МОШЕННИКИ В ЦИФРОВОМ МИРЕ

КАК СБЕРЕЧЬ СВОИ ДЕНЬГИ?

Светлана Толкачева

Авторский курс

Толкачева Светлана

Топ-менеджер банка / Группа ВТБ
Автор учебника «Финансовая грамотность. Цифровой мир»/ (издательство «Просвещение»)
Автор YouTube-канала «Финансовая грамотность со Светланой Толкачевой»

ХОЧУ ЗНАТЬ БОЛЬШЕ

www.youtube.com/c/SvetlanaTolkacheva

www.instagram.com/Tolkacheva_sv

ОБЩЕСТВЕННАЯ ДЕЯТЕЛЬНОСТЬ

- С 2015 года — мастер-классы по социализации и адаптации детей из интернатных учреждений по теме «Финансовая грамотность», автор и ведущая
- Член экспертного совета при Центральном банке Российской Федерации, руководитель рабочей группы по взаимодействию с образовательными организациями
- Член Наблюдательного совета Ассоциации развития финансовой грамотности
- Член Общественного совета при Департаменте образования и науки города Москвы

ОБРАЗОВАНИЕ

- 2007-2009 гг. — Бизнес-школа Университета Антверпена (UAMS) совместно с ИБДА АНХ при Правительстве РФ (Бельгия, Антверпен), executive MBA
- 2005 г. — Московский университет МВД России, кандидат юридических наук
- 2002-2003 гг. — Международная академия предпринимательства, консультант по налогам и сборам
- 1997-2002 гг. — Московский государственный социальный университет, юриспруденция
- 1995-2000 гг. — Российская экономическая академия им Г. В. Плеханова, экономика и управление на предприятии

ПРОФЕССИОНАЛЬНАЯ ДЕЯТЕЛЬНОСТЬ

Более 17 лет работы в финансовых компаниях, включая 13 лет в банковской сфере

СОДЕРЖАНИЕ

ПРЕДПОСЫЛКИ УВЕЛИЧЕНИЯ ЧИСЛА МОШЕННИЧЕСТВ

ПРЕДПОСЫЛКИ УВЕЛИЧЕНИЯ ЧИСЛА МОШЕННИЧЕСТВ

УВЕЛИЧЕНИЕ объема финансовых транзакций

ИЗБЫТОК противоречивой информации и **РАЗНООБРАЗИЕ** видов финансовых инструментов

ВОЗМОЖНОСТИ удаленной идентификации и аутентификации

УСКОРЕНИЕ технологических процессов и **ПЕРЕХОД** сделок и операций в цифровую среду

РАЗРЫВ между знаниями о финансовых инструментах и поведением граждан, в том числе в цифровой среде

Возраст ребенка, в котором большинство родителей инициирует пользование электронными устройствами, — 3 года*

(почти половина взрослых начинает давать ребенку телефон или планшет в автомобиле)

К 4-6 годам у 54% детей есть планшет или смартфон

К 11-14 годам — уже у 97%

«По итогам 2020 года мы вышли на уровень около 70% безналичных платежей. Это больше, чем мы ожидали в начале года. Конечно, в условиях пандемии был дополнительный стимул пользоваться безналичными платежами»

«Пять лет назад на безналичные платежи приходилось всего 30%, и никто не верил, что ситуация изменится»

Из выступлений председателя ЦБ РФ Э.Набиуллиной на пресс-конференции 12.02.2021 и в ГД в ноябре 2019

ФИНАНСОВАЯ ГРАМОТНОСТЬ БЕЗ ЗНАНИЙ О ЦИФРОВОЙ СРЕДЕ

не позволяет эффективно решать повседневные задачи

* По данным исследования «Лаборатория Касперского», представленного в марте 2019 - «Взрослые и дети в цифровом мире»

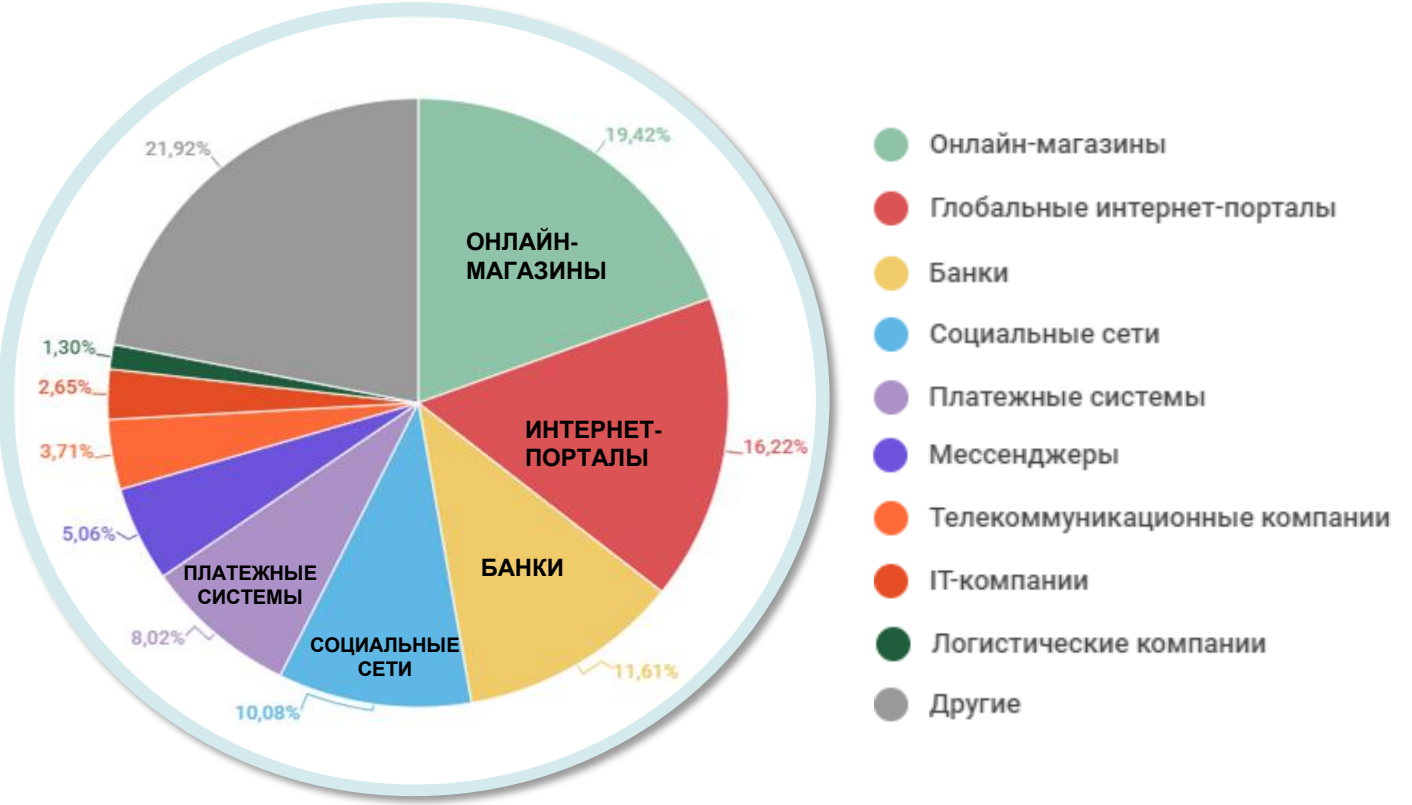
МИШЕНИ ФИШИНГОВЫХ АТАК

ОРГАНИЗАЦИИ — МИШЕНИ ФИШИНГОВЫХ АТАК ВО II КВАРТАЛЕ 2020*

ФИШИНГ (от англ fishing — «рыбная ловля, выуживание») - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (финансовым данным, а также логинам и паролям).

Это достигается путем:

- **проведения массовых рассылок электронных писем** от имени популярных брендов,
- **личных сообщений внутри различных сервисов**, например, от имени банков или внутри социальных сетей
- также перейти на фишинговый сайт можно **путем клика на баннеры,** всплывающие при открытии страниц в Интернете.



