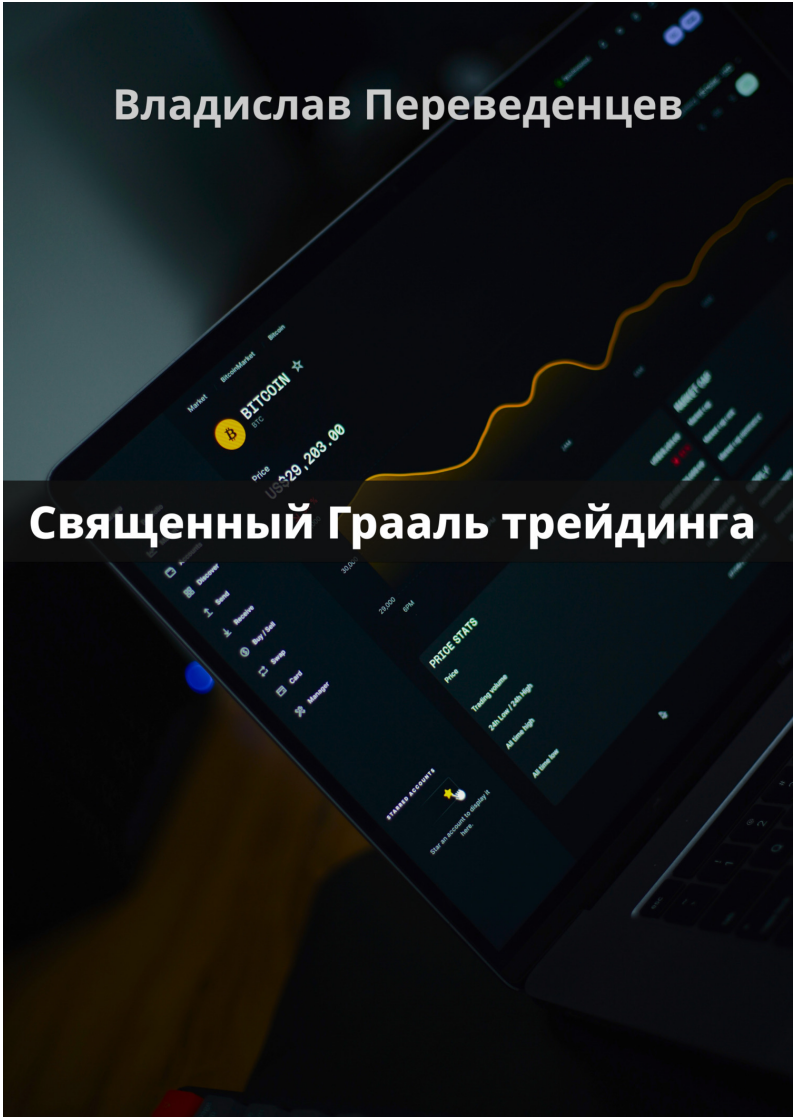
Владислав Переведенцев

Священный Грааль трейдинга



Владислав Переведенцев

Священный грааль трейдинга

http://www.litres.ru/pages/biblio_book/?art=69028870
ISBN 978-5-9965-0637-8

Аннотация

Священный Грааль трейдинга – книга о трейдинге от профессионального спекулянта, в которой он знакомит читателя с техническом анализом и различными торговыми стратегиями. Автор делится насыщенной выдержкой своего многолетнего опыта торговли и рассказывает о психологических барьерах, с которыми сталкиваются практически все начинающие трейдеры, а также приводит практические рекомендации по их преодолению. Книга подойдет как начинающим трейдерам, так и заядлым спекулянтам, так как автор раскрывает новые грани трейдинга.

Внутри книги вас ждет: свечной и технический анализ, индикаторы, более 30 системных точек входа в рынок, прикладная психология, торговые инструменты и стратегии по увеличению прибыли, а также вероятностный, системный и комплексный подходы.

Содержание

Предисловие

“Священный Грааль трейдинга” – это книга о трейдинге, из которой вы узнаете о лучших практиках топовых трейдеров, с нуля обучитесь управлению рисками, свечному и техническому анализу, а также изучите психологическую составляющую торговли.

Весь материал собирался по крупицам из десятков других книг и перенимался от лучших трейдеров. Данная книга не содержит практически ничего лишнего и является насыщенной выдержкой нашего личного опыта.

После прочтения этой книги у вас останутся фундаментальные знания, необходимые для успешной торговли на рынке, полное понимание происходящего на графике цены, а также подробная инструкция с порядком действий в различных рыночных ситуациях.

В данной книге вас ждет: психология трейдинга, инструменты анализа и заработка, стратегии внутридневной и среднесрочной торговли, графические паттерны, свечные формации, индикаторы и различные торговые стратегии, вокруг которых строилась торговая система автора книги.

Об авторе

Меня зовут Владислав Переведенцев, начиная с 2019 года трейдинг является моей единственной сферой деятельности и основным источником дохода. Основные цели написания этой книги: систематизация собственного опыта и желание поделиться своим опытом с вами, благодаря чему вы начнете свой торговый путь не с ошибок и потери денежных средств, а с осознанных, уверенных шагов к созданию собственной торговой системы и стабильному заработку.

На следующих страницах предлагаю познакомиться поближе: расскажу с чего начался мой торговый путь и как я пришел к созданию своей торговой системы. Если вам не интересен личный опыт – можете сразу перейти к следующей главе.

Моя история

Вся моя история с трейдингом началась с просмотра сериала «Миллиарды» в 2018 году, в котором акула с Уолл-Стрит по имени Бобби Аксельрод зарабатывал миллиарды долларов на манипуляциях рынком. Как такая мотивирующая история может не заинтересовать?

В 2018 году я попробовали поторговать на криптовалютном рынке, ничего не понял и забросил эту идею. Но после просмотра трех сезонов данного сериала остался под большим впечатлением и начал интересоваться фондовым рынком, а также задумался о приобретении asic-майнеров для добычи Bitcoin'a.

Майнинг

В мае 2019 располагая скромным бюджетом я приобрел 10 майнеров: 5 «средних» и 5 более мощных моделей, Bitcoin тогда стоил приблизительно $5 000. Я не занимался оборудованием лично, а делегировал это задачу на других людей.

Обслуживание майнеров в России было проблематичным, в связи с отсутствием законов и четкой позиции правительства на этот счет, поэтому я отправил оборудование в Абхазию, где этим вопросом занималась специальная компания.

Оборудование исправно работало без моего вмешатель-

ства, нужно было лишь платить небольшой процент от прибыли за обслуживание.

К теме майнинга вернемся чуть позже, а сейчас расскажу, чем занимался в 2020 году.

