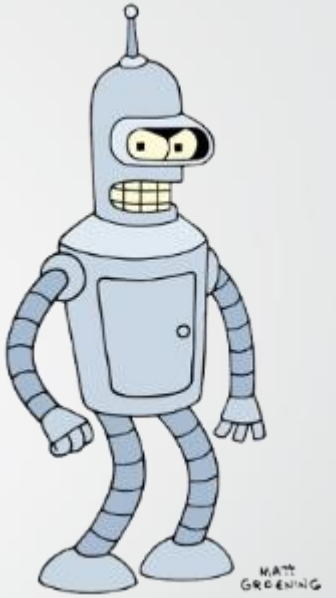
«Новые формы криптомошенничества»



ПАВЕЛ НИКОЛАЕВИЧ БИРЮКОВ

Доктор юридических наук, профессор,

заведующий кафедрой международного и евразийского права Воронежского государственного университета

E-mail: birukovpn@yandex.ru

Мы не знаем, что это такое. Если бы мы знали, что это такое, но мы не знаем, что это такое!

Исходим из двух тезисов.

1. ***В число виртуальных активов (далее ВА) не включаются цифровые валюты - фиатные деньги в электронной форме (цифровые рубли, юани, рупии и т.д.).***

2. ***Криптовалюты и другие ВА не являются фиатными деньгами, а считаются ИМУЩЕСТВОМ. Следовательно, ВА можно украсть.***

Подробнее по теме можно посмотреть:

Бирюков П.Н. Валютное право. М., 2022. – 286 с.

Бирюков П.Н. Виртуальные активы в зарубежном законодательстве и праве Российской Федерации // Публично-правовое обозрение. 2023. № 2.

Бирюков П.Н. Международные нормы о виртуальных активах: основные подходы // Академический юридический журнал. 2024. Vol. 25. № 2.

Бирюков П.Н. Криптобиржи: понятие и виды // Публично-правовое обозрение. 2024. № 4.

Различают ***три вида ВА***:

1) необеспеченные – классические «криптовалюты» (биткойн, альткойны). За ними ничего нет, кроме веры пользователей в их ценность. Их цена волатильна (прыгает как кенгуру) и зависит лишь от спроса на них. Таких ВА несколько тысяч;

2) обеспеченные – «стейблкойны» (Digix Gold, TrueUSD и др.). В их основании лежит имущество (золото, нефть, фиатные деньги и т.п.). Точное количество неизвестно, почти все они выпущены за рубежом (в РФ их выпускают всего 12 компаний);

3) токенизированные активы (далее ТА). Эмитент создает в блокчейне новый смарт-контракт, который содержит реестр пользователей этого проекта. Эмитент издает определённое число токенов, создает записи о праве владения в реестрах и выставляет объекты на торги или распределяет их иным образом. При совершении сделки в реестре меняются сведения о владельце ТА.

- Может вам еще дать ключи от криптокошелька, где мои активы лежат?

В целом, правовое регулирование ВА зависит от его вида и от тех действий, которые с ним совершаются (создание, владение, пользование, распоряжение).

Как взаимодействовать с ВА, распоряжаться ими? Через криптокошельки (КК). Они *хранят ключи пользователя — публичный и приватный. Так что КК - это, скорее, «ключница», а не кошелек.*

Древние славяне криптоактивы хранили в лукошках, а крипто-кошельки делали из бересты.