В ТОП-3 ПО КОЛИЧЕСТВУ ФИШИНГОВЫХ АТАК ВХОДЯТ ОНЛАЙН-МАГАЗИНЫ, ГЛОБАЛЬНЫЕ ИНТЕРНЕТ-ПОРТАЛЫ И БАНКОВСКИЙ СЕКТОР – совокупная доля атак на эти организации во втором квартале 2020 года составила **47,25%****.

Первое и второе место – без изменений по сравнению с предыдущим кварталом. На третье место вернулась категория «Банки» (11,61%), сместив «Социальные сети» (10,08%) на четвертое.

* По данным с сайта https://www.kaspersky.ru/.

** Рейтинг категорий атакованных фишерами организаций основан на срабатываниях компонента системы «Антифишинг» на компьютерах пользователей.

СТАТИСТИКА КИБЕРПРЕСТУПЛЕНИЙ

ПО ДАННЫМ СТАТИСТИКИ ГЕНПРОКУРАТУРЫ И МВД РФ
за январь-декабрь 2020*

ОБЩИЕ СВЕДЕНИЯ О СОСТОЯНИИ ПРЕСТУПНОСТИ

	ЗАРЕГИСТРИРОВАНО (в отчетном периоде)		Из числа преступлений, дела и материалы о которых находились в производстве в отчетном периоде:	
	ВСЕГО	+,- в %	РАСКРЫТО* ВСЕГО	+,- в %
ВСЕГО ПРЕСТУПЛЕНИЙ	2044221	1,0	1031987	-1,9
совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	510396	73,4	94942	45,5

25 %

СТРУКТУРА

Почти КАЖДОЕ ЧЕТВЕРТОЕ ПРЕСТУПЛЕНИЕ совершено с использованием IT-технологий или в сфере компьютерной информации

Из них:

- **БОЛЕЕ ПОЛОВИНЫ (52,4%) относится к категориям ТЯЖКИХ И ОСОБО ТЯЖКИХ (267,7 тыс.)**
- **БОЛЕЕ ПОЛОВИНЫ (58,8%) совершено с использованием СЕТИ ИНТЕРНЕТ (300,3 тыс.)**
- **СВЫШЕ 40 % - с помощью средств МОБИЛЬНОЙ СВЯЗИ (218,7 тыс.)**

САМЫЕ ПОПУЛЯРНЫЕ КБ

- неправомерный доступ к компьютерной информации (ст. 272 УК РФ)
- распространение вредоносных компьютерных программ (ст. 273 УК)
- мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК)

В феврале 2020 МВД России сообщило, что в структуре ведомства появились **подразделения по борьбе с киберпреступлениями**. Ранее такие подразделения создали в СК РФ

ДИНАМИКА

РОСТ КИБЕРПРЕСТУПЛЕНИЙ ЗА ГОД : +73,4 %, 510,4 тыс.

КОЛИЧЕСТВО КИБЕПРЕСТУПЛЕНИЙ В РОССИИ ЗА 7 ЛЕТ ВЫРОСЛО В 46 РАЗ!

2013 - 11 тыс.
2014 - 44 тыс.
2016 - 66 тыс.
2019 - 294 тыс.
2020 - 510 тыс.

* Из Отчета МВД РФ за январь-декабрь 2020 года «Состояние преступности в России»

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ В ЦИФРОВОМ МИРЕ

ИДЕНТИФИКАЦИЯ — КОМУ И ЗАЧЕМ НУЖНА?

ЦИФРОВЫЕ КОММУНИКАЦИИ

обмен информацией между устройствами через Интернет

- публичные — для открытого обмена информацией (соцсети, форумы, блоги)
- частные: в том числе для обмена значимой/ финансовой информацией (чат-боты, мессенджеры)

ЦИФРОВАЯ ИДЕНТИЧНОСТЬ

набор данных клиента, используемых системой для его идентификации

- государственные системы: ИНН, СНИЛС, паспорт, регистрация на портале «Госуслуги»
- частные системы: Facebook, «ВКонтакте» и другие

ГРАЖДАНИН

ЦИФРОВЫЕ РАСЧЕТЫ

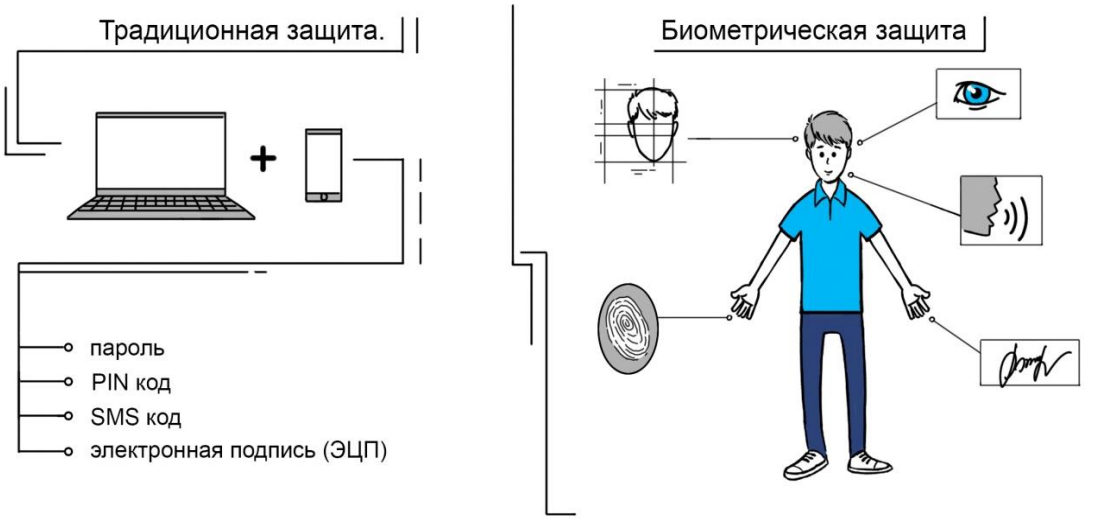
система безналичных расчетов между контрагентами с использованием банковских счетов, пластиковых карт, электронных кошельков

ГОСУДАРСТВО

ПЕРСОНАЛЬНЫЕ ДАННЫЕ НИКОМУ НЕЛЬЗЯ ПЕРЕДАВАТЬ!

ТРАДИЦИОННАЯ И БИОМЕТРИЧЕСКАЯ ЗАЩИТА

БИОМЕТРИЧЕСКИЕ ДАННЫЕ - это уникальные биологические и физиологические характеристики, которые позволяют установить личность человека (опечаток пальца, изображение лица, голос, радужная оболочка глаза, рисунок вен ладони и пальца, кровь и др.).



Карта точек банковского обслуживания, где все желающие могут сдать биометрические данные, размещена на сайте Банка России https://www.cbr.ru/ .

ЗАКОНОДАТЕЛЬСТВО

- С 30 июня 2018 года в силу вступил закон об удаленной биометрической идентификации граждан — Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»*.
- Рассмотрение законопроекта об обязательном сборе биометрических данных в банках и передаче их в ЕБС было отложено. Документ** был принят Госдумой в первом чтении в июле 2019 г. Предложенные поправки к закону предусматривают сбор биометрии непосредственно при открытии счетов и вкладов в банках и их филиалах.

* Внесение изменений в №115-ФЗ от 07.08.2001 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», №395-1 от 02.12.1990 «О банках и банковской деятельности»

** Документ, принятие которого было отложено на неопределенный срок в связи с вопросами силовых структур и бизнеса, представляет собой поправки к закону «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

ЭЛЕКТРОННАЯ ПОДПИСЬ

ЭЛЕКТРОННАЯ ПОДПИСЬ (ЭП, ранее – ЭЦП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и используется для определения подписывающего информацию

(Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»).