2020 год: коронавирус и крах фондового рынка США

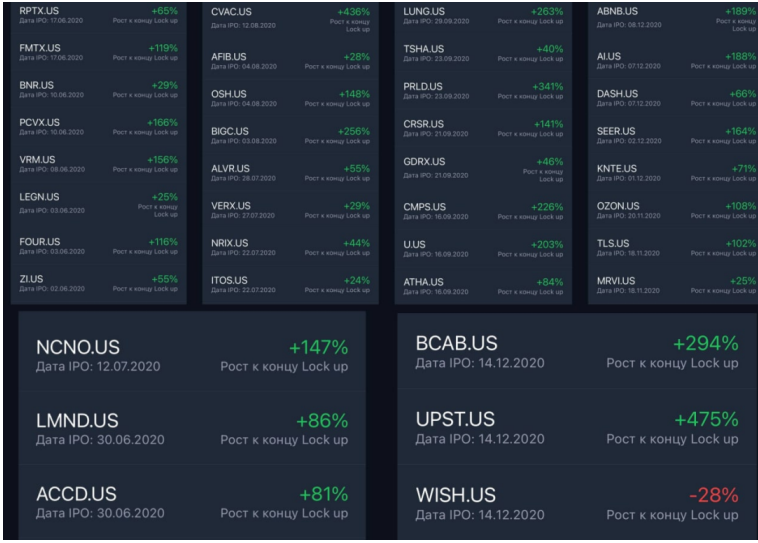
После коронавирусного дампа фондового рынка, пока майнеры работали и продолжали генерировать прибыль, я решил, что момента для входа в рынок лучше, чем сейчас не будет, поэтому начал изучать способы выхода на рынок акций и наткнулся на нескольких блогеров, которые рассказывали о каком-то «IPO».

IPO – главный тренд 2020 года

После непродолжительного изучения принципов работы "IPO" я открыл счет у российского брокера и начал погружаться в тему IPO.

IPO – это первичное размещение ценных бумаг на бирже. После участия в подобной сделке акции замораживаются на три месяца. В крипторынке есть альтернатива – ICO и IDO.

Принцип был прост: брокеру выделяли аллокацию для участия, после чего это аллокация распределялась между клиентами посредствам внутреннего рейтинга.



Практически все акции компаний, выходивших на публичный рынок в 2020, «стреляли» на несколько сотен процентов. В самом начале аллокация была большой, но со временем IPO вызвало ажиотаж и количество желающих поучаствовать в подобных сделках начало стремительно расти, из-за чего у российских брокеров возникли проблемы с аллокацией.

Путь к трейдингу через инвестиции

Я покинул рынок IPO и переключился на обычные американские акции: начал торговать на фондовом рынке США, застав вовлечение в торговлю десятки миллионов новых инвесторов по всему миру и стимулирование американского фондового рынка на триллионы долларов от правительства США, вызвавшее стадию эйфории на рынке.

К концк года я отлично заработал на FAANG и FinTech акциях, после чего перешел на торговлю по классическому техническому анализу, осознавая эйфорическую стадию на фондовом рынке США и не желая становиться "долгосрочным инвестором" на медвежьем рынке.

Если честно, на фондовом рынке в 2020 году зарабатывали все без исключения, потому что рынок рос из-за вливаний денежных средств (стимулирования экономики). Публика заработала виртуальные деньги, которые никто не выводил. Эти деньги так и остались в виртуальном пространстве, большинство трейдеров их просто растеряли после смены тренда. Но мне, в отличие от остальных, повезло чуть больше…

Начало 2021 года

В 2021 году появился новый тренд – криптовалюта.

Bitcoin стремительно рос, СМИ все чаще начали говорить

о загадочной шифропанковской валюте, и я задумался о полном переходе на криптовалютный рынок, так как там можно было заработать быстрые и легкие деньги. Как же я ошибался.

Тем временем в Абхазии из-за наплыва майнеров начались проблемы с электричеством, и начали поступать «первые звоночки» о том, что пришло время распрощаться с оборудованием, так как на майнинг фермы начали устраивать облавы.

10 asic-майнеров были проданы через своих знакомых, а весь добытый ранее Bitcoin выведен на Binance. Торговлю на фондовом рынке я также решили прекратить и вывели оттуда деньги.

Доход от майнинга

Так как я решил полностью перейти на криптовалютный рынок, мне нужно было распределить средства: продать свои BTC, часть вывести, а другую часть перевести в стейблкоины и торговать на них.

Доход от майнинга оказался огромным за счет роста BTC с $5 000 до $64 000, добытые BTC были проданы в первой половине мая 2021 года приблизительно по $60 000.

Маржинальная эпопея

Ворвавшись в рынок криптовалют и продав добытый ранее Bitcoin, я начал на личных средствах изучать специфику торговли на данном рынке, закрываясь по стоп-лоссам из раза в раз.

Безусловно, учиться на чужих ошибках замечательно, однако, на деле все обстоит совсем иначе. Подавляющее большинство начинающих трейдеров теряют деньги из-за одних и тех же ошибок: отсутствие риск-менеджмента, выдача желаемого за действительное и ожидания от рынка сиюминутной прибыли. Я не был исключением, разве что разбирался в техническом анализе.

В июле 2021 года я купил Ethereum на весь криптодепозит. Просто покупки мне было мало, поэтому я решил торговать купленным Ethereum'ом на инверсных фьючерсах (в инверсных фьючерсах обеспечением выступает купленная вами криптовалюта, вместо привычных стейблкоинов). И конечно же:

«Герои не носят плащи, а трейдеры не ставят стопы»

Открытую на весь депозит позицию я увеличивал по мере образования прибыли, стоп-лосс ордера не использовал, а профит не забирал, пересиживая все просадки и ожидая Bitcoin по $100 000, а Ethereum по $15 000.

Чем все закончилось?

Четыре раза до ликвидации моей позиции (всего криптодепозита) оставалось совсем ничего, но это "совсем ничего" заставляло меня фиксировать позицию в убыток частями, чтобы отодвинуть цену ликвидацию. Я просыпался от ценовых будильников практически каждую ночь на протяжении четырех месяцев.

Результат

Невероятное стечение обстоятельств сыграло мне на руку – я оказался в нужное время, в нужном месте и с нужным кредитным плечом. В декабре 2021 года моя прибыль составила порядком 480 % от изначально вложенных средств!

Полгода я просыпался в страхе и ужасе, а в течение дня не отходил от мониторов. История закончилась для меня крайне благоприятно, но ведь все могло сложиться совсем иначе.

Выводы, к которым я пришел

После долгого анализа своего подхода и отношения к торговле, осознав все свои ошибки и прочувствовав их на себе, было принято решение выписать на бумагу полный порядок действий и окончательно сформировать свою торговую си-

стему.

Теперь я торгую только согласно своей торговой системе, соблюдая риски и не пытаясь заглянуть в будущее, поставив на кон все свои деньги. В этой книге мне удалось собрать весь свой опыт воедино: фундаментальный, технический, трендовый, фрактальный и свечной анализ, а также лучшие торговые стратегии и практики.

Благодаря моему опыту вы сможете оградить себя от потери капитала, выделив на самообучение всего несколько недель, а также описанный в книге подход позволит вам зарабатывать вне зависимости от контекста на рынке: будь то восходящий тренд, нисходящий тренд или боковик.

Создание telegram-канала

На создание канала меня побудило повсеместное разочарование людей в трейдинге. Среди моих друзей и знакомых было много людей, потерявших в трейдинге огромные суммы. Я просто не могли оставаться в стороне: на просторах интернета существуют множество инфо блогеров, призывающих откупать дно, покупать низколиквидные shitcoins и заходить all-in в рынок, из-за чего страдают не разбирающиеся люди. Так ко мне и пришла идея создать telegram-канал GAP capital, который со временем вырос в целую экосистему и команду трейдеров.

