

Евгения Толкунова



ВСЯ ПРАВДА
о крипте в России:
от биткоина до цифрового рубля

Вся правда о крипте в России: от биткоина до цифрового рубля

**Честный гид по деньгам, законам
и свободе в новой реальности**

Евгения Толкунова

2026 г.

Содержание

Предисловие	6
Часть 1. Юридический лабиринт — как законы делают крипто легальной и нелегальной одновременно	
Глава 1. ФЗ-259 и «цифровые финансовые активы» (ЦФА)	9
• Что такое ЦФА простыми словами — это крипто или нет?	
• Почему биткоин в России не запрещён, но и не разрешён	
• Реестр операторов ЦФА: кто уже получил лицензию	
Глава 2. Закон о майнинге — что разрешено и что будет дальше	16
• Регистрация майнеров и лимиты потребления	
• Закон о майнинге	
• Регионы с полным запретом майнинга	
• Налог на майнинг: как считать и платить, чтобы не пришли с обыском	
• Что грозит тем, кто работает «в серую»	
Глава 3. 115-ФЗ и банки — почему вам блокируют карты за 5000 рублей	24
• Алгоритм работы «антиотмывочных» систем банков	
• Что такое «красная метка» и как её снять	
• Реальные кейсы: как люди теряли счета за перевод на Bybit	
• Почему P2P-обмен стал «котлом» с высокорисковым трафиком	
• Как защититься: практические рекомендации	
• Что делать, если блокировка уже произошла	
Глава 4. Уголовная ответственность: от мошенничества до госизмены	36
• Статья 159 УК (крипто-пирамиды и фейковые обменники)	
• Статья 174 (легализация) — когда обмен USDT на наличные становится статьёй	
• Статья 284.2 УК РФ: самый страшный нюанс — помощь подсанкционным лицам	
• Новые уголовные статьи на горизонте	
• Как не оказаться фигурантом уголовного дела	
Часть 2. Чёрная, серая и белая ликвидность — как на самом деле работают деньги	
Глава 5. P2P-обменники: главный риск для обычного человека	44
• Схема «безопасная сделка» — почему она опасна	
• Как мошенники подставляют вас через «дропперов»	
• Топ-5 сигналов, что вам перевели деньги с карты убитого или наркообщака	
• Безопасная стратегия работы с P2P	
Глава 6. Обменники, Telegram-боты и криптоматы	50
• Кто стоит за лучшими курсами (спойлер: ОПГ)	

<ul style="list-style-type: none"> • Реальный кейс задержания организатора криптообменника • Как работают инкассации крипты в Москве и регионах • Что ждет рынок нелегальных обменников 	
Глава 7. «Чёрные брокеры» и фейковые биржи	59
<ul style="list-style-type: none"> • Технология подмены сайтов бинанса • Почему вывод денег с поддельной биржи невозможен • Психология жертвы: как вас разводят на 100% депозита 	
Часть 3. Безопасность и анонимность — что реально работает в РФ	
Глава 8. Криптокошельки без KYC: последние убежища	67
<ul style="list-style-type: none"> • Два мира: кастодиальные vs некастодиальные кошельки • Почему VPN и Tor не скроют вас от ФНС • Как блокчейн-аналитика вычисляет ваши паспортные данные • Практические стратегии для разных сценариев 	
Глава 9. Миксеры и XMR — работают или нет после блокировок?	76
<ul style="list-style-type: none"> • Разгром миксера Bitcoin Fog и последствия для России • Monero (XMR) — действительно ли он не отслеживается? • Российские сервисы очистки крипты: миф или реальность 	
Глава 10. Аппаратные кошельки и конфискация	85
<ul style="list-style-type: none"> • Могут ли изъять Ledger или Trezor: правовая реальность 2026 года • Как хранить сид-фразу так, чтобы её не нашли • Техника «душа крипты» — что делать, если вас взяли 	
Часть 4. Экономика — крипта как спасение или ловушка?	
Глава 11. Инфляция, вклады и биткоин	91
<ul style="list-style-type: none"> • Биткоин и рубль: американские горки с российской спецификой • Банковские вклады: доходность тает на глазах • Майнинг: битва за рентабельность • Сколько россиян реально заработали на крипте 	
Глава 12. Цифровой рубль — самый страшный для крипты конкурент?	95
<ul style="list-style-type: none"> • Чем цифровой рубль отличается от биткоина (технически и юридически) • Programmable money: зачем ЦБ вводит «окрашенные» деньги • Прогноз: исчезнет ли P2P после полного внедрения цифрового рубля 	
Глава 13. Санкции, SWIFT и стейблкоины	99
<ul style="list-style-type: none"> • Почему USDT стал для России фактически второй валютой • Риски заморозки USDT: ваш кошелек может стать тыквой • Альтернативы для обычного пользователя 	
Часть 5. Стратегии выживания и процветания	
Глава 14. Как легально завести крипту в Россию	103
<ul style="list-style-type: none"> • Работа через операторов ЦФА (пошаговая инструкция) • Экспериментальный налоговый режим для майнеров • Покупка крипты у юрлиц на СПб Бирже 	
Глава 15. Как вывести крипту в рубли без потерь и блокировок	108

• Использование малых сумм (до 600 тысяч рублей в месяц), чтобы не привлекать внимания банков	
• Схема через самозанятость и договоры с физлицами	
• Полностью легальный выход через Уведомление в ФНС	
Глава 16. Чек-лист «Нулевой риск»	116
• Проверка контрагента по базе ФНС и сервисам блокчейн-разведки	
• Правило «трех кошельков»: архитектура безопасности	
• Если банк всё-таки заблокировал счет: алгоритм действий	
Часть 6. Жизненные ситуации: крипта в наследстве, разводе и бизнесе	
Глава 17. Крипта и наследство — как не похоронить свои монеты вместе с собой	125
• Цифра, которая должна вас напугать	
• Почему обычное завещание не работает для крипты	
• Решение: система «цифрового завещания» для крипты	
• Что делать, если близкий умер, а вы не знаете пароль от его кошелька	
• Чего делать категорически нельзя	
• Чек-лист «Криптонаследство за 30 минут»	
Глава 18. Крипта и развод — как делятся криптоактивы при разделе имущества	129
• Главный принцип: крипта — это имущество	
• Что считается совместно нажитым, а что — личным	
• Как суды узнают о существовании криптокошелька	
• Что требует бывшая супруга (бывший супруг)	
• Стратегии защиты (законные)	
• Реальный кейс из практики	
• Чек-лист «Крипта и развод: что сделать прямо сейчас»	
Глава 19. Бизнес на крипте в РФ + НОВОЕ: Законопроект о цифровой валюте (апрель 2026)	134
• Рынок на пороге больших перемен	
• Главный запрет: расплачиваться криптовалютой нельзя	
• Что можно: условия для инвесторов и бизнеса	
• Исключение для внешнеэкономической деятельности (ВЭД)	
• Лицензирование криптобизнеса	
• Стартапы и инновации — где есть возможности	
• Налогообложение криптобизнеса	
• Риски и ответственность для бизнеса	
• Пошаговая инструкция: как легально запустить криптобизнес в 2026 году	
• Чек-лист «Бизнес на крипте — что сделать прямо сейчас»	
Глава 20. Чек-лист для начинающего «Купил первую крипту — что делать, чтобы не попасть»	140
• До покупки (или сразу после)	

• Кошелёк и безопасность (сразу после покупки)	
• Налоги и ФНС (до первой продажи)	
• Продажа и вывод в рублей	
• Долгосрочное хранение и безопасность	
• Чрезвычайные ситуации	
• Итоговый чек-лист на одной странице	
Глава 21. Реальные судебные дела	148
• Мошенничество (ст. 159 УК РФ) — самый частый состав	
• Легализация (отмывание) криптовалюты (ст. 174 и 174.1 УК РФ)	
• Дела о вымогательстве криптовалюты	
• Жертвы — пенсионеры: самые уязвимые цели мошенников	
• Дело о хищении через «инвестиционный проект»	
• Верховный Суд РФ о криптовалюте в уголовных делах	
• Общие выводы по судебной практике	
Заключение	157
• Три главных вывода из книги	
• Что будет дальше? Прогноз на 2026–2028 годы	
• Что останется неизменным?	
• Последний совет автора	
Приложения:	
• Приложение 1. Образец договора купли-продажи криптовалюты	159
• Приложение 2. Форма заявления в банк о разблокировке счёта	161
• Приложение 3. Гайд по восстановлению доступа к кошельку без сид-фразы	163
• Приложение 4. Лимиты и риски (сводная таблица)	165
• Приложение 5. Регионы с запретом майнинга (по состоянию на апрель 2026 года)	166
• Приложение 6. Полезные информационные ресурсы	167
Глоссарий	168

© Евгения Толкунова, 2026. Электронная версия.

Бесплатное распространение в некоммерческих, образовательных и информационных целях приветствуется.

Предисловие

Перед вами книга, которая могла бы спасти вас от потери денег, блокировки счетов или даже уголовного дела.

Звучит громко? Возможно. Но за каждым абзацем этой книги — реальные судебные решения, интервью с пострадавшими и анализ тысяч страниц юридических документов.

Почему эта книга появилась на свет?

В 2024-2025 годах в России произошло то, чего многие не заметили: криптовалюта перестала быть «диким западом». Появились законы о майнинге, начала работать система «Прозрачный блокчейн», а суды один за другим стали выносить приговоры по криптоделам.

При этом в интернете — море устаревшей, противоречивой или откровенно вредной информации. Одни блогеры кричат «крипту запретили, всё пропало», другие — «заработай миллион за месяц, пока не поздно». Правда, как обычно, посередине.

Почему эта книга нужна именно сейчас?

Три года назад книга в такой тональности была бы немыслима. В 2026 году криптовалюта в России — это не «финансовая пирамида, которую вот-вот прикроют» и не «запрещенная секта айтишников». Это полноценная, хотя и очень нервная, часть экономической реальности. Биткоин обновляет исторические максимумы, стейблкоинами рассчитываются за параллельный импорт, а Центральный банк запустил цифровой рубль, который настойчиво пытаются привить населению.

Мы живем в уникальном моменте двойственности. С одной стороны, принят закон о майнинге, введены «драконовские» штрафы за его нарушение (апрель 2026-го это закрепил окончательно), и любой неучтенный ASIC может обернуться уголовным делом с конфискацией. С другой стороны, именно крипто стала тем финансовым шлюзом, который позволяет обычным людям и бизнесу выживать под санкциями, получать оплату из-за рубежа и защищать свои сбережения от инфляции.

Проблема в том, что большинство информации, которую вы можете найти, — это либо сухие, непонятные пересказы законов, либо реклама

сомнительных «гарантированных доходов» от блогеров. Между ними пропасть. В этой пропасти теряются реальные знания:

- Как не сесть в тюрьму на ровном месте, просто обналичив деньги через P2P?
- Почему выигрыш в суде по крипте почти ничего не значит без правильно составленного документа?
- Как пользоваться Monero, чтобы твои финансы оставались только твоими, и не нарушить при этом закон?

Я написала эту книгу как честный гид. Здесь нет советов в духе «купи этот токен, и будет счастье». Здесь нет агитации за то, чтобы скрываться от государства в лесном бункере. Но здесь есть правда о том, как работает система. Система, в которой ФНС и МВД научились читать блокчейн не хуже хакеров, а банкиры смотрят на каждое твое крипто-поступление как на потенциальное отмывание.

Мы с вами разберем юридический лабиринт, чтобы вы понимали, где заканчиваются ваши права и начинаются риски. Мы нырнем в черный и белый рынки ликвидности, чтобы вы видели разницу между легальным обменником и скам-ботом. Мы построим стратегию безопасного входа в крипту, выхода в рубли и грамотного хранения активов. И, конечно, разберем самые жизненные ситуации: наследство, развод, региональные запреты на майнинг и новый законопроект о цифровой валюте.

Новости апреля 2026 года оставили многих в растерянности — штрафы за майнинг выросли до масштабов, сопоставимых с ущербом от экономических преступлений, а закон о цифровой валюте угрожает полностью перекроить рынок. Я включила в книгу и эти свежие вводные.

Это не энциклопедия. Это карта минного поля. Изучив ее, вы не перестанете рисковать, но перестанете делать это вслепую.

Кому нужна эта книга?

- Новичку, который купил первую крипту и боится, что за ним придут
- Инвестору, который держит биткоины годами и хочет понять, как их не потерять в разводе или при наследстве
- Предпринимателю, который хочет принимать крипту легально (или понять, почему нельзя)
- Юристу, который ищет актуальную судебную практику
- Любому человеку, кто получил перевод в USDT и не знает, что делать дальше

Чего вы НЕ найдёте в этой книге?

- Советов «как обойти закон» (я пишу о том, как не идти против закона)
- Обещаний «разбогатеть на крипте за месяц» (это к блогерам)
- Технического описания блокчейна (этого добра и так полно)

Что вы найдёте?

- Честный разбор законов, которые реально работают
- Пошаговые инструкции на все случаи жизни
- Реальные приговоры и судебные решения (с номерами дел)
- Чек-листы, которые можно распечатать и повесить на стену

Как читать эту книгу?

Если вы новичок — начните с Главы 20 (Чек-лист для начинающего). Если готовитесь к суду или разводу — сразу к Главам 17, 18, 21. Если вы бизнесмен — Глава 19 ваш главный ориентир.

Но лучше — прочитайте всё по порядку. Потому что правда о крипте в России не укладывается в один чек-лист.

Последнее предупреждение (юридическое):

Я не являюсь адвокатом или налоговым консультантом. Эта книга — обобщение публичных источников, судебной практики и авторского анализа. Законы меняются, трактовки различаются. Перед любым важным действием (особенно если на кону крупные суммы или свобода) — проконсультируйтесь с практикующим юристом.

Автор не несёт ответственности за убытки, возникшие в результате использования материалов книги. Вы действуете на свой страх и риск.

С этим предупреждением — приятного и полезного чтения.

Часть 1. Юридический лабиринт — как законы делают крипту легальной и нелегальной одновременно

Глава 1. ФЗ-259 и «цифровые финансовые активы» (ЦФА)

Любое путешествие в мир легальной криптовалюты в России начинается здесь — с Федерального закона №259-ФЗ, который полностью называется «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Его приняли 31 июля 2020 года, а заработал он с 1 января 2021-го. Для обычного человека это звучит как заумная бюрократия, но именно этот документ — тот самый нулевой километр, с которого начинается дорога биткоина в России.

Давайте разберем его так, чтобы стало понятно даже тем, кто впервые слышит слово «блокчейн».

Что такое ЦФА простыми словами — это крипта или нет?

Представьте, что вы купили облигацию, дающую право на долю в компании. Это ценная бумага — физический или электронный документ. А теперь представьте, что ту же самую облигацию оцифровали, превратили в запись в системе на основе блокчейна. Вы держите в своем цифровом кошельке уже не бумагу, а токен, который подтверждает ровно те же права. Вот это, по сути, и есть цифровой финансовый актив (ЦФА).

Закон говорит о ЦФА так: это «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества». Звучит сложно, но суть проста: ЦФА — это токенизированные аналоги классических финансовых инструментов. С их помощью можно превратить в цифровой токен и долговую расписку, и право на акцию, и денежное требование. Некоторые эксперты сравнивают их с цифровым аналогом облигаций или акций, но записанных не в бумажном реестре, а в распределенном реестре — той самой технологии, что лежит в основе блокчейна.

Главное, что нужно понять: **ЦФА — это НЕ биткоин и НЕ криптовалюта** в привычном нам смысле. ЦФА — это регулируемый, поднадзорный государству инструмент. У каждого ЦФА есть эмитент — лицо, которое его выпустило и которое несет обязательства перед держателем. Выпускать их могут только операторы информационных систем, получившие лицензию

Центрального банка. В этом их коренное отличие от децентрализованной криптовалюты, где никакого эмитента и обязанного лица нет в принципе.

Более того, в 2025 году появилось понятие «долговых ЦФА» — это активы, включающие исключительно денежные требования в размере цены приобретения и сумм периодических выплат. Иными словами, это классическая долговая расписка, обернутая в блокчейн-токен.

С 1 января 2026 года правила игры для инвесторов в ЦФА изменились. Банк России утвердил классификацию ЦФА по уровню риска и установил лимиты. Теперь физические лица без статуса квалифицированного инвестора могут приобретать ЦФА только в пределах 600 тысяч рублей в год на одном операторе информационной системы или операторе обмена ЦФА. Для «квалов» (квалифицированных инвесторов) ограничений нет — они вправе без лимитов приобретать любые ЦФА.

Если у вас нет статуса квалифицированного инвестора, вам недоступны сложные ЦФА — те, что удостоверяют права на ценные бумаги для «квалов», содержат денежные требования без определенного срока исполнения или предполагают выплаты, зависящие от неопределенных обстоятельств.

Запутались? Сейчас все встанет на свои места.

Почему биткоин в России не запрещён, но и не разрешён

А вот тут начинается самое интересное — та самая «серая зона», о которой мы будем говорить на протяжении всей книги. Тот же самый закон 259-ФЗ вводит второе, совершенно отдельное понятие — **цифровая валюта**. И под это определение попадает именно биткоин, Ethereum, USDT, Monero и все остальные классические криптовалюты.

Закон определяет цифровую валюту как «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных». Проще говоря: нет центрального эмитента — перед вами цифровая валюта. Есть эмитент — перед вами ЦФА.

Здесь кроется ключевой парадокс российской крипто-реальности. Закон признает биткоин имуществом, но запрещает им расплачиваться на территории России. Это прямо записано в статье 14 закона 259-ФЗ. В апреле

2026 года Госдума приняла в первом чтении новый масштабный законопроект №1194918-8, который ужесточает этот запрет: нельзя принимать криптовалюту в оплату не только товаров, работ и услуг, но и ценных бумаг, цифровых прав, информации и интеллектуальной собственности.

Этот парадокс порождает ту самую двойственность, которую мы будем наблюдать во всех остальных главах книги:

- Вы **можете владеть** биткоином, это ваше законное имущество, и суд обязан защищать ваши права на него от хищения.
- Вы **обязаны платить** налог с дохода, полученного при его продаже.
- Но вы **не имеете права** расплатиться им в магазине, салоне красоты или при покупке недвижимости внутри страны.
- **Исключение сделано только для внешнеэкономической деятельности (ВЭД)**: расчеты криптовалютой по договорам между резидентами и нерезидентами разрешены.

Таким образом, криптовалюта в России — это имущество, которое нельзя использовать как средство платежа внутри страны, но можно покупать, продавать, инвестировать, майнить (с ограничениями) и использовать во внешней торговле. РБК отмечает, что на начало 2026 года «С одной стороны, совершать операции с криптовалютой в стране не запрещено, с другой — не урегулирована деятельность криптообменников и бирж, отсутствует правовой статус у стейблкоинов и ряда других криптовалютных активов, а также не до конца проработано налогообложение».

Если закон примут, с 1 июля 2026 года россияне и компании смогут легально приобретать криптовалюту через лицензированных посредников — обменники, брокеры и доверительные управляющие. При этом биржевые торги допустят только криптовалюты с капитализацией свыше 5 трлн рублей — к ним относятся Bitcoin, Ethereum и, возможно, еще несколько монет. Неквалифицированные инвесторы смогут покупать криптовалюты по результатам тестирования и в пределах годового лимита в 300 тысяч рублей. Кроме того, новый законопроект вводит обязательные цифровые депозитарии — специальные организации, которые будут «учитывать и хранить цифровые активы по аналогии с банковскими кастодиальными сервисами». Криптообменники смогут работать только при наличии лицензии ЦБ, а для неквалифицированных инвесторов торги будут идти исключительно через брокеров.

Важный момент: несмотря на то, что закон всё ещё находится в стадии рассмотрения, он демонстрирует вектор движения государства — от «серой зоны» к жёстко регулируемому рынку.

Реестр операторов ЦФА: кто уже получил лицензию

Если с криптовалютами всё пока находится на стадии законопроектов, то рынок ЦФА уже работает в полную силу. С 2022 года Банк России формирует реестр операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов. По состоянию на апрель 2026 года в реестре — 20 участников.

Последней компанией, получившей лицензию, стал Банк Уралсиб — он был включен в реестр 16 апреля 2026 года, прервав четырехмесячную паузу в расширении списка.

Актуальный состав реестра на апрель 2026 года выглядит так:

- **8 банков:** Сбербанк, Альфа-Банк, Т-Банк, Еврофинанс Моснарбанк, Газпромбанк, ВТБ, ПСБ (Токеон), Банк Уралсиб.
- **3 представителя бирж и брокеров:** СПБ Биржа, БКС Холдинг, Национальный расчетный депозитарий (НРД).
- **9 прочих компаний:** ООО «Атомайз» (дочка Интерроса), ООО «Лайтхаус», ООО «Системы распределенного реестра» (Мастерчейн), ООО «Токеник» (ВТБ Капитал Трейдинг), АО «МРЦ» (Межрегиональный регистраторский центр), ООО «Блокчейн Хаб» (дочка МТС), ООО «Компания БКС», АО «СТАТУС», Мадригал ОИС, Банк Синара.

Кстати, этот список не статичен — он периодически пополняется новыми участниками, а актуальную версию всегда можно найти на официальном сайте Банка России.

Главное из Главы 1

ФЗ-259 разделил цифровые активы на две большие группы:

- **ЦФА** — токенизированные акции, облигации и права требования. У них есть эмитент, они поднадзорны ЦБ, выпускаются на лицензированных платформах, для «неквалов» действует лимит 600 тысяч рублей в год. С точки зрения закона это полностью «белые», регулируемые инструменты.

- **Цифровая валюта** — биткоин, эфир, USDT и прочие децентрализованные монеты. Эмитента нет, владеть можно, платить налог нужно, но расплачиваться в магазинах — нельзя. Исключение — расчеты по внешнеторговым контрактам.

К лету 2026 года мы ожидаем полноценного запуска регулируемого крипторынка с лицензированными посредниками и цифровыми депозитариями. Но до того момента мы продолжаем жить в парадоксальной реальности, где крипто вроде бы и имущество, но вроде бы и «серая зона».

Использованные в главе источники:

- 1) Федеральный закон от 31 июля 2020 г. N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изменениями и дополнениями) <https://base.garant.ru/74451466/>
- 2) Цифровые финансовые активы, цифровая валюта https://www.consultant.ru/document/cons_doc_LAW_514313/68dec6476354961b2241ad9c9f6fe793abdcf685/
- 3) ЦФА как инструмент финансирования бизнеса <https://obplaw.ru/2025/10/tsfa-kak-instrument-finansirovaniya-biznesa/>
- 4) О цифровых финансовых активах и цифровой валюте https://achinskij-r04.gosweb.gosuslugi.ru/o-munitsipalnom-obrazovanii/naselennye-punkty/prichulymskiy-selsovet/informatsiya/prokuratura-informiruet/novosti_395.html
- 5) Статус долговых ЦФА будет закреплён на уровне закона <https://www.aksakov.ru/ru/publications/9522-status-dolgovykh-tsfa-budet-zakreplen-na-urovne-zakona>
- 6) Прокурор разъясняет https://epp.genproc.gov.ru/ru/gprf/web/proc_27/activity/legal-education/explain/e251412/
- 7) Как ЦБ РФ контролирует оборот цифровых активов? https://www.vedomosti.ru/press_releases/2025/10/10/kak-tsb-rf-kontroliruet-oborot-tsifrovih-aktivov
- 8) Цифровые финансовые активы в международных расчетах <https://companies.rbc.ru/amp/news/313d91b9-249d-46b5-8af1-e712d4760349/>
- 9) Установлены правила выпуска, учета и обращения цифровых финансовых активов https://epp.genproc.gov.ru/ru/proc_53/activity/legal-education/explain/e532473/
- 10) Цифровые финансовые активы в России: полное руководство https://www.tbank.ru/invest/social/profile/Investing_Glossary/b8599277-b52f-49b3-89bd-d18487887fec/?author=profile
- 11) Госдума приняла в 1-м чтении законопроект, признающий цифровую валюту имуществом <https://news.rambler.ru/politics/56337557-gosduma-prinyala-v-1-m-chtenii-zakonoproekt-priznayuschiy-tsifrovuyu-valyutu-imuschestvom/>
- 12) Госдума приняла в первом чтении законопроект об обращении криптовалют <https://www.bfm.ru/news/604421>
- 13) Что будет с регулированием рынка криптовалют в России в 2026 году https://www.rbc.ru/crypto/news/694e62239a7947ba7117a8b3?utm_source=amp_crypto_full-link
- 14) Россия блокирует режим криптовалютных платежей с 1 июля, чтобы обойти санкции <https://finance.yahoo.com/markets/crypto/articles/russia-locks-july-1-crypto-115919933.html>
- 15) ЦБ подготовил концепцию по регулированию криптовалют на российском рынке <https://regnum.ru/news/4009101>
- 16) Криптовалюту выводят из расчетов <https://www.kommersant.ru/doc/7922813>
- 17) ЦБ подготовил концепцию по регулированию криптовалют в России <https://expert.ru/news/tsb-podgotovil-kontseptsiyu-po-regulirovaniyu-kriptovalyut-v-rossii/>
- 18) ЦБ возьмёт под контроль оборот криптовалют в России <https://plusworld.ru/articles/71021/>
- 19) Государственная дума России приняла законопроект о криптовалютах в первом чтении, взяв на себя ведущую роль в регулировании таких активов, как биткойн <https://www.gate.com/zh/news/detail/russias-state-duma-has-passed-a-crypto-bill-on-first-reading-with-the-20496959>