Свойства ЭП	Вид ЭП		
	Простая	Неквалифи-цированная	Квалифициро-ванная
Способ получения	Генерируется самостоятельно	В любом удостоверяющем центре	В аккредитованном удостоверяющем центре
Защита подписанного документа	Не защищает документ от подделки	Защищает документ от подделки	Защищает документ от подделки
Юридическая значимость	Требует соглашения о признании	Требует соглашения о признании	Равна собственно-ручной подписи
Где хранится	—	На любом носителе	На защищенном носителе

ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ ЭП:

Электронный документооборот
(как аналог собственноручной подписи/ печати на бумажном документе)

- Во внутреннем документообороте как средство визирования и утверждения электронных документов внутри организации
- В межкорпоративном документообороте как гарант юридической силы (подлинности документа, доказательства в суде)

Электронная отчетность для контролирующих органов
(придание юридической значимости документам при сдаче отчетности через интернет с помощью сертификата ЭП, выпущенного надежным удостоверяющим центром)

Государственные услуги
(с помощью ЭП гражданин может заверять документы и заявления, отправляемые в ведомства в электронном виде, а так же получать подписанные письма и уведомления о том, что обращение принято)

Арбитражный суд
(при возникновении споров между организациями в качестве доказательства в суде могут использоваться электронные документы)

ЕСИА И ЕБС. ГРАЖДАНИН И ГОСУДАРСТВО

НА ЧТО НАПРАВЛЕН ЗАКОН ОБ УДАЛЕННОЙ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ГРАЖДАН?

НА УСТАНОВЛЕНИЕ ПОРЯДКА ПРОВЕДЕНИЯ ПОЛНОЙ УНИВЕРСАЛЬНОЙ УДАЛЕННОЙ ИДЕНТИФИКАЦИИ

ПОСРЕДСТВОМ:

ЕСИА

Доступ граждан к электронным услугам государства по системе «один пароль – доступ ко всем государственным сайтам»

Получение учётной записи ЕСИА – при удостоверении своей личности в многофункциональном центре госуслуг с помощью паспортных данных, ИНН и СНИЛС (www.gosuslugi.ru)

Оператор - Министерство цифрового развития, связи и массовых коммуникаций

ЕБС

Хранение БКШ (биометрических контрольных шаблонов - биометрических персональных данных физических лиц: изображение лица и голос)

Получение БКШ - банками при проведении идентификации при личном присутствии лица

Оператор - Ростелеком

ГЛАВНОЕ ПРЕИМУЩЕСТВО — ВОЗМОЖНОСТЬ ПОЛУЧАТЬ И ОФОРМЛЯТЬ УСЛУГИ ОНЛАЙН

ЕСИА И ЕБС. ЦИФРОВОЙ ПРОФИЛЬ

ЦИФРОВОЙ ПРОФИЛЬ ГРАЖДАНИНА (ЦП)

ЦП – совокупность:

- ✓ **всех данных о гражданине** (в распоряжении госорганов и ГИС*)
- ✓ **технических средств для управления** этими данными

ПРОЦЕСС ВНЕДРЕНИЯ ЦП

ЭКСПЕРИМЕНТ ПО ЗАПУСКУ ЦП**

В мае 2020 запущен в эксплуатацию сервис, позволяющий гражданам через ЛК ЕСИА дистанционно предоставлять банкам и страховщикам информацию о себе и получать услуги полностью в цифровом виде, не посещая офис.

УЧАСТНИКИ ПИЛОТНОГО ПРОЕКТА

- 20 банков, 4 страховщика, а также МФО и операторы финансовых платформ (по согласованию с ЦБ). С использованием ЦП возможно заключение любых сделок с банками, со страховщиками – КАСКО и ОСАГО.
- Согласие на обработку сведений из ЕСИА финорганизациям дали более 900 тыс.человек

СВЕДЕНИЯ В ЦП

На текущий момент в ЦП содержатся записи более 30 типов (паспорт, адрес, ИНН, водительские права, электронная трудовая книжка и др.), планируется дальнейшее расширение перечня

КОГДА ПРИМУТ ЗАКОН?

В ГД ожидают принятия закона***в первой половине 2021 (запуск с 2022). Эксперимент признан успешным и продлен до конца 2021 года

В БУДУЩЕМ ЦИФРОВОЙ ПРОФИЛЬ СТАНЕТ УНИВЕРСАЛЬНЫМ ИНСТРУМЕНТОМ УДАЛЕННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ ГРАЖДАНАМИ, ГОСУДАРСТВОМ И КОМПАНИЯМИ

* Государственные информационные системы

** В соответствии с постановлениями Правительства РФ от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах», от 27.03.2020 N 350 и от 24.11.2020 N 1911 (внесение изменений в ПП № 710) https://cbr.ru/press/event/?id=6723

*** Законопроект № 747513-7 "О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации) https://sozd.duma.gov.ru/bill/747513-7

КАКИМ БУДЕТ ПАСПОРТ ГРАЖДАНИНА?

УДОСТОВЕРЕНИЕ ЛИЧНОСТИ ГРАЖДАНИНА РФ НОВОГО ОБРАЗЦА
с расширенными функциями - на пластиковом носителе с чипом на базе технологии NFC*

- **На пластике** - фотография владельца и персональные данные
- **На чипе** – ИНН, СНИЛС, водительское удостоверение, полис ОМС, несколько вариантов фотографий в разных ракурсах, отпечатки пальцев, снимок радужки глаз (точный перечень цифровых данных должно утвердить правительство)
- **Срок действия** – 10 лет
- **Карта снабжена** голографическим изображением, имеет российскую криптографию, QR-код
- **При потере** возможна блокировка

Постепенный процесс перехода на новый паспорт:

- с 2025 года - выдача только электронных паспортов
- к 2028 году – полный переход
- с 2030 года - прекращение хождения бумажных паспортов

Получение в первую очередь:

- при выдаче паспорта при достижении ребенком 14 лет;
- при очередной (плановой) замене в 20 и 45 лет;
- при замене паспорта ввиду утраты, повреждения и т.д.

Помимо пластиковой карты планируется использовать **ПРИЛОЖЕНИЕ «МОБИЛЬНЫЙ ИНДЕНТИФИКАТОР»** (разработчик – Минкомсвязи)

В срок до 01.12.2021 в пилотной зоне Москвы планируется осуществить все подготовительные работы к запуску **эксперимента** по переходу на электронные паспорта и их дубликаты в мобильном приложении**

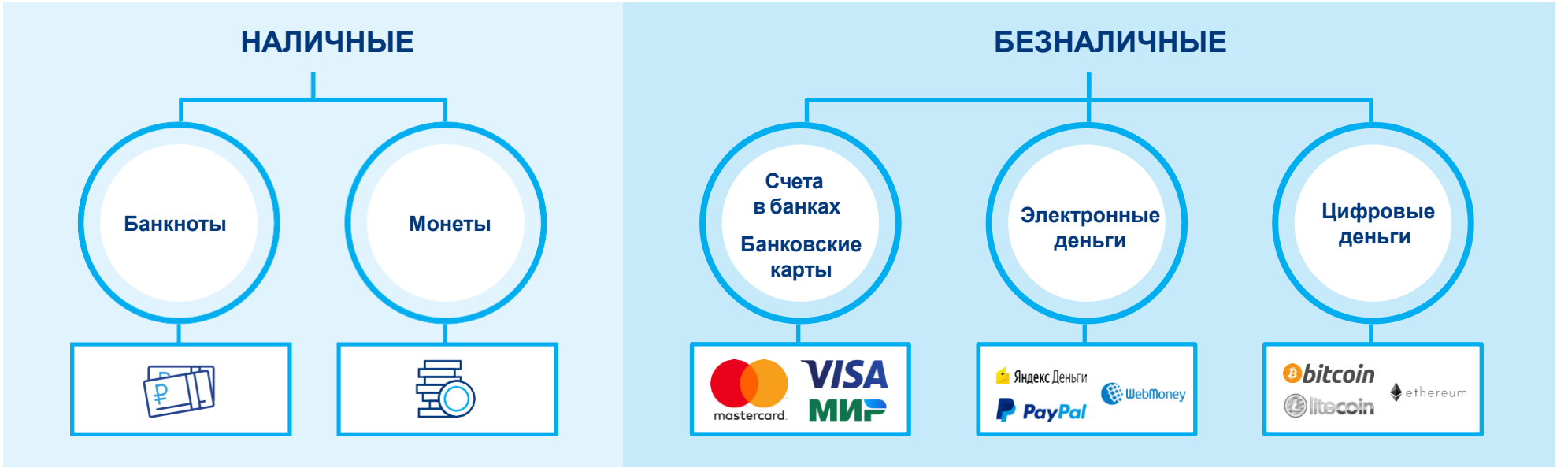
- *Не будет использоваться для значимых с юридической точки зрения услуг (продажа квартиры и т.п.)*
- *Авторизация гражданина в приложении проходит в пилотном МФЦ с получением специального QR-кода*