Управление приватными ключами

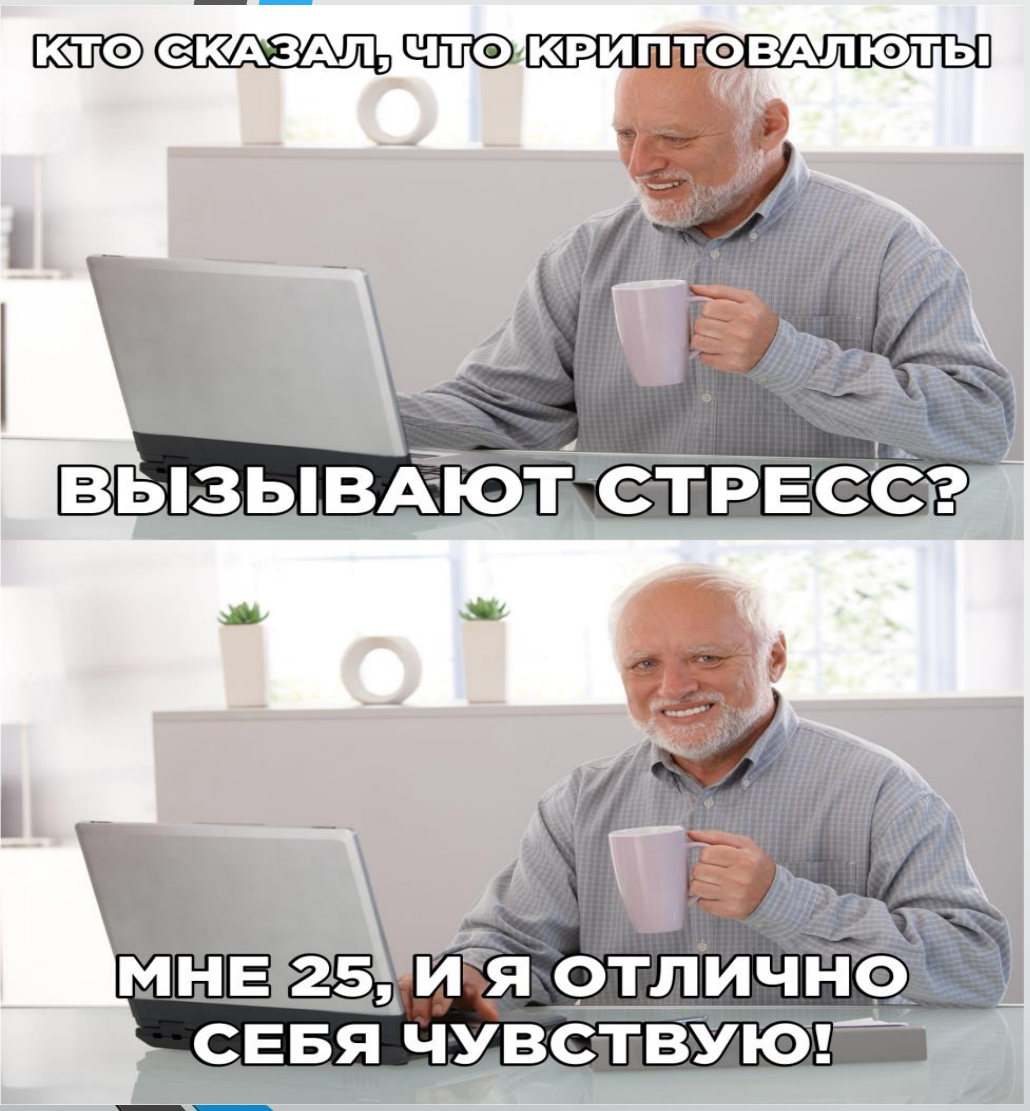
КК также делятся еще на два типа:

1) Кастодиальные;

2) Некастодиальные.

Разница между ними в том, у кого хранятся ключи.

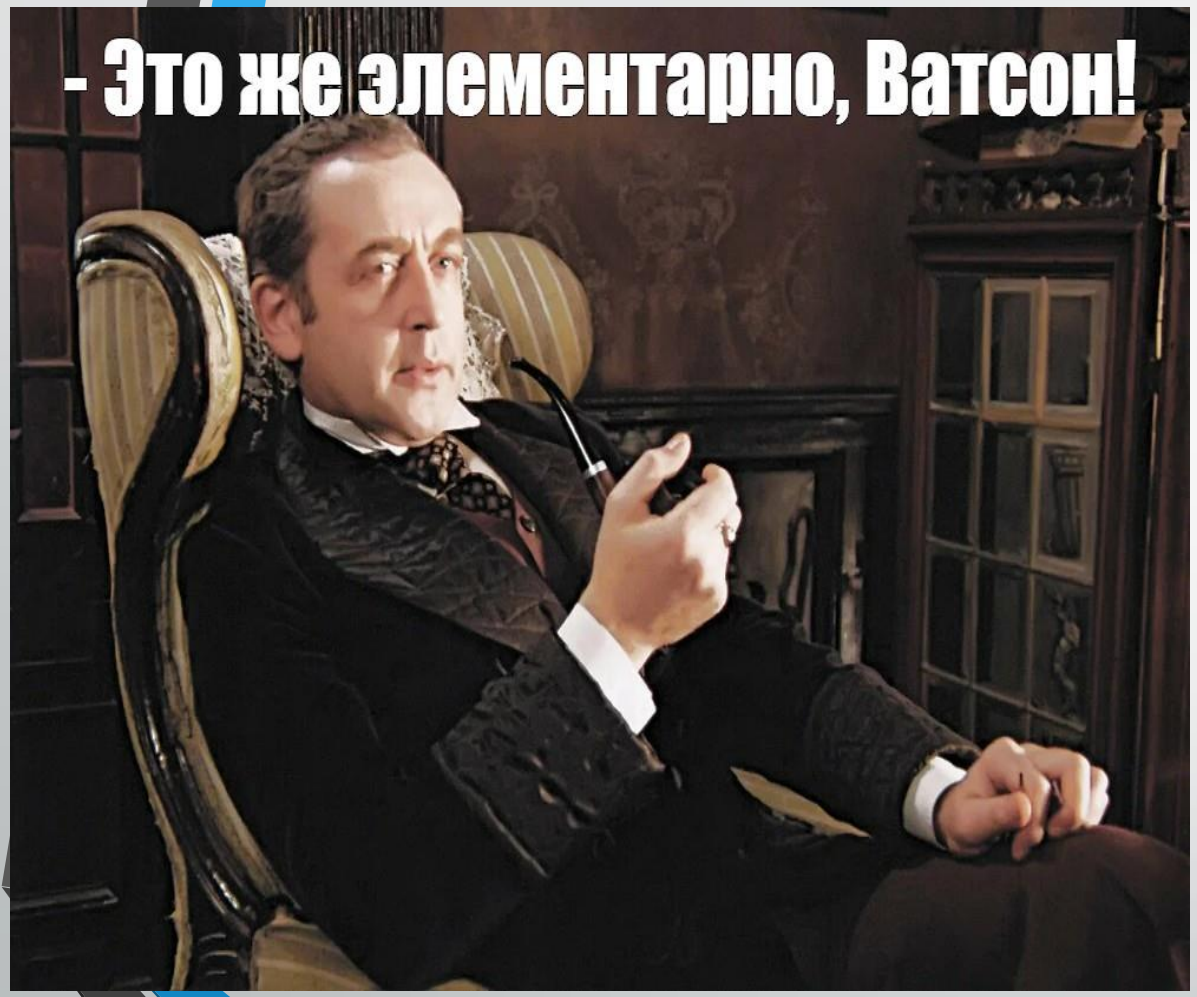
В ***кастодиальных*** кошельках приватные ключи хранит не сам пользователь, а третье лицо (например, биржа). В случае утери такого кошелька его можно восстановить, обратившись к кастодиану.