- 20) В России введут регулирование криптовалют. Как оно изменит рынок <https://www.rbc.ru/crypto/news/68e7a6c79a794746e7b57eb2>
- 21) Реестр операторов ЦФА расширился до 20 участников <https://ru.beincrypto.com/reestr-operatorov-czfa-20/>
- 22) Уралсиб получил право выпускать цифровые финансовые активы <https://ptzgovorit.ru/news/uralsib-poluchil-pravo-vypuskat-cifrovye-finansovye-aktivy?erid=2SDnjcJzka>
- 23) ЦБ включил Газпромбанк в реестр операторов ЦФА-платформ <https://myseldon.com/ru/news/index/335567390?requestId=71801578-0484-4e3a-9d3e-43267f1d37cd>
- 24) Российские операторы информационных систем ЦФА, кто они и как выбрать площадку для размещения <https://gidmark.ru/stati/platformyi-czfa-v-rossii-kak-sravnivat-i-vyibirat>
- 25) Банк Уралсиб получил возможность выпускать цифровые финансовые активы <https://www.dk.ru/news/237240563?erid=2W5zFGGwAqX>
- 26) Раскрытие информации о платформе ЦФА <https://mrz.ru/company/raskrytie-informatsii-o-platforme-tsfa/>
- 27) Кто может стать оператором информационных систем для выпуска ЦФА в России? https://ya.ru/neurum/c/tehnologii/q/kto_mozhet_stat_operatorom_informacionnyh_sistem_fb6e259e
- 28) Законопроект о регулировании цифровых валют прошел первое чтение <http://www.finmarket.ru/news/6605086>
- 29) Кто управляет цифровыми деньгами: операторы информационных систем в рамках 259-ФЗ https://vitvet.com/articles/cifrovye_dengi/#connectWaysPopUp
- 30) Операторы ЦФА: правовой статус и требования Банка России <https://brace-lf.com/informaciya/finansovoe-pravo/operatorov-tsfa>
- 31) Новые правила доступа инвесторов к цифровым финансовым активам (ЦФА) <https://www.pgplaw.ru/analytics-and-brochures/alerts/novye-pravila-dostupa-investorov-k-tsifrovym-finansovym-aktivam/>
- 32) Новые правила доступа инвесторов к цифровым финансовым активам (ЦФА) <https://www.pgplaw.com/analytics-and-brochures/alerts/novye-pravila-dostupa-investorov-k-tsifrovym-finansovym-aktivam/>
- 33) Таблица: «Анализ изменений законодательства по юридическим лицам» <https://www.v2b.ru/articles/tablitza-analiz-izmeneniy-zakonodatelstva-po-uridicheskim-litsam/>
- 34) Регулирование цифровой валюты и цифровых прав: масштабные изменения в 2026 году <https://www.klerk.ru/blogs/klerk365/687622/>
- 35) Федеральная налоговая служба продлит срок действия единого формата электронного заказа <https://www.akm.ru/eng/press/the-federal-tax-service-will-extend-the-validity-period-of-a-single-electronic-order-format/>
- 36) Законопроекты о цифровой валюте и цифровых правах приняты Госдумой в первом чтении <https://www.audit-it.ru/news/finance/1132344.html>
- 37) Цифровая валюта в России – где бизнесу нельзя ошибиться <https://nulevoybalans.ru/novosti/tsifrovaya-valyuta-v-rossii-gde-biznesu-nelzya-oshibitsya.html>
- 38) Закон о криптовалюте в России 2026: новые правила для бизнеса <https://nomium.ru/zakon-o-kriptovalyute-v-rossii/>
- 39) Условия перехода к налоговому контролю для предприятий были смягчены <https://www.akm.ru/eng/press/the-conditions-for-the-transition-to-tax-monitoring-have-been-relaxed-for-businesses/>
- 40) Законопроекты о цифровой валюте и цифровых правах приняты Госдумой в первом чтении <https://promia.ru/2026/04/21/zakonoproekty-o-cifrovoi-valute-i-cifrovyyh-pravah-priniaty-gosdymoi-v-pervom-chtenii/>
- 41) ЦБ РФ включил «Газпромбанк» в реестр операторов ЦФА-платформ <http://www.finmarket.ru/news/6481701>
- 42) Операторы по выпуску цифровых активов начали интегрироваться с банками <https://www.vedomosti.ru/finance/articles/2024/06/25/1045918-operatori-po-vipusku-tsifrovih-aktivov-nachali-integririvatsya-s-bankami>
- 43) «Т-инвестиции» анонсировали появление ЦФА до конца 2024 года <https://www.vedomosti.ru/investments/news/2024/10/22/1070207-anonsirovali-poyavlenie-tsfa-do-kontsa-goda>
- 44) ЦБ получит онлайн-доступ к информации о сделках, эмитентах и покупателях ЦФА <https://x-compliance.ru/publications/podft/tsb-poluchit-onlain-dostup-k-informatsii-o-sdelkah-emitentah-i-pokupatelyah-tsfa>
- 45) Мосбиржа получила «мягкое согласие» всех отечественных платформ по выпуску ЦФА на интеграцию с ней как оператором обмена для создания вторичного рынка ЦФА <https://www.tbank.ru/invest/social/profile/СТРЕИОК/2b5e94c2-01a2-456e-a334-cd1700c274f9/?author=profile>

- 46) Российский рынок ЦФА. Итоги, тренды и бизнес-кейсы
https://plusworld.ru/articles/58124/?sphrase_id=250028
- 47) «Токены имеют право на существование»: как в России развивается рынок ЦФА
<https://ko.ru/articles/tokeny-imeyut-pravo-na-sushchestvovanie-kak-v-rossii-razvivaetsya-rynok-tsfa/>
- 48) Цифровым активам пора определиться <https://monocle.ru/expert/2023/16/tsifrovym-aktivam-pora-opredelitsya/>
- 49) СПБ Биржа вошла в перечень операторов по выпуску ЦФА <https://ib-bank.ru/bisjournal/news/19055>
- 50) Дорожную карту развития рынка ЦФА Банк России опубликует в ближайшее время
<http://www.finmarket.ru/currency/news/5919637>

Глава 2. Закон о майнинге — что разрешено и что будет дальше

До недавнего времени майнинг в России был своего рода «призраком»: все знали, что он существует, но с точки зрения закона его как будто и не было. Огромные фермы потребляли мегаватты электричества, но не платили с этого дохода ни копейки налогов, потому что не существовало даже юридического определения, что же это за деятельность.

Эта эпоха «серого рая» официально завершилась. С 1 ноября 2024 года в России начал действовать Федеральный закон № 221-ФЗ, который впервые не просто признал майнинг видом деятельности, но и создал для него полноценную правовую и налоговую базу. В этой главе мы детально разберем, как теперь устроен легальный майнинг, кого и как будут контролировать и, что немаловажно, какие суммы и в какие сроки нужно платить государству.

Регистрация майнеров и лимиты потребления

Закон, вступивший в силу 1 ноября 2024 года, развел всех, кто хочет добывать криптовалюту, по трем разным правовым руслам. Главный критерий, по которому вас будет оценивать государство, — это масштаб деятельности, и измеряется он не в добытых биткоинах, а в киловатт-часах потребленного электричества. Федеральная налоговая служба (ФНС) ведет два реестра: реестр майнеров и реестр операторов майнинговой инфраструктуры.

Первая категория: «домашние» майнеры (физические лица без ИП)

Закон разрешает обычным гражданам, не регистрируясь в качестве предпринимателей, заниматься майнингом, но с жестким ограничением по электричеству. Правительство РФ своим постановлением установило лимит в **6000 киловатт-часов в месяц**. Это ключевая цифра, которую нужно запомнить. Если ваше оборудование укладывается в этот лимит, вы можете никуда не заявлять о себе и не вставать на учет.

Чтобы было понятнее, переведем эти цифры в реальные показатели. Предположим, у вас есть два производительных ASIC-майнера, каждый из которых потребляет по 3,8 кВт. Если они работают круглосуточно в течение месяца (30 дней), то их суммарное потребление составит около 5472 кВт·ч. В этом случае вы как раз находитесь в безопасной зоне и имеете право не

регистрироваться. Однако добавление еще даже одного маломощного устройства почти наверняка приведет к превышению, и вот тут-то и начинается зона ответственности.

В налоговой декларации физические лица-майнеры должны отразить как доход, полученный в результате майнинга цифровой валюты, так и доход, полученный от ее продажи. Срок подачи декларации — не позднее 30 апреля года, следующего за отчетным.

Вторая категория: промышленные майнеры (ИП и юрлица)

Любой, чья деятельность выходит за лимит в 6000 кВт·ч или кто изначально планирует вести бизнес, обязан зарегистрироваться как индивидуальный предприниматель (ИП) или юридическое лицо. Однако одного ИП недостаточно — с 1 ноября 2024 года вы должны быть включены в специальный реестр ФНС.

Требование о включении в реестр не формальность. Без этого любое превышение лимита, даже на несколько киловатт-часов, делает вашу деятельность незаконной со всеми вытекающими последствиями. Кроме того, для ИП и ООО установлены особые требования по отчетности. Они обязаны ежемесячно сообщать в ФНС об объеме добытой криптовалюты и адресах-идентификаторах кошельков.

Третья категория: кому майнинг запрещен в принципе

В законе есть прямой перечень лиц, которым запрещено заниматься майнингом даже при соблюдении лимитов. К ним относятся: лица с неснятой или непогашенной судимостью за экономические преступления, преступления против госвласти, а также за умышленные преступления средней тяжести, тяжкие и особо тяжкие. Кроме того, нельзя совмещать майнинг с деятельностью по передаче электроэнергии или оперативно-диспетчерскому управлению в электроэнергетике.

Закон о майнинге 2024: ключевые нормы и ограничения

Федеральный закон № 221-ФЗ был подписан Президентом 8 августа 2024 года и вступил в силу 19 августа 2024 года, за исключением статей 2 и 3, которые начали действовать с 1 ноября 2024 года. Именно с 1 ноября заработали реестры майнеров и операторов майнинговой инфраструктуры.

Принятый закон впервые на законодательном уровне закрепил понятия «майнинг цифровой валюты» и «майнинг-пул», установил требования к оператору майнинговой инфраструктуры, а также определил порядок обращения в России цифровой валюты. Кроме того, закон запретил рекламу криптовалют и их предложение неограниченному кругу лиц.

Отдельно закон прописал полномочия Правительства и Банка России в сфере майнинга, а также обязал Росфинмониторинг вести перечень адресов-идентификаторов, в отношении которых есть основания полагать, что операции осуществляются в целях отмыwania преступных доходов или финансирования терроризма.

Операторы майнинговой инфраструктуры — отдельная категория. Это компании, которые предоставляют майнерам помещения, оборудование, электричество. Им тоже необходимо войти в реестр, и на них распространяются те же требования по отчетности. По состоянию на начало 2025 года в реестр майнеров было включено более 500 компаний и ИП, а в реестр операторов майнинговой инфраструктуры — около 100 операторов.

Регионы с запретом майнинга (по состоянию на апрель 2026 года)

Правительство РФ получило право вводить полный или частичный запрет на майнинг в отдельных регионах. Это сделано для того, чтобы не допустить дефицита электроэнергии в энергодефицитных районах.

Постановлением Правительства № 1869 от 23 декабря 2024 года был установлен перечень регионов, где майнинг запрещен с 1 января 2025 года по 15 марта 2031 года. В него вошли **10 субъектов Российской Федерации**: Республика Дагестан, Республика Ингушетия, Кабардино-Балкарская Республика, Карачаево-Черкесская Республика, Республика Северная Осетия — Алания, Чеченская Республика, Донецкая Народная Республика, Луганская Народная Республика, Запорожская область и Херсонская область.

Кроме того, в Республике Бурятия и Забайкальском крае действовали сезонные ограничения на осенне-зимний период. Однако с 1 апреля 2026 года в этих двух регионах сезонный запрет был заменен на круглогодичный — также до 15 марта 2031 года.

Что это означает на практике? Если ваше оборудование физически находится в любом из перечисленных регионов, вы не имеете права майнить ни в каком виде — ни как физическое лицо в пределах лимита, ни как ИП из реестра. Любая такая деятельность будет считаться незаконной.

С апреля 2026 года в КоАП РФ появилась статья 15.50, которая вводит отдельные штрафы именно за майнинг в запрещенных регионах: для граждан — от 100 до 150 тысяч рублей с конфискацией оборудования; для должностных лиц — от 300 до 800 тысяч рублей; для организаций — от 1 до 2 миллионов рублей с конфискацией оборудования либо приостановкой деятельности на срок до 90 суток.

Налог на майнинг: как считать и платить, чтобы не пришли с обыском

С 1 января 2025 года вступил в силу Федеральный закон № 418-ФЗ, который внес в Налоговый кодекс РФ масштабные поправки, касающиеся налогообложения операций с цифровой валютой. Ключевых изменений несколько.

Криптовалюта признана имуществом для целей налогообложения. Это закреплено в статье 282.3 НК РФ. Доход в виде цифровой валюты, полученной в результате майнинга, признается доходом в натуральной форме — так же, как если бы вы получили товар вместо денег.

Момент признания дохода. Налог возникает не тогда, когда вы продали добытую криптовалюту за рубли, а тогда, когда она **зачислилась на ваш кошелек**. Именно на эту дату вы обязаны зафиксировать ее рыночную стоимость в рублях и включить в налоговую базу.

Важный нюанс уточнен в новом налоговом законопроекте, внесенном Правительством в Госдуму в апреле 2026 года: **доходом от майнинга считается рыночная стоимость криптовалюты на дату её получения**. Никаких «бумажных» оценок или заниженных курсов — ФНС будет брать данные с бирж с дневным оборотом свыше 100 млрд рублей и конвертировать в рубли по курсу ЦБ на тот же день. Это означает, что больше нельзя «оптимизировать» налог, ссылаясь на котировки малоизвестных площадок.

Как определить рыночную стоимость. Стоимость криптовалюты определяется по данным биржи с дневным оборотом свыше 100 млрд рублей и конвертируется в рубли по курсу ЦБ на дату получения. Это исключает возможность манипуляций с «бумажной» ценой.

Ставки налога для разных категорий майнеров:

- Физические лица платят НДФЛ по прогрессивной шкале от 13% до 22%, в зависимости от совокупного годового дохода.
- Индивидуальные предприниматели на общей системе налогообложения и юридические лица платят налог на прибыль по ставке 25%.
- Специальные налоговые режимы (УСН, патент, НПД) для майнинга не применяются, за исключением операций по продаже добытой криптовалюты, где можно использовать УСН «Доходы» (6%) или «Доходы минус расходы» (15%).

Расходы, которые можно учесть. При расчете налоговой базы физические лица могут уменьшить доход на документально подтвержденные расходы, понесенные в процессе майнинга. Это ключевой момент — все квитанции за электроэнергию, договоры аренды, документы на оборудование (с учетом амортизации) и тому подобное.

Рассмотрим **пример расчета** для физического лица на НДФЛ. Допустим, за месяц ваш ASIC добыл криптовалюту, стоимость которой на день зачисления на кошелек составила 200 тысяч рублей. Затраты на электричество, аренду и амортизацию оборудования за этот месяц составили 70 тысяч рублей. Налоговая база: $200\ 000 - 70\ 000 = 130\ 000$ рублей. Сумма налога (при ставке 13%): $130\ 000 \times 0,13 = 16\ 900$ рублей.

Для юридического лица на ОСН при тех же цифрах (прибыль 600 тысяч рублей, затраты 400 тысяч рублей, прибыль 200 тысяч рублей) налог на прибыль по ставке 25% составит 50 тысяч рублей.

Сроки уплаты и декларирования. Если вы продали криптовалюту в 2025 году, декларацию по форме 3-НДФЛ необходимо представить не позднее 30 апреля 2026 года.

Как ФНС контролирует майнинг на практике. Данные поступают по нескольким каналам одновременно: реестр и отчетность (объем добычи и адреса кошельков), данные энергосбыта о фактическом потреблении, банковский комплаенс при выводах и блокчейн-аналитика, которая связывает транзакции в сети с известными адресами и отчетами.

Что грозит тем, кто работает «в серую»

Государство настроено серьезно. В апреле 2026 года Госдума приняла в первом чтении пакет поправок в Кодекс об административных правонарушениях, который вводит многоуровневую систему штрафов.

Три эшелона административных санкций:

- **Майнинг без реестра или с превышением лимита:**
 - для граждан — 100-150 тысяч рублей с конфискацией оборудования;
 - для должностных лиц — 200-300 тысяч рублей;
 - для ИП — 300-400 тысяч рублей;
 - для организаций — 400-500 тысяч рублей.
- **Майнинг в запрещенном регионе:**
 - для граждан — 100-150 тысяч рублей с конфискацией;
 - для должностных лиц — 300-800 тысяч рублей;
 - для организаций — 1-2 млн рублей с конфискацией оборудования либо приостановкой деятельности до 90 суток.
- **Непредоставление сведений в ФНС о добытой валюте и адресе-идентификаторе:**
 - для граждан — 100-200 тысяч рублей;
 - для должностных лиц — 200-300 тыс. руб. или дисквалификация на 1-2 года;
 - для ИП — 300-400 тысяч рублей;
 - для юрлиц — 400-500 тысяч рублей или приостановление деятельности до 90 суток.

При повторных нарушениях штрафы возрастают до **5-10 млн рублей** для юрлиц, с конфискацией оборудования.

Уголовная ответственность по статье 171.6 УК РФ наступает при крупном ущербе или доходе от 3,5 млн рублей. Санкция — вплоть до 5 лет лишения свободы с конфискацией имущества.

Вывод из Главы 2

Майнинг в России образца 2026 года — это полностью легальный и прозрачный для налоговых органов бизнес. Правила просты и понятны:

- Хотите майнить для себя — укладывайтесь в лимит 6000 кВт·ч в месяц и ежегодно подавайте декларацию 3-НДФЛ.

- Переходите в промышленный масштаб — регистрируйте ИП или юрлицо, вносите себя в реестр ФНС и подавайте ежемесячные сведения о добыче.
- Не лезьте в запрещенные регионы — там штрафуют, конфискуют и при повторных нарушениях могут возбудить уголовное дело.
- Считайте налог с даты зачисления монет на кошелек и сохраняйте все документы, подтверждающие расходы на электроэнергию и оборудование.

Использованные в главе источники:

- 1) Федеральный закон от 08.08.2024 N 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» <https://base.garant.ru/409492967/>
- 2) Прокурор разъясняет https://epp.genproc.gov.ru/ru/gprf/web/proc_22/activity/legal-education/explain/e206538/
- 3) Обзор изменений Федерального закона от 31.07.2020 N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_420647/1a582777bf875ba54a6ad6ae03ecab4a5002b6bd/
- 4) Новое в регулировании цифровых активов https://www.birchlegal.ru/legal_alerts/1897/
- 5) Опубликован закон о майнинге и запрете рекламы криптовалют https://zavolzhsnij-r73.gosweb.gosuslugi.ru/deyatelnost/prokuratura-razyasnyet/novosti_1476.html
- 6) Можно ли в РФ заниматься добычей криптовалюты? https://pashkovskij-r38.gosweb.gosuslugi.ru/dlya-zhiteley/novosti-i-reportazhi/novosti_195.html
- 7) Росфинмониторинг <https://www.fedsfm.ru/releases/7971>
- 8) Урегулированы вопросы майнинга цифровой валюты в Российской Федерации <https://www.fedsfm.ru/special/releases/7971>
- 9) Законотворческие новеллы в регулировании майнинга и трансграничного оборота цифровых активов <https://civilrecht.usue.ru/sobytiya/1205-zakonotvorcheskie-novelly-v-regulirovanii-majninga-i-transgranichnogo-oborota-tsifrovyykh-aktivov/>
- 10) Как ФНС контролирует майнинг в 2025 году: реестр, лимиты, налоги <https://companies.rbc.ru/news/0osaHpT2NC/kak-fns-kontroliruet-majning-v-2025-godu-reestr-limityi-nalogi/>
- 11) Нюансы налогообложения доходов от цифровых активов <https://kontur.ru/articles/4246>
- 12) Как ФНС контролирует майнинг в 2025 году: реестр, лимиты, налоги <https://myseldon.com/ru/news/index/334614077>
- 13) Не позднее 30 апреля физические лица – майнеры должны представить декларации о полученном доходе <https://nalogkodeks.ru/%d0%bd%d0%b5-%d0%bf%d0%be%d0%b7%d0%b4%d0%bd%d0%b5%d0%b5-30-%d0%b0%d0%bf%d1%80%d0%b5%d0%bb%d1%8f-%d1%84%d0%b8%d0%b7%d0%b8%d1%87%d0%b5%d1%81%d0%ba%d0%b8%d0%b5-%d0%bb%d0%b8%d1%86%d0%b0-%d0%bc/>
- 14) Что изменится для майнеров и крипторынка в 2025 <https://companies.rbc.ru/news/lcitVCIYLW/chto-izmenitsya-dlya-majnerov-i-kriptorynka-v-2025/>
- 15) Вступил в силу приказ о передаче данных о майнинге в ФНС <https://plusworld.ru/articles/66224/>
- 16) Виталий Колесников рассказал о легализации майнинга криптовалют https://nalogypro.ru/news?news_id=937
- 17) Более 1000 майнеров и операторов майнинговой инфраструктуры уже легализовали свою деятельность https://www.akm.ru/press/bolee_1000_majnerov_i_operatorov_majningovoy_infrastruktury_uzhe_legalizovali_svoyu_deyatelnost/
- 18) Как работать майнерам цифровой валюты <https://ab-express.ru/news/kak-rabotat-majneram-tsifrovoy-valyuty/>
- 19) Более 1 тыс. майнеров и операторов инфраструктуры легализовали свою деятельность <http://lensk.gosnadzor.ru/news/67/15814/>
- 20) Запрет на майнинг криптовалют снимут в Бурятии и Забайкалье <https://news.rambler.ru/community/56115080-zapret-na-majning-kriptovalyut-snimut-v-buryatii-i-zabaykale/>
- 21) В двух российских регионах снова разрешили добычу криптовалют <https://news.ru/amp/regions/v-dvuh-rossijskih-regionah-snova-razreshili-dobychu-kripty>

- 22) Майнинг возвращается: в Бурятии и Забайкалье снимают сезонные ограничения <https://ulan.mk.ru/economics/2026/03/01/mayning-vozvrashhaetsya-v-buryatii-i-zabaykale-snimayut-sezonnye-ogranicheniya.html>
- 23) Пятилетний бан: в двух регионах России запретили майнинг <https://www.mk.ru/economics/2026/04/01/pyatiletniy-ban-v-dvukh-regionakh-rossii-zapretili-mayning.html>
- 24) В отдельных районах Бурятии и Забайкалья с апреля запретили майнинг криптовалют <https://www.interfax.ru/russia/1079148>
- 25) В Бурятии вновь разрешат майнинг криптовалюты <https://www.infpol.ru/277537-v-buryatii-vnov-razreshat-mayning-kriptovalyuty-/>
- 26) Продлен запрет на майнинг криптовалюты в ряде регионов России <https://ab-express.ru/news/prodlen-zapret-na-majning-kriptovalyuty-v-ryade-regionov-rossii/>
- 27) Майнерам гасят свет <https://expert.ru/amp/promishlennost/mayneram-gasyat-svet/>
- 28) Запрет майнинга криптовалют возобновлен в двух регионах РФ <https://www.vesti.ru/article/4781605>
- 29) Как платить налоги за майнинг и криптовалюту в 2025 году <http://taxpravo.ru/analitika/statya-484625-kak-platit-nalogi-za-mayning-i-kriptovalyutu-v-2025-godu>
- 30) Налогообложение майнинга криптовалюты в России: что изменилось <https://companies.rbc.ru/amp/news/d194fbd1-9622-441b-9c49-29b4041958a5/>
- 31) Майнинг криптовалюты: гайд по уплате налогов для предпринимателей <https://www.garant.ru/article/1778051/>
- 32) Информация ФНС РФ от 07.04.2025 <https://normativ.kontur.ru/document?moduleId=1&documentId=492666>
- 33) Налоги на майнинг с 2025 года: кто и сколько должен платить <https://buh.ru/articles/nalogi-na-mayning-s-2025-goda-kto-i-skolko-dolzhen-platit-.html>
- 34) Налог на майнинг криптовалют с 2025 года: кто должен платить https://www.nalog.gov.ru/rn25/ifns/r25_03/info/16544345/print/
- 35) Как платить налоги за майнинг и криптовалюту в России в 2025 году <https://companies.rbc.ru/news/j7Kq2G0y3z/kak-platit-nalogi-za-majning-i-kriptovalyutu-v-rossii-v-2025-godu/>
- 36) Эксперт. Каким будет регулирование цифровой валюты <https://news.tpprf.ru/ru/media/6274833/>
- 37) Налогообложение: публикации с тегом «полномочия налоговых органов» <https://buh.ru/digest/nalogooblozhenie/tag-polnomochiya-nalogovykh-organov/page7/>
- 38) Госдума в I чтении одобрила проект о штрафах за незаконный майнинг <https://www.kommersant.ru/doc/8589024>
- 39) Госдума одобрила проект о штрафах за незаконный майнинг <https://expert.ru/news/gosduma-odobrila-proekt-o-shtrafakh-za-nezakonnyy-mayning/>
- 40) Законопроект об административных штрафах за нарушение законодательства о майнинге цифровой валюты принят в первом чтении <https://imag.one/news/zakonoproekt-ob-administrativnyh-shtrafah-za/14372969>
- 41) Улов не оправдался. До 2 млн рублей штрафа грозит за майнинг криптовалюты https://finance.mail.ru/article/do-2-mln-rublej-shtrafa-grozit-za-majning-kriptovalyuty-69205421/?utm_partner_id=452
- 42) Госдума одобрила законопроект о штрафах за нелегальный майнинг <https://bits.media/gosduma-odobrila-zakonoproekt-o-nakazanii-za-nelegalnyy-mayning/>
- 43) Кнут и пряник для майнеров: как будут наказывать за нелегальную генерацию криптовалюты https://profile.ru/finance/knut-i-pryanik-dlya-majnerov-kak-budut-nakazyvat-za-nelegalnuju-generaciju-kriptovaljuty-1847671/?utm_from=must-amp
- 44) Депутаты предложили штрафы за нарушение запретов в сфере майнинга <https://atlant-pravo.ru/news/detail.php?ID=35648>
- 45) Обзор законопроектов <https://www.consultant.ru/law/review/lawmaking/zw2026-04-17.html>
- 46) Штрафы, конфискация и тюрьма - как изменится жизнь майнеров в 2026 году <https://smart-smi.ru/single/2938775?evt=center>
- 47) За нелегальный майнинг хотят ввести крупные штрафы <https://www.pnp.ru/social/za-nelegalnyy-mayning-khotyat-vvesti-krupnye-shtrafy.html>

Глава 3. 115-ФЗ и банки — почему вам блокируют карты за 5000 рублей

Представьте: вы только что успешно продали криптовалюту. Покупатель перевел вам на карту 5000 рублей. Вы проверяете баланс в мобильном приложении — деньги пришли. Через минуту экран гаснет, а на почту падает письмо: «Обслуживание вашего счета приостановлено. Просим предоставить документы, подтверждающие происхождение денежных средств». Знакомая ситуация? Для тысяч держателей криптовалют в России это не гипотетический сценарий, а суровая реальность 2025-2026 годов.