* Законопроект № 845287-7 Об основных документах, удостоверяющих личность (о правовом статусе основных документов, удостоверяющих личность, и систематизации таких документов, выданных гражданам РФ, иностранным гражданам и лицам без гражданства) – рассмотрение закона в первом чтении в ГД

** Пресс-центр МВД России от 27.11.2020 https://mvdmedia.ru/news/official/o-vnedrenii-pasporta-grazhdanina-rossiyskoy-federatsii-s-elektronnym-nositelem-informatsii/

ЭВОЛЮЦИЯ ДЕНЕГ И СПОСОБЫ УПРАВЛЕНИЯ ИМИ

ЭВОЛЮЦИЯ ДЕНЕГ



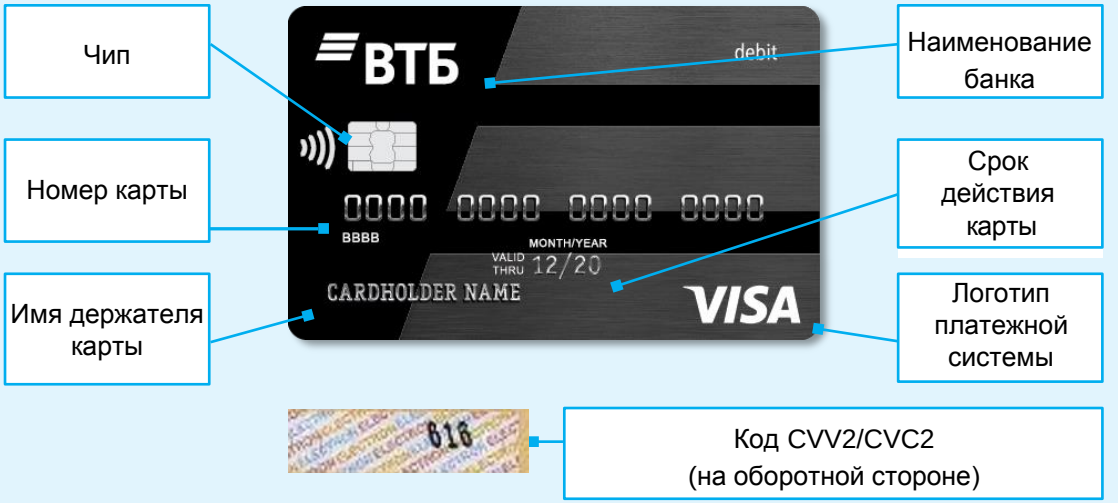
Цифровые деньги*
НЕ могут на текущем этапе выполнять функции традиционных денег

не применяются в качестве средства измерения стоимости	не являются средством платежа	не используются как средства накопления и сбережения

ЦИФРОВЫЕ ДЕНЬГИ — ЭТО ЦИФРОВОЙ АКТИВ, А НЕ ДЕНЬГИ

* Федеральным законом от 31.07.2020 N 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» цифровые деньги определены как имущество, а не денежные средства в традиционном смысле. Цифровые деньги могут выпускаться любыми лицами и не имеют единых правил обращения.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ПЛАСТИКОВОЙ КАРТЫ



1-6-цифры – BIN (банковский идентификационный номер):

1 - код платежной системы: **2** – МИР, **4** – Visa, **5** – Mastercard

2-6 - банковский идентификатор

7-8 цифры – код продукта

9-предпоследняя цифры – индивидуальный номер клиента

Последняя цифра – проверочное число (с помощью специального алгоритма можно проверить достоверность номера)

ПИН-код — четырехзначный секретный код, необходимый для совершения операций в банкоматах/магазинах

Код CVV2/CVC2 — трехзначный код на оборотной стороне карты для идентификации при совершении интернет-транзакций

- **Храните карту отдельно от ПИН-кода**
- **Никому не сообщайте свой ПИН и CVV-коды**
- **Всегда прикрывайте клавиатуру при вводе ПИН-кода**
- **При потере карты сразу звоните в call-центр банка для её блокировки**
- **Никогда и никому не передавайте карту**
- **Используйте двухфакторную аутентификацию во время платежа онлайн — 3D Secure**
  (перенаправление пользователя на страницу банка-эмитента для ввода одноразового кода, полученного по SMS на телефон, привязанный к карте)
- **Используйте мобильные приложения с технологиями для бесконтактной оплаты (NFC)**

ЭЛЕКТРОННЫЙ КОШЕЛЕК

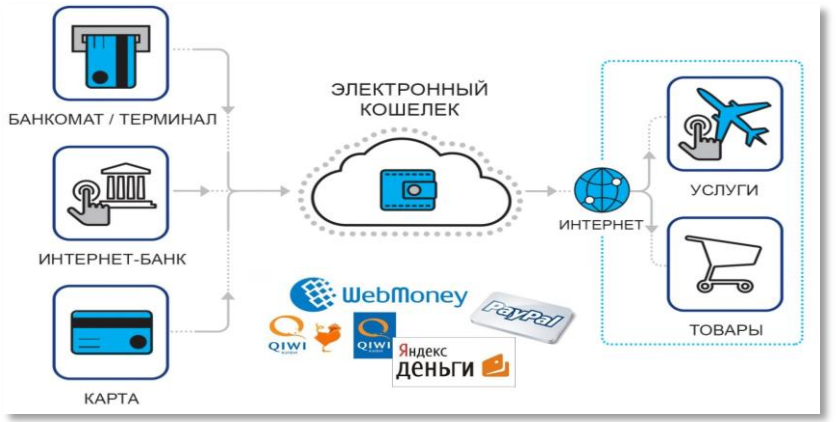
ЗАКОНОДАТЕЛЬНЫЕ ОГРАНИЧЕНИЯ НА ЭЛЕКТРОННЫЕ КОШЕЛЬКИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ*

ЭЛЕКТРОННЫЙ КОШЕЛЕК С ИДЕНТИФИКАЦИЕЙ

- ☑ **Для идентифицированного пользователя** остаток на счету в любой момент не должен превышать **600 тыс. руб.**

  (полная идентификация требует присутствия клиента в офисе платежного сервиса для подтверждения личности (для «Яндекс.Деньги» — привязка к карте Сбербанка))

- ☑ **При упрощенной идентификации** требуются только Ф.И.О. и номер паспорта:
  - остаток - не более 60 тыс.руб.
  - сумма операций в месяц - не более 200 тыс.руб.
  - операции только в пользу юридических лиц и ИП



ЭЛЕКТРОННЫЙ КОШЕЛЕК БЕЗ ИДЕНТИФИКАЦИИ

- ☑ Лимит в течение календарного месяца - в размере **40 тыс. руб.** на ввод
- ☑ Остаток электронных денежных средств на счету анонимного пользователя в любой момент не должен превышать **15 тыс. руб.**
- ☑ Нельзя использовать кошелек для платежей за рубеж, переводов другим физическим лицам и снятия наличных.
- ☑ Сейчас с анонимного кошелька можно оплатить товары и услуги только российских организаций.

Запрет на снятие наличных:

в марте 2019 г. российские власти ввели запрет на снятие наличных с анонимных кошельков.