Пользователь ***некастодиального*** КК полностью владеет своими приватными ключами. ***Холодные*** кошельки — всегда некастодиальные.

Некастодиальные кошельки чаще всего используются для взаимодействия с децентрализованными биржами, обменниками и P2P-площадками.

Этот вариант кошелька более надежен, ибо здесь не нужны посредники. Однако самостоятельное управление ключами накладывает на пользователя дополнительную ответственность.



Теперь перейдем к конкретным видам мошенничества с ВА. Их великое множество. Каждый из них имеет свой способ совершения, свой механизм следообразования на различным объектах.

Соответственно, методики расследования будут отличаться.

1. «Легальные» центр. криптобиржи

Централизованная криптобиржа — это электронная площадка, созданная юридическим лицом с лицензией от национального регулятора. На бирже организована торговля ВА.

В РФ легальных криптобирж две – ПАО «Московская биржа» и ПАО «СПБ Биржа». Они лишь для торговли ВА российских компаний и торговли в Эксп.-пр. режиме.

Большинство зарубежных криптобирж исключили россиян из сегмента, где можно купить и продать ВА. Некоторые арестовали российские криптоактивы.

Якобы «российские» криптобиржи Garantex (https://garantex.org) и ABCex (https://abcex.io) на самом деле – иностранные. Они ***работают вне законодательства РФ.***

Сделки на них, с точки зрения права РФ, незаконны. Работа на них сама по себе потенциально «тянет» на мошенничество (ст. 159 УК), отмывание денег (ст. 174 УК) или, как минимум, на нарушение валютного зак-ва (ст. 15.25 КоАП).

В марте 2025 г. средства криптобиржи «Garantex» были заморожены эмитентом стейбклоина USDT (компания Tether) на горячих кошельках биржи на сумму 2,5 млрд руб. в рамках санкций США и ЕС.