В предыдущей главе мы разобрали, как закон о майнинге регулирует «рождение» криптовалюты. Но мало просто добыть или купить цифровой актив — рано или поздно большинству из нас нужно превратить его в обычные деньги, которыми можно расплатиться в магазине. И вот здесь на сцену выходит главный барьер между миром крипты и миром рублей: банковская система, вооруженная Федеральным законом №115-ФЗ.

Если ФЗ-259 и закон о майнинге — это правила игры, которые более-менее понятны и предсказуемы, то 115-ФЗ — это скорее «минное поле». Здесь добросовестный пользователь криптовалюты и участник мошеннической схемы выглядят для банковского робота почти одинаково. И робот, как мы увидим, почти всегда предпочитает сначала заблокировать, а уже потом разбираться.

В этой главе мы детально разберем, как работают антиотмывочные системы банков изнутри, что такое «красная метка» и как не оказаться в черном списке, из которого почти невозможно выбраться, а главное — посмотрим на реальные истории людей, которые уже прошли через этот ад.

Закон 115-ФЗ: что это и почему он касается вас

Полное название закона звучит так: Федеральный закон №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Принятый еще в 2001 году, в контексте криптовалют этот закон обрел поистине второе дыхание. Его цель — не допустить попадания «грязных» денег в легальную экономику. Под действие закона попадают банки, платежные системы и операторы обмена цифровых валют.

Криптовалюта с её анонимностью и скоростью трансграничных переводов находится под особо пристальным вниманием Росфинмониторинга и Центрального банка. И хотя прямого запрета на владение криптоактивами для физических лиц в России нет, конвертация цифровых активов в рубли рассматривается банками как высокорисковая операция. Связка «115-ФЗ + криптовалюта» стала триггером для автоматических систем мониторинга: банки обязаны выявлять подозрительные транзакции без очевидной экономической цели.

Ключевая роль регуляторов: ЦБ РФ выпускает методические рекомендации, указывая на типичные схемы использования крипты для отмывания, а Росфинмониторинг ведет базы данных подозрительных адресов и кошельков. Каждый рубль, выведенный из криптомира, сегодня проходит проверку на «чистоту».

Два закона: 115-ФЗ и 161-ФЗ — в чем разница

Российское законодательство предусматривает два принципиально разных инструмента ограничения операций по счетам, и их часто путают даже опытные пользователи. Разница между ними критична.

Первый — 115-ФЗ. Это механизм, при котором банк вправе приостановить обслуживание клиента, если его транзакции соответствуют признакам подозрительной деятельности. Блокировка по 115-ФЗ действует только в конкретном банке. Клиент получает запрос на документы и при наличии убедительных обоснований — разблокировку.

Второй — 161-ФЗ «О национальной платежной системе». Этот механизм значительно жестче и опаснее. Если банк фиксирует признаки мошеннической операции или участия клиента в схеме несанкционированного перевода, он вносит клиента в единый реестр Центрального банка. После этого счета блокируются не в одном банке, а одновременно во всех банках страны, где у клиента открыты карты или счета. Разблокировка формально предусмотрена, но на практике представляет значительную сложность.

С середины 2025 года 161-ФЗ начали применять массово. По данным за первый квартал 2026 года, под действие этих мер попали миллионы счетов и карт. Среди заблокированных — значительная доля добросовестных пользователей, чьи операции внешне соответствовали признакам подозрительных схем. Именно 161-ФЗ стал причиной того, что люди, получившие один-единственный перевод за проданную криптовалюту,

внезапно обнаруживали, что не могут пользоваться ни одной своей картой ни в одном банке.

Алгоритм работы антиотмывочных систем: взгляд изнутри

Многие пользователи ошибочно полагают, что блокировка происходит вручную. «Менеджер увидел перевод и решил заблокировать». Это не так. Решение принимает автоматизированная система, и решение это — мгновенное.

Банковский робот оценивает операции не по их сути — он не понимает, что такое блокчейн или биткоин. Он анализирует исключительно цифровые паттерны поведения. И паттерны типичного P2P-трейдера выглядят для этого робота почти неотличимо от схемы дроппера — подставного лица, участвующего в обналичивании преступных денег.

Как банк видит вашу операцию. Предположим, вы продали USDT на 15 тысяч рублей через P2P-площадку. Покупатель — человек, которого вы никогда не видели, с картой в банке другого региона — переводит вам деньги. Назначение платежа: «Перевод средств». Для банковского алгоритма эта картина выглядит так: на карту клиента, который обычно получает зарплату 60 тысяч рублей в месяц от одного работодателя, внезапно поступает перевод в 15 тысяч рублей от совершенно постороннего человека. Нет ни договора, ни счета, ни очевидной экономической цели. Через неделю — еще один перевод на 23 тысячи рублей от другого незнакомца из другого города. А потом еще и снятие наличных через час после поступления.

Критерии, которые вызывают срабатывание автоматической блокировки:

- **Дробные переводы.** Много мелких поступлений от разных людей в короткий промежуток времени. Особенно «любят» P2P-выводы: много мелких переводов с назначениями «перевод», «возврат долга» или вообще без пояснений.
- **Несоответствие оборота профилю клиента.** Если официальный доход 50 тысяч рублей в месяц, а через карту проходит по 500 тысяч, система фиксирует аномалию.
- **Быстрое обналичивание.** Деньги упали на карту и через три минуты сняты в банкомате — это поведенческий паттерн не инвестора, а обнальщика.
- **Связь с токсичными счетами.** Если кто-то из отправителей ранее был замечен в мошеннических схемах, вся цепочка его транзакций помечается как подозрительная. Ваша карта может быть заблокирована просто

потому, что вам перевел деньги человек, который неделей ранее получил перевод от дроппера.

- **Отсутствие очевидной экономической цели.** Банк не видит контекста сделки: перевод от незнакомого человека выглядит одинаково, будь то обмен крипты или преступная схема.

С 2025 года автоматизированные банковские системы с AI-алгоритмами усилили мониторинг, что кратно увеличило число блокировок. Регуляторы закрутили гайки до предела, и системы противодействия мошенничеству начали работать по принципу «сначала блокируем все подозрительное, а разбираемся потом».

«Красная метка»: как устроен банковский «светофор»

Термин «красная метка» — не официальный юридический, а скорее профессиональный сленг. Но за ним стоит реальный и очень серьезный механизм — платформа Центрального банка «Знай своего клиента», запущенная 1 июля 2022 года. ЦБ присвоил всем юридическим лицам и индивидуальным предпринимателям один из трёх уровней риска проведения подозрительных операций по принципу «светофора»: высокий — красный, средний — жёлтый или низкий — зелёный.

Центробанк определяет уровень риска на основе анализа операций, налоговой нагрузки и другой информации о бизнесе. Банки учитывают эту оценку как дополнительный фактор при формировании собственной оценки клиента.

Что означает каждый уровень:

- **«Зелёные» клиенты** могут рассчитывать беспрепятственно при условии, что у банка отсутствуют подозрения.
- **«Жёлтые» клиенты** находятся в зоне повышенного внимания. Банк вправе отказать в проведении сомнительных операций или запросить документы.
- **«Красные» клиенты** подпадают под самые строгие ограничения: банк прекращает дистанционное обслуживание, ограничивает переводы и использование электронных средств платежа.

Важный нюанс: «красная» метка на платформе ЦБ существует в первую очередь для бизнеса — юрлиц и ИП. Но это не значит, что у физических лиц нет аналога. Для граждан существует **база данных Банка России о несанкционированных переводах**, о которой мы упоминали выше в

контексте 161-ФЗ. Попадание в эту базу — это и есть та самая «красная метка» для обычного человека.

Кроме того, существует база Росфинмониторинга, где аккумулируются любые нарушения, связанные с законом 115-ФЗ. Все банки отправляют туда информацию о сомнительных операциях. А у каждого банка есть еще и внутренний список клиентов, которые вызвали подозрение.

Что происходит после блокировки

Когда робот принимает решение о блокировке, начинается стандартный, но от этого не менее мучительный процесс.

Этап 1. Приостановка операции. Вы пытаетесь перевести деньги или снять наличные — операция отклоняется. На почту или в мобильное приложение приходит сообщение с требованием предоставить пояснения.

Этап 2. Запрос документов. Банк просит объяснить экономический смысл операций по счету. Вы приходите в отделение или отправляете сканы через интернет-банк. Здесь критически важно предоставить максимум подтверждений законности происхождения денег: скриншоты P2P-ордера, переписку с контрагентом, историю транзакций на бирже, выписку по криптокошельку.

Этап 3. Проверка. Банк рассматривает документы. Сроки могут растягиваться на недели и даже месяцы. В это время счет остается заблокированным, вы не имеете доступа к своим деньгам.

Этап 4. Вердикт. Если банк сочтет объяснения убедительными — ограничения снимаются. Если нет — договор банковского обслуживания расторгается в одностороннем порядке. Остаток средств вам выдадут через кассу, но клиентом этого банка вы больше не станете.

Этап 5. Попадание в черный список. Если блокировка была по 161-ФЗ, информация о вас попадает в базу данных ЦБ о несанкционированных переводах. Эта информация автоматически рассылается всем банкам, и после этого вы практически не сможете открыть счет ни в одном банке России. Это и есть состояние «финансовой гражданской смерти», о котором так много говорят криптоэнтузиасты.

Как снять «красную метку»: пошаговый алгоритм

Хорошая новость: «красная метка» не вечна. Но процесс выхода из черного списка требует терпения, документов и методичности. Вот алгоритм действий.

Шаг 1. Получите официальную информацию о причинах. Банк обязан предоставить письменное уведомление с описанием оснований для блокировки. Не удовлетворяйтесь устными объяснениями менеджера — требуйте документ. Без понимания причины невозможно построить защиту.

Шаг 2. Соберите полный пакет документов. Для криптовалютных операций стандартный набор доказательств включает: договор купли-продажи (даже в электронной форме), скриншоты ордера с биржи, переписку с контрагентом, выписку из криптокошелька, банковскую выписку о поступлении средств, налоговую декларацию с отметкой о приеме (если операция уже задекларирована).

Шаг 3. Обратитесь в банк. Предоставьте документы, приложите объяснительную записку с детальным описанием экономического смысла операций. Срок рассмотрения банком — обычно 5-10 рабочих дней.

Шаг 4. Если банк отказал — обратитесь в интернет-приемную Центрального банка. ЦБ рассматривает заявления и при наличии оснований может пересмотреть категорию риска. Срок ответа — до 15 рабочих дней.

Шаг 5. Обратитесь в Межведомственную комиссию при ЦБ РФ. Это следующий уровень обжалования. Комиссия состоит из представителей ЦБ и Росфинмониторинга и уполномочена пересматривать решения о включении в базу подозрительных операций. Срок рассмотрения — до 60 дней.

Шаг 6. В крайнем случае — обращайтесь в суд. Судебная практика по таким делам постепенно формируется в пользу добросовестных клиентов. Например, в феврале 2026 года суд признал незаконной блокировку счетов клиента Сбербанка, которому перевели деньги за проданную криптовалюту, и присудил клиенту проценты, штраф и компенсацию морального вреда.

Важно: в 2025 году около 15 тысяч клиентов, попавших в черные списки, были реабилитированы банками. Это доказывает: механизм восстановления работает, но он требует активных действий с вашей стороны.

Реальные кейсы: как люди теряли счета из-за криптовалюты

Теория важна, но ничто не иллюстрирует масштаб проблемы лучше, чем реальные истории. Вот несколько показательных случаев.

Кейс 1. Житель Екатеринбурга и блокировка в Сбербанке

17 июня 2025 года клиент Сбербанка после P2P-перевода на Bybit обнаружил, что его учетная запись и карты заблокированы. На следующий день он подал обращение о разблокировке, и банк запросил документы для подтверждения легальности операции. Клиент предоставил скриншоты ордера, переписку с контрагентом и данные аккаунта. Однако Сбербанк трижды переносил сроки проверки без запроса дополнительных документов.

Ситуация усугубилась, когда из ответа ЦБ выяснилось, что банк обосновал включение данных клиента в базу о несанкционированных переводах. В результате другие банки тоже ограничили дистанционное обслуживание, включая Т-Банк, где у клиента была основная карта. Человек на протяжении длительного времени оставался без доступа к значительной части своих средств. Чтобы снять деньги в Т-Банке, ему предлагали лететь в Москву.

Этот случай — классическая иллюстрация эффекта домино: блокировка по 161-ФЗ в одном банке мгновенно отключает карты во всех остальных.

Кейс 2. Артём Д. и «треугольник» со Сбербанком

31 марта 2025 года житель России Артём Д. обнаружил, что все его счета в Сбербанке, на которых находилось более 7,5 миллионов рублей, заблокированы. Ни предупреждений, ни объяснений. Карты не работали, снять наличные в отделении было невозможно.

Только на судебном заседании выяснилась причина. Оказалось, что 19 марта на счет Артёма поступил перевод от пенсионерки из Тюменской области, которая позже позвонила в банк и заявила, что стала жертвой мошенников. Сбербанк мгновенно заблокировал счета.

Но была деталь, которую банк в своих доводах умалчивал: Артём получил эти деньги абсолютно законно — как оплату за проданную криптовалюту USDT. Он предоставил скриншоты переписки с покупателем и запись транзакций. Суд признал блокировку незаконной и присудил клиенту проценты, штраф и компенсацию морального вреда.

Это классическая схема «треугольника»: мошенник похищает деньги жертвы, но переводит их не себе, а третьему лицу — криптотрейдеру, который продает USDT. Добросовестный продавец криптовалюты невольно становится последним звеном в цепочке хищения.

Кейс 3. Алексей из Санкт-Петербурга и восемь банков

Житель Санкт-Петербурга Алексей продал криптовалюту через P2P-биржу Bybit. После этого его счета были заблокированы сразу в восьми российских банках, включая Сбербанк, ВТБ, Альфа-банк и Райффайзенбанк. Ситуация для Алексея стала катастрофической: на руках ипотека, кредиты и двое маленьких детей, один из которых тяжело болен. Банки отказывались объяснять причины, лишь ссылаясь на подозрительную активность и попадание в базу Банка России о мошеннических операциях.

В Банке России подтвердили, что ограничение будет действовать до тех пор, пока информация о человеке находится в базе подозрительных операций. Оспорить включение можно через любой банк или интернет-приемную ЦБ, а при отказе — обратиться в суд.

Кейс 4. 500 тысяч рублей, которые испарились

39-летний москвич перевел 500 тысяч рублей в приложении Bybit. В стандартной P2P-схеме Bybit активы продавца блокируются еще на этапе размещения ордера, а после оплаты криптовалюта передается покупателю. Однако в этом случае что-то пошло не так, и деньги оказались потеряны. Это напоминает о том, что риски существуют не только на стороне блокировок, но и на стороне самой P2P-механики.

Кейс 5. Клиент Альфа-банка и два месяца без денег

Клиент Альфа-банка два месяца назад получил блокировку всех счетов и доступа к личному кабинету по 161-ФЗ через неделю после P2P-операции на Bybit. Он перевел контрагенту USDT, а тот через СБП перевел рубли на его счет. Прошло два месяца — счет все еще заблокирован.

Почему P2P-обмен стал «котлом» с высокорисковым трафиком

Ситуация с блокировками в 2025 году обострилась не случайно. Криптообмен превратился в котел, в котором смешались огромные объемы высокорискового трафика. По оценкам экспертов, в этом котле сегодня варятся одновременно: обычные инвесторы и трейдеры, майнеры,

фрилансеры, получающие оплату из-за рубежа в криптовалюте, но также и онлайн-казино, букмекерские конторы, нелицензированные брокеры и теневые P2P-площадки без контроля.

Для банковской системы такая смесь стала слишком взрывоопасной. Под раздачу попали все без разбора: обычные пользователи, инвесторы, майнеры, трейдеры и фрилансеры.

Важно понимать: банки не имеют ничего лично против вас и не стремятся наказать именно держателей крипты. Их задача — защититься от санкций со стороны ЦБ, который штрафует банки за обслуживание сомнительной клиентуры. Поэтому банки предпочитают перебдеть — заблокировать и разбираться.

Как защититься: практические рекомендации

Юридическая реальность такова, что 115-ФЗ превратился в фильтр, через который проходят все крипто-рубли, и избежать внимания банков полностью практически невозможно. Но минимизировать риски и подготовиться к возможной блокировке — вполне реально.

Правило 1. Отдельная карта для крипто-операций. Никогда не используйте зарплатную карту или карту, на которой хранятся основные сбережения, для получения денег от продажи криптовалюты. Заведите отдельную дебетовую карту. Если ее заблокируют — вы не останетесь без средств к существованию.

Правило 2. Документируйте каждую сделку. Скриншот P2P-ордера, переписка с контрагентом, информация об аккаунте покупателя, выписка по криптокошельку — сохраняйте все. В случае блокировки этот пакет документов станет вашим главным аргументом.

Правило 3. Не храните крупные суммы на транзитной карте. Как только деньги от продажи криптовалюты поступили — сразу переводите их на другой счет или снимайте наличными. Минимизируйте сумму, которая может быть заморожена при блокировке.

Правило 4. Не ведитесь на курс значительно выше рыночного. Курс, который отличается от рыночного на 10-15% в лучшую сторону, обычно означает одно: при обмене через вашу карту проведут деньги из подозрительного источника или по сомнительной схеме. Экономия на комиссии может стоить вам всех счетов.

Правило 5. Работайте через проверенные каналы. Выбирайте P2P-мерчантов с тысячами завершенных сделок и высоким процентом успешных операций. Избегайте новичков и предложений с подозрительно хорошим курсом.

Правило 6. Платите налоги. Налоговая декларация — лучшая страховка от обвинения в отмывании. Если вы задекларировали доход от продажи криптовалюты и уплатили НДФЛ, у вас есть железобетонное доказательство законного происхождения денег. Подробно о налоговых аспектах мы поговорим в Части 5.

Что делать, если блокировка уже произошла

- **Не паникуйте.** Это отключает рациональное мышление и мешает действовать эффективно.
- **Немедленно запросите у банка письменное основание блокировки.** Ссылайтесь на ст. 7 115-ФЗ, которая обязывает банк информировать клиента о причинах. Устные объяснения не имеют юридической силы, вам нужен документ.
- **Соберите и предоставьте документы.** Чем быстрее и полнее вы ответите на запрос банка, тем выше шанс на разблокировку без долгих разбирательств.
- **Если блокировка по 161-ФЗ — готовьтесь к худшему.** Подайте заявление на исключение из базы через тот же банк, а параллельно — через интернет-приемную ЦБ. При отказе — Межведомственная комиссия и суд.
- **Ищите юриста.** Специалист по финансовому мониторингу и блокировкам сэкономит вам недели времени и десятки тысяч рублей.

Что еще важно: операция с криптовалютой не равна правонарушению. Постановление Пленума Верховного Суда РФ № 16 от 2021 года прямо разъясняет отсутствие запрета на приобретение гражданами криптовалют и разрешает подобные операции. Вы имеете полное право покупать и продавать цифровые активы. Проблема в том, что банковским алгоритмам это пока что трудно объяснить — и ваша задача состоит в том, чтобы предъявить им неопровержимые бумажные доказательства.

Использованные в главе источники:

1) Почему банки блокируют добросовестных участников P2P
<https://companies.rbc.ru/news/iifdq1iEwE/pochemu-banki-blokiruyut-dobrosovestnyih-uchastnikov-p2p/>

- 2) «Курс +10% к рынку — не подарок, а приманка». Руководитель продуктов BestChange — о блокировках карт и борьбе с «грязным» трафиком <https://forklog.com/exclusive/kurs-10-k-rynku-ne-podarok-a-primanka-rukovoditel-produktov-bestchange-o-blokirovkah-kart-i-borbe-s-gryaznym-trafikom/amp/>
- 3) Криптовалюта в РФ: стратегии защиты от блокировок счетов <https://companies.rbc.ru/news/ACkd788MuE/kriptovalyuta-v-rf-strategii-zaschityi-ot-blokirovok-schetov/>
- 4) Банки блокируют карты за крипту в 2026: моя карта «улетела» после вывода 40 тысяч <https://www.klerk.ru/user/2551474/685216/>
- 5) Что делать при блокировке карты после обмена криптовалюты <https://companies.rbc.ru/amp/news/2e9ad7fd-ebe8-4c72-a347-4dcea783a49e/>
- 6) 115-ФЗ и криптовалюта: почему банки блокируют счета и как это предотвратить <https://pod-ft.ru/baza-znaniy/115-fz-i-kriptovalyuta-pochemu-banki-blokiruyut-scheta-i-kak-eto-predotvratit/>
- 7) Как российские банки отслеживают P2P-платформы и криптовалютные биржи для выявления и устранения финансовых рисков? <https://www.gate.com/zh-tw/post/status/17454327>
- 8) Как безопасно покупать и продавать криптовалюту: правовые риски P2P-сделок и блокировки счетов <https://pravo163.ru/kak-bezopasno-pokupat-i-prodavat-kriptovalyutu-pravovye-riski-p2p%E2%80%91sdelok-i-blokirovki-schetov/>
- 9) Продажа криптовалюты через P2P для покупки автомобиля: почему банк блокирует карту и считает вас «обнальщиком»? <https://krasnoyarsk-news.net/other/2026/01/22/501820.html>
- 10) Банк России обновил рекомендации для компаний и ИП по блокировке счетов <https://www.law.ru/news/43617-bank-rossii-obnovil-rekomendatsii-dlya-kompaniy-i-ip-po-blokirovke-schetov>
- 11) Как «светофор» ЦБ влияет на бизнес: новое в практике 115-ФЗ https://www.sberbank.com/ru/s_m_business/pro_business/svetofor_tsb
- 12) Компании могут «позеленеть» только через запрос в свой банк <https://e.gd.ru/1140837?forceDeviceType=1&forceDeviceType=1>
- 13) Как снять блокировки со счета по «антиотмывочному» закону 115-ФЗ? <https://krd.iusov.ru/kak-snyat-blokirovki-so-scheta-po-antiotmyvochnomu-zakonu-115-fz/>
- 14) Реабилитация из красной зоны риска по 115-ФЗ <https://shupikov.com/115-fz/reabilitatsiya-iz-krasnoj-zony-riska-po-115-fz>
- 15) Как безболезненно выйти из «красной зоны» банковского светофора? <https://rosco.su/press/kak-bezboleznennno-vyyti-iz-krasnoj-zony-bankovskogo-svetofora/>
- 16) Как снизить категорию риска в банке <https://www.4dk.ru/content/art/35858-cplus-kak-snizit-kategoriyu-riska-v-banke-20241119>
- 17) Началась массовая блокировка карт по 115-ФЗ! Как спасти свои деньги от банка <https://www.restate.ru/material/nachalas-massovaya-blokirovka-kart-po-115fz-kak-spasti-svoi-dengi-ot-banka-180855.html>
- 18) Черные списки ЦБ РФ по 115-ФЗ: Как проверить себя и контрагента и выйти из списка в 2025 году <https://shupikov.com/razblokirovka/chernye-spiski-cb-rf-po-115-fz-kak-proverit-i-vyyti-iz-spiska>
- 19) Как снизить риски и оперативно решить проблемы по 115-ФЗ. Инсайд от службы комплаенса коммерческого банка https://e.gazeta-unp.ru/1177550?utm_source=www.gazeta-unp.ru&utm_medium=refer&utm_campaign=placeholder&utm_term=placeholder_docs&utm_content=art_hl
- 20) Продал крипту — поражен в правах <https://www.bfm.ru/news/579815>
- 21) Банки массово блокируют счета россиян после продажи криптовалюты <https://rus.bashgazet.ru/novosti/print:page,1,40206-banki-massovo-blokirujut-scheta-rossijan-posle-prodazhi-kriptoaljutj.html>
- 22) Russians Report Account Freezes at Bybit EU and Revolut <https://forklog.com/en/russians-report-account-freezes-at-bybit-eu-and-revolut/>
- 23) Москвич «потерял» полмиллиона рублей при покупке крипты — но как? <https://www.ossetia.tv/2025/12/03/moskvich-poteryal-polmilliona-rublej-pri-pokupke-kripty-no-kak/>
- 24) Блокировка аккаунта, обращения: №250618-7000-163394, №250724-7000-524622 <https://www.banki.ru/services/questions-answers/question/788967/>
- 25) Как разобраться с блокировкой счета по 161-ФЗ: личный опыт и советы <https://harant.ru/questions/q-108976/>
- 26) Я получил СМС-сообщение от ПАО Сбербанк о том, что операции по моим картам и доступ в СберБанк Онлайн были ограничены в соответствии с Федеральным законом №161-ФЗ <https://pravoved.ru/question/4622001/>
- 27) Заблокировали личный кабинет после перевода <https://www.banki.ru/services/responses/bank/response/12535446/>
- 28) Блокировка по 161-ФЗ: как один перевод на бирже мог привести к ограничению счетов? <https://harant.ru/questions/q-76321/>

- 29) ЦБ обязал банки раскрывать причины блокировки счетов и карт <https://www.bfm.ru/news/582351>
- 30) Реабилитация деловой репутации по 115-ФЗ: шаги и документы <https://odobrili.com/journal/reabilitatsiya-delovoy-reputatsii-po-115-fz-shagi-i-dokumenty/>
- 31) Портал «Финансист» https://finansist-kazan.ru/search/?tags=%D0%A6%D0%91%2C%D0%9F%D0%9E%D0%94%2F%D0%A4%D0%A2%2C%D1%87%D0%B5%D1%80%D0%BD%D1%8B%D0%B9+%D1%81%D0%BF%D0%B8%D1%81%D0%BE%D0%BA&PAGEN_2=8
- 32) ЦБ прорабатывает механизмы исключения добросовестных клиентов из базы мошенников <https://dalekayaokraina.ru/news/ekonomika/tsb-prorabatyvaet-mekhanizmy-isklyucheniya-dobrosovestnykh-klientov-iz-bazy-moshennikov/>
- 33) Что такое «черный» список ЦБ и как удалить себя из него — совет эксперта <https://riamo.ru/news/ekonomika/chto-takoe-chnyj-spisok-tsb-i-kak-udalit-sebja-iz-nego-sovet-eksperta/>
- 34) Новые инициативы и разъяснения в связи с "черным списком" Росфинмониторинга https://rrost.ru/ru/press/review_legal/2307-05082018/page4/
- 35) Клиенты реабилитации не подлежат <https://news.rambler.ru/community/36024794-klienty-reabilitatsii-ne-podlezhat/comments/>
- 36) ARTICLE BY OLGA PLESHANOVA IN ADVOKATSKAYA GAZETA <https://up.infraclex.ru/en/news/op-article-advokatskaya-gazeta-15092025/>
- 37) Сегодня государственной думой приняты поправки в тот самый 115-ФЗ в части ужесточения требований к блокировкам счетов <https://tgstat.ru/channel/@blogbankir/5095>
- 38) ЦБ РФ в 2025 г. реабилитировал 67 финансистов, исключив их из черного списка <https://fomag.ru/news-stream/tsb-rf-v-2025-g-reabilitiroval-67-finansistov-isklyuchiv-ikh-iz-chnogo-spiska/>
- 39) “Операция не выполнена”: как Сбер заплатил за самоуправство, история обычного гражданина против финансового гиганта <https://www.genesis-law.ru/17088/>
- 40) В каких случаях могут заблокировать расчетный счет https://www.consultant.ru/law/podborki/v_kakih_sluchayah_mogut_zablokirovat_raschetnyj_schet/#link-to-assistant
- 41) 115-ФЗ в Газпроме <https://www.banki.ru/services/responses/bank/response/12749774/>
- 42) Риски операций с криптовалютой для физлиц и ИП в России: налоги, банки, законы в 2026 году <https://amp.spark.ru/user/265425/blog/292141/riski-operatsij-s-kriptovalyutoj-dlya-fizlits-i-ip-v-rossii-nalogi-banki-zakoni-v-2026-godu>
- 43) Заблокировали карты и онлайн-банк по 115-ФЗ <https://www.banki.ru/services/responses/bank/response/12284318/>
- 44) После чего я направил повторное заявление в Центробанк, более подробно рассказав о поступившем переводе <https://d0.pravoved.ru/question/4745815/>
- 45) Закон № 115-ФЗ: Реальность российского финансового контроля в 2025 году <https://www.gate.com/zh/post/status/14144242>

Глава 4. Уголовная ответственность: от мошенничества до госизмены

Представьте ситуацию: вы продали USDT через P2P-площадку, а через неделю к вам приходят сотрудники полиции и сообщают, что на вашу карту поступили деньги от жертвы мошенников. Или другая ситуация: вы помогаете другу вывести деньги за границу через криптовалюту, а потом узнаете, что эти операции подпадают под статью об обходе санкций. В обоих случаях вы рискуете не просто блокировкой счёта, но и реальным уголовным сроком.

