

Роджер

Деньги по методике спецслужб



Роджер Роджер

Деньги по методике спецслужб

Серия «По методике спецслужб», книга 3

<https://litres.ru/74254829>

SelfPub; 2026

Аннотация

Эта книга — не учебник по личным финансам и не пособие по инвестициям. Это инструкция по выживанию в мире, где ваши деньги перестают быть вашими в ту секунду, когда банк или государство решают иначе. Её автор, опираясь на реальные протоколы оперативных служб, разбирает три главных канала хранения капитала — банковские счета, криптовалюту и наличные — и показывает уязвимости каждого из них. Вы узнаете, почему биткоин не анонимен, как конфискуют цифровые активы и что делать, если счёт заблокирован по 115-ФЗ.

Главная ценность этой книги не в разборе угроз, а в системе. Здесь собраны готовые алгоритмы действий: от повседневной финансовой маскировки и построения бизнес-легенды до экстренной мобилизации ресурсов в первые 24 часа после потери доступа к деньгам. Отдельная глава посвящена протоколу «Мертвая рука» — передаче активов преемнику в случае смерти владельца, чтобы накопленное не исчезло бесследно.

Содержание

Глава 1: Банковский счет — красивая иллюзия владения	4
Глава 2: Криптовалюта — цифровое золото под цифровым арестом	11
Конец ознакомительного фрагмента.	16

Роджер

Деньги по методике спецслужб

Глава 1: Банковский счет — красивая иллюзия владения

Что такое банковский счет с точки зрения оперативника
и как его блокируют за секунду

Ты просыпаешься утром, варишь кофе, открываешь приложение банка, чтобы оплатить коммуналку или проверить баланс перед поездкой и видишь это: «Счет заблокирован. Операции приостановлены». Либо того хуже — баланс \$0.00, а в истории платежей — принудительное списание.

Ты звонишь в поддержку, робот, потом живой оператор с металлическим голосом: «Ваш счет заблокирован в соответствии с Федеральным законом №115-ФЗ. Для разблокировки предоставьте документы, подтверждающие происхождение средств». Ты спрашиваешь, сколько это займет. «До

30 рабочих дней». Либо еще хуже №161-ФЗ, где сроков нет вообще. Ты понимаешь, что ипотека через неделю, кредитке конец месяца, а наличных в кошельке — три тысячи.

Поздравляю, ты только что узнал на своей шкуре то, что оперативник знает с первого дня подготовки: банковский счет — это не твои деньги. Это деньги банка, которыми он тебе разрешил пользоваться до первого подозрения.

Юридическая реальность: ты не владелец, ты кредитор. Когда ты кладешь деньги на счет, с точки зрения права ты не хранишь их, а даешь их банку в долг. Банк становится твоим должником, а ты — кредитором. Твое право требования к банку — это всего лишь запись в базе данных, когда государство или сам банк решают, что ты нарушил какие-то правила, эту запись обнуляют одним кликом.

В России это 115-ФЗ («О противодействии легализации доходов»). В США — Bank Secrecy Act и Patriot Act. В Европе — директивы AML (Anti-Money Laundering). Формулировки разные, суть одна: банк обязан следить за твоими операциями и докладывать о подозрительных. Если банк этого не делает, его штрафуют и лишают лицензии. Поэтому банк перестраховывается, он заблокирует тебя быстрее, чем ты скажешь «криптовалюта».

Что именно кажется банковскому роботу подозрительным? Вот краткий список вещей, которые оперативник избегает как огня:

Снятие крупной суммы наличными сразу после за-

числения. Зачисление безнала от юрлица и мгновенный обнал — классический признак обнальной конторы. Даже если ты не обнальщик, ты попадаешь под этот фильтр.

Частые переводы физическим лицам. Особенно если в назначении платежа есть слова «за квартиру», «долг», «вознаграждение», «за услуги». Робот видит в этом незаконную предпринимательскую деятельность или уклонение от налогов.

Слово «Биткоин», «крипта», «USDT», «криптовалюта» в назначении платежа. Это мгновенный красный флаг. В некоторых банках — автоматическая блокировка до выяснения. Никогда, никогда не пиши эти слова в банковских переводах.

Поступление из-за границы от незнакомого отправителя. Особенно из офшорных юрисдикций или стран, подпадающих под санкции. Даже если это перевод от родственника, который живет в Лондоне, робот может пометить его как подозрительный.

Резкое изменение профиля активности. Ты годами получал зарплату 50 тысяч рублей и вдруг получил 500 тысяч, либо наоборот — у тебя был стабильный бизнес-счет, и вдруг ты снял всё до копейки. Аномалия = подозрение.

Дробление суммы. Ты хочешь снять 500 тысяч, но знаешь, что от 600 тысяч начинается обязательный контроль Росфинмониторинга. Ты снимаешь 500, потом еще 500, потом еще. Это называется structuring, и за это сажают даже в

США.

Мой знакомый (назовем его Д.) получил перевод от друга. Друг недавно увлекся криптой и в назначении платежа написал: «Возврат долга за биткоин». Сумма — 80 тысяч рублей. Обычный перевод между двумя физлицами внутри страны.