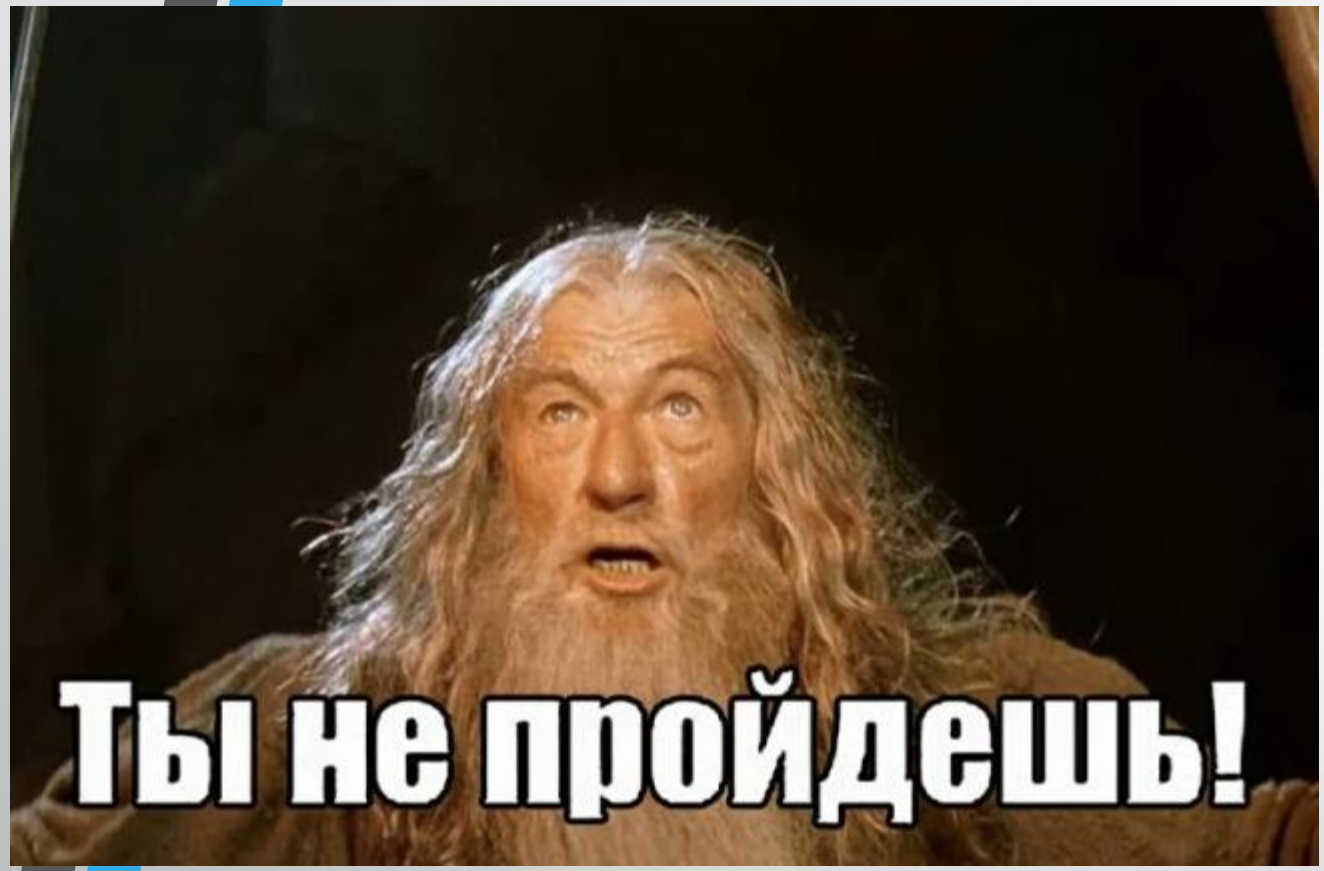
Рубенс. «Криптобиржа заблокировала криптоактивы»

2. Мошеннические действия официальных криптобирж

Обменные сервисы, работающие на легальных КБ, стали произвольно блокировать активы клиентов, требовать прохождения KYC, устраивать допросы о происхождении средств, требовать записывать на видео показания о происхождении ВА. Так, в 2024 г. тысячи клиентов известной биржи BestChang, пытаясь обменять свои средства, столкнулись с блокировками во время обменных операций. Администрация этой КБ использовала действия по «сравнительно честной схеме отъема денег».

С. Корсун. «Биржа предлагает инвестору пройти верификацию»

После получения средств на счета пользователя представители КБ заявляют, что провели AML-проверку и в результате выявили «высокий риск» или «грязную» криптовалюту. Средства клиента на бирже сразу же замораживаются; путем шантажа владельца принуждают к верификации: отказываешься проходить процедуры – остаешься без денег. Владельцев просят предоставить документы, записать видеообращения, в которых они объясняют происхождение средств, и даже требуют признания в нелегальной деятельности.



Многих клиентов такая постановка вопроса не устраивает, и в итоге они остаются без своих активов. Если же клиент соглашается на требования сервиса, процесс “проверки” затягивается на месяцы, и не факт, что владелец когда-нибудь получит свои активы.

3. Криптосервисы-однодневки

С.Корсун. «Банкротство криптобиржи»

Между тем, увеличивается количество обменных сервисов, криптобирж, которые предлагают пользователям «простые и выгодные условия». В их числе: торговля без идентификации личности, якобы «полная анонимность», спецпредложения и бонусы.

Многие из таких бирж существуют недолго, забирают средства пользователей и исчезают навсегда.

4. «Интернет-зеркала» известных криптобирж

Злодеи могут убедительно копировать контент и социальные сети известной биржи, P2P-площадки. Они «накручивают» адреса и подписчиков. Далее мошенники пользуются невнимательностью и доверием лохов, отправляя им рассылки с ISO, IPO, розыгрышами, спецпредложениями и прочими «плюшками». После получения средств лжебиржа исчезает.

5. Фейковые обменники

Обменник - это сайт, на котором происходит купля-продажа крипты. Вообще-то обменные сервисы: а) созданы для заработка на обмене КВ на комиссии с продажи/покупки КВ; б) используют банковские карты для совершения обмена.