GAP capital — это сообщество трейдеров, которые делят-

ся своими фундаментальными и техническими взглядами на криптовалютный рынок, акцентируя психологическую составляющую торговли и пропагандируя системность в трейдинге.

Со временем я осознал, что, если я не веду свой блог и не делюсь своим опытом – людям приходится читать других, менее опытных трейдеров.

Летом 2022 года был создан telegram-канал, в котором я начал публиковать обучающие статьи, дублируя их на платформе TradingView, где всего за три месяца существования блога количество прочтений моих статей превысило 110 000.

Статьи касаются психологии в трейдинге и различных торговых стратегий, также я писал о более практических вещах: например, о цифровой безопасности и инструментах

трейдера.

Немногим позже по многочисленным просьбам я сформировал закрытое комьюнити трейдеров, где начал делиться своими сделками и в режиме реального времени применял свои знания на практике, но об этом чуть позже.

Заключение

Я не боюсь признавать свои ошибки и не собираюсь скрывать их от вас. В моей торговле были и триумфы, и поражения. Точно также, как абсолютное большинство трейдеров, я не принимал чужих советов, делая ставку на Zero из раза в раз. Я успел совершить всевозможные ошибки и столкнулся лицом к лицу с огромным количеством подводных камней, скрывающихся за привлекательным словом «Trading». Я такой же человек, как и вы, и совершал точно такие же ошибки.

Моя задача – делиться своим видением рынка через призму собранного опыта, остерегая вас от ошибок, потерь денежных средств и нервных клеток. Мое стремление не ограничивается желаем улучшить ваше материальное состояние, я также намерен мотивировать вас на личностный рост и развитие.

Социальные сети

- Telegram-канал – https://t.me/+lFHNcrzGsiphOGU6
- Закрытый клуб – https://teletype.in/@gap_capital/GAP_club
- Telegram-бот – https://t.me/gap_capital_bot
- TradingView – https://ru.tradingview.com/u/gap_capital/

Почему рынок криптовалют?

В этой главе поделюсь своим видением текущих тенденций развития криптовалют и трансформации общества.

Материал предназначен исключительно для того, чтобы заставить вас задуматься и ни в коем случае не претендует на истину точно также, как я не претендую на звание "пророков".

CBDC

Central Banks Digital Currencies – это цифровые валюты центральных банков.

Население нашей планеты перестанет пользоваться наличными деньгами, получив взамен полностью контролируемый извне электронный аналог денег с искусственной ценностью.

Больше половины стран мира на момент написания этой книги активно разрабатывают национальные цифровые валюты на основе технологии «блокчейн», которые в дальнейшем будут использовать для проведения платежей как внутри стран, так и за их пределами.

Благодаря такому решению государства получат ряд преимуществ:

- Полный контроль за оборотом денежных средств.
- Искусственное экономическое стимулирование.
- Изъятие «лишних» денежных средств у людей.
- ДеЦентрализованное управление.
- Абсолютный контроль граждан.
- Монополизация экономики.

Прозрачность и безопасность

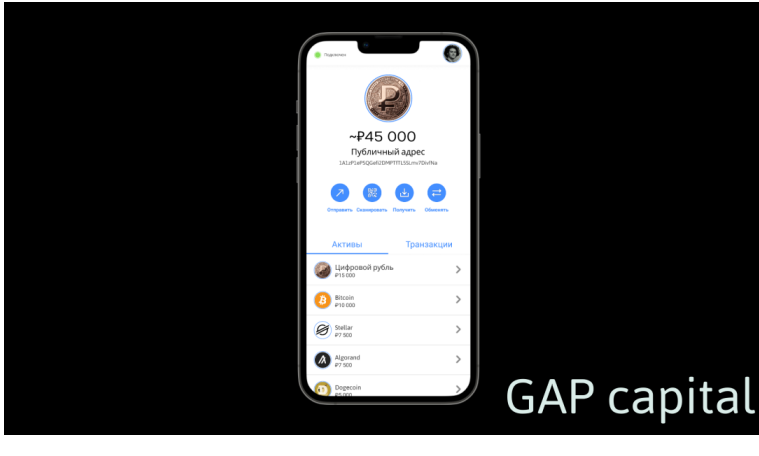
С большой долей вероятности эмитент государственной

цифровой валюты оставит возможность производить анонимные транзакции для государственных структур и их подопечных, вместе с откатами транзакций и блокировками адресов, а контроль над эмиссией и запрет майнинга государственной цифровой валюты сделают невозможным вмешательство извне.

Цифровые кошельки

С приходом CBDC появятся государственные цифровые кошельки с привязкой к личности, так как цифровые ~~жетоны~~ деньги в банках хранить не получится.

Люди смогут моментально переводить свою криптовалюту за минимальные комиссии, отсканировав QR-код или написав персональный DNS-идентификатор в поиске получателей, например: @Medvedev



За каждым новорожденным будет закрепляться цифровой кошелек, который будет содержать:

1. Цифровой идентификатор личности (паспорт) в виде

NFT-токена (неизменяемый и непередаваемый), включающий в себя свидетельство о рождении, медицинскую страховку, СНИЛС и другие необходимые документы.

2. DAO-токен гражданина, наделяющий человека правом принимать участие в голосованиях на уровне страны (изменяемый, но непередаваемый).

3. Документы, подтверждающие права́ собственности в виде списка NFT-токенов (изменяемые и передаваемые).

4. Адрес кошелька в сети (для получения и отправки средств) с полной историей когда-либо совершенных транзакций.

5. DNS-идентификатор для быстрого и удобного поиска получателя.

6. Список локальных DAO-токенов.

7. Социальный рейтинг кошелька.

DAO-токены

DAO – децентрализованная автономная организация, имеющая организационную форму управления с заранее установленным сводом правил, контроль за исполнением которых происходит автоматически, с помощью смарт-контрактов[1].

DAO-токены, как и NFT-токены, будут разделяться на четыре категории:

1. Изменяемые токены.
2. Неизменяемые токены.
3. Передаваемые токены.
4. Непередаваемые токены.

Изменяемые DAO-токены – имеют встроенный функционал ограничения действий владельца в то время, как изменяемые NFT-токены могут быть модифицированы.

Применение DAO-токенов

DAO-токены будут использоваться как государствами, так и частными компаниями, сообществами людей. Для получения DAO-токена вам потребуется подтвердить свою причастность к тому или иному сообществу, например,

[1] Смарт-контракт – это алгоритм, обеспечивающий и отслеживающий исполнение обязательств между отправителем и получателем криптовалюты.

NFT-документом о праве собственности.

Заселяясь в новый жилищный комплекс, вы получите на свой цифровой кошелек DAO-токен своей ЖК, который позволит вам проголосовать со своего телефона за выбор новой управляющей компании, или, проголосовать за строительство спортивной площадки у себя во дворе.

Аналогичным способом депутатами будут приниматься или отклоняться законы в государственной думе. Немногим позже государственная дума, как и банки, станет не нужна.