Запрет на пополнение наличными:

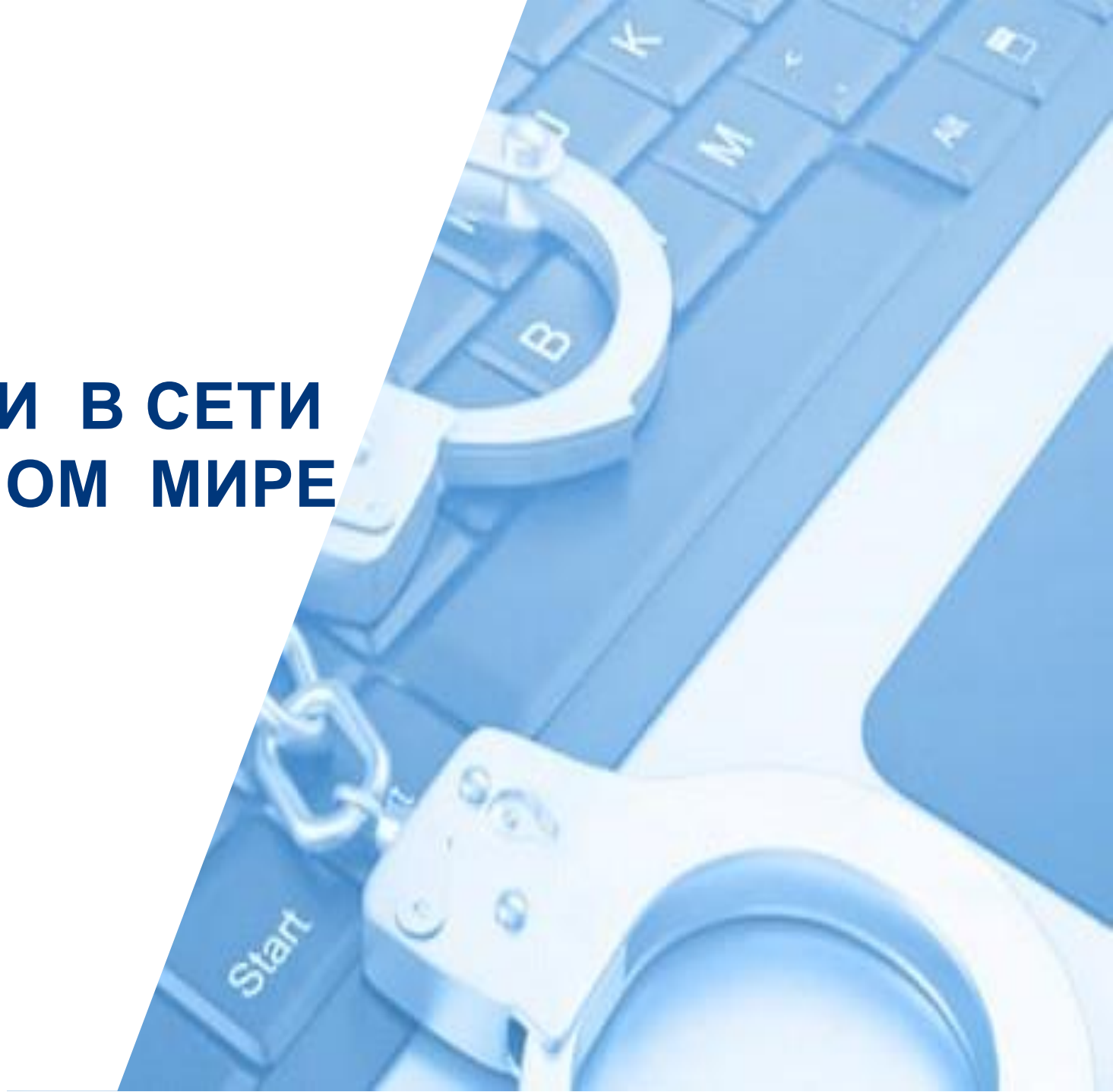
с 3 августа 2020 года вступили в силу поправки в Закон «О национальной платежной системе», в соответствии с которыми физические лица не смогут пополнять электронные кошельки без предварительной идентификации личности**.

ЭЛЕКТРОННЫЕ ДЕНЬГИ В ОТЛИЧИЕ ОТ ЦИФРОВЫХ ПРИВЯЗАНЫ К ТРАДИЦИОННЫМ ДЕНЬГАМ, К КОТОРЫМ ОРГАНИЗОВАН УДАЛЕННЫЙ ДОСТУП

* Российский закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ.

** Федеральный закон от 02.08.2019 № 264-ФЗ.

МОШЕННИКИ В СЕТИ
И В РЕАЛЬНОМ МИРЕ



ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО И IP-ТЕЛЕФОНИЯ

Звонки с целью кражи ваших средств, выманивания реквизитов банковских карт и одноразовых паролей*

- **звонки по размещенным объявлениям** о продаже личного имущество через сайты «Авито», «Юла» якобы для приобретения товара
- **Звонки из социальных служб** (мошенники сообщают о необходимости получить материальные компенсации за неиспользованные льготы; могут попросить сделать якобы возвратный «идентификационный» платеж)
- **звонки с номеров телефонов банка** (мошенники представляются работниками службы безопасности банка и сообщают клиенту о якобы проведенных операциях по его карте и необходимости их отмены)

- **звонки из налоговой** (мошенники представляются работниками налоговых служб и предлагают вернуть НДС, ссылаясь на фейковое постановление о праве на получение денежной компенсации затрат на оплату товаров иностранного производства, и просят оплатить ряд услуг: консультацию юриста, заполнение анкеты и др.)
- **звонки от «представителя сотового оператора»** (мошенники предлагают перерегистрировать SIM-карту, пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного списываются деньги)

❖ **МОШЕННИЧЕСТВО ЧЕРЕЗ IP-ТЕЛЕФОНИЮ**: номера мошенников могут отражаться как номера телефонов банка или любого номера из вашей телефонной книжки**

РАБОТАЕТ ТОЛЬКО НА ВХОДЯЩИЕ ЗВОНКИ - ЧТОБЫ РАЗВЕЯТЬ СОМНЕНИЯ, НУЖНО ПЕРЕЗВОНИТЬ

❖ **СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ИНФОРМАЦИЮ О БАНКОВСКИХ СЧЕТАХ И КАРТАХ, А ТАКЖЕ КОНТАКТЫ РОДНЫХ И БЛИЗКИХ ЛЮДЕЙ НЕЛЬЗЯ ПРЕДОСТАВЛЯТЬ НИКОМУ!**

* По данным ЦБ, в марте-мае 2020 года (с начала пандемии) количество мошеннических телефонных звонков выросло примерно на 300%. На мошенников работают целые так называемые «черные call-центры» (могут находится заграницей, и даже в тюрьмах*) На ликвидацию последних ФСИН планирует потратить 3 млрд.руб. По инициативе Минкомсвязи и МВД создана межведомственная рабочая группа по противодействию телефонному мошенничеству. В нее вошли также представители ФСБ, Роскомнадзора, ЦБ РФ, банков и операторов связи

** В июле 2020 Минкомсвязи предложило поправки к закону "О связи", которые обяжут операторов отслеживать и пресекать исходящие звонки с "подменных" номеров.

SMS-МОШЕННИЧЕСТВО

- Напоминаем о необходимости погасить задолженность по кредиту. Ц.Б.Р.Ф. Информация 8 800 XXX XX XX
- Оплата на сайте Ozon.ru на сумму 3500 руб. успешно зарезервирована. Если не совершали операцию, необходимо перезвонить по номеру 8800-511-51-36
- Ваша карта заблокирована в целях безопасности. Для уточнения информации необходимо перезвонить по определившемуся номеру. +79961763523
- Поздравляем!!! Пополнение Вашего телефона через карты Visa, MasterCard вошел в число призовых! Вы выиграли 100000 руб.! Информация по тел. 8-800-511-3725 или Giperkassa.ru