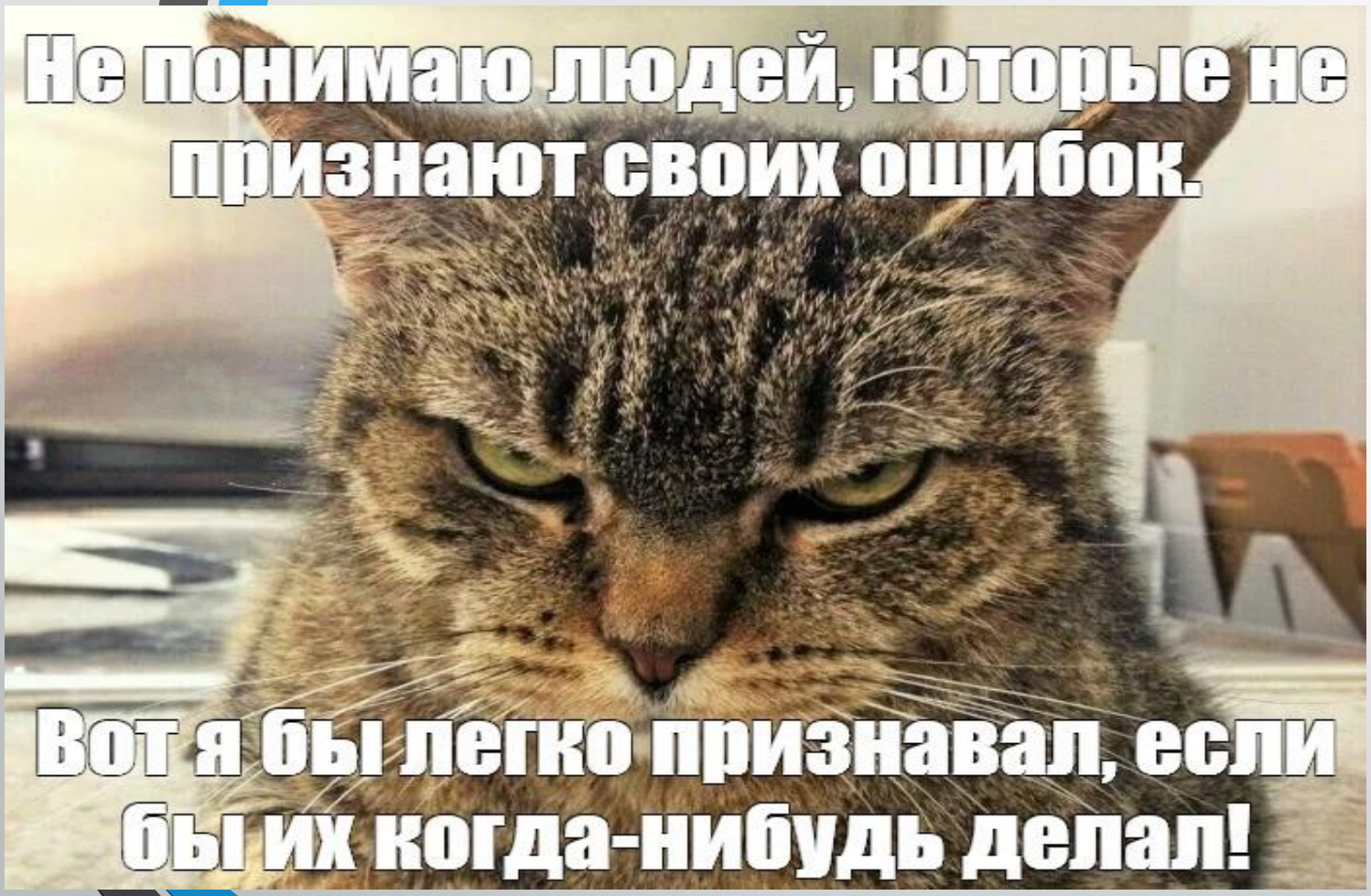
«Недобросовестный» обменник обычно предлагает курс значительно ниже, чем у остальных. Лох, что называется, ведется, однако в результате злодеи забирают средства и ничего не дают взамен.

В «официальных» обменниках велик риск блокировки банковских карт банками или финслужбами. Однако еще более велик риск получить «грязную крипту». А если уж совсем повезет ☺, можно вообще ничего не получить.

Конечно, можно проверить чистоту адреса контрагента до совершения операции через т.н. «сервисы безопасности». Однако и они не дают полной гарантии законности сделки и ее завершения. Да и сами такие сервисы зачастую фейковые.