Социальный рейтинг

Социальный рейтинг – коэффициент, закрепляемый за цифровым кошельком гражданина, получаемый из следующего уравнения:

1. Судимости.
2. Наличие долгов.
3. Количество полученных штрафов.
4. Экологический вклад гражданина.
5. Количество просроченных выплат по задолженностям.
6. Количество полученных на кошелек транзакций с необъясненным происхождением.
7. Количество удачно совершенных сделок с другими людьми (аналог рейтинга продавца на Amazon).

Социальный рейтинг может стать большой проблемой для людей, желающих переехать в новую квартиру в "экологически чистом районе", которую сдают исключительно лицам с социальным рейтингом 75 % и выше.

Люди с низким рейтингом не смогут посещать большинство приличных заведений, потеряют возможность пользоваться общественным транспортом и будут получать отказы вне зависимости от своего опыта и резюме при попытках устроиться на работу.

Экологический вклад

Показатель "экологического вклада" будет складываться из соотношения купленных вами "экологически чистых" и "экологически грязных" продуктов питания и прочих товаров. Также будет учитываться на какой машине вы ездите и чем заправляетесь – бензином или электричеством.

Звучит невероятно, однако, отследить, как и на что вы тратите «свои» деньги с повсеместным внедрением цифровых кошельков, предоставляющих полный доступ к истории ваших транзакций любому человеку, станет элементарной задачей, с которой справятся незамысловатые алгоритмы.

Черный список

DAO-токены будут иметь функционал "лишения голоса" инакомыслящих, что будет сказываться на их "социальном рейтинге".

Например, если гражданин протестовал против употребления в пищу насекомых[2] и не изменил свой рацион на "экологически нейтральный"[3], то его персональный DAO-токен гражданина, при достижении определенной отметки социального рейтинга, будет деактивирован, сильно ограничив

[2] Angelina Jolie eats spiders – https://youtu.be/xZlYiD3dASs.

[3] Nicole Kidman eats bugs – https://youtu.be/e3UqLAtdZ04.

его в социальной жизни.

Бум. png картинок за миллионы долларов

В неокрепших умах прочно засел навязанный нарратив о том, что технология "NFT[4]" имеет за собой огромный и до конца не раскрытый потенциал.

Именно эти люди будут продвигать и всячески приветствовать новые законы по внедрению в повседневную жизнь миллиардов людей новых, цифровых оков.

Цифровизация документов

Абсолютно все документы, начиная паспортом и заканчивая документами на права́ собственности, будут оцифрованы и переведены в формат NFT-токенов, которые будут закрепляться за ~~гражданином~~ цифровым кошельком.

Бумажные документы более выдаваться не будут, а для продвижения оцифровки документов будут продвигать тезис о сохранности лесов и заботе об экологии.

[4] NFT (non-fungible token) – это уникальный и невзаимозаменяемый токен, каждый экземпляр которых не может быть замещен другим аналогичным токеном.

NFT-награды

Вместо орденов и медалей, заслуженные герои и просто замечательные люди будут получать на свой цифровой кошелек награды в виде NFT-токенов, которые будут отображаться в профиле кошелька и добавлять бонус к социальному рейтингу.

Экономика на стероидах

Экономика будет стимулироваться с помощью концепции денег со сроком годности.

Согласно данной концепции, граждане смогут воспользоваться своими деньгами только в установленный срок, по истечению которого они станут бесполезны и потратить их будет невозможно.

Благодаря такому подходу люди станут активнее тратить свои деньги, растягивая таким образом фазы экономического «подъема» и «пика», сокращая фазы «рецессии» и «дна». Люди не смогут откладывать деньги, что практически уничтожит социальный лифт и, в совокупности с социальным рейтингом, породит либеральную сансару.

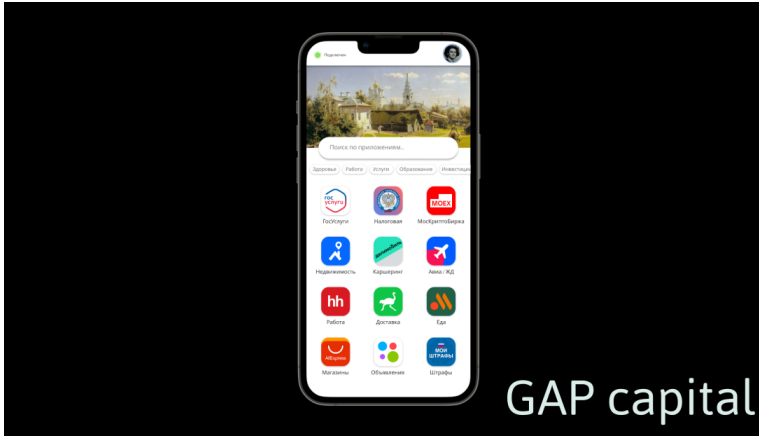
Пособия

Со временем всем людям будут приходить ежемесячные выплаты на цифровой кошелек, равные минимальному размеру оплаты труда в рамках программы по борьбе с безработицей, ведь не все успеют быстро адаптироваться к новым условиям, не так ли?

Децентрализованные приложения

SuperApp-приложение – это экосистема, предоставляющая доступ практически ко всем видам услуг, начиная внутренним общением и заканчивая банковскими услугами, фактически становясь всеобъемлющей, автономной онлайн-платформой.

Цифровой кошелек станет модульным SuperApp'ом, из которого люди будут подключаться к децентрализованным приложениям, предоставляющим практически все виды услуг напрямую, начиная от доставки еды и заканчивая покупкой недвижимости.



Государственная монополизация и национализация

Государства уже начинают поджимать под себя различные сферы, что в конечном счете приведет к разорению компаний, существующих за счет таких услуг, как: каршеринг, страховка, такси, доставка, оформление сделок, покупка недвижимости и так далее.

Монополизация экономики будет происходить постепенно, пока государство не получит абсолютную монополию во всех сферах нашей жизни. Все сделки без исключения будут происходить посредствам цифрового кошелька между покупателем и продавцом напрямую.

Далее, частные компании будут постепенно национализироваться, продаваясь за безостановочно печатаемые деньги.

Метавселенные

Метавселенные – виртуальное пространство, в котором люди могут взаимодействовать друг с другом и с цифровыми объектами через свои аватары, с помощью технологий виртуальной реальности.

Безусловно, человечество еще успеет погрязнуть в "цифровом пространстве", предварительно переместив туда все сферы своей жизни, однако, в текущем виде метавселенные больше напоминают малобюджетные игры из нулевых, созданные на коленке из «камней» и палок.

Единственная причина, по которой сейчас намеренно удерживают наш фокус внимания на метавселенных – подготовка коллективного бессознательного к новой реальности и повсеместного "crypto adoption[5]".

[5] Mass crypto adoption – повсеместное принятие криптовалют в качестве платежного средства.

Преимущества

Антиутопическое будущее, на первый взгляд, кажется слишком темным и пасмурным, однако, вы легко сможете найти в нем множество положительных аспектов:

1. Экономическое рабство искоренит бедность.

2. Тотальный контроль всех сфер жизни искоренит преступность.