В предыдущих главах мы разобрали административные риски — блокировки карт, штрафы за незаконный майнинг, запреты в отдельных регионах. Всё это неприятно, но поправимо. Уголовная же ответственность — это та черта, за которой заканчиваются штрафы и начинаются годы заключения с конфискацией имущества.

В этой главе мы разберём три главные статьи Уголовного кодекса, которые прямо касаются любого, кто работает с криптовалютой в России. Статья 159 — за мошенничество. Статья 174 — за легализацию преступных доходов. И статья 284.2 — за помощь в обходе санкций. Мы посмотрим на реальные приговоры, разберём механизмы, по которым возбуждаются дела, и, главное, поймём, как не оказаться фигурантом уголовного дела, даже если вы действовали с чистыми намерениями.

Статья 159 УК РФ: мошенничество с криптовалютой — от пирамид до фейковых обменников

Когда речь заходит об уголовных делах с криптовалютой, статья 159 УК РФ (мошенничество) — самая «популярная». Именно по ней привлекают организаторов пирамид, создателей фальшивых обменников, «чёрных брокеров» и всех, кто обманным путём завладевает чужими крипто-активами.

Что говорит закон. Мошенничество — это хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Биткоин и другие криптовалюты признаются имуществом, а значит, их кража — это такое же преступление, как и кража денег или машины.

Статья 159 УК РФ разделена на несколько частей в зависимости от тяжести:

- **Часть 2 (значительный ущерб)** — до 5 лет лишения свободы;
- **Часть 3 (крупный размер, от 3,5 млн рублей)** — до 6 лет;
- **Часть 4 (особо крупный размер, от 13,5 млн рублей или организованная группа)** — до 10 лет.

Обратите внимание: 1 BTC в апреле 2026 года стоит больше 7 млн рублей. То есть даже кража одного биткоина — это уже крупный размер, который тянет на часть 3. Кража двух-трёх биткоинов — особо крупный размер и перспектива сесть на 10 лет.

Именно такая реальность сегодня стоит за цифрами. С 2025 по апрель 2026 года по всей стране прошла волна громких дел. В Хакасии осуждён к лишению свободы один из организаторов мошеннической схемы по продаже криптовалюты, который в период с 2022 по 2023 годы, используя сеть, обманывал людей при сделках с цифровыми активами. В Ингушетии участковый раскрыл дистанционное мошенничество на 300 тысяч рублей под видом торговли криптовалютой, по факту которого возбуждено дело по ч. 3 ст. 159 УК.

Но особенно показательно свежее дело из Махачкалы. 15 апреля 2026 года Ленинский районный суд признал виновным организатора финансовой пирамиды, которая с 2019 по 2022 год действовала под видом криптопроекта. Участники преступной группы привлекали деньги граждан под обещание сверхвысокого дохода от инвестирования в токен, не имеющий реальной ценности, а выплаты производились исключительно за счёт средств новых вкладчиков. Ущерб от деятельности пирамиды составил более 585 млн рублей. Организатору назначено 4 года колонии общего режима.

Профессиональные мошенники создают видимость инвестиционной деятельности — сайты, личные кабинеты, графики доходности, но все эти цифры не имеют ничего общего с реальной торговлей криптовалютой. Это просто записи в базе данных, созданные для того, чтобы усыпить бдительность жертвы.

Отдельного внимания заслуживает дело, которое прокуратура Иркутской области поставила на контроль в апреле 2026 года. Схема там была иной. Заместитель генерального директора компании в сговоре с неустановленными лицами разместил не менее 100 единиц оборудования для майнинга в производственных помещениях города Шелехова и в частных домах

Шелеховского района. Подключив оборудование к электросетям, он осуществлял безучётное потребление энергии, а там, где платил — использовал льготный тариф для населения. Оплата более чем за 4 млн кВт·ч не производилась. Общий ущерб энергосбытовой компании превысил 40 млн рублей. Дело квалифицировано по ч. 4 ст. 159 УК РФ — мошенничество в особо крупном размере.

Но по статье 159 могут привлечь не только организаторов. «Дроппер» — человек, на карту которого поступают украденные у пенсионеров деньги, — тоже рискует. В апреле 2026 года 22-летняя жительница Забайкальского края, получившая на свой банковский счёт похищенные у челябинской пенсионерки деньги, не смогла оспорить взыскание. Суд установил, что эти деньги поступили на её счёт, а сама она участвовала в сделках на бирже криптовалют, о чём и сообщила в своих показаниях. Это классический пример того, как обычный P2P-трейдер может стать последним звеном в цепочке хищения — и оказаться фигурантом уголовного дела.

Как не стать фигурантом дела по статье 159 УК РФ:

1. Проверяйте контрагентов на P2P-площадках. Используйте только проверенных мерчантов с тысячами завершённых сделок.
2. Избегайте переводов от третьих лиц, чьи данные не совпадают с данными аккаунта на бирже.
3. Всегда фиксируйте доказательства сделки (скриншоты ордеров, переписку, выписки).
4. Если вам предлагают доходность выше рыночной на 5% и более — это почти гарантированно схема с «грязными» деньгами.

Статья 174 УК РФ: когда обмен USDT на наличные превращается в легализацию

Если статья 159 — это про кражу, то статья 174 — про отмывание. И здесь криптовалюта создаёт особые риски, потому что сама технология блокчейна построена на анонимности и необратимости транзакций — ровно тех свойствах, которые так ценят преступники.

Статья 174 УК РФ карает за «совершение финансовых операций и других сделок с денежными средствами или иным имуществом, заведомо приобретёнными другими лицами преступным путём, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом».

Простыми словами: если вы помогли кому-то «очистить» грязные деньги или криптовалюту — вы соучастник легализации.

Статья 174.1 УК РФ — смежная норма, которая применяется, когда человек сам совершил преступление, а потом отмывает полученный доход.

С появлением криптовалют статья 174 претерпела самые масштабные изменения. Как отмечает юрист Олег Ритман, теперь наказание может последовать и за использование криптовалют, полученных преступным путём. Проблема в том, что судебная практика по таким делам ещё не сформировалась до конца, из-за чего возникают сложности при квалификации действий, связанных с криптовалютами.

Реальный пример. В сентябре 2025 года в Москве было возбуждено уголовное дело по ч. 2 ст. 174.1 УК РФ против 23-летнего жителя столицы, который занимался сбытом наркотиков. Он получал оплату на свой криптокошелёк, а затем через интернет-обменник переводил криптовалюту в рубли с зачислением на банковские счета. Общая сумма легализованного дохода превысила 4,5 млн рублей.

Этот кейс важен вот чем: для банка и для правоохранительных органов схема «криптовалюта → обменник → рубли на карте» выглядит одинаково, кто бы её ни использовал — наркодилер или добросовестный держатель биткоина. Именно поэтому банки так нервно реагируют на P2P-переводы, как мы разбирали в Главе 3.

Обмен USDT на наличные может стать составом преступления по статье 174 в нескольких случаях:

- Если вы осознанно принимаете средства от лица, которое получило их преступным путём, и помогаете конвертировать их в рубли.
- Если вы систематически оказываете услуги по обналичиванию криптовалюты без лицензии ЦБ и ваш клиент использует эти операции для сокрытия доходов.
- Если вы участвуете в схемах, где криптовалюта используется как промежуточное звено для разрыва цепочки отслеживания денежных средств.

Наказание по статье 174 УК РФ — до 7 лет лишения свободы со штрафом.

Ключевое правило защиты: всегда фиксируйте источник происхождения криптовалюты. Если вы покупаете биткоин — сохраняйте скриншоты

ордеров и банковские выписки. Если вы продаёте — оформляйте договор и фиксируйте данные контрагента. Уплаченный налог — это ваше лучшее алиби.

Статья 284.2 УК РФ: самый страшный нюанс — помощь подсанкционным лицам

И вот мы подошли к тому, о чём большинство пользователей крипты либо не знают, либо предпочитают не думать. Статья 284.2 УК РФ — одна из самых новых и самых суровых в нашем обзоре.

Статья предусматривает ответственность за оказание содействия подсанкционным лицам или помощь в обходе санкционных ограничений. В контексте криптовалют это означает: если вы перевели криптовалюту лицу, в отношении которого введены санкции, или помогли такому лицу вывести активы, вы подпадаете под действие этой статьи.

Криптоэнтузиасты часто говорят: «Биткоин — это свобода, это деньги вне политики». Но реальность 2025-2026 годов такова: криптовалюта активно используется для обхода международных санкций, и правоохранительные органы научились это отслеживать.

По данным экспертов, криптовалюта превратилась в удобный канал не только для легальных инвестиций, но и для схем, позволяющих обходить санкции, отмывать преступные доходы и скрывать движение капитала.

Что именно считается нарушением по статье 284.2 УК РФ:

- Прямой перевод криптовалюты на кошелёк, аффилированный с подсанкционным лицом или организацией.
- Участие в схемах, направленных на сокрытие принадлежности активов подсанкционному лицу (использование цепочек кошельков, миксеров, Monero).
- Оказание услуг по обмену криптовалюты для подсанкционных лиц или организаций.
- Содействие в выводе активов из-под блокирующих санкций через криптовалютные каналы.

Наказание по статье 284.2 УК РФ — до 10 лет лишения свободы с конфискацией имущества.

Более того, здесь действует принцип экстерриториальной юрисдикции: если в вашей операции есть хоть какой-то элемент, связанный с иностранной валютой, банком, сервером или контрагентом в ЕС или США, вы попадаете под их уголовный кодекс. Незнание не спасает: используется юридический стандарт «должен был знать». Если вы меняете «тёмную» криптовалюту на фиат или переводите средства через подставных лиц, суд может признать вас соучастником, даже если вы не знали деталей источника средств.

С 2025 года криптовалютные операции в России перешли из «серой» зоны в фокус силовых ведомств. Ключевое правило: избегать анонимных P2P-переводов, особенно в сторону юрисдикций с высоким риском, и всегда проверять, не находится ли ваш контрагент в санкционных списках.

Что делать, чтобы не попасть под статью:

- Проверять контрагентов через публичные санкционные списки.
- Не принимать и не отправлять крупные суммы в криптовалюте на адреса, происхождение которых вам неизвестно.
- Отказываться от сделок, если контрагент настойчиво предлагает обойти КУС/AML-процедуры.
- Понимать, что даже «помощь другу» с выводом денег за границу через криптовалюту может обернуться уголовным делом.

Новые уголовные статьи на горизонте

В апреле 2026 года правительственная комиссия по законопроектной деятельности одобрила проект поправок в УК РФ, который вводит **статью 171.7 «Незаконный оборот цифровой валюты»**. Законопроект был внесён в Госдуму и в случае принятия вступит в силу с 1 июля 2027 года.

Согласно проекту, за незаконный оборот цифровой валюты без лицензии ЦБ в крупном размере (ущерб от 3,5 млн рублей) будет грозить до 4 лет лишения свободы. За особо крупный размер (от 13,5 млн рублей) или совершение преступления организованной группой — до 7 лет лишения свободы.

Важный нюанс: Верховный суд РФ дал отрицательный отзыв на этот законопроект, посчитав введение уголовной ответственности преждевременным, пока в законодательстве нет чётких критериев легального и нелегального оборота криптовалюты. Однако сам факт внесения такого законопроекта — сигнал о том, куда движется государство.

Как не оказаться фигурантом уголовного дела

Главное, что нужно понять из этой главы: уголовные дела по криптовалюте — не миф и не редкость. Суды уже научились рассматривать такие дела, а правоохранительные органы — собирать доказательства в блокчейне.

Пять принципов, которые снизят ваши риски:

1. **Прозрачность.** Каждая операция должна быть документально подтверждена. Биржевые отчёты, скриншоты транзакций, договоры с контрагентами — собирайте всё.
2. **Налоги.** Уплаченный налог — это доказательство того, что вы действовали в правовом поле, а не скрывали доходы. Декларация по форме 3-НДФЛ — ваша лучшая защита.
3. **Проверка контрагентов.** Прежде чем совершить сделку, особенно на крупную сумму, убедитесь, что ваш контрагент не находится в санкционных списках и не связан с подозрительными адресами.
4. **Избегайте анонимности там, где она неуместна.** P2P-площадки с непроверенными контрагентами, миксеры, Monero — всё это может быть истолковано как приготовление к преступлению.
5. **Знайте, когда остановиться.** Если вам предлагают «сверхвыгодный» курс или просят не задавать вопросов о происхождении денег — отказывайтесь от сделки. Сиюминутная выгода не стоит лет заключения.

Использованные в главе источники:

- 1) Прокуратура Иркутской области контролирует уголовное дело о мошенничестве на сумму свыше 40 млн рублей https://epp.genproc.gov.ru/ru/proc_38/mass-media/news/regional/e8457459/
- 2) Прокуратура информирует (12+) <https://poisktv.ru/prokuratura-informiruet-12-132/>
- 3) Покупка материалов в валюте https://www.consultant.ru/law/podborki/pokupka_materialov_v_valyute/#link-to-assistant
- 4) Организатор криптовалютной пирамиды из Дагестана получил 4 года колонии <https://www.interfax-russia.ru/index.php/south-and-north-caucasus/news/organizator-kriptovalyutnoy-piramidy-iz-dagestana-poluchil-4-goda-kolonii>
- 5) Дроппер не смогла оспорить взыскание денег в пользу челябинской пенсионерки https://pchela.news/news/detail/50074?utm_source=internal&utm_medium=announce&utm_campaign=lenta&utm_content=50074
- 6) В Ингушетии участковый раскрыл дистанционное мошенничество на 300 тыс. рублей <https://gazetaingush.ru/v-ingushetii-uchastkovyy-raskryl-distancionnoe-moshennichestvo-na-300-tys-rublej>
- 7) В Хакасии осужден к лишению свободы один из организаторов мошеннической схемы по продаже криптовалюты https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/%D1%83%D0%B1%D0%BA/Publikacii_i_vistuplenija/item/68341289/
- 8) Только за прошедшие выходные жители Калининградской области под влиянием обмана перевели мошенникам свыше 9,6 млн рублей https://epp.genproc.gov.ru/ru/proc_39/mass-media/news/main/e8470248/
- 9) Перед судом в Хакасии предстанет один из организаторов мошеннической схемы по продаже криптовалюты https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/%D1%83%D0%B1%D0%BA/Publikacii_i_vistuplenija/item/66453501/?year=2025&month=7&day=7

- 10) В Хакасии вынесен приговор по уголовному делу о мошенничестве при проведении операций с криптовалютой <https://epp.genproc.gov.ru/ru/gprf/mass-media/news/archive/e5867113/>
- 11) На юге столицы обвиняемый в покушении на сбыт наркотиков подозревается в легализации денежных средств, приобретенных преступным путем <https://77.xn--b1aew.xn--p1ai/news/item/69857067/>
- 12) Сотрудниками полиции выявлен факт легализации криминального дохода <https://64.xn--b1aew.xn--p1ai/news/item/65165109/>
- 13) Актуальные вопросы уголовно правовой ответственности в сфере легализации (отмывании) доходов, полученных преступным путем https://epp.genproc.gov.ru/ru/proc_11/activity/legal-education/explain/e6347880/
- 14) Житель Нижнекамска предстанет перед судом за покушение на сбыт наркотиков и легализацию денежных средств https://epp.genproc.gov.ru/ru/proc_16/mass-media/news/archive/e6362733/
- 15) Юрист Ритман рассказал, как появление криптовалюты изменило законодательство <https://postnews.ru/n/49117>
- 16) «Внутренние санкции»: По кому ударит новый закон об обороте криптовалюты в России <https://nsn.fm/economy/no-kriminal-ostaetsya-v-rossii-vvodyat-vnutrennie-sanktsii-na-kriptu>
- 17) Криптовалюта как инструмент обхода санкций: почему «помочь другу» может закончиться тюрьмой <https://fakeoff.org/kriptovalyuty/kriptovalyuta-kak-instrument-obkhoda-sanktsiy-pochemu-pomoch-dругu-mozhet-zakonchitsya-tyurmoy>
- 18) Какие операции с криптовалютой привлекают внимание правоохранительных органов <https://ru.beincrypto.com/kriptovalyuta-pravoohranitelnye-organv/>
- 19) Мне придет штраф или будит уголовная ответственность? <https://d0.pravoved.ru/question/4681396/>
- 20) Куприянов предупредил, что за незаконные операции с криптовалютой грозит штраф <https://www.osnmedia.ru/obshhestvo/kupriyanov-predupredil-cto-za-nezakonnye-operatsii-s-kriptovalyutoi-grozit-shtraf/amp/>
- 21) Как законно работать с криптовалютой в России в 2026 году: разбор действующих норм <https://dtf.ru/grinex/4520735-regulirovanie-kriptovalyuty-v-rossii-v-2026-godu#comments>
- 22) Международный эквайринг vs крипто эквайринг для бизнеса в 2026 <https://habr.com/ru/users/SlavaKulakov/articles/>
- 23) Власти намерены штрафовать россиян за использование криптовалюты уже с 2026 года <https://sotaproject.com/news/100735>
- 24) Новый этап регулирования: что ждет крипторынок в России <https://igtec.ru/news/kriptonovosti/novyy-etap-regulirovaniya-cto-zhdet-kriptorynok-v-rossii/>
- 25) Forbes узнал, какое наказание грозит за торговлю криптовалютой <https://glavny.tv/last-news/russia/dveri-zakryvayutsya-kakoe-nakazanie-grozit-za-torgovlyu-kriptovalyutoy/>
- 26) Кабмин предложил лишать свободы за незаконный оборот цифровой валюты <https://www.kp.ru/online/news/6917014/>
- 27) Вызвать из тени: незаконный оборот криптовалюты добавят в УК <https://iz.ru/2078173/iana-shturma-evgenii-grachev/nezakonnyy-oborot-kriptovalyuty-dobavyat-v-uk>
- 28) До семи лет тюрьмы предложили давать за незаконный оборот криптовалюты <https://www.tks.ru/politics/2026/04/13/0014/print/>
- 29) В ГД внесли законопроект о сроке за незаконный оборот криптовалюты // Новости НТВ <https://www.ntv.ru/novosti/2977526>
- 30) ВС счел преждевременной уголовную ответственность за незаконный оборот криптовалюты <https://www.interfax.ru/russia/1084601>
- 31) В Госдуму внесли проект о наказании за незаконный оборот цифровой валюты <https://www.osnmedia.ru/obshhestvo/v-gosdumu-vnesli-proekt-o-nakazanii-za-nezakonnyj-oborot-tsifrovoi-valyuty/amp/>
- 32) В России предложили привлечь ФСБ к борьбе с нелегальными криптообменниками <https://www.gazeta.ru/social/news/2026/04/13/28254235.shtml>
- 33) За незаконный оборот крипты в России предложили сажать на срок до семи лет <https://meduza.io/amp/news/2026/04/13/za-nezakonnyy-oborot-kripty-v-rossii-predlozhili-sazhat-na-srok-do-semi-let>
- 34) Правительство одобрило идею об ответственности за оборот криптовалюты в России https://mt.gazeta.ru/blog/43100736716/Pravitelstvo-odobrilo-ideyu-ob-otvetstvennosti-za-oborot-kriptov?utm_referrer=mirtesen.ru
- 35) ЦБ предложил ввести уголовную ответственность за криптодеятельность без лицензии <https://iz.ru/2076137/2026-04-09/tcb-predlozhil-vvesti-ugolovnuu-otvetstvennost-za-kriptodeiatelnost-bez-litsenzii#main-content>

Часть 2. Чёрная, серая и белая ликвидность — как на самом деле работают деньги

Глава 5. P2P-обменники: главный риск для обычного человека

Представьте: вы хотите купить или продать криптовалюту — быстро, без посредников и по выгодному курсу. Вы заходите на платформу, находите продавца с тысячами сделок и почти мгновенно получаете свои USDT. Кажется, что может быть проще? Именно эта иллюзия простоты и контроля сделала P2P-обменники главным каналом входа и выхода из криптовалюты для миллионов россиян.

Однако, начиная с 2025 года, мы наблюдаем системный кризис этого рынка. То, что раньше воспринималось как удобный инструмент, превратилось в главную ловушку для добросовестных пользователей. По данным на начало 2026 года, в схемах P2P-обмена оказались задействованы десятки тысяч «дропперов», а банки ответили на это массовыми блокировками счетов. В этой главе мы детально разберем, как именно работают эти ловушки, почему «безопасная сделка» не является безопасной и какие сигналы должны заставить вас немедленно отказаться от операции.

Схема «безопасная сделка» — почему она опасна

Технически P2P-обмен на таких площадках, как Binance, Bybit или Huobi, выглядит следующим образом: вы размещаете ордер на покупку или продажу криптовалюты, система находит контрагента и блокирует его средства на внутреннем счете (эскроу). Покупатель переводит вам фиатные деньги (рубли) на карту, вы подтверждаете получение, после чего криптовалюта «размораживается» и переходит к нему. Считается, что за счет этого механизма сделка защищена.

Но проблема в том, что банк, через который проходит ваш фиатный перевод, не видит этот красивый механизм защиты. Банковский алгоритм видит лишь то, что на вашу карту от неизвестного лица поступает перевод на сумму, например, 50 тысяч рублей, который вы сразу же обналичиваете или переводите. Никаких договоров купли-продажи или подтверждений о блокировке средств на криптобирже у банка нет.

Ключевой парадокс P2P: техническая гарантия сделки, которую вы считаете «безопасной», абсолютно невидима для вашего банка. Для его автоматизи-

рованной системы это просто перевод от незнакомца, который выглядит подозрительно.

Более того, с 1 июля 2026 года любые сделки между гражданами с использованием криптовалют вне лицензированных посредников будут под полным запретом: «серый» P2P полностью уйдет в прошлое, а все операции должны будут проходить исключительно через лицензированные площадки. Это означает, что даже технически исправный механизм P2P-сделки скоро станет юридически ничтожным.

Как мошенники подставляют вас через «дропперов»

Главный риск, который разрушил доверие к P2P-рынку, — это повсеместное использование так называемых **дропперов**. Дроппер — это человек, который за небольшое вознаграждение предоставляет свою банковскую карту или счет для транзита чужих денег. При этом сам дроппер может даже не подозревать об истинном происхождении этих средств, считая себя обычным участником крипто-сделок.