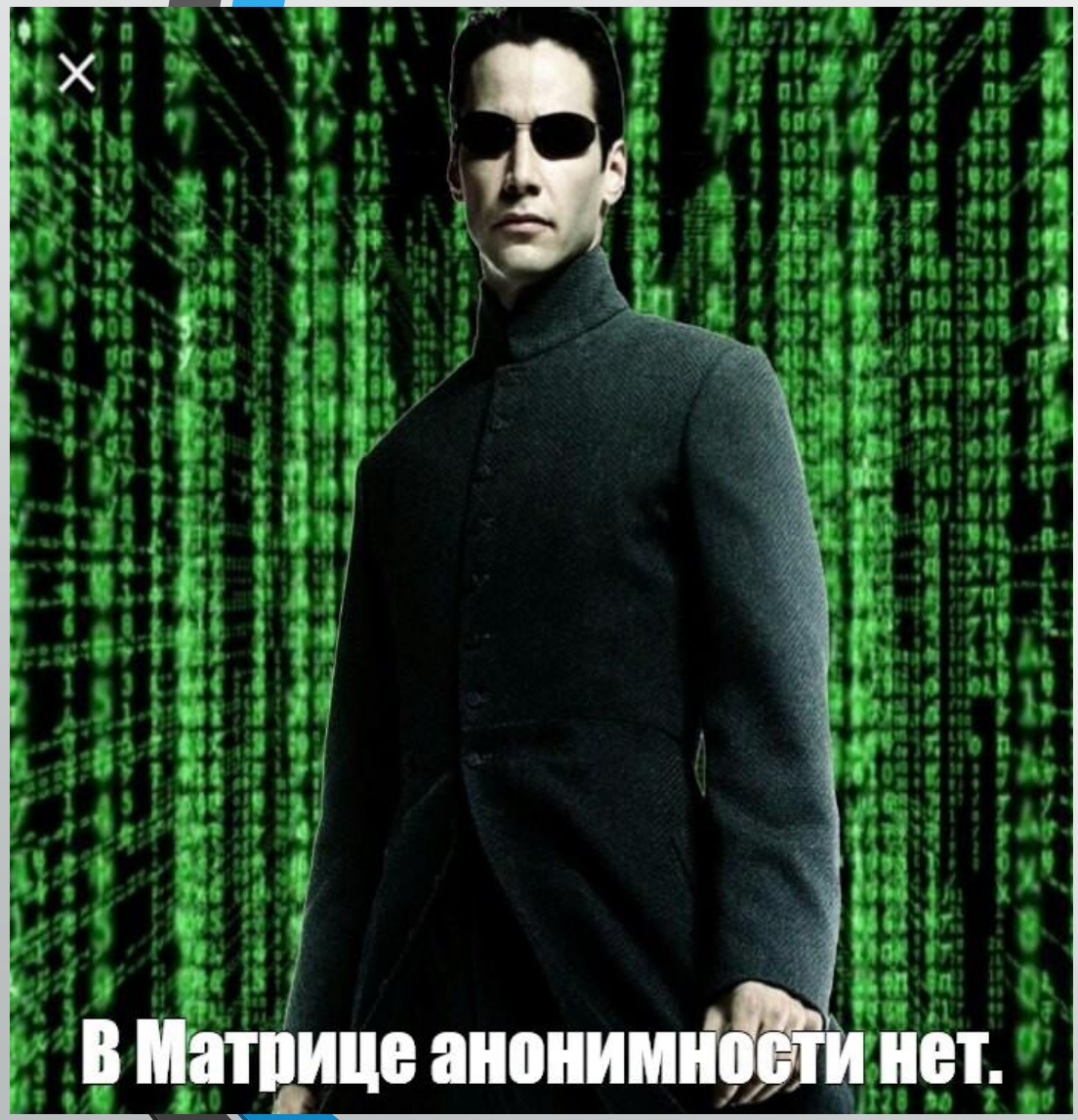
6. Фейковые службы поддержки

Мошенники маскируются под службу поддержки IT-проекта, биржи, майнинговой компании и другого сервиса. Клиенту предлагается заполнить специальную форму, отправить данные на электронную почту или передать информацию лично. В процессе общения «работники поддержки» могут попросить логин и пароль, приватный ключ и другие сведения якобы для решения проблемы.



7. Лохотрон на P2P-площадке.