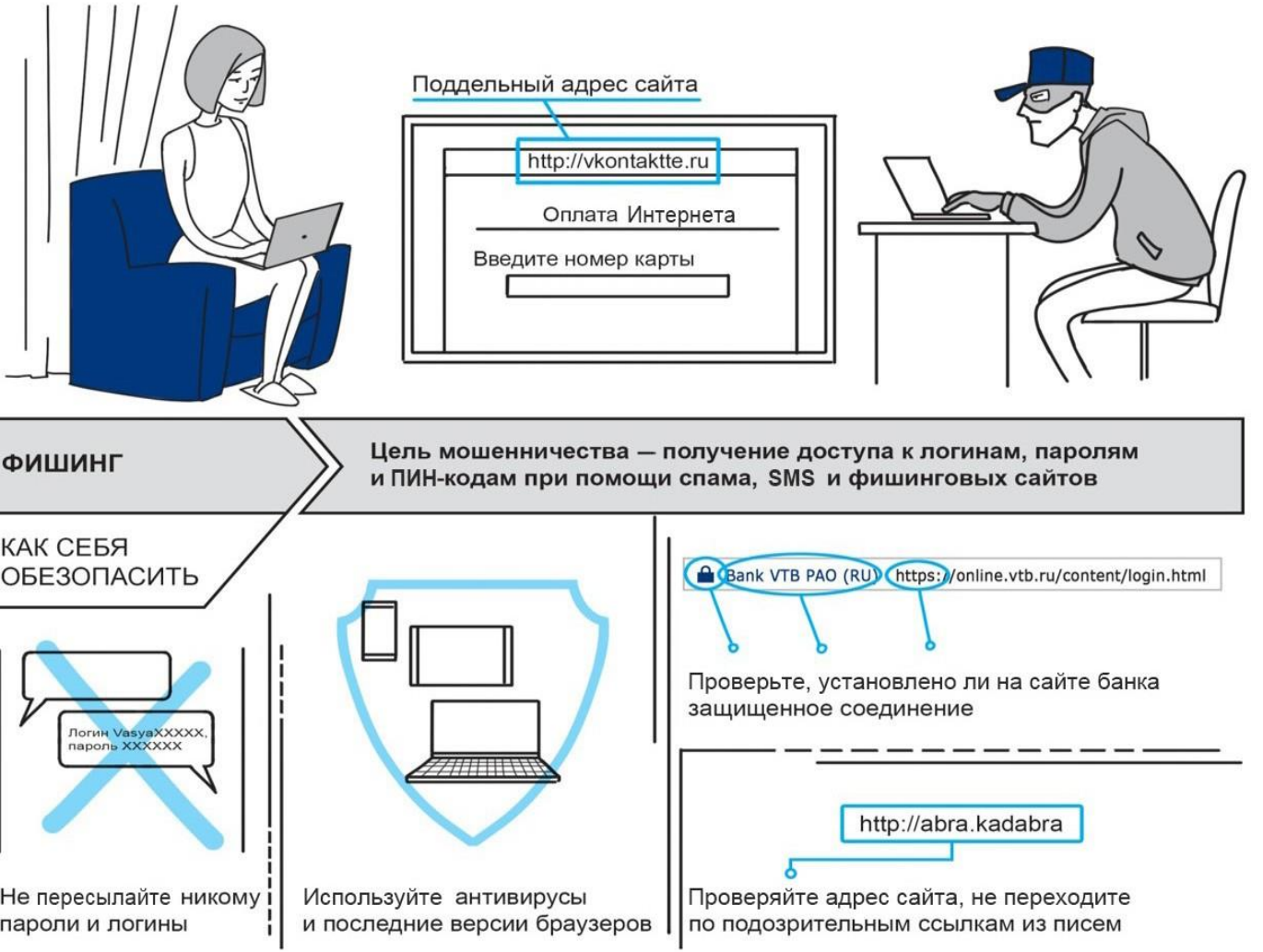
Рассылка SMS-сообщений с указанием номера телефона для обратной связи

Рассылка SMS-сообщений, нацеленная на вынуждение жертвы перевести деньги на счета и телефоны мошенников

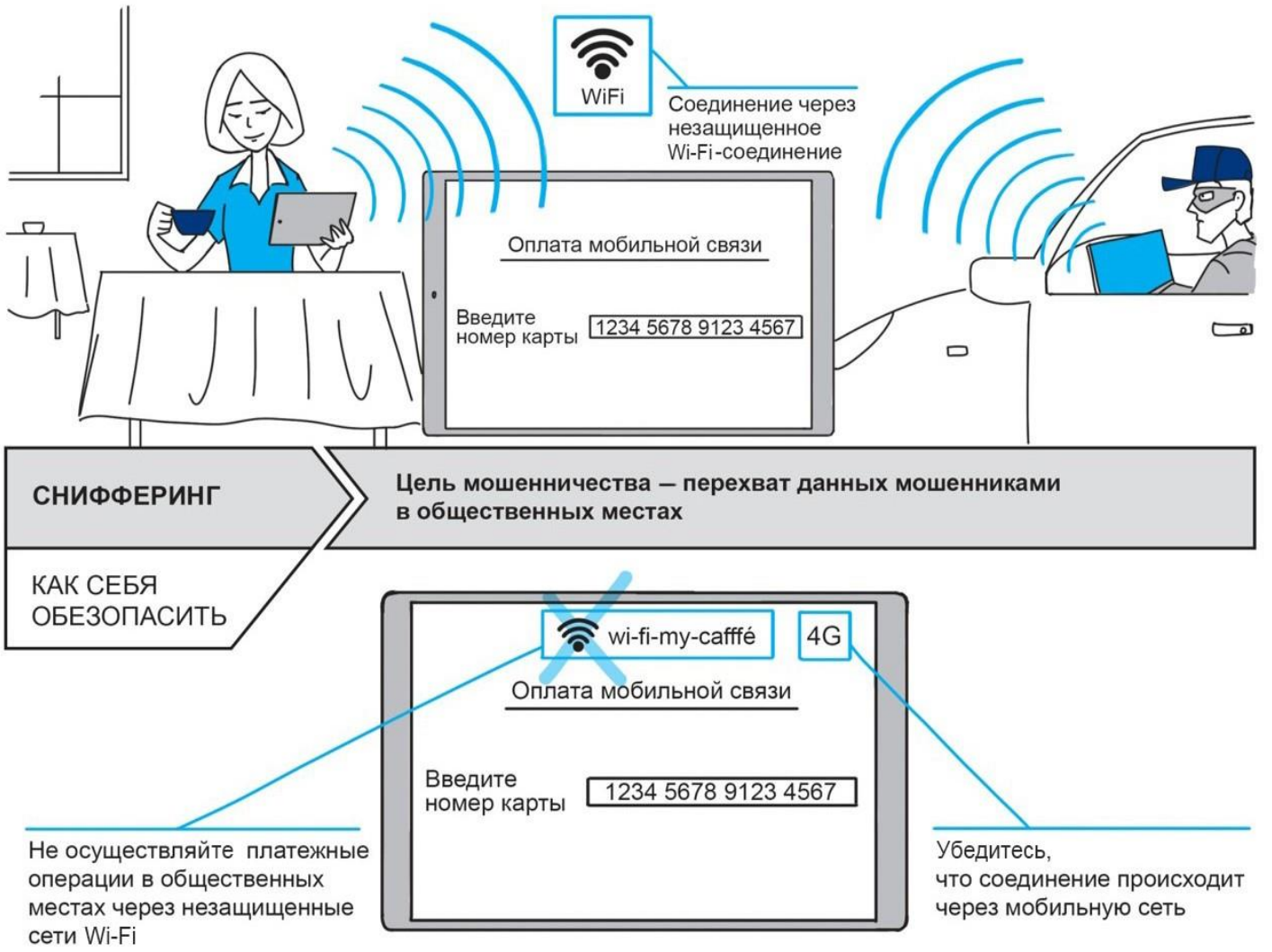
- Мама, пополни счет на этот номер на 1000 рублей. Мне не перезванивай – позже перезвоню. Нужно срочно!
- Извините, по ошибке положила вам 500 руб. Прошу вернуть на этот номер
- Чтобы перейти на более выгодный тариф, отправьте смс на короткий номер XXXX
- Иванова Ирина Викторовна. Согласно геолокации, вами был нарушен режим карантина согласно ст. 20.6.1 КоАП РФ. Вам необходимо оплатить штраф согласно постановлению ФСИН №168-322 от 09-04-2020года в размере 4000 рублей на номер 8 800 XXX XX XX

- НЕ ПЕРЕЗВАНИВАЙТЕ ПО ТЕЛЕФОНАМ, УКАЗАННЫМ В SMS, И НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ИЗ SMS
- НЕ ОТПРАВЛЯЙТЕ ОТВЕТНЫЕ СООБЩЕНИЯ — ЭТО РИСК ПОДПИСАТЬСЯ НА ПЛАТНУЮ УСЛУГУ