3. Эко-повестка заставит людей думать об окружающей среде, несмотря на то, в каком виде она сейчас преподносится.

В отличии от комфортной жизни, экстремальные условия для существования заставляют человека обращаться к самому себе, искать ответы, работать над собой и самосовершенствоваться.

Заключение

Вышеописанное звучит крайне утопично и несбыточно, однако не стоит считать, что все произойдет по щелчку пальцев, нет. Общество будут долго и планомерно подготавливать, создав все необходимые условия для того, чтобы мы сами захотели подобных изменений.

В нулевых никто не выходил на улицу без наличных денег, а сейчас наличными деньгами никто не пользуется, потому что расплачиваться кредитной картой намного удобнее.

Точно также будет удобно получать любой вид услуг из единого приложения, не стоять в очередях и никуда не ездить при покупке или продаже вещей, транспорта и недвижимости. Намного удобнее будет не подавать декларацию о доходах, ведь всю прибыль будет видно в истории транзакций вашего цифрового кошелька, откуда подоходный налог удержится автоматически.

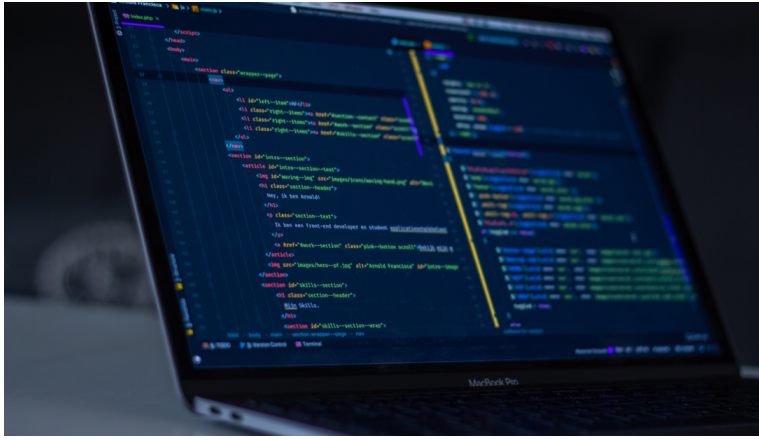
Я не преследую цели вызвать чувство страха, напротив, хочу предупредить вас, подметив то, чего не замечают остальные. Если вы начнете самостоятельно наблюдать и выявлять тенденции, проводя логические связи и не считая что-либо невозможным – обязательно откроете для себя много нового.

Пытаться изменить игру бессмысленно и бесполезно, лучшее, что вы можете сделать – изменить свое положение в

этой игре, своевременно распознав тенденции, ведь кто владеет информацией, тот владеет миром.

Цифровая безопасность

Крипто-пространство – опасное место, где вы можете потерять деньги буквально на каждом шагу, и для этого вовсе необязательно нарушать риск-менеджмент или покупать неликвидные монеты, достаточно просто перейти по ссылке или подключиться к ненадежной Wi-Fi сети. Поэтому предлагаю начать ваше знакомство с крипторынком с азов: поговорим о цифровой безопасности, мерах предосторожности, приведу практические рекомендации и помогу вам свести к нулю риск потери денежных средств.



Пароли

Всегда создавайте сложные пароли, используя различные регистры, цифры и специальные символы.

*Пример надежного пароля: 2x-F?mF*RemsnZT*

Утечки паролей

В случае утечки паролей хакеры начинают проверять почтовые ящики из украденной базы данных пользователей на наличие регистраций в разных сервисах, после чего перебирают пароли.

Так как большинство людей используют одинаковые пароли для всех сервисов, вероятность их компрометации стремится к 100 %.

Чтобы избежать взлома, необходимо крайне внимательно относиться к своим почтовым ящикам, паролям, устройствам и сервисам, которыми вы пользуетесь.

Общие рекомендации

1. Не используйте онлайн-сервисы для генерации паролей.
2. Не храните все свои пароли в одном месте.
3. Не храните свои пароли на электронных носителях.

4. Не храните свои пароли в облаке, мессенджерах и заметках.

5. Храните свои пароли на физических носителях в разных местах, предварительно создав несколько копий.

6. Создавайте разные пароли для каждого сервиса.

7. Для создания сложных паролей используйте слова из категорий: животные, машины, песни, цветы и тому подобное.

8. Для усиления пароля умышленно делайте орфографические ошибки в написании слов и словосочетаний.

Проверка наличия утечки

Проверить свои пароли на предмет утечки можно здесь:

1. https://haveibeenpwned.com/
2. https://password.kaspersky.com/ru/

Диверсификация почты

Диверсификация почты является залогом безопасности.

Разграничьте почту для разных потребностей, разделив ее на личную, рабочую и ненужную:

1. Отдельный почтовый аккаунт для личного пользования.

2. Отдельный почтовый аккаунт для регистрации торговых счетов.

3. Отдельный почтовый аккаунт для привязки облачных сервисов.

4. Отдельный почтовый аккаунт для регистрации на различных ненужных сервисах, вроде интернет-магазинов.

Общие рекомендации

• Регулярно очищайте почтовый ящик от спама.

• Прежде чем перейти по ссылке из письма, сравните почтовый адрес отправителя с указанным почтовым адресом на сайте сервиса.

Двухфакторная аутентификация

Для более надежной защиты используйте двухфакторную аутентификацию.

Двухфакторная аутентификация или 2FA – это дополнительный уровень безопасности помимо вашего пароля или PIN-кода.

В большинстве сервисов 2FA – это использование смс-сообщений, однако, это не самый безопасный способ, поэтому используйте дополнительно приложение "Google Authenticator".

Скачать Google Authenticator можно в магазинах приложений:

1. App Store
2. Play Market

Используйте двухфакторную аутентификацию везде, где только можно:

- Мессенджеры
- Онлайн-сервисы
- Приложения бирж
- Облачные сервисы
- Банковские приложения

Важно: обязательно создавайте резервные копии ключей, хранящихся в приложении, иначе при утере устройства вам придется обращаться в службу поддержки для восста-

новления доступа к аккаунтам.

Идеальный usecase – использование «чистого» (отдельного) мобильного устройства для Google Authenticator'a, которое вы не подключаете к интернету и храните в надежном месте.

FIDO U2F

FIDO U2F (Universal 2nd Factor) – дополнительный способ двухфакторной аутентификации, основанный на вызов-ответной аутентификации, позволяющий использовать U2F устройство как второй фактор для аутентификации на большом количестве онлайн-сервисов.

Иными словами, FIDO U2F – это физическое устройство, выступающее дополнительным фактором аутентификации.

Для более надежной защиты своих учетных записей вы можете использовать устройства FIDO U2F, настроив их таким образом, чтобы авторизация без них была невозможной. Даже если злоумышленник получит данные от ваших учетных записей (логин, пароль, доступ к сим-карте и к authenticator'у), он не сможет авторизоваться без физического устройства, выступающего дополнительным и обязательным способом аутентификации.

В качестве устройств FIDO U2F используются устройства YubiKey и Ledger.