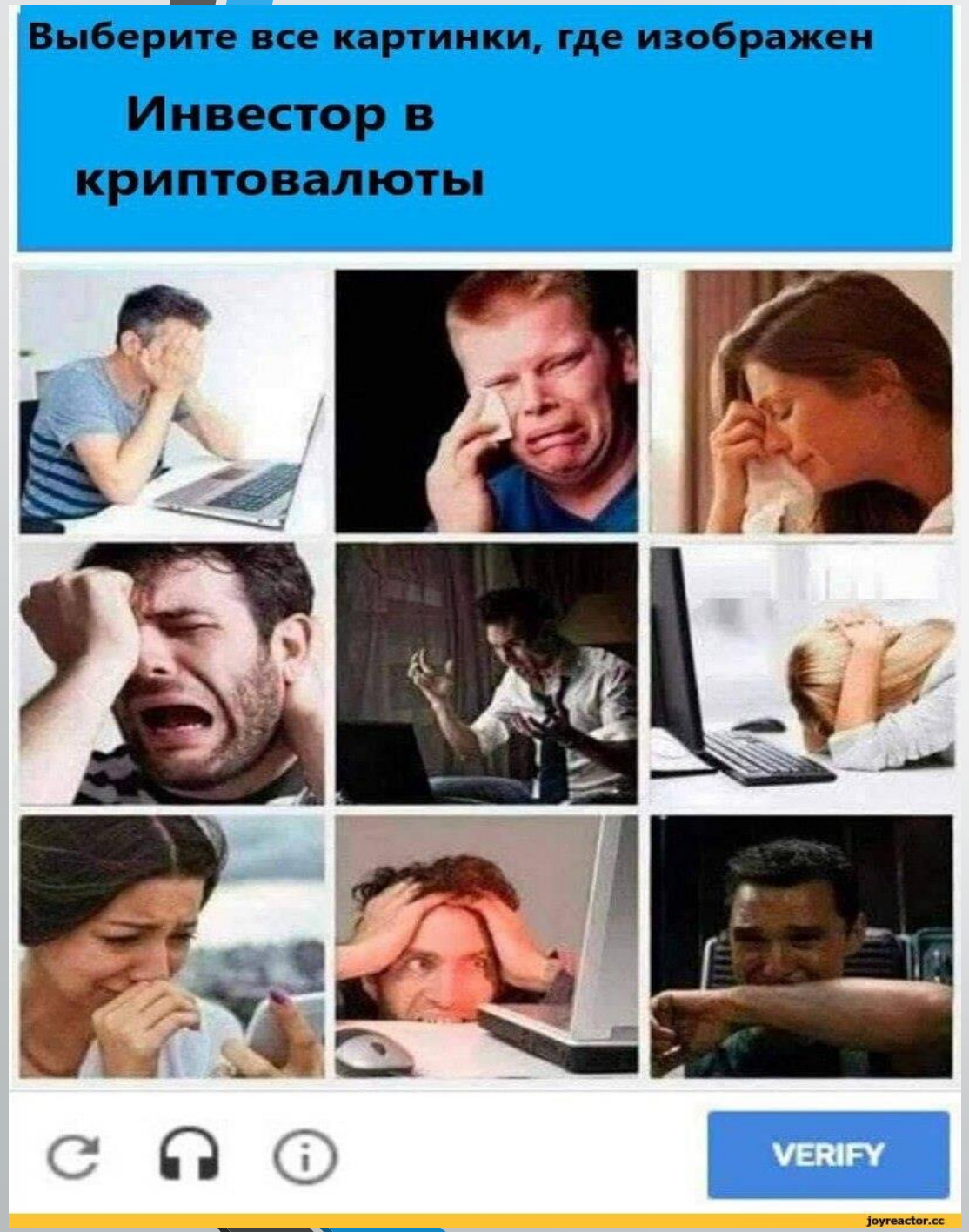
Участники регистрируются и работают на инфраструктуре P2P-площадки, которая обычно создается при крупной криптобирже. Участники обязаны иметь аккаунты на площадке, которой платят комиссию за совершение операций.



Злодеи здесь применяют два варианта:

Первый. Используются реально существующие добросовестные P2P-площадки. Потерпевшие часто азартны и невнимательны, на этом и погорают. «Без лоха и жизнь плоха».

Второй. Используются недобросовестные P2P-площадки, изначально настроенные на развод лохов. Там нет идентификации лиц, совершаются «подозрительные» транзакции, передается «грязная» крипта и т.д.



8. Продажа неизвестных токенов

Лоху сообщают, что есть новые токены, которые взлетят после листинга (выставления на биржу и торговли). Ему горячо советуют купить «здесь и сейчас, и побольше». Такие сообщения гуляют по всем скам-каналам. Их также нередко за деньги рекламируют жадные админы нормальных каналов. По факту новый токен — мусорный, и никто не собирается его нигде «листить», куплен «воздух».

9. Фишинг

Фишинг — схема, направленная на получение конфиденциальных данных пользователей (логины, пароли). Мошенники создают фальшивые торговые платформы или криптокошельки и подбирают доменные имена, похожие на оригинальные. Как правило, пользователи не обращают внимания на адресную строку, вводят свои данные. Получив доступ, скамеры заходят в реальный аккаунт и похищают средства.

10. Copy-and-paste вирусы

Программы copy-and-paste перехватывает данные из буфера обмена пользователя и отправляют деньги напрямую преступникам.

Допустим, клиент хочет перевести крипту контрагенту. Он присылает реальный адрес своего криптокошелька, чтобы его могли скопировать и вставить в форму. Однако если на компе или в гаджете «сидит» copy-and-paste вирус, то в момент, когда вставляется адрес контрагента из буфера обмена, его автоматически заменят на адрес злодея. Таким образом, кидают и продавца, и покупателя.