Счет Д. был заблокирован через два часа. Банк запросил: происхождение средств, скриншоты переписки, историю операций с криптобиржей, выписку с кошелька. Д. предоставил всё. Разблокировка заняла две недели. Две недели он не мог платить за квартиру, покупать еду и заправлять машину. Его деньги лежали на счете, но он не мог ими воспользоваться.

Роботу всё равно, виноват ты или нет. Робот видит слово «биткоин» и ставит галочку «подозрительно». Дальше — живой оператор, который завален сотнями таких же кейсов, и он будет разбираться с тобой, когда у него дойдут руки.

Разведчик никогда не держит все деньги в одном банке. Даже в одной стране. Идеальная структура ликвидности для оперативника выглядит так:

Банк А (зарплатный): счет, на который приходят легальные доходы по легенде. С него оплачиваются налоги, коммуналка, кредиты. Он всегда чист и прозрачен. Операции — скучные и предсказуемые.

Банк Б (оперативный): счет для текущих расходов, не связанных с легендой. Суммы небольшие. При малейшей угрозе блокировки — закрывается без сожаления.

Банк В (зарубежный): счет в нейтральной юрисдикции, куда выводятся резервы. Не привязан к твоему налоговому резидентству напрямую. Используется для оплаты билетов, отелей, VPN-серверов.

Наличные: сумма на месяц жизни в тайнике. Подробнее в Главе 3.

Крипта: холодный кошелек с сид-фразой в голове. Подробнее в Главе 2.

Если блокируют Банк А, ты живешь на Банк Б и наличные, пока разбираешься. Если блокируют всё в стране, у тебя есть Банк В и крипта. Если блокируют всё везде — ты провален, и это уже не финансовая проблема, а протокол эвакуации.

Что делать прямо сейчас (до того, как заблокировали)

Проверь свои счета. Открой историю операций за последний месяц. Есть ли там что-то, что может показаться подозрительным роботу? Слова «крипта», «обнал», переводы от незнакомцев, дробление сумм?

Прекрати писать лишнее в назначениях платежа. Перевод другу? Пиши «Возврат долга» или «Подарок». Без деталей. Чем короче, тем лучше.

Разнеси средства. Если у тебя всё лежит на одном зарплатном счете, открой второй в другом банке и переведи туда хотя бы 20-30% резерва. Не ленись. Это час времени сейчас против двух недель ада потом.

Сними наличные на неделю. Прямо сегодня. Сумму, которой хватит на еду, транспорт и базовые нужды. Храни дома в надежном месте. Это твой «нулевой рубеж».

Что делать, если счет уже заблокирован

Не паниковать. Паника — это ошибки. Ошибки — это усугубление ситуации.

Запросить официальный ответ. Банк обязан письменно объяснить причину блокировки и перечень документов для разблокировки. Получи этот перечень.

Предоставить документы. Даже если ты считаешь, что ты чист как стеклышко, банк так не считает. Дай им то, что они просят: справку о доходах, договор займа, скриншоты переписки, выписку с биржи. Чем быстрее ты это сделаешь, тем быстрее разблокируют.

Подключить резервный канал. Не жди разблокировки, чтобы поесть. У тебя должны быть наличные или второй счет. Если их нет — Глава 4 этой книги ждет тебя.

Ты понял главное: банковский счет — это не сейф. Это кредит доверия, который могут отозвать в любой момент. В следующей главе мы разберем криптовалюту — инструмент, который многие считают спасением от банковского произвола. Ты узнаешь, почему биткоин не анонимен, как конфискуют крипту через биржи, что такое атака 5-долларовым гаечным ключом и как защитить сид-фразу так, чтобы даже под пытками её нельзя было выдать. Готовь холодный коше-

лек. Мы ныряем в мир, где ты сам себе банк и сам себе тюремщик.

Глава 2: Криптовалюта — цифровое золото под цифровым арестом

Почему биткоин не анонимен, как конфискуют крипту и что такое атака 5-долларовым гаечным ключом

Ты открыл счет в банке, увидел, как легко его блокируют. Ты решил: «Ухожу в крипту. Биткоин — это свобода, никаких банков, никаких блокировок, никакого государства». Ты покупаешь USDT на бирже, выводешь на кошелек и чувствуешь себя неуловимым.

Поздравляю, ты только что добровольно записал себя в реестр владельцев криптовалюты, твой паспорт, твоё селфи, твой IP-адрес, твой банковский счет — всё это уже связано с твоим криптокошельком, ты не исчез, а просто сменил одну прозрачную систему на другую, которая кажется тебе непрозрачной только потому, что ты не знаешь, как она устроена.

Криптовалюта — это мощный инструмент, но, как любой инструмент, он требует навыка. В неумелых руках это не оружие, а улика.

Миф №1: Биткоин анонимен

Биткоин — это не анонимная валюта. Это псевдонимная валюта. Разница огромна.