YubiKey

YubiKey – это аппаратный ключ безопасности, производимый компанией Yubico, который поддерживает протокол универсальной двухфакторной аутентификации, одноразовые пароли и асимметричное шифрование. Это позволяет пользователям выполнять безопасный вход в учетные записи, при помощи вырабатываемых одноразовых паролей, или с использованием открытых и закрытых ключевых пар, генерируемых на устройстве.

Приобрести устройство можно на официальном сайте компании или у проверенных продавцов – https://

www.yubico.com/.

Ledger

Ledger – это аппаратный кошелек для хранения криптовалюты. Его разработала и произвела французская компания Ledger, которая занимается гаджетами для работы с криптовалютами с 2014 года. Устройство выглядит просто, как Flash-накопитель премиум класса.

Помимо хранения криптовалюты, Ledger можно использовать в качестве устройства U2F. Для этого необходимо установить на устройство приложение "Fido".

Подробная инструкция – https://www.ledger.com/ru/fido-

u2f.

Приобрести оригинальное устройство с 10 % скидкой здесь (официальный сайт Ledger) – https://shop.ledger.com?r=9b2e16001e92.

Гаджеты

Мобильные телефоны

Существуют две основные операционные системы для мобильных телефонов: iOS и Android. Главное различие между операционными системами Android и iOS заключается в том, что Android – это система с открытым исходным кодом. По этой причине устройства Android легче поддаются процедуре взлома, так как в открытом исходном коде проще обнаружить уязвимости.

В настоящий момент большинство людей используют устройства на базе android, и, с точки зрения хакеров, имеет смысл писать вредоносный код для той системы, которую не только легче взломать, но и которой пользуется большее количество потенциальных жертв. Поэтому большая часть хакерских атак нацелена на android-устройства.

Если вы хотите обезопасить себя и свои средства – наилучшим решением будет выбор продукции Apple.

Компьютеры

Аналогичная ситуация сложилась вокруг операционных систем Windows и MacOS, продукция Miscrosoft более по-

пулярна и уязвима.

Если вы храните деньги на торговых счетах, доступ к которым есть на вашем персональном компьютере – вам следует использовать MacOS.

Не забывайте про общие правила безопасности при использовании ПК: вам не следует устанавливать софт из непроверенных источников, открывать ссылки, архивы и. pdf-файлы от неизвестных отправителей. Также не стоит посещать сомнительные сайты.

Обновление программного обеспечения

Регулярно обновляйте программное обеспечение телефона, персонального компьютера и всех используемых вами приложений, так как практически каждое обновление программного обеспечение касается безопасности.

Иными словами, разработчики с каждым обновлением убирают всевозможные уязвимости в программном обеспечении, которые могут быть использованы злоумышленниками против вас.

Бесплатные версии платных программ

В сети существует масса сервисов со взломанными версиями платных программ. Такие программы называются «активаторы» и «кряки». Созданы они для обхода акти-

ваций и бесплатного использования таких программ, как «Photoshop», "Word" и тому подобное.

Многие люди используют такие программы в повседневной жизни и совсем не подозревают о том, что скрывается внутри. Следует запомнить простое правило:

“Если вы не платите за товар, значит, товаром являетесь вы”

Подобный софт создают не из-за каких-нибудь идейных побуждений или альтруистических наклонностей. Авторы такого софта, как правило, преследуют личные интересы. Нередко при установке «активатора» в систему проникает троянская программа, которая ворует ваши пароли от учетных записей и устанавливает удаленный доступ к вашему устройству.

Антивирусы никак не помогут решить эту проблему и не смогут обезопасить ваше устройство, поскольку многие передовые противовирусные программы попросту ничего не обнаруживают.

Общие рекомендации

• Пользуйтесь услугами антивирусных программ и надейтесь, что они хоть как-то вам помогут.

• Диверсифицируйте устройства на личные и рабочие.

• Регулярно обновляйте программное обеспечения на всех устройствах.

• Не скачивайте никакие исполняемые файлы и архивы с неофициальных сайтов приложений.

• Приучите себя платить за софт, иначе вы рискуете потерять свои данные, учетные записи, деньги, время и нервы.

• Регулярно создавайте резервные копии своих устройств или настройте автоматическое создание резервных копий, чтобы в случае взлома, утери, кражи или поломки устройства вы оперативно могли получить доступ к своим данным.

Облачные сервисы

Хакеры регулярно взламывают облачные сервисы знаменитых людей (iCloud, Google Disk и т. п.) в целях шантажа и вымогательства.

Во избежание утечки важных для вас данных заранее позаботьтесь о содержимом своих облачных сервисов: почистите хранилища и перенесите данные на более безопасные (физические) накопители.

Мессенджеры

Telegram, WhatsApp и ВКонтакте являются самыми популярными мессенджерами. Не стоит хранить в них важные “чувствительные” данные и свои пароли, так как в случае взлома вы рискуете потерять доступ к остальным учетным записям.

Для того чтобы обезопасить себя от взлома, следует установить "облачный пароль" и двухфакторную аутентификацию.

Общие рекомендации

• Регулярно обновляйте приложения до последних версий.

• Не храните в мессенджерах свои пароли от учетных записей.

• Установите "облачный пароль" и двухфакторную аутентификацию.

• Скачивайте приложения только из проверенных источников (App Store и Play Market).

• Не храните в мессенджерах информацию, которую могут использовать против вас.

Сим-карты

Один из самых распространенных способов взлома – перевыпуск сим-карты.

Этим способом часто пользуются злоумышленники: оформляют перевыпуск вашей сим-карты, после чего получают доступ к аккаунтам через восстановление пароля.

Чтобы исключить данный способ компрометации, необходимо сделать две вещи:

1. Установить PIN-код на сим-карту.

2. Запретить перевыпуск своей сим-карты у сотового оператора.

Публичные Wi-Fi сети

В наше время, когда беспроводные Wi-Fi сети есть практически везде: на вокзалах, в кафе, ресторанах и даже глубоко под землей в вагонах метро, далеко не все знают об угрозах информационной безопасности, которые касаются каждого пользователя, включившего Wi-Fi на своем устройстве.

Перехват трафика

Если вы подключены к публичной Wi-Fi сети, злоумышленник может легко перенаправить весь трафик между вашим устройством и роутером через свой ноутбук, тем самым он получит доступ ко всем данным, которые вы передаете или загружаете. Для этого злоумышленник будет использовать MitM-атаку (“человек посредине”) – ARP-spoofing.

Создание поддельных точек доступа

Большинство современных телефонов и ноутбуков ав-

томатически ищут Wi-Fi сети и подключаются к ним. В первую очередь такие устройства будут искать сети со знакомыми названиями, такими как «MosMetro_Free» или «MT_FREE». Во время поиска устройства отправляют запросы на подключение к сетям.

Злоумышленник может создавать сети с идентичными названиями и паролями для того, чтобы ваше устройство автоматически подключились к его точке доступа. Пользователь, увидев открытую сеть с названием кафе, скорее всего подключится к ней, не подозревая о том, что после подключения злоумышленник сможет управлять его соединением.

Атака

Далее злоумышленник подменит протокол шифрования с "https://", который защищен и не подвержен атакам, на "http://", который поддается взлому, после чего успешно перехватит ваши пароли и сможет обманным путем заставить вас скачать на свое устройство вирус, с помощью фишинговой атаки.