Ключевой механизм, который напрямую угрожает добросовестным трейдерам, — это **схема «Треугольник»**. Это наиболее распространенный и опасный сценарий, при котором мошенник действует одновременно в двух направлениях:

1. Одна группа мошенников обрабатывает «жертву» (например, пенсионера) и выманивает у него деньги.
2. Параллельно другой мошенник размещает на P2P-площадке объявление о продаже криптовалюты, которое выглядит максимально привлекательно.
3. Вы как добросовестный покупатель переводите деньги со своей карты, ожидая получить USDT.
4. Мошенник перенаправляет ваши деньги на счет «дроппера», который затем переводит их основному организатору, а ваша криптовалюта уходит в неизвестном направлении

Когда схема раскрывается, именно ваш счет и ваш IP-адрес оказываются последним звеном в этой цепочке. Для правоохранительных органов вы становитесь не пострадавшим, а потенциальным соучастником, поскольку именно ваш платеж был использован для финансирования преступной цепочки.

Именно из-за этого и появилась уголовная ответственность за дропперство, которая теперь грозит не только организаторам, но и тем, кто добросовестно

пытался обменять криптовалюту. В результате добросовестные трейдеры массово теряют счета: под раздачу попали миллионы карт.

Топ-5 сигналов, что вам перевели деньги с нелегальной карты

Поскольку напрямую проверить происхождение фиатного перевода от P2P-контрагента практически невозможно, жизненно важно научиться распознавать косвенные признаки нелегальных схем. Мы собрали пять ключевых сигналов, заметив которые, вы должны немедленно прекратить операцию.

Сигнал 1. Назначение платежа содержит «зашифрованные» или нестандартные пометки.

Если в графе «Назначение платежа» или в сообщении к переводу вы видите слова «за USDT», «за биткоин», «за крипту», «оплата по сделке №...», это стопроцентный триггер для банковской системы безопасности. Легитимный P2P-мерчант никогда не будет использовать такие пометки, так как они прямо указывают на обход валютного контроля.

Сигнал 2. Несовпадение имен плательщика и аккаунта на P2P-площадке.

Если перевод приходит от человека, имя которого не совпадает с именем, указанным в верифицированном аккаунте криптобиржи, это указывает на использование дропперской (подставной) карты. Мошенники часто используют до 20-30 карт на один аккаунт, и каждое несовпадение многократно повышает риск блокировки.

Сигнал 3. Курс сделки значительно отличается от рыночного.

Если контрагент предлагает вам купить USDT по цене, которая на 5-7% ниже рыночной, или продает их на 5-7% дороже рынка, это практически всегда означает, что он работает с «грязными» деньгами. Легальный обменник или мерчант не может позволить себе такие «щедрые» курсы, так как его маржа редко превышает 1-2%. Слишком хорошее предложение — самый верный признак того, что вам пытаются быстро «загнать» криминальные средства.

Сигнал 4. Контрагент настаивает на немедленном подтверждении сделки.

Если покупатель агрессивно требует от вас подтвердить получение денег и «отпустить» криптовалюту в течение 1-2 минут, не давая времени даже зайти в онлайн-банк, это признак того, что он пытается успеть до того, как банк заблокирует транзакцию. Добросовестный трейдер спокойно ждет проверки. Всегда проверяйте поступление средств именно в интернет-банке, а не по SMS или скриншоту.

Сигнал 5. Продавец просит перейти в сторонний мессенджер или нажать на подозрительную ссылку.

Как только обсуждение сделки переносится в Telegram, WhatsApp или Skype, а от вас просят перейти по ссылке для «проверки AML» или «создания холодного кошелька», немедленно прекращайте общение. Это классический фишинг: после перехода по такой ссылке и подключения вашего кошелька все средства с него будут мгновенно списаны через вредоносные смарт-контракты.

Безопасная стратегия работы с P2P

Мы настоятельно рекомендуем в принципе отказаться от P2P-обмена, особенно в преддверии его полного запрета с 2027 года. Однако, если в данный момент у вас нет альтернативы, соблюдение строгого протокола безопасности жизненно необходимо:

- 1. Работайте только с проверенными контрагентами.** Используйте только тех продавцов и покупателей, у которых верифицированный аккаунт с десятками тысяч завершенных сделок и рейтингом выше 99%. Никогда не связывайтесь с новичками или «однодневками».
- 2. Заведите отдельную карту.** Категорически нельзя использовать для P2P-платежей зарплатную или основную дебетовую карту. Риск ее блокировки слишком высок, и вы останетесь без доступа к основным средствам.
- 3. Фиксируйте все доказательства.** Скриншот объявления продавца, переписка в чате биржи, подтверждение завершения сделки, выписка из банка о поступлении — всё должно быть сохранено. В случае блокировки счета только эти документы помогут вам доказать банку, что вы не являетесь участником преступной схемы.
- 4. Никакой экономии на курсе.** Помните золотое правило: разница в курсе — это плата за ваш риск. Выбирайте не самый дешевый вариант, а самый надежный. Курс на 5% ниже рынка почти гарантированно означает, что вас делают крайним в цепочке отмывания денег.

Рынок P2P деформировался настолько, что даже юристы, специализирующиеся на криптовалютах, открыто заявляют: «P2P как способ входа и выхода из криптовалюты скоро умрет». Если вы хотите сохранить свои деньги и не стать фигурантом уголовного дела, лучше начать подготовку к уходу из этого сегмента уже сейчас. В следующей главе мы разберем альтернативы — как работают онлайн-обменники, Telegram-боты и криптоматы и кто на самом деле стоит за лучшими курсами.

Использованные в главе источники:

- 1) Почему банки блокируют добросовестных участников P2P <https://companies.rbc.ru/news/iifdq1iEwE/pochemu-banki-blokiruyut-dobrosovestnyih-uchastnikov-p2p/>
- 2) Новый закон и будущее криптоопераций в России: к чему готовиться бизнесу <https://www.klerk.ru/user/2672354/688638/>
- 3) P2P-сделки с криптовалютой <https://obplaw.ru/2026/01/p2p-sdelki-s-kriptovalyutoj/>
- 4) Новый закон о крипте от 1 апреля 2026: что изменится для обычных людей уже этим летом <https://www.klerk.ru/user/2551474/687356/>
- 5) Покупка и продажа криптовалюты в 2026 году: ключевые ошибки бизнеса в новых реалиях <https://www.klerk.ru/blogs/exchagent/678522/>
- 6) Кто заберет приватные ключи россиян? Разбор проекта нового криптозакона <https://forklog.com/news/kto-zaberet-privatnye-klyuchi-rossiyan-razbor-proekta-novogo-kriptozakona/amp/>
- 7) Российские криптообменники могут получить правовое регулирование <https://www.tks.ru/politics/2026/01/15/0001/print/>
- 8) Что будет с регулированием рынка криптовалют в России в 2026 году <https://www.htx.com.pk/feed/community/17886967/?back=1>
- 9) Каким будет будущее регулирования криптовалютного рынка в России в 2026 году? <https://www.htx.com/zh-tc/news/Regulation-kIBkDShr/>
- 10) Все о рисках криптовалютных операций на P2P в России <https://companies.rbc.ru/news/yfInMFcGIp/vse-o-riskah-kriptovalyutnyih-operatsij-na-p2p-v-rossii/>
- 11) Как избежать мошенничества в P2P-торговле при общении на сторонних платформах? <https://www.okx.com/ru-eu/help/how-do-i-avoid-scams-from-off-site-communication-in-p2p-transactions>
- 12) Эксперты выявили схему мошенничества при P2P-сделках с криптовалютой <https://fomag.ru/news-streem/eksperty-vyavili-skhemu-moshennichestva-pri-p2p-sdelkakh-s-kriptovalyutoj/>
- 13) Все о рисках криптовалютных операций на P2P в России <https://myseldon.com/ru/news/index/337798439>
- 14) Рекомендации по предотвращению мошенничества и поведения с высоким риском в P2P-торговле <https://support.coinex.com/hc/ru/articles/32750483491609-%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D0%B8%D0%B8-%D0%BF%D0%BE-%D0%BF%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D1%8E-%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%B0-%D0%B8-%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F-%D1%81-%D0%B2%D1%8B%D1%81%D0%BE%D0%BA%D0%B8%D0%BC-%D1%80%D0%B8%D1%81%D0%BA%D0%BE%D0%BC-%D0%B2-P2P-%D1%82%D0%BE%D1%80%D0%B3%D0%BE%D0%B2%D0%BB%D0%B5>
- 15) Как защититься от фишинга на P2P? <https://www.okx.com/ru-eu/help/how-do-i-protect-myself-from-phishing-scams-on-p2p>
- 16) Гниение российского P2P https://forklog.com/exclusive/gnienie-rossijskogo-p2p-chto-sluchilos-s-segmentom-kriptoobmenov/?doing_wp_cron=1719203020.1649570465087890625000&sntzd_campaign=1&utm_campaign=el-salvador-bitcoin-big-tech-middle-east-s-crypto-oasis-crypto-lows-in-hong-kong
- 17) Как Избежать P2P-мошенничества С Криптовалютой <https://www.bybit.com/ru-RU/help-center/article/How-to-Avoid-Crypto-P2P-Scams?category=b6d242f62c21ee2ae3>
- 18) Как P2P превратилось в точку входа для «серых схем» и уголовных рисков <https://companies.rbc.ru/news/mNEIDpD87z/kak-p2p-prevratilos-v-tochku-vhoda-dlya-seryih-shem-i-ugolovnyih-riskov/>
- 19) Осведомленность о мошенничестве на Binance <https://www.binance.com/ru/square/post/28063539761378>
- 20) Почему ты покупаешь дороже, чем продаёшь — и ещё радоваться должен https://www.tbank.ru/invest/social/profile/Victoria_Business/b3fd04dc-087d-4006-bf99-7cbf2c3c49c2/?author=profile
- 21) P2P-обменники превратились в ловушку для россиян: что скрывается за простым интерфейсом <https://myseldon.com/ru/news/index/336122078>
- 22) Мошенники нашли способ обхода закона о дропперах <https://smotrim.ru/article/4834502>
- 23) DLBI: мошенники нашли способ обхода закона о дропперах <https://cisoclub.ru/dlbi-moshenniki-nashli-sposob-obhoda-zakona-o-dropperah/>
- 24) Стало известно, как обманывают россиян при вложениях в криптовалюту <https://www.gazeta.ru/business/news/2025/09/23/26786438.shtml>

- 25) Мошенники с помощью незаконных схем начали обходить закон о дропперах <https://cisoclub.ru/moshenniki-s-pomoshhju-nezakonnyh-shem-nachali-obhodit-zakon-o-dropperah>
- 26) Не поддавайтесь на уловки мошенников! <https://tbilisskoe-sp.ru/about/info/news/15034/?type=pda>
- 27) 115-ФЗ убивает P2P обмен криптовалютой: что делать в 2025 <https://vc.ru/life/2576967-115-fz-i-p2p-obmen-kriptovaljuty>
- 28) Как обменивать криптовалюту без P2P и риска блокировки по 115-ФЗ и 161-ФЗ <https://www.sostav.ru/blogs/286884/79525>
- 29) P2P умер?! Как выводить криптовалюту в 2026 году, чтобы избежать 115-ФЗ и 161-ФЗ <https://habr.com/ru/articles/989158/>
- 30) P2P переводы в 2026 году — риски, блокировки по 115-ФЗ и как безопасно обменивать криптовалюту <https://dtf.ru/ask/5011413-p2p-perevody-riski-blokirovki-i-bezopasnyj-obmen-kriptovaljuty>
- 31) Вывод крипты в 2025 = риск блокировки <https://www.youtube.com/watch?v=wF25Pz-ERk8>
- 32) Запросили документы по 115-ФЗ: полная инструкция что делать в 2026 году <https://vc.ru/life/2624570-dokumenti-po-115-fz-chto-delat-pri-zaprose-v-2025-godu>
- 33) Криптовалюта в РФ: стратегии защиты от блокировок счетов <https://companies.rbc.ru/news/ACkd788MuE/kriptovalyuta-v-rf-strategii-zaschityi-ot-blokirovok-schetov/>
- 34) Банки блокируют карты! Как не попасть под уголовную ... <https://www.youtube.com/watch?v=ixlWWKQcF-k>
- 35) P2P как избежать блокировки карты при торговле <https://advokat-sheriev.ru/blokirovka-p2p-torgovlya.aspx>
- 36) Криптовалюта и 115-ФЗ: почему P2P не нарушает законы Российской Федерации <https://myseldon.com/ru/news/index/337526911>
- 37) Покупка криптовалюты P2P? <https://harant.ru/questions/q-59868/>
- 38) Первый приговор за P2P-торговлю на криптобирже: мнение экспертов <https://pravo.ru/story/245547/>
- 39) «P2P скоро умрет». Что происходит с обменом криптовалют в России <https://lenta.profinansy.ru/news/4417534>
- 40) Обмен криптовалюты на рубли стал рискованнее <https://investfuture.ru/articles/obmen-kriptovalyuty-na-rubli-stal-riskovannee-vedomosti>
- 41) Крипто переводы денег: Как мошенники заставляют вас отправлять монеты (И как их избежать) <https://www.gate.com/ru/post/status/15613130>
- 42) Распространённые схемы мошенничества в P2P-торговле с криптовалютами, которых стоит опасаться <https://www.htx.com/ru-ru/support/25007575911787>
- 43) Почему P2P-мерчанты дробят платежи и как избежать рисков <https://www.bitget.com/ru/amp/news/detail/12560604803278>
- 44) Топ-5 мошенничеств в криптомире <https://sbersova.ru/sections/protection/top-5-moshennichestv-v-kriptomire>
- 45) Как обнаружить и избежать мошенничества в C2C-криптовалютах <https://onekey.so/blog/ru/ecosystem/how-to-detect-and-avoid-c2c-crypto-scams-and-frauds/#%d0%bd%d0%b0-%d1%87%d1%82%d0%be-%d1%81%d1%82%d0%be%d0%b8%d1%82-%d0%be%d0%b1%d1%80%d0%b0%d1%82%d0%b8%d1%82%d1%8c-%d0%b2%d0%bd%d0%b8%d0%bc%d0%b0%d0%bd%d0%b8%d0%b5>
- 46) Блокировка Bybit: Что делать российским трейдерам и куда переходить в 2025 году <https://vc.ru/crypto/2313910-blokirovka-bybit-dlya-rossijan-alternativy-i-sovety>
- 47) Following Binance and OKX, the Bybit exchange has removed all banks affected by sanctions from the P2P section — including Sber, Tinkoff, and Alfa <https://www.binance.com/en-TR/square/post/31224508122337>
- 48) Лучшие криптобиржи для россиян: рейтинг платформ 2025 года <https://ru.beincrypto.com/learn/rejting-kriptobirzh/>
- 49) Рейтинг криптобирж 2026: замена Binance <https://guidecrypto.ru/rejting-kriptobirzh-2026-zamena-binance/#Bybit>
- 50) From Peer-to-Peer to Fraud-to-Fraud <https://forklog.com/en/the-rot-in-russias-p2p-market/?noamp=mobile>
- 51) P2P-платформы в России в 2025 году: как миллионы пользователей покупают биткоин без посредников <https://s119perm.ru/p2p-platformy-v-rossii-v-2025-godu-kak-milliony-polzovatelej-pokupayut-bitkoin-bez-posrednikov/>
- 52) Криптобиржа Binance запретила россиянам P2P-операции в любых валютах, кроме рубля <https://3dnews.ru/1092107/kriptobirga-binance-zapretila-rossijanam-operatsii-cherez-p2pservis-v-lyubih-valyutah-krome-rublya/print>
- 53) Топ криптобирж для пользователей из России: Ваш мост между фиатом и криптой <https://uk.tgstat.com/en/channel/@moneysurff/341>
- 54) No CEX: A guide to alternative crypto-exchange services <https://forklog.com/en/no-cex-a-guide-to-alternative-crypto-exchange-services/>

Глава 6. Обменники, Telegram-боты и криптоматы

Мы уже разобрали P2P-площадки — стихийный рынок, где тысячи незнакомцев меняют крипту на рубли, а банки блокируют их карты. Теперь мы спускаемся на ступень ниже по лестнице риска — в мир, где не действуют ни правила бирж, ни банковский комплаенс, ни, зачастую, Уголовный кодекс. В этой главе мы рассмотрим три главные формы нелегальной и полуправовой ликвидности в России: онлайн-обменники, Telegram-боты и криптоматы.

Эти инструменты — позвоночник теневого рынка криптовалюты в России. Их совокупный оборот, по оценкам экспертов, составляет миллиарды рублей ежемесячно. Именно через них происходит основная масса обналичивания крипты в обход банковского надзора. И именно здесь работает организованная преступность — с колл-центрами, дропперами и сложной логистикой.

Кто стоит за лучшими курсами

Главный парадокс теневого рынка обмена: курс, который выглядит как подарок, почти всегда оказывается приманкой. «Курс, который отличается от рыночного на 10-15% в лучшую сторону, обычно означает одно: при обмене через вашу карту проведут деньги из подозрительного источника или по сомнительной схеме», — объясняет руководитель продуктов BestChange Евгений Алексеев. Разница может выглядеть впечатляюще — в отдельных случаях речь идет о десятках тысяч рублей. Но вопрос в том, чем на самом деле оплачивается такая «выгода». Ответ, как правило, один: уголовным делом.

Рынок обменников в России устроен как слоеный пирог. На верхнем уровне находятся легальные операторы, работающие по лицензии ЦБ или зарегистрированные как операторы обмена ЦФА. Таких — единицы. На среднем уровне — сотни сервисов, зарегистрированных в офшорах (Эстония, Гонконг, Дубай, Сейшелы), которые формально не нарушают российские законы, но работают с серыми схемами получения рублей. А на нижнем уровне — откровенно криминальные площадки.

Структура этого рынка глубоко поражена организованной преступностью. Ядро проблемы — классические колл-центры. Их участники обзывают граждан, представляются сотрудниками банков или полиции и убеждают жертв перевести деньги на «безопасный счет». Похищенные средства

мгновенно, за считанные минуты, проходят цепочку из нескольких банковских карт (дропперских), после чего конвертируются в криптовалюту. Именно криптообменники становятся финальным звеном в этой цепочке — «пылесосом», который всасывает грязные рубли и выдает взамен анонимные USDT, которые затем уходят организаторам.

По данным Банка России, только в 2025 году было выявлено более 7 тысяч субъектов с признаками нелегальной деятельности на финансовом рынке. Из них 5,7 тысяч — финансовые пирамиды и псевдоброкеры, почти все они действовали в интернете. При этом 84% мошеннических схем требовали переводов в криптовалюту. Чтобы привлечь молодую аудиторию, создатели схем делали акцент на использовании искусственного интеллекта. Регулятор направил информацию обо всех выявленных нелегальных проектах в правоохранительные органы, по результатам было возбуждено более 440 административных дел и принято более 650 различных мер реагирования.

Онлайн-обменники: мониторинги и BestChange

Центральное место в мире онлайн-обменников занимают мониторинги — сайты-агрегаторы, которые собирают курсы десятков и сотен обменных пунктов в одной таблице. Крупнейший из них — BestChange, работающий с 2007 года. Однако даже этот флагман индустрии находится под постоянным давлением. В апреле 2025 года доступ ко всем доменным именам BestChange был заблокирован Роскомнадзором. Сервис уже блокировался трижды — в 2017, 2019 и 2020 годах. Для разблокировки Банк России потребовал удалить из каталога не только информацию по покупке и продаже иностранной валюты за рубли, но и пары с двумя иностранными платежными системами и валютами.

Более того, в 2025 году агрегатор был вынужден исключить десятки сервисов из своего каталога. Причина — массовые жалобы пользователей на блокировки карт после обмена через некоторые обменники. В октябре 2025 года BestChange внедрил многоуровневую систему верификации обменников: проверка возраста домена, мониторинг жалоб в реальном времени, выборочные тестовые сделки и блокировка обменников с признаками мошенничества в течение нескольких часов. По данным на март 2026 года, агрегатор скрыл рублевые направления у 95 обменных пунктов из-за роста жалоб пользователей и признаков сомнительных операций.

Telegram-боты: за анонимным фасадом

Telegram стал главной операционной средой для криптообменников в России по двум причинам: во-первых, мессенджер относительно устойчив к блокировкам, во-вторых, он позволяет создавать полностью автоматизированные обменные сервисы без какого-либо внешнего сайта.

Стандартный Telegram-бот работает так: вы выбираете направление обмена (USDT → Сбербанк, BTC → Тинькофф и т. д.), вводите сумму, получаете адрес кошелька и реквизиты карты — и сделка закрывается в течение нескольких минут. Для пользователя это выглядит как удобный и быстрый сервис. Но за этим фасадом часто скрывается сложная криминальная инфраструктура.

Показательно расследование Transparency International — Россия, опубликованное в сентябре 2025 года. Авторы документально зафиксировали, что преемники попавшей под санкции криптобиржи Garantex перестроились в распределенную систему под новыми вывесками — Exved и Grinex. Операционная деятельность была полностью выстроена в Telegram. Эта сеть маскировала криптотранзакции под рублевые «агентские» платежи, уводила расчеты в офшорные звенья и обслуживала, в том числе, поставки товаров двойного назначения (микроэлектроника и телеком-оборудование). Объем транзакций через эту сеть за несколько месяцев достиг \$9,3 млрд. «Garantex не исчез; он перестроился в распределенную систему, которая прячет криптооперации за агентскими договорами, офшорными звеньями и процессами, выстроенными в Telegram», — подчеркивала автор расследования Кристина Багдасарян.

Еще один опасный тренд, зафиксированный в 2025-2026 годах, — это рост числа преступных групп, работающих через Telegram. Была зафиксирована деятельность как минимум шести крупных преступных групп, которые использовали Telegram-ботов для поиска потенциальных жертв и романтический скам с фальшивыми аккаунтами «финансово независимых девушек».

Криптоматы: вымирающий вид

Криптоматы — физические терминалы, через которые можно купить или продать криптовалюту за наличные, — это классический инструмент офлайн-обмена. В мире их насчитывается более 30 тысяч, но в России их история коротка и трагична.

До 2021 года в Москве и Санкт-Петербурге работало несколько сетей криптоматов, но после ужесточения регулирования и отсутствия четкого закона об обороте наличной криптовалюты большинство из них было демонтировано или ушло в подполье. В 2024 году российская криптобиржа AVCEX запустила криптофиатный банкомат в своем офисе в Москва-Сити, через который клиенты могли пополнять биржевые счета и выводить средства в рублях без комиссии.

Однако с июля 2026 года ситуация изменится радикально. Согласно новому законопроекту, принятому Госдумой в первом чтении, криптообменники смогут работать только при наличии лицензии ЦБ. При этом для неквалифицированных инвесторов торги будут идти исключительно через брокеров, а самостоятельно выйти на рынок рядовой гражданин уже не сможет. Фактически это означает, что нелегальные криптоматы и обменники без лицензии будут полностью запрещены, а за их организацию введут уголовную ответственность.

Кроме того, регулятор обсуждает введение штрафов за расчеты в криптовалюте внутри страны: от 100 тысяч до 200 тысяч рублей для физических лиц и до 1 млн рублей для юридических лиц. Одновременно вводится уголовная ответственность за незаконный оборот криптовалюты с максимальным наказанием до 7 лет лишения свободы.

Реальный кейс: задержание организатора криптообменника

Теория без практики мертва. Обратимся к реальному уголовному делу апреля 2026 года.

21 апреля 2026 года сотрудники управления по борьбе с киберпреступностью ГУ МВД России по Челябинской области совместно с ФСБ провели масштабную операцию. Была задержана банда, организовавшая три офиса нелегального криптообменника — в Челябинске и Москве.

Схема была построена на классическом дропперстве. Организаторы за деньги скупали банковские карты и сим-карты у жителей Челябинской области, фактически превращая их в соучастников преступлений. Через эти счета проходили потоки денег с нелегальных интернет-площадок — онлайн-казино, мошеннических колл-центров, букмекерских контор. Только в одном Южноуральске за одну ночь полиция установила и задержала более 30 молодых людей, предоставлявших свои банковские карты преступникам.

В ходе обысков в офисах обменника изъяли около 200 мобильных телефонов и свыше 100 банковских карт. Возбуждены уголовные дела по статье «Неправомерный оборот средств платежей» (ст. 187 УК РФ). Организаторы всех трех офисов арестованы, остальных участников схемы продолжают устанавливать.

Другие громкие задержания:

- **Санкт-Петербург, март 2026 года.** Задержаны 40-летний организатор и две его сообщницы, которые создали теневой криптообменник для конвертации похищенных у пенсионеров денег в криптовалюту. В ходе обысков изъято 35 банковских карт, 15 мобильных телефонов, ноутбуки, жесткие диски, десятки пластиковых карт USDT и 635 тысяч рублей наличными.
- **Башкирия, август 2025 года.** Арестованы организаторы преступного сообщества, которое вывело за рубеж более 3 млрд рублей доходов мошеннических колл-центров, нелегальных онлайн-казино и криптообменников.

Эти дела объединяет одна общая черта: все они построены на цепочке «грязные деньги → криптообменник → неотслеживаемый вывод за рубеж». И во всех случаях используются дропперы — обычные люди, продавшие или одолжившие свою банковскую карту преступникам.

Как работают инкассации крипты в Москве и регионах

Отдельный, чрезвычайно важный сегмент теневого рынка — офлайн-обмен. В Москве, Санкт-Петербурге и крупных региональных центрах существует развитая сеть физических пунктов обмена криптовалюты на наличные. По данным ForkLog, крупнейшая сеть таких офисов — AVCEX, которая к началу 2025 года открыла 53 офиса в Москве, Санкт-Петербурге, Уфе, Казани, Екатеринбурге и других городах. В этих пунктах клиенты могут легально вносить или снимать наличные со своего биржевого счета. Для офлайн-операций требуется паспорт, который проверяют при входе.

Но параллельно с легальными офисами существует и теневая сеть инкассации. Ее стандартный алгоритм включает пять шагов. Сначала трейдер фиксирует курс и сумму сделки. Затем проводится идентификация — через паспорт либо биометрию. После этого криптовалюта вносится на указанный адрес кошелька обменника, и клиент получает наличные.

