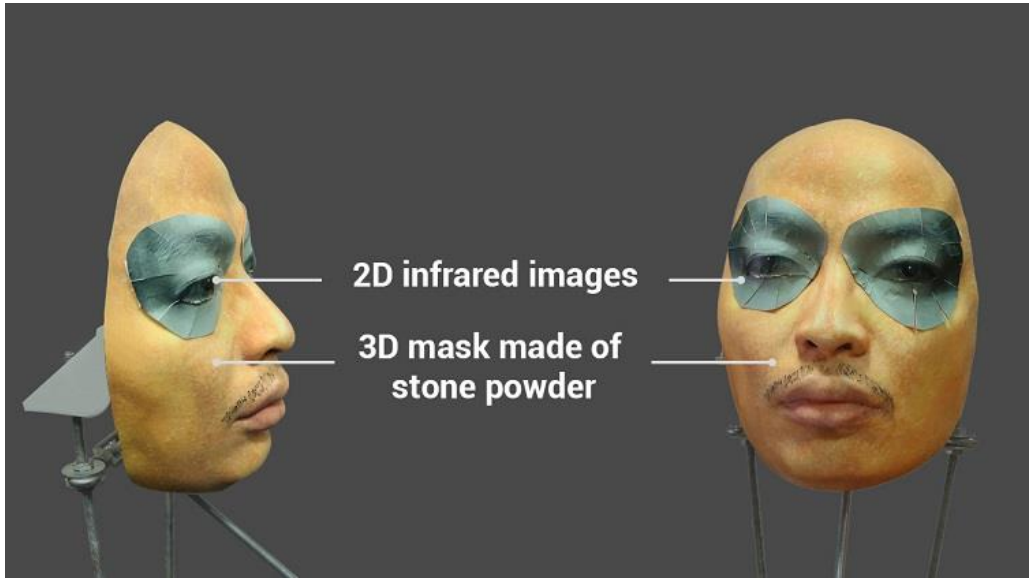
нейросети смогут и лица заменять лучше голливудских художников.

https://wylsa.com/nejroset-baidu-uzhe-umeet-imitirovat-vash-golos/

Атаки на биометрические данные

ЭКСПЕРТАМ УДАЛОСЬ ОБОЙТИ ЗАЩИТУ IPHONE X

Для этой цели они создали маску одного из сотрудников, зарегистрированного в системе тестового телефона. Маска состояла из распечатанных двухмерных изображений глаз, сделанного вручную силиконового носа и других частей лица, а также каркаса, распечатанного на популярном 3D-принтере. Кроме того, для обмана системы щеки и область вокруг лица подверглись «специальной обработке».
https://www.securitylab.ru/news/489643.php



Атаки на биометрические данные

Специальные очки меняют личность человека для системы распознавания лиц

Группа исследователей из Университета Карнеги-Меллона подробно изучила вопрос и на днях опубликовала результаты своего исследования на эту тему. Фактически, исследователи ведут речь о новом типе атак. Атаки, которые физически меняют внешность, но при этом выглядят безобидными для внешнего наблюдателя.

Например, для лица белого мужчины специально подобранные очки имперсонифицируют личность Милы Йовович в 87,87% случаев. Три автора научной работы (три белых мужчины) испытали очки на себе и заявили, что напечатанные очки с специфическим паттерном позволяют провести атаку на уклонение в 80% случаев против самых современных коммерческих систем распознавания лиц.

https://geektimes.ru/post/282192/

Атаки на биометрические данные

Атаки на биометрические данные

Китайские исследователи создали бейсбольную кепку, оснащенную миниатюрными инфракрасными светодиодами, которые размещены таким образом, что инфракрасные лучи, падающие на лицо владельца головного убора, помогают не только скрыть его личность, но и «выдать себя за другого человека для прохождения основанной на распознавании лица аутентификации».

Для проверки своей теории исследователи использовали фотографии четырех случайных людей, им удалось обмануть системы распознавания лиц в 70% случаев при условии наличия небольшого внешнего сходства между жертвой и самозванцем.

Атаки на биометрические данные

представители Университета Северной Каролины смогли обмануть четыре из пяти систем распознавания на конференции по безопасности Usenix в 2016 г.

В основе биометрии лежат статистические методы, поэтому алгоритмы способны ошибаться, признает Дырмовский из ЦРТ. Типов ошибки два: система пропускает «чужого» и отказывает в доступе «своему». Чувствительность системы (вероятность ошибки в ту или иную сторону) настраивает ее владелец. Система с высоким порогом пустит владельца в квартиру в лучшем случае с пятого раза, но не даст войти злоумышленникам, а менее строгая, например в call-центре банка, всегда будет узнавать владельца голоса, но и ошибаться будет чаще
https://www.vedomosti.ru/technology/articles/2018/03/28/755116-obmanut-sistemi

Атаки на биометрические данные

Позволяют ли биометрические данные осуществить идентификацию?

Да: Уникальность.

Позволяют ли биометрические данные осуществить аутентификацию?

С помощью чего проводят аутентификацию?

Что-то знаю: секрет, пароль и т.п.