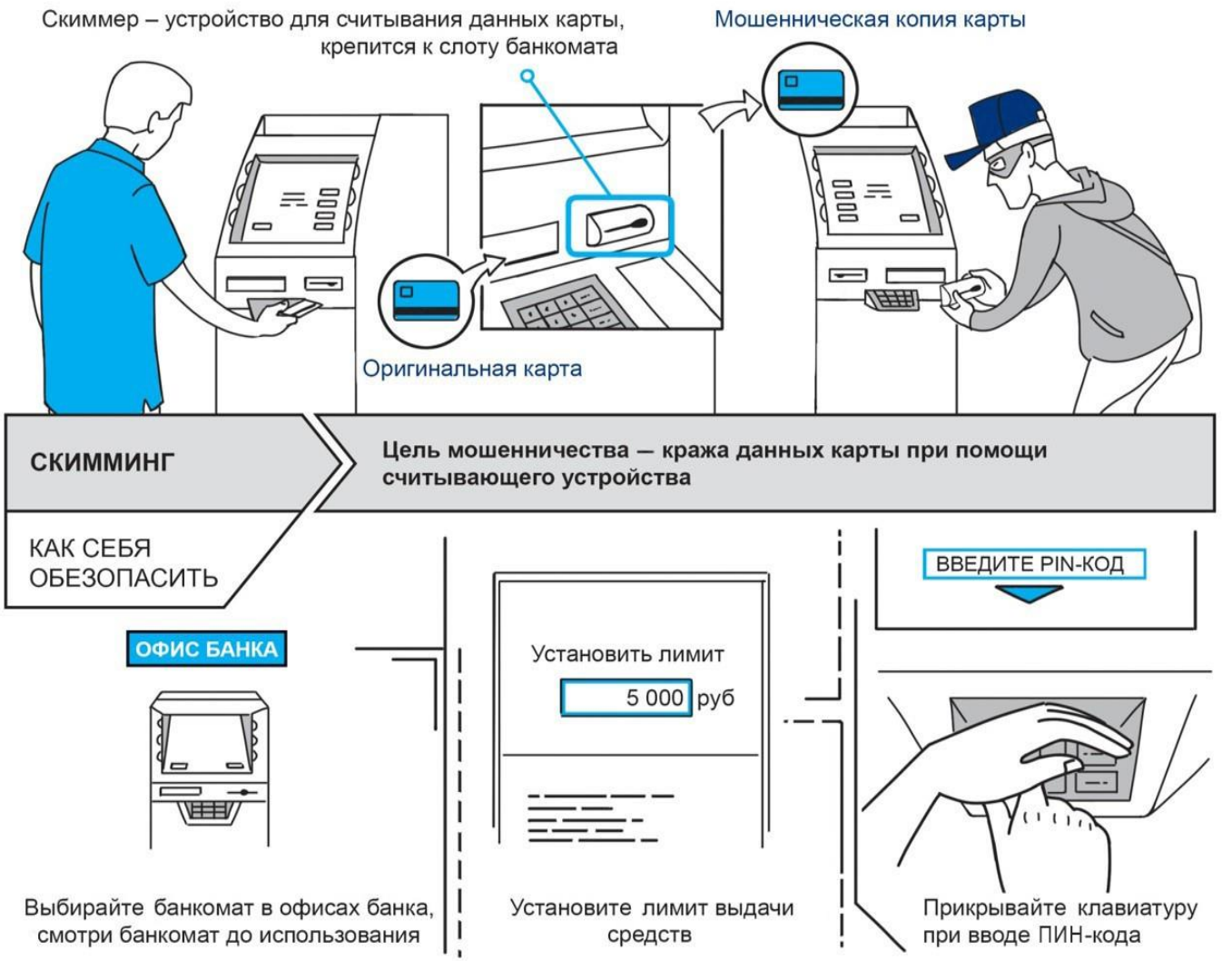
ФИШИНГ


Поддельный адрес сайта
http://vkontaktte.ru
Оплата Интернета
Введите номер карты
ФИШИНГ
Цель мошенничества — получение доступа к логинам, паролям и ПИН-кодам при помощи спама, SMS и фишинговых сайтов
КАК СЕБЯ ОБЕЗОПАСИТЬ
Bank VTB PAO (RU)
https://online.vtb.ru/content/login.html
Проверьте, установлено ли на сайте банка защищенное соединение
Логин VasyaXXXXX, пароль XXXXXX
http://abra.kadabra
Не пересылайте никому пароли и логины
Используйте антивирусы и последние версии браузеров
Проверяйте адрес сайта, не переходите по подозрительным ссылкам из писем

СНИФФЕРИНГ


WiFi
Соединение через незащищенное Wi-Fi-соединение
Оплата мобильной связи
Введите номер карты
1234 5678 9123 4567
СНИФФЕРИНГ
Цель мошенничества — перехват данных мошенниками в общественных местах
КАК СЕБЯ ОБЕЗОПАСИТЬ
wi-fi-my-cafffé
4G
Оплата мобильной связи
Введите номер карты
1234 5678 9123 4567
Не осуществляйте платежные операции в общественных местах через незащищенные сети Wi-Fi
Убедитесь, что соединение происходит через мобильную сеть

СКИММИНГ


Скиммер – устройство для считывания данных карты, крепится к слоту банкомата
Мошенническая копия карты
Оригинальная карта
СКИММИНГ
Цель мошенничества — кража данных карты при помощи считывающего устройства
КАК СЕБЯ ОБЕЗОПАСИТЬ
ОФИС БАНКА
Выбирайте банкомат в офисах банка, смотри банкомат до использования
Установить лимит
5 000 руб
Установите лимит выдачи средств
ВВЕДИТЕ PIN-КОД
Прикрывайте клавиатуру при вводе ПИН-кода

ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ

ЗАЩИТИТЕ СВОИ УСТРОЙСТВА

- обновляйте операционную систему (информационные системы и любые софты)
- используйте антивирус (следите за «свежестью» вирусных баз)
- не подключайте к своим устройствам не проверенные антивирусом новые носители информации (флешки, диски)
- создавайте резервные копии (используйте облачное хранилище или физические носители)
- следите за кибербезопасностью своего мобильного устройства (установите пароли, разделите учетные записи на личную и рабочую)

ЗАЩИТИТЕ СЕБЯ В ИНТЕРНЕТЕ

- не разглашайте личную информацию (ПИН-код, CVV/CVC, SMS-код, логин, пароль и др.)
- контролируйте содержание размещаемой информации (неразрешенное использование материала влечет гражданскую или уголовную ответственность)
- закрывайте сомнительные всплывающие окна
- используйте сложные пароли к разным ресурсам (например, с помощью менеджера паролей) и двухфакторную идентификацию
- используйте общественный Wi-Fi только в случае крайней необходимости (мобильный Интернет безопаснее)

ПРЕВЕНТИВНЫЕ МЕРЫ

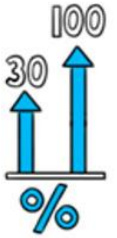
- бережно храните документы, удостоверяющие личность, старайтесь не допустить их потери или кражи.
- умейте говорить «нет»! Оставляйте сканы документов только там, где этого требует закон (например, откажите охранникам, которые пытаются снять копию с паспорта, вместо того чтобы переписать данные для оформления пропуска).

ФИНАНСОВЫЕ ПИРАМИДЫ В ИНТЕРНЕТЕ

КАК РАСПОЗНАТЬ ФИНАНСОВУЮ ПИРАМИДУ

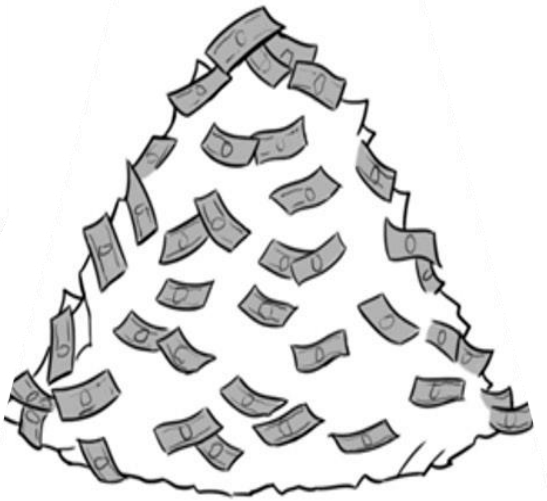
ВЫСОКИЕ ПРОЦЕНТНЫЕ СТАВКИ

20 лет назад пирамиды обещали до 500%, сейчас предлагают меньше — 30-100%.