В Москве работает несколько узнаваемых брендов офлайн-обменников, в том числе Bitokk с несколькими офисами по городу. Поддержка сделок за наличные, простая схема работы и стабильная ликвидность делают его востребованным инструментом для тех, кому нужен крупный кеш. Однако надо понимать: как только регулятор запустит лицензирование обменников с июля 2026 года, все подобные сервисы должны будут либо получить лицензию ЦБ, либо уйти в глубокое подполье.

Исследователи блокчейна также фиксируют схемы с участием российских ОТС-брокеров, которые отмывают криптовалюту, полученную от программ-вымогателей. В марте 2026 года анонимный блокчейн-расследователь ZachXBT идентифицировал российского ОТС-брокера Александра Хинкиса как центральную фигуру в схеме отмывания более \$4,7 млн, полученных от трех отдельных атак программ-вымогателей на общую сумму 796 BTC. Расследование включало тайную беседу в Telegram.

Что ждет рынок нелегальных обменников

Ключевой вывод, который должен сделать читатель из этой главы: эпоха вольницы для нелегальных обменников заканчивается. С 1 июля 2026 года вступает в силу пакет поправок, который вводит обязательное лицензирование криптобирж и обменников через ЦБ. Как пояснил эксперт в области криптовалют Евгений Каминский, «новый закон не про обычных людей, которые просто покупают или хранят биткоин для себя. Он направлен только против серых обменников, Telegram-ботов и площадок без лицензии». Эксперт добавил, что пользователи со временем перейдут на банки или лицензированные биржи. С июля 2026 года правила станут понятнее.

А с 1 июля 2027 года планируется ввести полноценную уголовную ответственность за нелегальную деятельность на крипторынке — по аналогии с ответственностью за нелегальную банковскую деятельность.

Для обычного пользователя это означает две вещи. Во-первых, с каждым месяцем работать через «серые» и «черные» обменники становится все опаснее — как с точки зрения потери денег, так и с точки зрения уголовного преследования. Во-вторых, государство целенаправленно закручивает гайки, выдавливая крипто-ликвидность в легальное русло. И чем раньше вы перейдете в это русло, тем меньше рисков понесете.

Использованные в главе источники:

- 1) ФСБ: На территории Якутии работает финансовая пирамида, представители которой действуют с Украины <https://smtp.sakhapress.ru/archives/309837>
- 2) Crypto Sleuth Links Russian OTC Desk To \$4.7M Laundering <https://www.htx.com.hk/news/crypto-sleuth-links-russian-otc-desk-to-47m-laundering-ED3FUtvD/>
- 3) Преемники Garantex: от биржи к мессенджеру <https://ti-russia.org/blog/preemniki-garantex-rassledovaniye/>
- 4) Россиян начали обманывать от лица «финансово независимых девушек» <https://versia.ru/rossiyan-nachali-obmanyvat-ot-lica-finansovo-nezavisimyx-devushkek>
- 5) GORILLA P2P, Enot Trade и Triumph Speculant: Георгий Спекулянт и сеть криптоканалов с криминальным следом <https://informpotok.com/novosti/item/137696-gorilla-p2p-enot-trade-i-triumph-speculant-georgiy-spekulyant-i-set-kriptokanalog-s-kriminalnym-sledom>
- 6) Lady on a Million, 2trade и CryptoClub: Прокофьев, Соболев и Шорохов в общей схеме крипторазвода <https://nezigar.net/vse-novosti/item/304436-lady-on-a-million-2trade-i-cryptoclub-prokofev-sobolev-i-shorohov-v-obschey-sheme-kriptorazvoda>
- 7) Authorized Russian cryptocurrency operators bypass oversight by executing trades via Telegram <https://m.kartoteka.news/news/135238-authorized-russian-cryptocurrency-operators-bypass-oversight-by-executing-trades-via-telegram>
- 8) The Interior Ministry told about scammers trading digital assets through Telegram bots https://en.iz.ru/en/2024959/2026-01-15/interior-ministry-told-about-scammers-trading-digital-assets-through-telegram-bots?main_click
- 9) Загрузчик заблокирован, кастомы мертвы: как ЕС уничтожает свободу Android <https://pikabu.ru/tag/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%2C%D0%9D%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8?page=20&page=17&page=30&page=28>
- 10) Компромат Групп <https://t.me/s/criminalru?after=42088>
- 11) В Челябинской области полицейские задержали банду лже-криптовалютчиков <https://www.1obl.ru/tv/proisshestiya/proisshestiya-dnya-21-04-2026/v-chelyabinskoy-oblasti-politseyskie-zaderzhali-bandu-lzhe-kriptovalyutchikov/>
- 12) В Петербурге задержали создателей криптообменника за обман пенсионеров <https://russiatoday.ru/russia/news/1610385-peterburg-kriptoobmennik-moshenniki-pensionery>
- 13) Наводил ОПГ на владельцев криптовалюты: в чем обвиняют тхэквондиста Четинбага <https://ren.tv/news/kriminal/1401363-chempion-mira-iz-opg-tkhekvondist-chetinbag-koshmaril-kriptobiznesmenov>
- 14) В Башкирии арестовали предполагаемых организаторов группировки, которая незаконно вывела за рубеж миллиарды мошеннических колл-центров и криптообменников <https://gov.tadviser.ru/index.php/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0:%D0%9A%D1%83%D0%B2%D0%B0%D1%82%D0%BE%D0%B2%D0%90%D0%B7%D0%B0%D0%BC%D0%B0%D1%82>
- 15) Задержан подозреваемый в ограблении криптовалютного обменника <https://news.rambler.ru/incidents/56173202-zaderzhan-podozrevaemyy-v-ograblenii-kriptovalyutnogo-obmennika/>
- 16) В Забайкалье полицейскими пресечена деятельность лже-инвесторов: злоумышленники похитили у клиентов около 60 млн рублей https://www.gubnews.ru/news_mvd.php?id=44365
- 17) Российское правительство предложило заключать в тюрьму за незаконное обращение цифровой валюты https://en.iz.ru/en/2078056/2026-04-13/russian-government-has-proposed-imprison-illegal-circulation-digital-currency?main_click
- 18) Moscow police detained organizer and participant of fraud disguised as training for work with cryptocurrency exchanges <https://en.mvd.ru/news/item/69349503/>
- 19) Тюрьма за «серый» обмен крипты <https://cryptochan.net/stream/id/1776088773/>
- 20) В России предложили привлечь ФСБ к борьбе с нелегальными криптообменниками <https://www.gazeta.ru/social/news/2026/04/13/28254235.shtml>
- 21) ABCEX: как работает сеть офлайн-офисов для обмена криптовалют в России <https://forklog.com/exclusive/abceh-kak-rabotaet-set-oflajn-ofisov-dlya-obmena-kriptovalyut-v-rossii/amp/>
- 22) Ошибка 403 <https://epamlaw.com/public/ru/legal-updates/view/obmennyy-manevr:-kak-v-rf-nelegalno-vyvodyat-cifrovye-dengi-v-nalichnye-or>
- 23) Options for Withdrawing Rubles via Crypto Exchangers in Russia: Comprehensive Guide 2026 <https://www.bitget.com/amp/academy/options-for-withdrawing-rubles-via-crypto-exchangers-in-russia-comprehensive-guide-2026>

- 24) Лучшие криптообменники в Москве в 2025: как выбрать и где найти <https://finbazar.ru/hashtag/%d0%ba%d1%80%d0%b8%d0%bf%d1%82%d0%be%d0%be%d0%b1%d0%bc%d0%b5%d0%bd%d0%bd%d0%b8%d0%ba>
- 25) ABCEX Launches Crypto-Fiat ATM in Moscow <https://forklog.com/en/abce-launches-crypto-fiat-atm-in-moscow/>
- 26) Как выгодно обменять криптовалюту в москве <https://ipotekaved.ru/kak-vygodno-obmenyat-kriptovalyutu-v-moskve.html/#i-2>
- 27) Использование криптообменников в Москве: простое руководство для каждого <https://www.klerk.ru/blogs/exnode/606944/>
- 28) Криптообменники с обменом на наличные в Москва-Сити 2026 <https://www.klerk.ru/blogs/exnode/688674/>
- 29) Обменник Citykripto - обзор и отзывы <https://wellcrypto.io/ru/exchangers/citykripto/>
- 30) Покупка и продажа криптовалюты за наличные RUB и USD в городах России <https://crypto-city.pro/services/>
- 31) Агрегатор обменников BestChange сообщил о разблокировке по решению ЦБ <https://amp.rbc.ru/crypto/news/68937c029a79477ab74cd135>
- 32) BestChange ограничил рублевые предложения 95 криптовалютных <https://www.tbank.ru/invest/social/profile/Morgan2684/0cfe45fb-9656-465a-bb17-320d28d20b10/?author=profile>
- 33) «Курс +10% к рынку — не подарок, а приманка». Руководитель продуктов BestChange — о блокировках карт и борьбе с «грязным» трафиком <https://forklog.com/exclusive/kurs-10-k-rynku-ne-podarok-a-primanka-rukovoditel-produktov-bestchange-o-blokirovkah-kart-i-borbe-s-gryaznym-trafikom/>
- 34) Роскомнадзор заблокировал агрегатор онлайн-обменников BestChange <https://expert.ru/news/roskomnadzor-zablokiroval-agregator-onlayn-obmennikov-bestchange/>
- 35) ЦБ инициировал разблокировку BestChange при условии удаления некоторых направлений обмена <https://x-compliance.ru/publications/podft/tsb-initsiiroval-razblokirovku-bestchange-pri-uslovii-udaleniya-nekotoryh-napravlenii-obmena>
- 36) Полет нормальный: как агрегатор криптообменников BestChange справился с ограничениями и восстановил работоспособность в России <https://yar.mk.ru/economics/2025/10/06/polet-normalnyy-kak-agregator-kriptoobmennikov-bestchange-spravilsya-s-ogranicheniyami-i-vosstanovil-rabotosposobnost-v-rossii.html>
- 37) После снятия ограничений популярный агрегатор криптовалютных бирж возвращается в Россию <https://www.binance.com/zh-CN/square/post/27996242484338>
- 38) Роскомнадзор заблокировал сайт агрегатора криптообменников BestChange <https://rozetked.me/index.php/news/37655-roskomnadzor-zablokiroval-sayt-kriptoobmennika-bestchange#comments>
- 39) Роскомнадзор ограничил доступ к агрегатору онлайн-обменников BestChange <https://govoritmoskva.ru/news/441394/>
- 40) Аналитик BestChange раскрыл детали блокировки 95 обменников и рассказал о возможных рисках для пользователей <https://www.bitget.com/ru/news/detail/12560605020057>
- 41) Госдума приняла в 1-м чтении законопроект, признающий цифровую валюту имуществом <https://news.rambler.ru/politics/56337557-gosduma-prinyala-v-1-m-chtenii-zakonoproekt-priznayuschiy-tsifrovuyu-valyutu-imuschestvom/>
- 42) Что будет с регулированием рынка криптовалют в России в 2026 году https://www.rbc.ru/crypto/news/694e62239a7947ba7117a8b3?utm_source=amp_crypto_full-link
- 43) Россиянам рассказали о новых мерах по контролю за оборотом криптовалюты <https://russian.rt.com/business/news/1619992-ekspert-oborot-kriptovalyuty>
- 44) ЦБ возьмёт под контроль оборот криптовалют в России <https://plusworld.ru/articles/71021/>
- 45) Ограничить и защитить: рынок криптовалют в России выводят из серой зоны <https://www.ntv.ru/novosti/2977135>
- 46) ЦБ подготовил концепцию по регулированию криптовалют в России <https://expert.ru/news/tsb-podgotovil-kontseptsiyu-po-regulirovaniyu-kriptovalyut-v-rossii/>
- 47) Власти задумали штрафовать россиян за оплату криптовалютой <https://moscowtimes.org/2025/07/21/vlasti-zadumali-shtrafovat-rossiyan-za-oplatu-kriptovalyutoi-a169263/>
- 48) Двери закрываются: как будут наказывать за торговлю криптовалютой <https://www.forbes.ru/investicii/557842-dveri-zakryvautsa-kak-budut-nakazyvat-za-torgovlu-kriptoalutoj>
- 49) Россиянам запретят нелегально торговать криптовалютой <https://riamo.ru/news/ekonomika/rossijanam-zapretjat-nelegalno-torgovat-kriptoalutoj/>

- 50) Путин решил штрафовать россиян за оплату криптовалютой
<https://charter97.link/be/news/2025/7/21/649006/>
- 51) Искусственный интеллект, криптовалюты и дропперство: как действовали пирамиды и другие нелегалы в 2025 году <https://www.cbr.ru/press/event/?id=28351>
- 52) Противодействие нелегальной деятельности на финансовом рынке
https://www.cbr.ru/analytics/inside/2025_2/
- 53) Крипторазводы 2026: схемы, которые работают прямо сейчас, — и как не стать следующей жертвой
<https://www.securitylab.ru/analytics/571260.php>
- 54) Пирамиды перестроились в кредиты <https://www.kommersant.ru/doc/8477364>
- 55) ЦБ за год выявил более 7 тыс. финансовых пирамид и псевдоброкеров
<https://www.rbc.ru/rbcfreenews/69a14aff9a7947043a8622b4>
- 56) ИИ, криптоактивы и дропперы: как действовали финансовые нелегалы в 2025 <https://bcs-express.ru/novosti-i-analitika/ii-kriptoaktivy-i-dropperiy-kak-deistvovali-finansovye-nelegaly-v-2025>
- 57) Банк России выявил более 7000 нелегальных участников финрынка в 2025 году
<https://www.vedomosti.ru/economics/news/2026/02/27/1179525-nelegalnih-uchastnikov-finrinka>
- 58) ЦБ РФ: в 2025 году криптовалюта стала главным инструментом мошенников <https://nbj.ru/news/tsb-rf-v-2025-godu-kriptoalyuta-stala-g/72283/>
- 59) ЦБ в 2025 году выявил более 7 тыс. нелегальных участников финрынка <https://bosfera.ru/press-release/cb-v-2025-godu-vyavil-bolee-7-tys-nelegalnyh-uchastnikov-finrynka>
- 60) На 21,5% снизилось количество нелегальных участников финрынка в 2025 году
<https://pravo.ru/news/262617/>

Глава 7. «Чёрные брокеры» и фейковые биржи

Представьте, что вы видите во сне идеальную криптобиржу. Интерфейс радует глаз, котировки мелькают как на настоящем Bloomberg, а личный менеджер с безупречным произношением каждый день поздравляет вас с ростом депозита. Вы заводите 10 тысяч рублей — через неделю на экране уже «₽25 000». Вы заводите ещё 100 тысяч рублей, потом берёте кредит на миллион — баланс становится похож на номер телефона. А когда приходит время вывести деньги, сайт оказывается недоступен, менеджер превращается в тыкву, и вы остаётесь один на один с пустым кошельком.

Это не страшилка. Это статистика. По данным Банка России, только за девять месяцев 2025 года в стране выявлено около 5,8 тысяч нелегальных финансовых проектов. Количество псевдоброкеров, предлагающих торги криптовалютой, увеличилось на 63% и достигло 1,8 тысяч. Более 1,2 тысяч финансовых пирамид работают под видом инвестиций в криптовалюту.

Это значит, что прямо сейчас, пока вы читаете эти строки, в интернете действуют сотни сайтов, единственная цель которых — украсть ваши деньги. Их создатели — не хакеры в толстовках, а профессиональные психологи, маркетологи и актёры, объединённые в настоящие колл-центры с KPI, скриптами и бонусами. В этой главе мы разберём, как работает технология подмены настоящих бирж, почему вы никогда не сможете вывести деньги с фейковой площадки и какие струны вашей души перебирают мошенники, чтобы вы сами несли им свои сбережения.

Технология подмены сайтов: как вас встречают у входа

В декабре 2025 - январе 2026 года эксперты по кибербезопасности зафиксировали настоящий взрыв: за два месяца обнаружен 701 поддельный сайт, мимикрирующий под криптовалютные платформы, включая российскую доменную зону, а в январе число таких ресурсов превысило 700. По данным компании [BI.ZONE](#), мошенники чаще всего создают клонов под известные площадки для торговли и обмена.

Первая линия атаки — подмена домена. Фишинговые сайты имитируют интерфейс Binance, Bybit, MetaMask, Trust Wallet, Ledger — тех платформ, которым пользователи привыкли доверять. Внешне сайт идентичен оригиналу до пикселя: те же кнопки, те же цвета, тот же логотип. Отличие спрятано в адресной строке — и оно микроскопическое:

- Вместо «binance.com» — «binance.com» (с буквой «i» из украинского алфавита).
- Вместо «bybit.com» — «bybitt.com» или «bybit-exchange.com».
- Вместо «metamask.io» — «metamask-wallet.net».
- Вместо «trustwallet.com» — «trustwallet-verify.cc».

Существует целая индустрия по производству таких подделок. Мошенники покупают контекстную рекламу, чтобы их клон поднимался в поисковой выдаче выше настоящего сайта. Ссылки распространяются через Telegram, Instagram и даже в комментариях к новостям. Расчёт прост: большинство пользователей не проверяет адресную строку. Они набирают «бинанс войти» в поиске, кликают по первой ссылке и, увидев знакомый дизайн, без колебаний вводят логин, пароль и даже двухфакторный код. С этого момента их аккаунт принадлежит злоумышленникам.

Но фишинг не ограничивается подделкой сайтов. Осенью 2025 года кибербез-специалисты выявили новую двухэтапную схему. Сначала мошенники пишут жертве от лица реально существующего агентства по подбору персонала с предложением «взаимовыгодного сотрудничества». На втором этапе с другого аккаунта связывается «партнёр агентства» — якобы специалист Binance — и подробно описывает схему пассивного заработка, похожую на банковский вклад. Жертву убеждают скачать «официальные приложения» Trust Wallet и одной из криптобирж, после чего просят пройти по ссылке из письма и «привязать кошелёк» к аккаунту. Вот только аккаунт этот уже создан мошенниками на почту жертвы — и после привязки они получают полный доступ ко всем средствам.

А самая изощрённая схема 2025-2026 годов — поддельные торговые дашборды — получила на профессиональном сленге название «rig-butchering» («разделка свиньи»). Мошенники создают клон интерфейса Binance или Bybit, который в реальном времени показывает якобы рыночные котировки, баланс и прибыль. Жертва наблюдает, как график растёт, баланс пухнет, а аналитик объясняет, почему нужно «доливаться» именно сейчас. На самом деле никакого подключения к рынку нет — это просто красиво свёрстанная веб-страница, где все цифры нарисованы на сервере мошенников.

Почему вывод денег с поддельной биржи невозможен

Когда жертва пытается вывести средства с фейковой биржи, включается второй — самый жестокий — акт спектакля. На экране появляется сообщение: «Вывод заблокирован, требуется дополнительная AML-провер-

ка, оплатите комиссию 2% от суммы». Или: «Поздравляем! Ваш доход составил 300%. Для вывода необходимо оплатить налог на прибыль — 13%, переведите на указанный кошелёк». В ход идут разные сценарии: требование заплатить «страховку транзакции», «комиссию за конвертацию», «верификацию личности через платный сервис».

Добросовестный человек рассуждает: я вижу прибыль на экране, для её получения нужно заплатить налог, это логично — банки тоже удерживают налог при выплате процентов по вкладу. Эта логика убийственна. Жертва переводит требуемую сумму — и получает новое требование. И так до тех пор, пока у неё не закончатся деньги или пока она не осознает, что её обманывают. В этот момент сайт перестаёт открываться, менеджер блокирует контакт, и жертва остаётся один на один с нулевым балансом на своём реальном кошельке — а всё, что она видела на экране, было просто цифрами в поддельном интерфейсе.

Именно это произошло с 25-летним машинистом из Ачинска. В январе 2025 года в поиске подработки он познакомился в интернете с девушкой, занимающейся торговлей на бирже. Она дала контакты «биржевого аналитика», тот рассказал о новом способе заработка и помог зарегистрироваться на фейковой бирже. Машинист внёс первые 10 тысяч рублей, но мошенникам этого показалось мало, и они убедили его вложить более крупную сумму. Мужчина одолжил у знакомой 2,8 млн рублей и перечислил их на продиктованный счёт. Платформа продолжала требовать «произвести полный оборот денежных средств по синхронизации». Он снова обратился к подруге, та оформила кредит на 800 тысяч рублей. Общая сумма ущерба составила 3,6 млн рублей. Когда мужчина осознал, что стал жертвой аферистов, он обратился в полицию, но деньги уже ушли через цепочку кошельков.

А вот история из Сыктывкара: женщина в течение семи месяцев наблюдала, как «растёт» её доход на фейковой бирже. За это время она не только вложила все свои сбережения, но и привлекла трёх знакомых, оформила несколько кредитов, включая заём под залог автомобиля. Общая сумма ущерба превысила 6 млн рублей.

Эти истории — не единичные случаи, а системное явление. По данным ЦБ, более 84% мошеннических схем сразу требуют переводы в криптовалюту через иностранные платежные сервисы. Почему? Потому что блокчейн-транзакция необратима. Невозможно «отозвать платёж», «оспорить перевод», «позвонить в банк и заблокировать». Криптовалюта, отправленная на кошелёк мошенника, уходит безвозвратно. Её тут же — в автоматическом

режиме — разбивают на множество сумм, конвертируют в Monero или миксеруют, после чего отследить её невозможно.

Особая боль — выходной скам (exit scam), когда мошенники создают платформу, которая месяцами работает безупречно: даёт выводить средства, платит «проценты», нарабатывает репутацию. Как только на счетах скапливается крупная сумма — сайт объявляет «технические работы» и закрывается, унося депозиты тысяч пользователей. В 2025 году таким образом исчезла платформа «Garantex Europe» (клон печально известной российской Garantex, попавшей под санкции), собравшая \$3,5 млн.

Психология жертвы: как вас разводят на 100% депозита

Главный вопрос, который задают себе все, кто никогда не попадался: как вообще можно повестись на такое? Ответ сложнее, чем кажется. Психолог Наталья Бехтерева, специализирующаяся на кибермошенничестве, подчёркивает: людей со стопроцентным иммунитетом к действиям жуликов не существует, ключи можно подобрать к любому человеку.

Механика развода строится на трёх китах: жадность, страх и авторитет. Плюс один специфически криптовалютный фактор — лотерейное мышление. Когда человеку обещают быстрый заработок на «новом, закрытом от всех» инструменте, том самом, на котором зарабатывают избранные, включается дофамин ожидания. Мошенники апеллируют к так называемому лотерейному мышлению: человеку кажется, что он исключительный и редкая удача может случиться именно с ним. Вырабатывается дофамин ожидания, появляется азарт, открывается тоннель внимания на «шанс». Страх упустить возможность — знаменитое FOMO (fear of missing out) — полностью отключает критическое мышление. «Сейчас уникальная точка входа», «рынок уходит через час», «нужно срочно долить, чтобы не потерять прибыль» — все эти фразы бьют в одну точку: отключить рациональный анализ и заставить действовать на эмоциях.

Сразу после того, как капкан захлопнулся, начинаются более сложные манипуляции — шокировать, заставить паниковать, создать ложное ощущение, что ситуация под контролем. А затем — эффект «невозвратных затрат» (sunk cost fallacy). Когда вы уже вложили крупную сумму, признать, что вас обманули, психологически невыносимо. Гораздо легче поверить, что нужно «ещё немного» — оплатить последнюю комиссию, последний налог, чтобы разблокировать вывод. На этом этапе жертва сама становится двигателем схемы: она занимает у знакомых, оформляет кредиты, закладывает машину — только бы не признать, что всё потеряно.

Искусственный интеллект вывел эти манипуляции на новый уровень. Мошенники научились социальной мимикрии: они копируют речевые паттерны, термины, создают ощущение формальной процедуры. Мозг жертвы узнаёт сценарий и заполняет пробелы доверием. Работают сразу несколько когнитивных искажений: эффект авторитета (имя должностного лица автоматически снижает критичность), гало-эффект (положительная репутация «подсвечивает» и сам звонок), чувство исключительности (личный контакт с якобы известной персоной придаёт значимости).

Ещё одна линия атаки — романтический скам, который бьёт по самой уязвимой категории: эмоционально нестабильным людям после развода или потери. Сначала жертву «любят» — переписка, голосовые, комплименты. Когда эмоциональная зависимость сформирована, «партнёр» между делом рассказывает о своём успешном опыте торговли на криптобирже и предлагает «попробовать вместе». Отказать любимому человеку практически невозможно.

Итог этой главы прост и страшен: жертвой чёрных брокеров может стать кто угодно. Среди потерпевших есть профессора и таксисты, программисты и пенсионеры, топ-менеджеры и студенты. Единственная надёжная защита — знать, как работает схема, и остановиться в тот момент, когда вам обещают гарантированную прибыль.

Пять признаков, которые должны заставить вас немедленно закрыть вкладку:

1. Обещание гарантированной доходности. В крипте гарантий не существует — ни 10%, ни 2% в месяц. Тот, кто их обещает, — мошенник.
2. Агрессивный маркетинг. Вам звонят, пишут в личку, добавляют в «закрытые чаты для инвесторов» — это не эксклюзив, это воронка.
3. Требование внести деньги немедленно — «только сегодня специальный курс».
4. Просьба оплатить вывод. Ни одна настоящая биржа не требует платить за вывод средств сверх комиссии сети.
5. Ошибки в URL и отсутствие истории. Поддельный сайт не светится на CoinMarketCap, у него нет блога, нет страниц с юридической информацией, а в футере ссылки ведут в никуда.

Помните: ваш кошелёк — ваша ответственность, а ваша бдительность — единственная страховка, которая работает на 100%.