Секрет может узнать, перехватить злоумышленник, необходимо менять

Что-то имею: ключ, токен, карта и т.п.

Можно утратить (потерять, похитили), клонировать

Биометрические данные?

Атаки на биометрические данные

Биометрические данные не являются секретом или труднодоступным объектом.

Параметры лица и голоса легко можно записать.

Изготовление дубликата – зависит от уровня технологий.

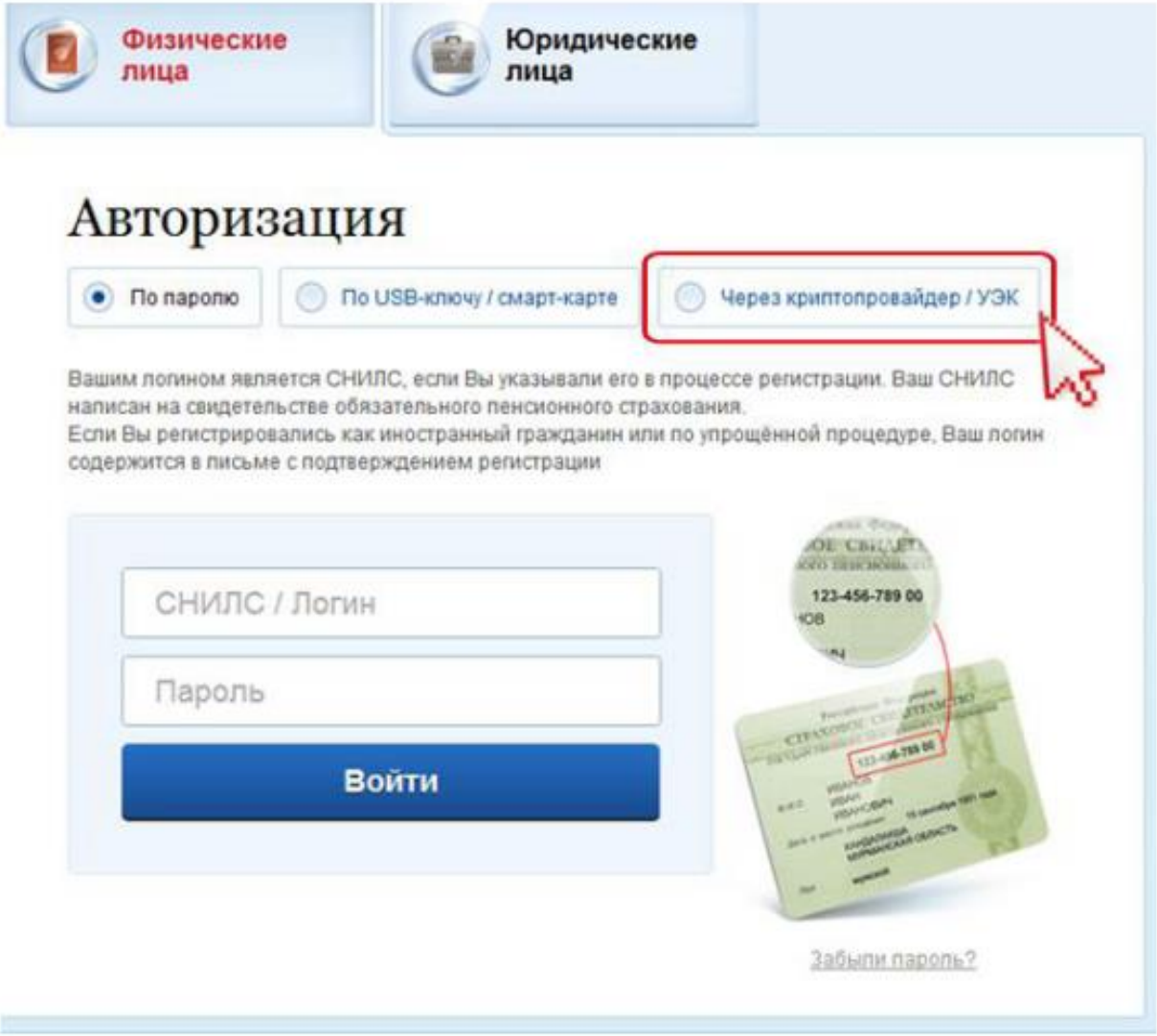
Если сейчас сложно (невозможно) и дорого, то в будущем может быть реализуемо и дешево.

Затраты – выгода.

Удаленная биометрическая идентификация не является 100% безопасной, необходимо устанавливать ограничения, лимиты, чтобы атаки были экономически не выгодны.

6. Вход в личный кабинет на сайте Государственных услуг

• На открывшейся странице выберите вариант авторизации «Через криптопровайдер» и нажать «Войти»:



АО «УЭК» сообщает о закрытии проекта по выпуску универсальных электронных карт

16 Января 2017

АО «УЭК» сообщает об отмене выпуска и выдачи универсальных электронных карт (УЭК) с 1 января 2017 года. Соответствующее решение было принято на федеральном уровне и закреплено Федеральным законом от 28.12.2016 №471-ФЗ.

СПАСИБО!