АГРЕССИВНАЯ РЕКЛАМА

Интернет
СМИ
SMS-рассылки



ЗАМАЛЧИВАНИЕ ВОЗМОЖНЫХ РИСКОВ

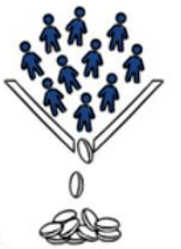
БЕСКОНЕЧНАЯ МОТИВАЦИЯ И МАССА ЛОЗУНГОВ

«Только сегодня!»

«Подпишись раньше — получишь больше!»

«Это ваш последний шанс!»

ПРИБЫЛЬ ЗА СЧЕТ ПРИВЛЕЧЕНИЯ ДРУГИХ ЛЮДЕЙ



ПИРАМИДЫ В ЦИФРОВОМ МИРЕ

Маскируются под реально действующий бизнес

Позиционируют себя обладателями эксклюзивной информации

Предлагают вступать в закрытые сообщества

Закрытые клубы, обладающие «особой» информацией, «гарантирующей» выигрыш

Работа на рынке через иностранного брокера с высокорискованными инструментами

Маржинальная торговля валютой через иностранного брокера (с кредитным плечом)

Инвестиции в криптовалюту, майнинг

Сайты-агрегаторы с предложениями дешевых туров и авиабилетов

Вложения с высоким «гарантированным» доходом

ЖЕЛАНИЕ БЫСТРО ЗАРАБОТАТЬ БЕЗ АНАЛИЗА ИНФОРМАЦИИ МОЖЕТ ПРИВЕСТИ ВАС К ТАКОЙ ЖЕ БЫСТРОЙ ПОТЕРЕ ДЕНЕЖНЫХ СРЕДСТВ.

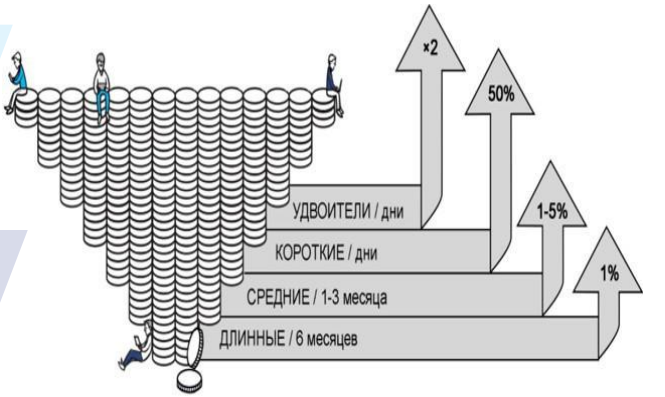
ПИРАМИДЫ В ЦИФРОВОМ МИРЕ. HYIP

Причины популярности финансовых пирамид в Интернете

- полная или частичная анонимность организатора
- доступность и простота рекламы в Интернете

Самый популярный тип финансовой пирамиды в Интернете

HYIP* (High Yield Investment Program, высокодоходная инвестиционная программа) — высокорискованные инвестиции, которые могут просуществовать как несколько дней, так и несколько лет.



СМЕНА ТРЕНДА — ПОЛЬЗОВАТЕЛИ КРИПТОВАЛЮТ ПО ВСЕМУ МИРУ ТЕРЯЮТ ДЕНЬГИ В РЕЗУЛЬТАТЕ КРАЖ И МОШЕННИЧЕСКИХ ICO.

ПРИМЕРЫ ФИНАНСОВОЙ ПИРАМИДЫ В МИРЕ ЦИФРОВЫХ ДЕНЕГ

OneCoin — болгарский проект, запущенный в 2015 г. Мошенничество на сумму 11 млрд долларов. Только в Германии насчитывается более 25 тысяч его жертв. Основным бизнесом проекта является продажа материалов, обучающих торговать на бирже. По делу OneCoin уголовные дела возбудили власти Великобритании, Германии, Бельгии, Италии, Латвии, Финляндии и др.

Plexcoin — первый случай, когда SEC** вмешалась и предъявила обвинение, что, вероятно, объяснялось тем, что токены Plexcoin были классифицированы как ценные бумаги.
В ходе ICO Plexcoin было собрано более $15 млн на разработку улучшенной системы транзакций, которая должна была составить серьезную конкуренцию Биткоину (имела бы среднюю скорость операций в системе 30 секунд вместо свойственных Биткоину 40 минут). Инвесторам было обещано более 1300% дохода от инвестиций в месяц. К счастью, все средства были заморожены SEC, создатель арестован.

* Не путать с популярным неологизмом «хайп» от английского hype (навязчивая реклама, шумиха, ажиотаж, раскрутить, раздуть).
** Комиссия по ценным бумагам и биржам США.

ПРИМЕРЫ ФИНАНСОВЫХ ПИРАМИД

По данным Банка России, за 2019 г. в России было зафиксировано 237 действующих финансовых пирамид, что на 41% больше показателя 2018 г.

88 из этих мошеннических организаций действовали в форме ООО, 55 — как интернет-сайты

Число пирамид возрастает, однако одновременно сами пирамиды становятся более мелкими и их деятельность оказывается менее продолжительной

Частная компания, организованная Сергеем Мавроди в начале 90-х гг., традиционно рассматривается как классическая и крупнейшая в истории России финансовая пирамида

- 1000% дивидендов по акциям, 10-15 млн вкладчиков. За месяц стоимость акций (в последующем билетов «МММ», официально не являвшихся ценными бумагами) росла в 2 раза, а количество вкладчиков — в 4 раза. Выплаты первым вкладчикам обеспечивались за счет средств, поступающих от последующих участников пирамиды.
- Ущерб от деятельности оценивается в 53-79 млрд руб., 23,5 млн официальных банкротов (около полусотни людей покончили с собой). Довольно быстро в стране было зарегистрировано около двух тысяч пирамид (наиболее известные — «Тибет», «Русский дом Селенга», «Хопер-Инвест»), от которых пострадали миллионы граждан.

Пример финансовой пирамиды с инновационными приемами привлечения капитала, основанной в 2016 г.

- Деньги привлекались в рублях и криптовалюте без ведения реальной экономической деятельности. Доходность зависела от того, сколько вкладчиков приводишь с собой: «Кэшбери» с самого начала была сетевым бизнесом с интегрированной финансовой пирамидой. Обещанные доходы — от 200 до 600% годовых.
- Пока сумма ущерба от действий компании точно не подсчитана, но в ЦБ предполагают, что она может достигнуть 3 млрд руб., пострадавших более 200 тыс.

УЧАСТНИКИ ФИНАНСОВЫХ ПИРАМИД НЕВОЛЬНО МОГУТ СТАТЬ СОУЧАСТНИКАМИ ПРЕСТУПЛЕНИЯ, ОРГАНИЗОВАННОГО ЕЕ ОСНОВАТЕЛЯМИ, ПРИВЛЕКАЯ НОВЫХ УЧАСТНИКОВ (СТАТЬЯ 172.2 УК РФ)

**ЕСЛИ ХОЧЕШЬ БЫТЬ БОГАТЫМ,
НУЖНО БЫТЬ ФИНАНСОВО ГРАМОТНЫМ.**

**РОБЕРТ КИЙОСАКИ,
АМЕРИКАНСКИЙ ПРЕДПРИНИМАТЕЛЬ**

Толкачева Светлана

www.youtube.com/c/SvetlanaTolkacheva

www.instagram.com/Tolkacheva_sv

ХОЧУ ЗНАТЬ БОЛЬШЕ