Как избежать взлома?

Чтобы избежать взлома – не пользуйтесь публичными сетями, вместо них используйте мобильную сеть, либо раздавайте точки доступа со своих устройств, предварительно

установив на них защиту.

Домашний Wi-Fi роутер

Не забывайте, что, находясь у себя дома вы также можете стать жертвой хакерской атаки или предметом слежки, если ваш домашний Wi-Fi роутер и система "умного дома" не защищены должным образом.

Незащищенные роутер и беспроводная сеть могут стать точкой входа для соседа, который практикует свои знания, или для настоящего злоумышленника. Постоянно обновляйте ПО на роутере, но только от доверенного разработчика.

Как настроить роутер?

Для настройки вам необходимо получить доступ к админ-панели роутера. Инструкция для получения доступа находится в договоре о предоставлении услуг, либо на наклейке, приклеенной к обратной стороне устройства.

В большинстве случаев доступ к админ-панели можно получить, используя заводские адреса и пароли:

Адрес – 192.168.0.1 или 192.168.1.1

Логин – admin или 12345.

Пароль – admin или 12345.

Общие рекомендации

• Измените стандартный IP-адрес устройства.

• Отключите WPS и удаленный доступ к роутеру.

• Регулярно обновляйте прошивку и программное обеспечение.

• Установите сложные пароли для сети Wi-Fi, админ-панели и устройств "умного дома".

• Установите в качестве механизма защиты беспроводной сети алгоритм WPA3-PSK (Wi-Fi Protected Access) и ни в коем случае не используйте механизмы WEP, WPA и WPA2.

Virtual Private Network (VPN)

Чаще всего пользователи скачивают VPN на мобильные устройства. Более надежными для использования являются платные VPN-сервисы, но даже их использование лишь снижает, а не исключает риск использования вашей информации для получения прибыли.

Главная опасность VPN – высокий риск утечки данных. Пользователи думают, что VPN лишь дает возможность пользоваться недоступными в регионе сайтами, но вместо этого рискуют потерять свои данные, которые находятся на их устройстве.

Использование VPN-сервисов равносильно тому, если бы вы отдали свой паспорт первому встречному. Помните, что ни один заблокированный сайт никогда не представит большей ценности, чем безопасность ваших персональных данных.

Если вам необходимо использовать VPN – лучшим решением будет создание собственного. Создание собственного VPN стоит не так дорого, как может показаться на первый взгляд, однако, личный сервер сведет к нулю риски потери данных.

Безопасность в сети

Не скачивайте файлы с непроверенных сайтов, не открывайте "исполняемые файлы" и архивы от неизвестных людей. Будьте бдительны и не переходите по полученным в spam-рассылках ссылкам.

Фишинговые атаки

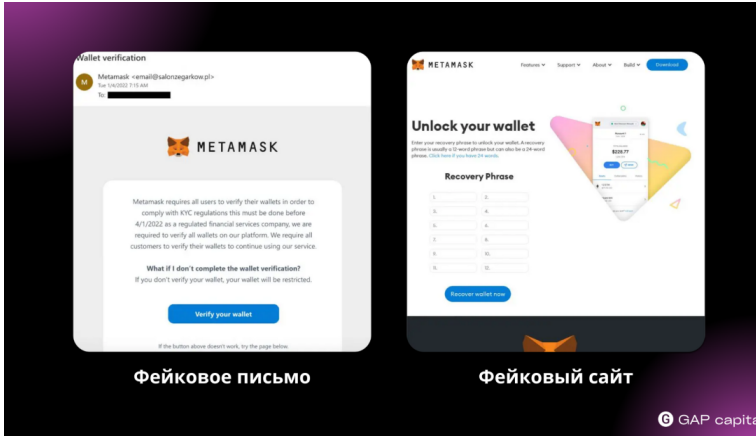
Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Получение доступа к данным достигается путем проведения массовых спам-рассылок электронных писем и личных сообщений, якобы от имени популярных брендов. В таких письмах и сообщениях содержатся ссылки на сайты-подделки, внешне неотличимых от настоящих. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами, играя на эмоциях пользователя, заставить его отправить свои логин и пароль, что позволяет мошенникам получить доступ к аккаунтам и счетам.

Иными словами, фишинг – это разновидность социальной инженерии, основанная на незнании пользователями основ сетевой безопасности. Многие интернет-пользователи не знают простого факта: сервисы не рассылают письма с

просьбами отправить данные от своей учетной записи.

Пример spam-рассылки

На электронные адреса была произведена spam-рассылка, якобы от MetaMask'а[6]. В письмах содержалась информация о необходимости прохождения KYC[7] для разблокировки кошелька:



Ссылка из письма ввела на фейковый сайт. Внешне он никак не отличался от оригинала, однако имел другой адрес:

1. metamask.io – настоящий сайт.

---

[6] MetaMask – это “горячий” кошелек для хранения криптовалюты.

[7] KYC (Know Your Customer) – процедура верификации личности.

2. metanask.io – фишинговый сайт.

Адрес сайта отличался всего одной буквой. Жертвы фишинговой атаки не заметили отличия и потеряли доступ к своим кошелькам, поэтому будьте крайне бдительны, когда переходите по незнакомым ссылкам.

Как избежать фишинговой атаки?

Чтобы избежать фишинговой атаки:

• Не подключайтесь к сети с помощью публичных Wi-Fi.

• Внимательно проверяйте адрес сайта в поисковой строке, сверяя каждый символ.

• Сверяйте адрес отправителя электронного письма с электронным адресом, указанным на сайте сервиса.

• Никогда и ни под каким предлогом не вводите свои данные на сайтах, на которые вы попали, перейдя по ссылке.

Криптовалютные кошельки

Кошельки внутри криптовалютной экосистемы делятся на «горячие» и «холодные». Если вы хотите надежно хранить свои средства – используйте холодные кошельки и не держите на горячих кошельках ощутимую для себя сумму, так как они могут быть взломаны.

Горячие кошельки

Горячие кошельки – это онлайн-платформы, доступ к которым обеспечивается через мобильное устройство, ноутбук или ПК. Такие кошельки называются «кастодиальными», то есть предполагают хранение криптоактивов посредниками, а значит приватные ключи для доступа к их содержимому принадлежат посредникам. Именно здесь скрывается уязвимость в системе безопасности, поскольку доверенные посредники часто оказываются ее брешью.

Холодные кошельки

Холодные кошельки – это хранилища цифровых активов, которые не подключены к интернету и чаще всего представлены аппаратными или бумажными кошельками. Можно с уверенностью утверждать, что холодные кошельки являются

стандартом безопасности для криптоактивов в криптоиндустрии.

Поскольку холодные кошельки не подключаются к интернету, это делает их недосягаемыми для хакеров и обеспечивает лучшую защиту криптоактивов, так как вы владеете приватными ключами.

Владение приватными ключами предполагает полный контроль над криптоактивами. Однако, это также предполагает определенную ответственность за их безопасность.

Хранение активов в альтернативных сетях

Конвертация и хранения криптоактивов в неродных сетях (например, BTC —> WBTC и ETH —> WETH) небезопасны, так как в случае взлома протокола хакеры могут достать базовый актив, обеспечивающий «обернутый», оставив вам ничем не обеспеченные и ничего не стоящие фантики.