Использованные в главе источники:

- 1) Мошенники атакуют криптоинвесторов через фишинговые сайты <https://kiberboloid.ru/novosti/moshenniki-atakuyut-kriptoinvestorov-cherez-fishingovye-sayty/>
- 2) 5 признаков фишинговых схем и как их распознать <https://vc.ru/crypto/2330142-priznaki-fishinga-v-kriptovalute-i-kak-ikh-raspoznat>
- 3) Binance раскрыла сфабрикованный случай мошенничества, нацеленный на получение компенсации от службы поддержки <https://bingx.com/ru-ru/news/post/binance-exposes-fabricated-scam-case-aimed-at-forcing-payout-from-customer-support-on-january>
- 4) Fake Binance / Bybit Dashboards: Spot Pig-Butchering Sites <https://www.redsecuretech.co.uk/blog/post/fake-binance-bybit-dashboards-spot-pig-butchering-sites/997>
- 5) Уязвимость безопасности <https://securenews.ru/tag/%D1%83%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D0%B8/page/19/>
- 6) Кибермошенники усложнили фишинг-атаки <https://petropavlovskkamchatskiy.monavista.ru/news/4980274/>
- 7) Кибермошенники усложняют фишинг для пользователей <https://sevastopol.monavista.ru/news/4980212/>
- 8) Пользователи Binance стали жертвами SMS-фишинга, выдающего себя за предупреждения о безопасности https://www.binance.me/ru/square/post/22898781567825?_cf_chl_rt_tk=xTswLAHdniR1KduUOZamCrHNulGGoAj7R39Bg.CAB0Y-1777028166-1.0.1.1-qIB6_xVRGdrdjyhyh5ztRYjnz9CDqr_wrq9uKwu59xs
- 9) Против россиян применили новую мошенническую криптосхему <https://www.tradingview.com/news/bitsmedia%3Afd07625dc67b8%3A0/>
- 10) Против россиян применили новую мошенническую криптосхему <https://bits.media/v-rossii-vyavlena-novaya-moshennicheskaya-kriptoskhema/?amp>
- 11) Четверых новосибирцев будут судить за мошенничество с криптовалютой <https://www.nsktv.ru/news/crime/chetverykh-novosibirtsev-budut-sudit-za-moshennichestvo-s-kriptovalyutoy>
- 12) Инвестиции в фейк: житель Заволжского района Ульяновска попал на миллион <https://media73.ru/2025/investitsii-v-feyk-zhitel-zavolzhschskogo-rayona-ulyanovska-popal-na-million>
- 13) Фейковая криптобиржа отняла у 25-летнего машиниста из Ачинска 3,6 миллиона рублей
Подробнее: <https://krasrab.ru/news/finansy/44473> <https://krasrab.ru/news/finansy/44473>
- 14) Житель Воронежской области хотел вернуть вложения в крипту, но суд встал на сторону куратора <https://tv-gubernia.ru/novosti/obwestvo/zhitel-voronezhskoj-oblasti-hotel-vernut-vlozheniya-v-kriptu-no-sud-vstal-na-storonu-trenera/#respond>
- 15) Сыктывкарка потеряла 6 миллионов рублей на инвестициях в криптовалюту <https://www.bnkomi.ru/data/news/185152/>
- 16) Деньги брали и исчезали: двоих жителей Хакасии обвиняют в мошенничестве <https://gazeta19.ru/news/kriminal-i-proisshestviya/dengi-brali-i-ischezali-dvoikh-zhiteley-khakasii-obvinyayut-v-moshennichestve/>
- 17) Лже-брокеры похитили у жителя Тарбагатайского района более 800 тысяч рублей <https://03.xn--b1aew.xn--p1ai/news/item/59981947/?year=2025&month=8&day=7>
- 18) Мошенники убедили сыктывкарца в положительной волне на ниве криптовалюты, а затем похитили 1,8 млн кредитных рублей <https://11.xn--b1aew.xn--p1ai/news/item/67153077>
- 19) Криптоинвестор из Сыктывкара потерял 1,8 миллиона рублей, взятых в кредит <https://www.bnkomi.ru/data/news/187196/>
- 20) Общественный совет при УФНС России по Московской области <https://rsnmo.ru/index.php?id=96735>
- 21) ЦБ с начала 2025 года выявил 5,8 тыс. нелегальных финансовых проектов <https://bosfera.ru/press-release/cb-s-nachala-2025-goda-vyavil-58-tys-nelegalnyh-finansovyh-proektov>
- 22) ЦБ в 2025 году выявил более 7 тыс. финансовых пирамид и других мошенников <https://x-compliance.ru/publications/risk-management/tsb-v-2025-godu-vyavil-bolee-7-tys-finansovyh-piramid-i-drugih-moshennikov>
- 23) ЦБ заблокировал почти 16 тыс. сайтов нелегальных проектов <https://incrusia.ru/news/tsb-zablokiroval-pochti-16-tys-sajtov-nelegalnyh-proektov/>
- 24) Фейковые криптоброкеры «рисуют прибыль» и выманивают у россиян новые вложения <https://www.ossetia.tv/2025/12/18/fejkovye-kriptobrokeriy-risuyut-pribyl-i-vymanivayut-u-rossiyan-novye-vlozheniya/>
- 25) ЦБ зафиксировал рост связанных с торгами криптовалютой нелегальных проектов <https://www.vesti.ru/article/4783731>

- 26) Осторожно, фейковые биржи: как работают брокеры-мошенники в Тюменской области <https://tumentoday.ru/2026/02/17/ostorozhno-fejkovyve-birzhi-kak-rabotayut-brokerymoshenniki-v-tyumenskoy-oblasti/>
- 27) Аферисты начали использовать «документы» от иностранных регуляторов <https://vedtver.ru/news/proisshestviya/aferyisty-nachali-ispolzovat-dokumenty-ot-inostrannyh-reguljatorov/>
- 28) «Открыли душу и кошелёк»: десятки россиян могут лишиться жилья из-за лжеброкеров <https://kazan2024.rt.com/russia/article/1527388-moshennichestvo-investiciya-kriptovalyuta-uscherb>
- 29) На Ставрополье лжеброкеры все изощреннее обманывают своих жертв <https://rg.ru/2024/11/12/reg-skfo/investicii-v-chuzhoj-karman.html>
- 30) ЦБ рассказал о новых схемах нелегальных финансистов <https://iz.ru/1840270/2025-02-17/cb-rasskazal-o-novyh-shemah-nelegalnyh-finansistov>
- 31) В Тюменской области вынесен приговор по уголовному делу о мошенничестве в отношении пенсионеров на сумму около 1 млн рублей <https://epp.genproc.gov.ru/ru/gprf/mass-media/news/archive/e8473494/>
- 32) Прокуратура информирует (12+) <https://poisktv.ru/prokuratura-informiruet-12-132/>
- 33) В Хакасии вынесен приговор по уголовному делу о мошенничестве при проведении операций с криптовалютой <https://epp.genproc.gov.ru/ru/gprf/mass-media/news/archive/e5867113/>
- 34) Организатор криптовалютной пирамиды из Дагестана получил 4 года колонии <https://www.interfax-russia.ru/index.php/south-and-north-caucasus/news/organizator-kriptovalyutnoy-piramidy-iz-dagestana-poluchil-4-goda-kolonii>
- 35) Россиянина приговорили к 6 годам колонии за мошенничество с криптовалютой <https://www.ossetia.tv/2025/12/03/rossiyanima-prigovorili-k-6-godam-kolonii-za-moshennichestvo-s-kriptovalyutoj/>
- 36) В Якутии житель Дагестана обвиняется в кибермошенничестве на 10 млн рублей <https://1sn.ru/v-yakutii-zitel-dagestana-obvinyaetsya-v-kibermosennicestve-na-10-mln-rublej>
- 37) Житель Республики Башкортостан осуждён в Тобольске за мошенничество https://tobolsk.info/news_tob/zhitel-respubliki-bashkortostan-osuzhdjon-v-tobolske-za-moshennichestvo/
- 38) Саратовец купил на украденный миллион рублей криптовалюту и перевел главарю банды мошенников: теперь его будут судить <https://sarinform.ru/news/sud/saratovets-kupil-na-ukradennyj-million-rublej-kriptovalyutu-i-perevel-glavaryu-bandy-moshennikov-teper-ego-budut-sudit>
- 39) Перед судом в Хакасии предстанет один из организаторов мошеннической схемы по продаже криптовалюты https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/%D1%83%D0%B1%D0%BA/Publikacii_i_vistuplenija/item/66453501/?year=2025&month=7&day=7
- 40) Афера с криптовалютой ApolloX: не позволяйте "инвестиции" вас поймать <https://chat.deepseek.com/a/chat/s/389c1654-6a66-4d94-a055-fb20167d8648>
- 41) Exit scam в криптовалютах: как распознать мошенничество и защитить свои средства <https://trusteeglobal.com/ru/academy/what-is-an-exit-scam-in-cryptocurrency/>
- 42) Эксперты выявили схему мошенничества при P2P-сделках с криптовалютой <https://fomag.ru/news-stream/eksperty-vyavili-skhemu-moshennichestva-pri-p2p-sdelkakh-s-kriptovalyutoj/>
- 43) Основные мошеннические схемы инвестиций и вывода криптовалют <https://aws.okx.com/ru-learn/crypto-investment-withdrawal-scams>
- 44) Яркая реклама и фальшивые биржи — в милиции рассказали, как действуют криптомошенники <https://www.sb.by/articles/yarkaya-reklama-i-falshivye-birzhi-v-militsii-rasskazali-kak-rabotayut-kriptomoshenniki.html>
- 45) Что такое Rug Pull? <https://onekey.so/blog/ru/ecosystem/what-is-a-rug-pull/>
- 46) Мошенническая схема «Игра на бирже» <http://smoyashkul.ru/moshennicheskaya-skHEMA-igra-na-birzhe.html>
- 47) Gerolax Крипто Мошенничество - Remove Spyware & Malware with SpyHunter - EnigmaSoft Ltd <https://www.enigmasoftware.com/ru/gerolaxcryptoscam-udaleniye/>
- 48) Раскрытие 10 самых распространенных схем мошенничества <https://www.gate.com/ru/post/status/17721398>
- 49) Минус шесть миллионов рублей: как жительница Тарко-Сале попала в лапы мошенников https://vesti-yamal.ru/ru/vjesti_jamal/minus_shest_millionov_rublej_zhitelnica_tarko-sale_popalas_v_lapy_moshennikov/
- 50) Наталья Бехтерева: в схватке с кибермошенниками главное — научиться не бояться бояться <https://tass.ru/interviews/25294929>
- 51) Треугольник мошенничества: определение, примеры и анализ <https://www.bittrue.com/ru/blog/the-fraud-triangle-definition-cases-and-analysis>

- 52) Искусственный интеллект и романтические ловушки: как мошенничество с "криптовалютными ублюдками" лишает инвесторов всех сбережений <https://www.gate.com/ru/post/status/16855450>
- 53) Мошенники обманом лишили жителя Бреста крупной суммы <https://onlinebrest.by/novosti/moshenniki-obmanom-lishili-zhitelya-bresta-krupnoy-summy>
- 54) На каждого мудреца довольно простоты <https://ceur.ru/news/specproekty/na-kazhdogo-mudrecza-dovolno-prostoty/>
- 55) «Ломка наступает»: как и почему сходят с ума криптозависимые люди <https://static.ren.tv/longread/1315129-lomka-nastupaet-kak-i-pochemu-skhodiat-s-uma-kriptozavisimye-liudi>
- 56) Россиянам объяснили, как мошенники манипулируют своими жертвами <https://life.ru/p/1824401>
- 57) Новая эра криптомошенничества: как защитить себя от психологической манипуляции <https://rus.delfi.ee/statja/120394079/novaya-era-kriptomoshennichestva-kak-zashchitit-sebya-ot-psiologicheskoy-manipulyacii>
- 58) «Это крах?» Психолог объясняет, как не попасться на удочку мошенникам и как жить дальше, если попался <https://myseldon.com/ru/news/index/329015790>

Часть 3. Безопасность и анонимность — что реально работает в РФ

Глава 8. Криптокошельки без KYC: последние убежища

Вы купили криптовалюту. Обменяли рубли на USDT на бирже, выстояли под градом банковских блокировок, разобрались с налогами и готовы хранить заработанное. Но где? Оставить на бирже — довериться кастодиану, который в любой момент может заблокировать ваш аккаунт по требованию регулятора или заморозить активы из-за санкций. Перевести на кошелёк без KYC — значит взять ответственность в свои руки, но одновременно потерять «подушку безопасности» в виде службы поддержки, кнопки «забыл пароль» и возможности оспорить транзакцию. Эта глава — карта местности для тех, кто решился на второй путь.

Два мира: кастодиальные vs некастодиальные кошельки

Ключевое различие, без понимания которого невозможно говорить о безопасности, — это контроль над приватным ключом.

Кастодиальный кошелёк — это когда ваши приватные ключи хранит третья сторона: биржа, обменник или специализированный сервис (например, PGON Wallet в Telegram, который позиционирует себя как кастодиальное решение без верификации с поддержкой девяти монет и выводом на карту через СБП за 5% комиссии). Вы видите баланс в интерфейсе, можете нажимать кнопки «отправить» и «получить», но настоящий контроль — у сервиса. Преимущество такой модели очевидно: забыли пароль — обратились в саппорт, взломали — возможно, вернут средства. Недостатки перечислены в предыдущих главах: блокировка по KYC/AML, заморозка активов, санкционные ограничения, запросы от ФНС.

Некастодиальный кошелёк — прямая противоположность. Приватные ключи хранятся только у вас, на вашем устройстве. Никто — ни биржа, ни государство, ни сам создатель кошелька — не может заблокировать транзакцию или заморозить активы. Это и есть та самая «финансовая свобода», о которой говорят криптоэнтузиасты. Но у неё есть цена: потеряли сид-фразу — потеряли всё, безвозвратно, навсегда. Никакой службы поддержки, никакого «восстановить доступ по паспорту». В 2025 году некастодиальные кошельки предотвратили потенциальные убытки пользователей на сумму более 2 миллиардов долларов, по данным Messari. Но лишь при условии, что пользователь сам не стал причиной утраты.

Для тех, кто ищет промежуточный вариант, существуют так называемые «гибридные» решения вроде SimpleHold или Zengo. Они предлагают встроенные DEX-функции с поддержкой более 70-120 токенов, не требуют KYC и при этом частично сохраняют удобство централизованных сервисов. Однако эксперты сходятся во мнении: универсального победителя не существует — «ни один кошелек не выигрывает всё».

Сравнение популярных некастодиальных кошельков

Рассмотрим три кошелька, которые чаще всего фигурируют в дискуссиях о приватности.

Trust Wallet — пожалуй, самый популярный мультивалютный кошелек, официальный партнёр Binance. Поддерживает более 70 блокчейнов, удобен для повседневных операций, интегрирован с DeFi и dApps. Но именно его универсальность оборачивается уязвимостью. Каждое взаимодействие со смарт-контрактом — потенциальная точка входа для атаки. Trust Wallet идеален как «горячий» кошелек для оперативных сумм, но хранить на нём весь капитал — всё равно что носить зарплату в заднем кармане джинсов на прогулке по рынку. Его главный недостаток — отсутствие встроенных механизмов приватности: любая транзакция с вашего адреса видна в блокчейне и легко связывается с другими адресами через кластеризацию. При этом сам кошелек не блокирует россиян: «некастодиальные решения работают как программа — никто не может "выключить" доступ к вашим средствам». По состоянию на начало 2026 года Trust Wallet и MetaMask не требуют KYC «вообще никаких».

Cake Wallet — мобильный кошелек с открытым исходным кодом, ориентированный на Monero (XMR). Это выбор тех, кто осознанно стремится к приватности. В отличие от Trust Wallet, Cake Wallet изначально проектировался для работы с анонимной криптовалютой: он поддерживает кольцевые подписи Monero, скрытые адреса и технологию Bulletproofs, которые делают невозможным определение отправителя, получателя и суммы транзакции. Monero — это приватность по умолчанию, а не опционально, как в Zcash. Важное преимущество Cake Wallet — встроенный обменник, позволяющий конвертировать биткоин в XMR и обратно без KYC. Однако у этой модели есть существенный минус: само использование Monero в России 2026 года находится под пристальным вниманием. Регулятор может расценить факт владения XMR как косвенное доказательство намерения скрыть финансовую активность — а это уже потенциальный состав по статье 174 УК.

Samourai Wallet — легендарный биткоин-кошелёк для Android, созданный с маниакальным фокусом на приватность. Открытый исходный код, встроенная поддержка Tor и VPN для сокрытия IP-адреса, технология CoinJoin (пул Whirlpool) для смешивания транзакций, скрытые адреса, защита от кластеризации через Ricochet — дополнительные «прыжки» транзакции, чтобы запутать следы. Разработчики описывали свою миссию так: «Мы строим то, что Кремниевая долина не выпустит, регуляторы не благословят, а венчурный капитал не профинансирует».

Именно эта философия и привела к финалу. В апреле 2024 года Министерство юстиции США предъявило обвинения создателям Samourai Wallet Кеонну Родригесу и Уильяму Хиллу: власти утверждали, что сервис способствовал отмыванию более 100 миллионов долларов преступных доходов и действовал как нелегальный сервис денежных переводов. Основатели были арестованы, а сам Samourai Wallet прекратил существование. Позднее вскрылся меморандум Минюста, признававший, что «законность сервисов крипто-микширования не полностью урегулирована действующим законодательством и что эти инструменты не являются inherently illegal». Сам факт этого документа говорит о том, что граница между законной приватностью и преступным отмыванием не определена до конца. Но для пользователя из России это слабое утешение: если американский Минюст смог арестовать разработчиков, то российские правоохранители могут арестовать пользователя.

Некастодиальный кошелёк — не гарантия безопасности

Важно понимать: отсутствие KYC не означает отсутствие рисков. Некастодиальный кошелёк лишь передаёт полную ответственность пользователю, не снимая угрозы взлома или фишинга. Поддельные приложения MetaMask, Trust Wallet и других популярных кошельков в магазинах приложений и на фишинговых сайтах — массовое явление, о котором мы подробно говорили в Главе 7. Злоумышленники копируют интерфейс и после ввода сид-фразы мгновенно опустошают кошелёк.

Кроме того, любой некастодиальный кошелёк — это программное обеспечение с открытым или закрытым исходным кодом, которое может содержать уязвимости. Пользователь, скачавший обновление с вредоносным кодом или подключивший свой кошелёк к поддельному смарт-контракту, теряет средства так же необратимо, как если бы он хранил их на бирже-однодневке. Разница лишь в том, что в случае с биржей можно подать в суд, а в случае с утерянным приватным ключом — некого.

Почему VPN и Tor не скроют вас от ФНС

Самый распространённый совет в интернете: «Включи VPN или Tor — и твои криптооперации никто не отследит». Это опасное упрощение.

VPN и Tor скрывают ваш IP-адрес от провайдера и от сайтов, к которым вы обращаетесь. Это эффективная защита от массовой слежки на сетевом уровне. Однако блокчейн-транзакция не содержит IP-адреса отправителя. Блокчейн фиксирует только адрес кошелька, сумму и временную метку. Скрывая свой IP через VPN, вы прячете действие, которое и так не записывается напрямую в блокчейн.

При этом VPN может вас выдать. Chainalysis и аналогичные системы блокчейн-аналитики помечают транзакции, исходящие с IP-адресов, принадлежащих VPN-сервисам или юрисдикциям высокого риска, как «красные флаги» для комплаенс-проверок. Если вы используете популярный коммерческий VPN, ваш трафик с высокой вероятностью будет маркирован как подозрительный.

Ещё опаснее — ложное чувство безопасности. Самая надёжная защита сетевого уровня бессильна против главного механизма деанонимизации: момента «входа в систему с паспортом». Как только вы хотя бы раз вывели криптовалюту на банковскую карту, привязанную к вашему паспорту, или пополнили счёт на бирже с верификацией, ваш адрес в блокчейне оказывается связан с вашей личностью — и дальше аналитическая система прослеживает всю цепочку транзакций от этого адреса, вплоть до его создания. VPN тут не поможет.

Tor — более серьёзный инструмент, маршрутизирующий трафик через несколько случайных узлов. Но и он не панацея. Во-первых, выходные узлы Tor могут контролироваться спецслужбами, и трафик, проходящий через них, может быть перехвачен. Во-вторых, сам факт использования Tor — «красный флаг» для комплаенс-систем. В-третьих, метаданные (размер транзакции, время, паттерны использования) позволяют деанонимизировать вас без расшифровки трафика. Наконец, как и в случае с VPN, блокчейн-аналитика обходит сетевые уровни защиты и работает непосредственно с публичным реестром транзакций.

Как блокчейн-аналитика вычисляет ваши паспортные данные

Главный тезис: блокчейн — это не анонимная, а псевдонимная среда. Ваш биткоин-адрес — не имя, а цифровой псевдоним. Но стоит один раз связать его с реальной личностью — и вся история операций с этого адреса становится вашей кредитной историей, выложенной в открытый доступ.

Российская Федеральная налоговая служба и Росфинмониторинг используют для этого «Прозрачный блокчейн» — систему, разработанную совместно с Физическим институтом имени Лебедева и внедрённую в рамках федерального проекта «Искусственный интеллект». Бюджет разработки превысил 760 млн рублей. Система анализирует блокчейн биткоина и ещё более 30 криптовалют, выявляет связи между криптовалютными транзакциями и банковскими переводами жителей России и СНГ и формирует базу «серых адресов», в которой на начало 2025 года насчитывалось свыше 19 тысяч записей. С её помощью было проведено 120 расследований и возбуждено 60 уголовных дел, включая дела о заказных убийствах, оплаченных криптовалютой, и о финансировании террористических актов.

Как именно работает деанонимизация? Когда вы регистрируетесь на Binance или Bybit, вы загружаете скан паспорта, привязываете номер телефона и банковскую карту. Этот пакет данных — ваше «KYC-досье» — хранится у биржи. Когда вы выводите средства с биржи на некастодиальный кошелёк, в блокчейне остаётся запись: адрес биржи → ваш адрес. Комплаенс-система сопоставляет открытую блокчейн-запись и данные из KYC-досье — и адрес деанонимизирован. После этого аналитический сервис вроде КоинКит объединяет тысячи транзакций в кластеры, визуализирует цепочки перемещений и находит закономерности: повторяющиеся суммы, паттерны времени, общие адреса-узлы, мосты и миксеры. Современные AML-сервисы (Crystal Blockchain, Elliptic, Chainalysis) присваивают каждому адресу оценку риска, а метаданные — IP-адреса, геолокация, телефон, устройство — довершают картину. ФНС в 2024 году массово запросила данные о криптооперациях у Binance и OKX, и даже вывод средств через P2P больше не гарантирует анонимность.

К 2025 году ФНС планировала подключить к «Прозрачному блокчейну» все российские банки. Взаимодействие трёх источников — банковских выписок, блокчейн-транзакций и данных от бирж — замыкает контур, в котором каждая операция, от майнинга до вывода в рубль, может быть отслежена и идентифицирована.

Практические стратегии для разных сценариев

Если ваша цель — инвестиции и накопление. Используйте аппаратный кошелёк (о них — в Главе 10). Храните сид-фразу на бумаге в надёжном месте. Для оперативных операций держите Trust Wallet с ограниченной суммой, но основной капитал уводите в холодное хранение.

Если ваша цель — максимальная приватность. Рассмотрите Cake Wallet для Monero. Но учитывайте: в России использование XMR может привлечь внимание регулятора. Если вы выбираете биткоин, используйте несколько адресов для разных целей, избегайте их пересечения и никогда не выводите средства напрямую с «приватного» адреса на биржу с вашим паспортом — это одномоментно деанонимизирует всю цепочку.

Если ваша цель — повседневные расчёты. Trust Wallet или MetaMask. Не храните на них больше суммы, которую готовы потерять. Регулярно проверяйте, что вы не давали разрешений сомнительным смарт-контрактам, и никогда не вводите сид-фразу на сайтах, открытых по ссылке из письма или мессенджера.

Общее правило для всех сценариев: диверсифицируйте хранение. Разделите активы между горячим кошельком (повседневные суммы), холодным кошельком (основной капитал) и «смертным» кошельком (пустой адрес, который вы готовы показать под принуждением). Подробнее об этой модели — в Главе 16.

Вывод из Главы 8

Некастодиальные кошельки без KYC остаются последним убежищем финансовой приватности в России, но это убежище — не крепость с непробиваемыми стенами, а скорее лес, в котором укрывшийся невидим, если знает, как не оставлять следов на земле. Каждый вывод средств на верифицированную карту, каждый вход на централизованную биржу под своим паспортом — это след, который рано или поздно приведёт к вашей личности. VPN и Tor защищают от массовой слежки, но не от целенаправленного расследования с использованием блокчейн-аналитики.

Выбор кошелька — лишь первый шаг. Дальше начинается территория, где приватность достигается не столько технологиями, сколько дисциплиной. О том, как работают миксеры, Monero и другие инструменты запутывания следов, которые мы лишь упомянули вскользь, — следующая глава.