Каждая транзакция в блокчейне биткоина записана навсегда, открыто, публично, доступно для анализа. Твой адрес кошелька — это псевдоним. Сам по себе он не содержит имени, но как только ты связываешь этот адрес со своей реальной личностью (например, покупая биткоин на бирже, которая требует паспорт), этот псевдоним навсегда привязан к тебе.

Компании вроде Chainalysis, CipherTrace и Elliptic строят графы связей между адресами. Они анализируют потоки транзакций, кластеризуют кошельки, вычисляют биржи и обменники. Если ты хоть раз вывел крипту на биржу с KYC, вся твоя финансовая история в блокчейне становится читаемой для аналитика. Они видят, кому ты переводил, от кого получал, сколько у тебя на балансе и где ты прячешь резервы.

Создатель крупнейшего даркнет-маркета Silk Road думал, что биткоин анонимен. ФБР отследило его транзакции и связало их с его реальной личностью через цифровые отпечатки в ранних постах на форумах. Его приговорили к двум пожизненным срокам без права досрочного освобождения.

«У тебя же сид-фраза в голове. Значит, никто не может отобрать твою крипту». Так думают новички. Профессиона-

лы знают: есть минимум четыре способа конфискации.

Способ 1: Давление на биржу.

Если ты держишь крипту на централизованной бирже (Binance, Coinbase, Bybit), она тебе не принадлежит. Она принадлежит бирже. Так же, как деньги в банке. Биржа обязана соблюдать законы юрисдикции, в которой она зарегистрирована, и юрисдикций, резидентов которых она обслуживает. Если государство присылает ордер на заморозку счета, биржа подчиняется. Твой аккаунт замораживают. Крипта конфискована.

брата украли 120 000 BTC с биржи Bitfinex в 2016 году. В 2022 году ФБР отследило движение средств через блокчейн, нашло биржу, где преступники пытались отмыть крипту, и конфисковало 94 000 BTC. На тот момент это было крупнейшее изъятие в истории. Ключевая ошибка хакеров: они вывели украденное на централизованные биржи.

Способ 2: Компрометация сид-фразы.

Сид-фраза (мнемоническая фраза из 12 или 24 слов) — это мастер-ключ к твоему кошельку. Тот, кто знает сид-фразу, владеет средствами. Если ты хранишь сид-фразу в облаке, в заметках телефона, в зашифрованном файле на компьютере, подключенном к интернету, — она под угрозой. Вредоносное ПО, фишинг, удаленный взлом — и твоя криптоа уходит в неизвестном направлении. Аналитик спецслужбы, получивший доступ к твоему устройству, первым делом ищет сид-фразы.

Способ 3: Атака 5-долларовым гаечным ключом (Rubber - hose cryptanalysis).

Это не шутка. Это термин в криптографии, означает попытку. Самый надежный способ расшифровать данные или получить пароль — это физическое воздействие на владельца пароля. Не нужно взламывать шифр, нужно взломать человека. Если к тебе в дом пришли люди с оружием и требуют перевести крипту или назвать сид-фразу, никакое шифрование тебя не спасет. Спасет только подготовка к такому сценарию.

Способ 4: Юридическое преследование и гражданская конфискация.

Даже если ты хранишь крипту на холодном кошельке и никому не говоришь, суд может обязать тебя передать доступ. Отказ — неуважение к суду, штрафы, арест активов, тюремное заключение. В США и Европе гражданская конфискация (civil forfeiture) позволяет изымать активы без обвинительного приговора, если есть подозрение в их связи с преступной деятельностью.

Как защитить крипту: оперативные протоколы

1. Холодное хранение (Cold Storage).

Аппаратный кошелек (Ledger, Trezor, Coldcard) не подключен к интернету. Злоумышленник не может украсть твою крипту удаленно. Он должен физически завладеть устройством и PIN-кодом.

2. Мультиподпись (Multisig).

Кошелек требует несколько подписей для транзакции. Например, 2 из 3. Один ключ у тебя в доме, второй — у доверенного лица в другой стране, третий — в банковской ячейке. Компрометация одного ключа не дает доступа к средствам.

3. Разделение сид - фразы (Shamir's Secret Sharing).

Ты можешь разделить сид-фразу на несколько частей, которые по отдельности бесполезны. Три части. Хранятся в трех разных местах. Чтобы восстановить доступ, нужно собрать две из трех. Даже если одну часть найдут, это белый шум.

4. Сид-фраза в голове (Brain Wallet).

Ты заучиваешь сид-фразу наизусть. Никаких бумажек. Никаких файлов. Только твоя память. Это защищает от обыска, но создает риск: удар по голове, травма, стресс — и ты можешь забыть или, наоборот, под пытками ты её выдашь.

5. Ложный кошелек (Decoy Wallet).

Ты держишь на виду «жертвенный» кошелек с небольшой суммой. Если на тебя давят физически или юридически, ты отдаешь доступ к ложному кошельку. Основные средства хранятся в другом месте, о существовании которого не знает никто. Легенда: «Это всё, что у меня есть».

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.