Имейте ввиду, что хранение активов в «неродных» сетях из-за желания сэкономить на комиссиях может лишить вас денежных средств.

Общие рекомендации

- Не храните активы в неродных сетях.
- Не храните фразу восстановления на электронных носи-

телях.

• Храните несколько копий фразы восстановления в надежных местах (дома, на даче и т. д.).

• Не контактируйте с незнакомыми токенами и NFT, особенно на децентрализованных биржах и незнакомых вам площадках. Существует вероятность потери доступа к кошельку и к денежным средствам.

• Никому, никогда и никуда не отправляйте seed-фразы от своих холодных и горячих кошельков. Разработчики не будут отправлять вам письма с просьбой повторить seed-фразу, чтобы убедиться, что вы ее не забыли.

Виды мошенничества

Многие начинающие криптоблогеры продают свои telegram-каналы мошенникам, либо вовсе начинают всячески обманывать свою аудитории с целью заработать.

Приведу несколько общих рекомендаций:

1. Никому не переводите свои средства ни под каким предлогом.

2. Никогда и ни при каких обстоятельствах не передавайте свои средства в доверительное управление. Никто не будет зарабатывать деньги за вас.

3. Не покупайте неизвестные токены, особенно на децентрализованных биржах. Создание и выпуск собственного токена на децентрализованной бирже весьма простая задача. Токены не проходят никаких проверок и биржевых аудитов.

4. Не покупайте токены блогеров, многие из них замечены в откровенном обмане, например, чего стоит история с нашумевшем токеном $AZY – https://www.tradingview.com/x/HAutBRg9/. Схема работы: продают как можно больше токенов, после чего вытаскивают всю ликвидность из проекта, оставляя несколько человек для создания видимости жизнедеятельности проекта.

5. Не участвуйте в марафонах по заработку миллионов с нескольких долларов – это мошенничество. Подобные марафоны преследуют две основных цели:

5.1 – получить от вас деньги за участие в марафоне.

5.2 – получить от вас деньги продав вам собственный токен.

6. Не контактируйте с незнакомыми токенами и NFT, особенно на децентрализованных биржах и незнакомых вам площадках. Существует вероятность потери доступа к кошельку и к денежным средствам.

7. Не верьте скриншотам с информацией о листингах на Binance и других площадках, а также не доверяйте скриншотам с твитами известных людей, якобы призывающих к покупке какого-либо токена, так как с вероятностью в 99 % это обман с целью нажиться на вас.

8. Не участвуйте в первичных размещениях (ICO / IDO) с непроверенными каналами, так как участились случаи сбора средств без предоставления аллокации и возврата.

9. Не участвуйте в PUMP'ах и DUMP'ах низколиквидных монет, организованных различными сообществами, так как на подобных мероприятиях зарабатывают исключительно организаторы.

10. Никому, никогда и никуда не отправляйте seed-фразы от своих холодных и горячих кошельков. Разработчики не будут отправлять вам письма с просьбой повторить seed-фразу, чтобы убедиться, что вы ее не забыли.

11. Прежде чем переходить по полученным в личных сообщениях или по почте ссылкам на сайты проектов, проверяйте их с помощью coinmarketcap.com, так как злоумыш-

ленники маскируют свои фишинговые сайты под известные проекты, а при получении вашего пароля или при подключении кошелька крадут средства.

12. Для того чтобы добиться доверия читателей, некоторые мошенники нанимают актеров, которые записывают видеоролики якобы от лица администраторов, а потом продают своим же читателям фантики.

Прежде чем что-либо сделать, купить, отправить, перейти по ссылке – несколько раз подумайте и все перепроверьте. Если вы наткнулись на очевидное мошенничество – обязательно отправьте жалобу на проверку администраторам ресурса. Таким образом вы сможете помочь людям, предотвратив потерю чьих-то денежных средств.

Чек-лист

Необходимо сделать прямо сейчас

- Диверсифицировать почту и устройства.
- Установить 2FA везде, где только можно.
- Проверить свои пароли на предмет утечки.
- Создать сложные пароли для учетных записей.
- Обновить всевозможное программное обеспечение.
- Перестать пользоваться общественными Wi-Fi сетями.
- Обновить настройки безопасности домашнего роутера.
- Удалить из облачного хранилища важную информацию.
- Зарегистрировать новые торговые аккаунты на биржах[8].
- Письменно запретить перевыпуск своей SIM-карты у своего сотового оператора.
- Перестать пользоваться бесплатными VPN-сервисами и заказать собственный VPN-сервер.
- Создать резервные копии фразы восстановления от холодных кошельков на надежных (офлайн) носителях.
- Перевести всю свою криптовалюту с горячих (кастодиальных) на холодные (некастодиальные) кошельки.

---

[8] Используйте наши партнерские ссылки для получения бонусов – teletype.in/@gap_capital/affiliate_program.

Необходимо делать постоянно

- Не скачивать пиратские версии программ.
- Отключить автоматическое подключение к Wi-Fi.
- Быть осторожным при открытии файлов, ссылок и архивов.
- Пользоваться только официальными магазинами приложений.
- Контролировать доступ приложений к устройству и запретить отслеживание.

Необходимо делать регулярно

- Очищать почту от спама.
- Сканировать устройства антивирусом.
- Удалять ненужные файлы и приложения.
- Обновлять пароли от своих учетных записей.
- Создавать резервные копии своих устройств.
- Обновлять всевозможное программное обеспечение.

Регистрация новых торговых аккаунтов

Самое время заново зарегистрировать торговые аккаунты на криптобиржах, предварительно диверсифицировав почтовые ящики, для того чтобы обезопасить свои средства.

Вы можете пройти процедуру регистрации по нашим партнерским ссылкам, заручившись нашей поддержкой и получив ряд преимуществ. Подробнее здесь – teletype.in/@gap_capital/affiliate_program.

Заключение

Цифровая безопасность в наше время является необходимой мерой, которую современный криптотрейдер просто не может игнорировать. Следите за своей цифровой гигиеной и с вашими средствами все будет в порядке.

На какой бирже мы торгуем?

Первый шаг в трейдинге – это выбор криптобиржи. Следует крайне внимательно относиться к выбору сервиса, которому вы собираетесь доверить свои средства, так как ненадежная криптобиржа может разорить вас из-за ликвидации прибыльной позиции[9], проскальзывания стоп-лосса, внезапной блокировки счета в самый неподходящий момент или отказа в обслуживании из-за места вашего рождения.

Мы ведем спотовую и маржинальную торговлю исключительно на криптобирже ByBit.

[9] Некоторые криптобиржи ликвидируют прибыльные позиции трейдеров, прикрываясь механизмом ADL (автоделевереджинг).


BYBIT
GAP_capital

Почему ByBit?

Криптобиржа ByBit не будет накладывать какие-либо ограничения на граждан РФ, так как находится вне юрисдикции, с которой идет давление. Кроме того, ByBit не передает данные пользователей правоохранительным органам и налоговой службе.

Конец ознакомительного фрагмента.