11. Рег-пулл

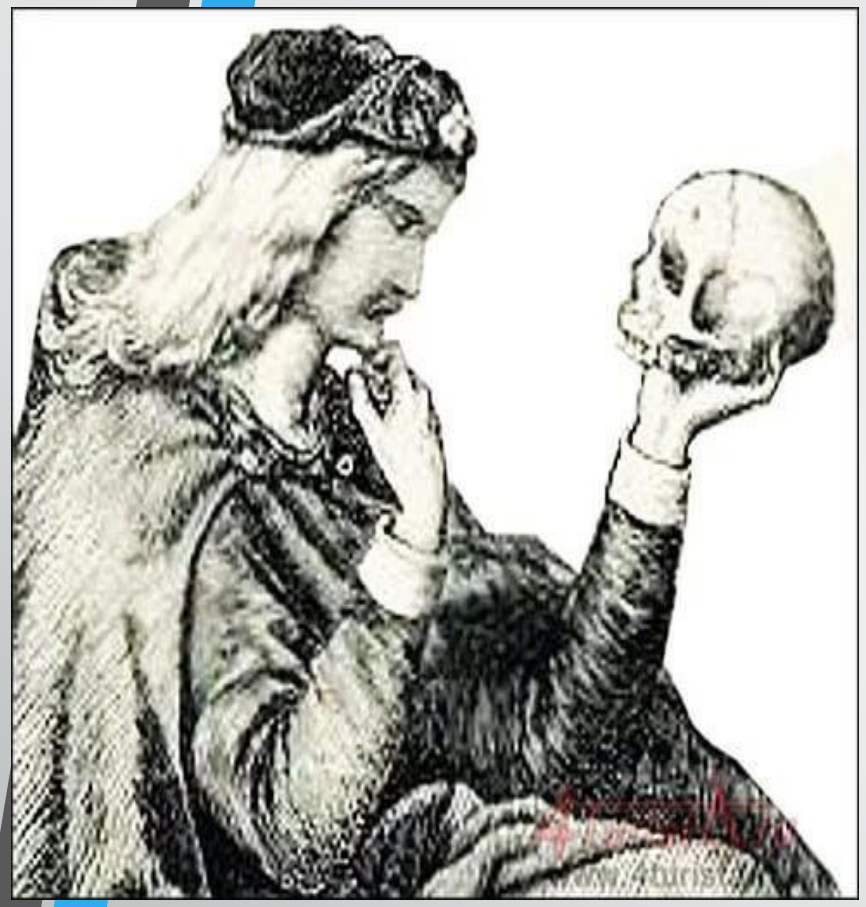
Злодеи начинают пиарить какой-то реальный BA (например, NFT), заявляя, что это «всерьез и надолго», токен будет активно развиваться и вырастет в цене. Обещают покупателям дивиденды и «жениться».

Поначалу всё идет хорошо, цена растёт, и возможно даже кто-то успеет заработать. Однако как только все коллекция NFT распродаётся, проект забрасывается, создатели делят бабки. Коллекцию перестают пиарить и дополнять, а NFT падает в цене.

12. Продажа торгового бота

Торговый бот – это программа, которая отслеживает ситуацию на крипто-бирже, а затем сама совершает выгодные сделки. Вот их-то и продают – «стабильная прибыль в 500% в месяц»).

Торговые роботы, действительно, существуют, однако их используют крупные инвестиционные фонды, маркет мейкеры, трейдинговые компании. Цены таких роботов измеряются в десятках тысяч **$**; они не универсальны, и их никто не продает в свободном доступе и по дешевке.



- **Переводить или не переводить крипту?**
- **Вот в чем вопрос.**

13. «Художники»

Мошенники при совершении сделки через P2P-платформу присылают в подтверждение отправки от них фиатных денег СМС-сообщение, похожее на СМС из банка о зачислении средств на счет (в случае, если перевод фиатнвх денег планируется совершать через СБП по номеру телефона).

Кроме того, направляется подделанный чек о проведенном переводе, в расчете на то, что невнимательный участник не проверит поступление средств в приложении банка и отправит мошеннику свою крипту.

14. Аппаратные кошельки «с прицепом»

При продаже холодного криптокошелька в виде гаджета в него «вшивается» криптоадрес-мошенника. При совершении сделки по реализации ВА они «уходят» не по тому адресу, который ввел в кошелек владелец. В результате он остается без активов.

- Мы не сторонники разбоя. Переведи нам свою крипту сам.

Есть и другие способы мошенничества с ВА. Их основная цель – получить доступ к криптокошелькам владельцев ВА. Однако жертву можно убедить и самому отдать информацию или активы, сыграв на жадности либо невнимательности.

Словом, «лох - не мамонт, он не вымрет» ☺

Спасибо за внимание!

© Бирюков П.Н., 2025