Использованные в главе источники:

- 1) Обзор кошелька Samourai: биткоин-кошелек для конфиденциальных транзакций <https://coinspot.io/en/technology/deep-look-at-samourai-wallet-for-bitcoin-privacy-first-android-app/>
- 2) Кошелек Samourai — обзоры и характеристики <https://www.cryptocompare.com/wallets/samourai>
- 3) Анонимные криптокошельки: лучшие варианты и руководство на 2025 год <https://ecos.am/en/blog/anonymous-crypto-wallets-best-options-and-guide-for-2025?srsId=AfmBOoov4r450NP8fg3ptv-FOpVW7GgVMBzceUs793ykpQ27l2rGfG->
- 4) Samourai Wallet - Google Play <https://samourai-wallet.apps112.com/>
- 5) Samourai Wallet - Wikipedia https://en.wikipedia.org/wiki/Samourai_Wallet
- 6) Гид по выбору криптокошельков в 2025 году для новичков <https://tenchat.ru/media/3895155-gid-po-vyboru-kriptokoshelkov-v-2025-godu-dlya-novichkov>
- 7) Анонимные криптокошельки: лучшие варианты и условия для 2025 года <https://ecos.am/de/blog/anonyme-kryptokoshelki-die-besten-optionen-und-anleitungen-fur-2025>
- 8) Полная анонимность: в Samourai Wallet добавлена поддержка формата bech32 и механизма STONEMASK <https://tgstat.ru/channel/@criptogazeta/446>
- 9) Trust Wallet <https://finswin.com/operatsii/bags/trust-wallet.html>
- 10) Samourai Wallet – обзор мобильного биткоин-кошелька с повышенной конфиденциальностью <https://profinvestment.com/samourai-wallet/>
- 11) Криптокошелёк для России в 2026 году: какие работают, как вывести на карту и что выбрать новичку <https://dtf.ru/howto/4895779-kriptokoshelki-dlya-rossii-2026>
- 12) Где хранить крипту без верификации кошелька в 2026 <https://vc.ru/life/2879369-gde-hranit-kriptoalyutu-bez-verifikatsii-koshelka>
- 13) Постоянные запросы на доплату и блокировка средств <https://www.sikayetvar.com/ru/metamask-ru/metamask-postoannye-zaprosy-na-doplatsu-i-blokirovka-sredstv>
- 14) Список 15 криптокошельков 2026, не блокирующих активы из-за санкций <https://profinvestment.com/cryptocurrency-wallets-not-block-russians/>
- 15) Как импортировать Trust Wallet в MetaMask? Пошаговая инструкция: 2 метода <https://bytwork.com/articles/trust-wallet-v-metamask>
- 16) Безопасные переводы в Германию из России и обратно: полная инструкция на 2026 год <https://www.sostav.ru/blogs/286884/80239>
- 17) Лучшие криптокошельки в 2026 году: рейтинг для России и как выбрать <https://dtf.ru/flood/4919022-kriptokoshelki-dlya-rossii-v-2026-godu-kak-vybrat-luchshiy-variant>
- 18) Злоумышленники используют новую уловку для кражи криптовалюты у пользователей MetaMask <https://www.itsec.ru/news/zloushislenniki-ispolzuyut-novuyu-ulovku-dlia-krazhi-kriptoaluti-u-polzovateley-metamask>
- 19) Россиянам запретили пользоваться криптовалютой в ... <https://meduza.io/cards/rossiyanam-zapretili-polzovatsya-kriptoalyutoy-v-evrope-a-eto-kasaetsya-vseh-vseh-bez-isklyucheniy-nakopleniya-teper-nikak-ne-vyvesti>
- 20) 11 криптокошельков, которые реально работают в России: тест за Q1 2026 <https://vc.ru/life/2852944-kriptokoshelki-dlya-rossii>
- 21) Конфиденциальность против удобства: какой анонимный кошелек биткойн на самом деле подходит вам? <https://www.gate.com/ru/post/status/16392790>
- 22) Криптовалютные биржи, не требующие прохождения процедуры KYC: Ежегодный рейтинг 2025-2026 гг. <https://web.gate.it/zh-tw/crypto-wiki/article/no-kyc-cryptocurrency-exchanges-2025-2026-rankings-20260201>
- 23) Торговля с плечом без идентификации: лучшие платформы и основы безопасности кошелька <https://onekey.so/blog/ru/ecosystem/no-id-margin-trading-hacks-best-platforms-and-wallet-security-essentials/?srsId=AfmBOoq4EO1ndmdEicHxmqrW9BnRrAeCO5cudjG1DsRcOT-fHCMttB8U>
- 24) support@kycspot.cc (Все сообщения пользователя) <https://www.1nep.ru/forum/user/35134/post/all/>
- 25) Некастодиальный кошелек больше не гарантия безопасности средств https://ru.monoup.com/mono_talks/articles/Nekastodialnyy-koshelek-bolshe-ne-garantiya-bezopasnosti-sredstv?a=427
- 26) Интерактивные брокеры: перевод криптовалюты на аппаратный кошелек без верификации KYC в 2026 году <https://onekey.so/blog/ru/ecosystem/interactive-brokers-crypto-to-hardware-wallet-transfer-without-kyc-verification-2026/?srsId=AfmBOooliTzGfyTmIgtEAsPRAAgOPZoU9-5BrLP0hnrV2IHpTmj9y73Z>
- 27) Криптовалютные биржи без KYC: руководство по юридическим рискам, безопасности и соблюдению нормативных требований 2025 года <https://www.bitget.com.vn/academy/no-kyc-crypto-exchan>

- 28) Руководство по массовому переводу USDT с Bybit на холодный кошелек без KYC по низкоследовой цепочке в 2026 году https://onekey.so/blog/ru/ecosystem/bybit-usdt-to-cold-wallet-no-kyc-bulk-transfer-guide-2026-low-trace-chain/?srsltid=AfmBOooqneA0Q4r_aL0kEuU_Q6T2bZrX4pPNw2i8Vv90YPU5zQo6OC8p
- 29) Какие криптокошельки действительно защищают вашу приватность? <https://dev.to/safewallet/kakiie-kriptokoshelki-dieistvitelno-zashchishchaiut-vashu-privatnost-1bbb>
- 30) KYCNOT.cc - Анонимный обмен криптовалют без KYC / AML с гарантией чистоты монет <https://www.1nep.ru/forum/forum13/topic1906/>
- 31) «Совершенно не сообщают»: можно ли скрыть преступление в интернете <https://m.5-tv.ru/news/462871/sovershenno-nesoobrazaut-kak-skryt-prestuplenie-v-internete/>
- 32) Могут ли ваш интернет-провайдер или правительство видеть ваши криптовалютные сделки? <https://www.purevpn.com/blog/can-your-isp-or-government-see-your-crypto-trades/>
- 33) Is trading on Bitmex over a VPN a crime for US traders? <https://bitcointalk.org/index.php?topic=5241166.msg54759525#msg54759525>
- 34) Российские власти начали войну с сайтами в сети Tor https://safe.cnews.ru/news/top/rossijskie_vlasti_nachali_vojnu_s_sajtami
- 35) Скрыть преступление в интернете стало невозможно <https://19rusinfo.ru/politika/58559-skryt-prestuplenie-v-internete-stalo-nevozmozhno>
- 36) Отслеживание биткойн-транзакций: проблемы для правоохранительных органов <https://www.gate.com/zh-tw/post/status/14040100>
- 37) Как Chainalysis помогает командам по обеспечению соответствия требованиям противодействовать санкциям <https://www.chainalysis.com/blog/fincen-russia-sanctions-red-flags-chainalysis/>
- 38) Российские майнеры биткоинов опасаются санкций, поскольку правительство начало собирать адреса кошельков https://www.binance.me/sv/square/post/19983762131698?_cf_chl_rt_tk=Wo9T4eh_bdYjBohctdlvnUtEI3Ah2owTACq.VwXHiBQ-1777081618-1.0.1.1-pGfbmAuL4Kxq_cQzP0AfvSmfv1oq2x0HxiCQssKNdA8
- 39) Блокчейн следит за вами: мифы об анонимности криптовалют <https://bithide.io/blog/ru/security/why-blockchain-and-crypto-are-not-anonymous/#contents-0>
- 40) Избегай крадущейся твари <https://by.tgstat.com/en/channel/@cryptobelarusik/791>
- 41) В традициях Большого брата. Как “Прозрачный блокчейн” следит за тобой <https://getblock.net/research/it-is-the-one-how-the-transparent-blockchain-de-anonymizes-crypto-users>
- 42) Мониторинг блокчейна Kaiko <https://www.kaiko.com/products/blockchain-monitoring>
- 43) Можно ли отследить биткойн? Всё, что вам нужно знать <https://www.mexc.com/ru-RU/learn/article/is-bitcoin-traceable-everything-you-need-to-know/1>
- 44) Как расследования раскрывают KYC анонимных криптомошенников: роль on-chain аналитики и AML инструментов <https://vc.ru/crypto/2290667-rassledovaniya-kyc-anonimnykh-kryptomoshennikov-on-chain-analitika-i-aml>
- 45) Отслеживается ли Биткойн? Понимание приватности и прозрачности в криптовалютах <https://ecos.am/ru/blog/otslezhivaetsya-li-bitkoin-ponimanie-privatnosti-i-prozrachnosti-v-kriptovalyutah>
- 46) Как отследить биткойн: методы деанонимизации транзакций <http://forensicanvil.ru/blog/bitcoin-tracking-deanonymization/>
- 47) WildVis <https://wildvisualizer.com/conversation/wildchat/2401908>
- 48) Приложения в Google Play – Blockchair: Block Explorer <https://play.google.com/store/apps/details?id=com.bdc.blockchair.app&hl=ru>
- 49) Использование блокчейн-аналитики для улучшения пользовательского опыта в криптосфере <https://coinkyt.com/article/ispolzovanie-blokchejn-analitiki-dlya-uluchsheniya-polzovatel'skogo-opyta-v-kriptosfere>
- 50) Как следят за каждым вашим платежом в крипте <https://bemining.ru/posts/kak-sledyat-za-kazhdym-vashim-platezhom-v-kripte-1762666860>
- 51) P2P-сделки под прицелом налоговой: как работать с криптовалютой в 2025 <https://companies.rbc.ru/news/A31i8H5UiE/p2p-sdelki-pod-pritselom-nalogovoj-kak-rabotat-s-kriptoalyutoj-v-2025/>
- 52) Как правильно вести учет и формировать налоговые отчеты в 2025 году <https://companies.rbc.ru/news/93T3aaTmaW/kak-pravilno-vesti-uchet-i-formirovat-nalogovyye-otchetiy-v-2025-godu/>
- 53) P2P-сделки под прицелом налоговой: как работать с криптовалютой в 2025 <https://myseldon.com/ru/news/index/334529414>
- 54) Налогоплательщикам в прямом эфире рассказали об особенностях операций с цифровой валютой <https://www.nalog.gov.ru/rn64/news/smi/16052258/print/>

- 55) ФНС начала публиковать курсы криптовалют <https://expert.ru/news/fns-nachala-publikovat-kursy-kriptoalyut/>
- 56) Минфину передадут контроль за оборотом цифровой валюты <https://pravo.ru/news/259637/>
- 57) Профессор Шайхразеева: в России усиливается контроль за цифровыми активами <https://www.osnmedia.ru/ekonomika/professor-shajhrazeeva-v-rossii-usilivaetsya-kontrol-za-tsifrovymi-aktivami/amp/#>
- 58) CRYPTO SUMMIT 2025 <https://anpzenit.ru/crypto-summit-2025-2/>
- 59) Дата-центры будут передавать данные о российских майнерах криптовалют <https://ru.investing.com/news/cryptocurrency-news/article-2852440>
- 60) ФНС запустила новый сервис для работы с криптовалютами <https://xn--90aivcdt6dxbc.xn--p1ai/articles/news/fns-zapustila-novyy-servis-dlya-raboty-s-kriptoalyutami/>
- 61) Узнайте о 10 самых привлекательных для конфиденциальности криптовалютах 2025 года и о том, как их использовать <https://www.facebook.com/BitPinas/posts/%EF%B8%8F%EF%B8%8F-discover-the-top-10-privacy-coins-of-2025-and-how-their-stealth-tech-hides-you/1305191194954091/>
- 62) Многообразие сатоши: CoinJoin, PayJoin, бесшумные платежи или миксеры — что выбрать в 2025 году? <https://forklog.com/en/the-many-faces-of-satoshis-coinjoin-payjoin-silent-payments-or-mixers-what-to-choose-in-2025/>
- 63) Топ-10 частных токенов 2025: нейтральный обзор <https://phemex.com/ru/blogs/top-privacy-tokens-2025-december>
- 64) Топ-10 самых анонимных криптовалют в 2025 году <https://vc.ru/crypto/1250175-top-10-samyh-anonimnyh-kriptoalyut-v-2025-godu>
- 65) Новый вид малярной ленты сэкономит аэрокосмической отрасли миллионы <https://taperite.com/a-new-kind-of-masking-tape-will-save-the-aerospace-industry-millions/>
- 66) Криптовалюты с повышенным уровнем ... <https://coinspaidmedia.com/ru/learn/privacy-oriented-cryptocurrencies-what-are-they/>
- 67) Какой криптокошелек выбрать: обзор вариантов и тест <https://ru.beincrypto.com/learn/obzor-samyh-populyarnyh-kriptoalyutnyh-koshelkov/>
- 68) Как выбрать надёжный обменник криптовалюты: 7 признаков проверенного сервиса <https://keine-exchange.com/news/>
- 69) Монеро (XMR) против Биткоина (BTC): конфиденциальность, производительность и динамика рынка в 2025 году <https://www.mexc.io/crypto-pulse/article/monero-xmr-vs-bitcoin-btc-39588>
- 70) В конкурентном анализе рынка Монеро (XMR) обладает уникальными преимуществами в плане конфиденциальности по сравнению с Bitcoin и Ethereum, но все еще отстает от них по уровню принятия на рынке и зрелости экосистемы <https://www.gt-io.com/zh/crypto-wiki/article/how-does-monero-xmr-compare-to-bitcoin-and-ethereum-in-competitive-market-analysis-20251223>
- 71) Новости о биткоине сегодня: инвесторы оценивают преимущества Монеро в плане конфиденциальности на фоне борьбы криптовалют за прозрачность <https://www.bitget.site/news/detail/12560604934544>
- 72) <https://www.gate.tv/tr/crypto-wiki/article/monero-xmr-privacy-in-the-age-of-financial-surveillance>
- 73) Монеро лучше, чем Bitcoin? Понятное сравнение для новичков в мире криптовалют <https://www.mexc.io/crypto-pulse/article/is-monero-better-than-bitcoin-a-clear-comparison-for-crypto-beginners-41721>
- 74) Тенденции рынка Web3 и инвестиционные руководства <https://www.bydfi.com/en-za/cointalk?relatedId=1192899417779212288>
- 75) Биткоин против Монеро: всестороннее сравнение для инвесторов <https://komodoplatfom.com/en/academy/bitcoin-vs-monero/>
- 76) Почему Zcash превосходит Монеро и даже Bitcoin: мнение научного сотрудника Массачусетского технологического института <https://www.mexc.com/news/124964>
- 77) Почему мобильные кошельки для обеспечения конфиденциальности важны — и как на самом деле оставаться анонимным в дороге <https://bigdataweek.com/blog/2025/06/07/why-mobile-privacy-wallets-matter-and-how-to-actually-stay-anonymous-on-the-go/>

Глава 9. Миксеры и XMR — работают или нет после блокировок?

На протяжении нескольких лет в криптосообществе существовала иллюзия, что анонимность транзакций — это просто ещё одна функция, которую можно включить по желанию. Нужно скрыть происхождение биткоинов — отправляешь их в миксер. Хочешь полной конфиденциальности — покупаешь Monero. Государственные органы, как считали многие, останутся где-то позади, не в силах проникнуть сквозь эту криптографическую завесу. Однако 2025 год наглядно показал, что эта иллюзия больше не работает. Правоохранительные системы разных стран, включая Россию, научились не только отслеживать такие транзакции, но и привлекать к ответственности их организаторов и пользователей.

Эта глава развеивает мифы о неуязвимости криптографической анонимности через призму трёх знаковых кейсов: разрома биткоин-миксера Bitcoin Fog, анализа реального уровня приватности Monero и изучения российского рынка «сервисов очистки».

Разгром миксера Bitcoin Fog и его последствия для России

История Романа Стерлингова, создателя Bitcoin Fog, стала поворотным моментом в борьбе с теневыми финансовыми потоками в криптовалюте. Приговор, вынесенный в 2025 году, на годы вперед определил, как правоохранительные органы по всему миру будут квалифицировать деятельность операторов подобных сервисов.

Дело Романа Стерлингова: 12,5 лет за «крипто-стирку». Суд в США признал Романа Стерлингова, гражданина России и Швеции, виновным в отмывании десятков миллионов долларов, полученных преступным путем, в частности от продажи наркотиков в даркнете. Его сервис Bitcoin Fog был одним из старейших и крупнейших миксеров в даркнете. За свою деятельность он был приговорен к 12,5 годам лишения свободы. Общая сумма отмывтых средств, по данным следствия, составила около 400 миллионов долларов за десятилетие работы сервиса — с 2011 по 2021 год.

Несмотря на суровость приговора, защита Стерлингова немедленно начала процесс обжалования, и в сентябре 2025 года была подана апелляция. В 139-страничном документе адвокаты указали на ряд серьезных процессуальных нарушений и нестыковок в деле. Ключевой аргумент защиты состоял в том, что «Стерлингов был осужден в неконституционном порядке,

исключительно на основании косвенных доказательств и домыслов...», а сам приговор был вынесен «за якобы имевшее место отмывание денег конечными пользователями Bitcoin Fog». Более того, защита обратила внимание на принципиальный факт: в конечном счете американский Минюст отказался от преследования администраторов криптомиксеров, которые «сами по себе существуют в правовом поле», за действия их пользователей. Этот нюанс создает важнейший прецедент: сам по себе инструмент не всегда является преступлением, но его использование в незаконных целях — безусловно.

Дело Сэмюрая: целенаправленная охота на анонимность. Вторым громким процессом, который окончательно сформировал правовой ландшафт, стало дело создателей биткоин-кошелька Samourai Wallet со встроенной функцией микширования Whirlpool. Основатели сервиса Кионн Родригес и Уильям Лонерган Хилл были арестованы в апреле 2024 года. Им были предъявлены обвинения в управлении нелегальным бизнесом по переводу денег и в отмывании средств. В августе 2025 года они признали свою вину и согласились на конфискацию 237,8 миллиона долларов — общей суммы криминальных средств, отмытых через их платформу. По информации следствия, через сервис прошло более 80 000 биткоинов (на сумму более 2 миллиардов долларов), а комиссии принесли основателям от 4,5 до 6 миллионов долларов. В ноябре 2025 года суд вынес приговор: CEO компании Кионне Родригес получил 5 лет, а технический директор Уильям Хилл — 4 года тюремного заключения.

Прокуроры подчеркивали, что создатели Samourai не были пассивными наблюдателями, а намеренно продвигали свой сервис как инструмент для отмывания преступных доходов. Они публично призывали хакеров использовать Samourai для сокрытия доходов от взломов. По версии обвинения, через платформу прошло не менее 237 миллионов долларов от торговли наркотиками в даркнете, кибератак и мошенничества.

Последствия для российских пользователей. Эти процессы имеют прямое отношение к любому российскому пользователю, который задумывается об использовании миксеров. Дела Bitcoin Fog и Samourai Wallet четко обозначили: правоохранные органы научились не только вычислять операторов таких сервисов, но и успешно проводить сложные трансграничные расследования. Для россиян это означает, что использование миксера для сокрытия происхождения средств почти гарантированно привлечет внимание Росфинмониторинга, если эти средства когда-либо коснутся российской банковской системы. Как заявили в

ведомстве, анонимность криптовалютных транзакций — «не больше, чем миф».

Стоит подчеркнуть, что использование миксеров само по себе не всегда преступно, но в России оно создает крайне высокие риски блокировки счетов и уголовного преследования, поскольку автоматически классифицирует вас как «подозрительного» участника в глазах банковского комплаенса.

Monero (XMR) — действительно ли он не отслеживается?

На фоне разгрома биткоин-миксеров Monero (XMR) для многих стал главной альтернативой — криптовалютой, где анонимность встроена на уровне протокола, а не обеспечивается внешними сервисами. Но действительно ли она не отслеживается?

Как работает приватность Monero. Архитектура приватности Monero построена на нескольких уровнях, каждый из которых скрывает часть данных о транзакции. Первый уровень — кольцевые подписи, маскирующие отправителя путем объединения его транзакции с несколькими фиктивными, что делает «невозможным» вычислить настоящий адрес отправителя. Второй уровень — скрытые адреса: одноразовые публичные ключи, генерируемые для каждой операции и исключающие возможность связывания транзакций с получателем. Третий уровень — скрытые суммы транзакций, исключающие анализ движения средств. В довершение ко всему, Dandelion++ помогает скрыть IP-адрес отправителя при отправке транзакции. Такая многоуровневая система гарантирует, что монеты XMR нельзя связать с прошлой историей переводов — свойство, называемое взаимозаменяемостью.

Благодаря этому суточный объем транзакций Monero в 2025 году достиг 90,51 млн долларов, капитализация составила около 7,36-8,08 млрд долларов, а ежедневно проводится более 26 тысяч транзакций.

Можно ли отследить Monero на практике? Несмотря на всю криптографическую защиту, Monero не дает 100-процентной гарантии анонимности. В 2024 году Национальное бюро расследований Финляндии сумело отследить транзакции Monero (XMR), связанные с хакером Юлиусом Кивимяки, что помогло собрать доказательства для его обвинения в суде. Как это было сделано? Ключевую роль сыграл анализ «инфраструктурных паттернов». Когда хакер выводил средства через централизованные биржи или конвертировал XMR обратно в фиатные деньги, правоохранительные органы могли сопоставить время и объемы транзакций с данными интернет-провайдеров и бирж.

Более того, анализ временных паттернов и метаданных за пределами блокчейна также может деанонимизировать пользователя. Другими словами, сам протокол Monero остается в основном устойчивым к стандартным методам анализа (по данным TRM Labs), но это не спасает от комплексного расследования, где данные из разных источников накладываются друг на друга.

Правовой статус Monero в России. С юридической точки зрения, в России Monero формально не запрещен. Закон не запрещает владеть или передавать анонимные криптовалюты, но требует соблюдения налоговых обязательств и декларирования доходов. Однако, как отмечают эксперты, использование Monero может столкнуться с законодательными ограничениями, связанными с борьбой с отмыванием денег. Главный риск — не прямой запрет, а презумпция виновности. Если налоговые или правоохранительные органы обнаружат у вас операции с Monero, это почти наверняка станет поводом для углубленной проверки с потенциально катастрофическими последствиями для ваших банковских счетов и свободы.

Российские сервисы очистки крипты: миф или реальность

С ростом давления на традиционные миксеры и усилением контроля за криптотранзакциями в России начал формироваться рынок так называемых «сервисов очистки». Их реклама обещает клиентам полную анонимность, «чистую» криптовалюту и отсутствие каких-либо рисков. Стоит ли им верить?

Как работает «Прозрачный блокчейн» Росфинмониторинга. Для начала нужно понять, с каким уровнем контроля сталкиваются подобные сервисы. С 2021 года Росфинмониторинг использует собственную систему отслеживания криптотранзакций под названием «Прозрачный блокчейн». Эта система анализирует блокчейны более 30 криптовалют, выявляет связи между адресами и оценивает их риски. Ее эффективность подтверждена на практике: только в 2025 году сервис был использован при проведении 120 финансовых расследований и возбуждении более 40 уголовных дел по отмыванию преступных доходов.

В декабре 2025 года стало известно о планах Росфинмониторинга создать специализированный реестр «подозрительных» криптокошельков. Система будет аккумулировать данные, поступающие от банков, налоговой службы, МВД и спецслужб, и в режиме реального времени отслеживать движение средств по таким адресам. Количество уголовных дел с оборотом криптовалюты, возбуждаемых по материалам ведомства, ежегодно растет.

Почему «российские сервисы очистки» — это миф. Главное, что нужно понять: рынок «сервисов очистки» криптовалют в России — это в подавляющем большинстве случаев мошенничество. Практически все предложения «очистить биткоин» или «обеспечить анонимность» можно разделить на три категории:

1. **Прямое мошенничество.** Жертва переводит криптовалюту на кошелек «сервиса», и деньги просто исчезают. Классический exit scam.
2. **Псевдо-миксеры с завышенными комиссиями.** Сервис действительно может смешать средства, но с комиссией в 10-20% и без каких-либо гарантий сохранности.
3. **Инструменты под колпаком.** Сервис, созданный или контролируемый правоохранительными органами для выявления участников теневых финансовых схем.

Правовое регулирование криптовалют в России до сих пор окончательно не сформировано. Рынок «де-факто существует, но де-юре остается в правовом вакууме». Это означает, что любой, кто обращается к подобным сервисам, работает в «серой» зоне без какой-либо правовой защиты.

В 2025 году было выявлено более 5,7 тысяч финансовых пирамид и псевдоброкеров, многие из которых маскировались под «сервисы очистки». Регулятор направил информацию о всех этих проектах в правоохранительные органы, что привело к возбуждению более 440 административных дел.

Вывод из Главы 9

1. **Эпоха анонимных миксеров закончилась.** Приговоры по делам Bitcoin Fog и Samourai Wallet показали, что создатели инструментов анонимизации несут ответственность за их использование. В России «Прозрачный блокчейн» и создаваемый реестр подозрительных кошельков делают использование миксеров крайне рискованным.
2. **Monero — мощный, но не абсолютный инструмент.** Криптографические протоколы Monero делают прямое отслеживание транзакций невозможным, однако комплексный анализ метаданных (IP-адреса, связь с биржами, временные паттерны) позволяет деанонимизировать пользователя. В России Monero формально не запрещен, но его использование — это «красный флаг» для любого банка или госоргана.
3. **Российские сервисы очистки крипты — миф.** В подавляющем большинстве случаев это либо прямое мошенничество, либо инструменты, контролируемые государством. Риск потери средств или уголовного преследования перевешивает любые обещанные выгоды.

Подлинная финансовая приватность сегодня требует не столько технологических уловок, сколько глубокого понимания правового поля и готовности работать в его рамках. В следующей главе мы рассмотрим, как защитить свои активы с помощью аппаратных кошельков и как вести себя в случае попытки их конфискации со стороны государства.

Использованные в главе источники:

- 1) 12,5 лет за крипто-стирку: создатель Bitcoin Fog осужден за отмывание миллионов! <https://www.ossetia.tv/2025/12/02/12-5-let-za-kripto-stirku-sozdatel-bitcoin-fog-osuzhden-za-otmyvanie-millionov/#content>
- 2) Осужденный в США на 12,5 лет Роман Стерлингов потребовал отменить приговор https://rapsi-pravo.ru/international_news/20250929/311198936.html
- 3) Оператору Bitcoin Fog Миксер грозит многолетнее тюремное заключение за отмывание 400 миллионов долларов <https://www.cybersecurity-help.cz/blog/3863.html>
- 4) Осужденный в США на 12,5 лет Роман Стерлингов потребовал отменить приговор <https://worldinform.ru/articles/id-osuzhdennyi-v-ssha-na-12-5-let-roman-sterlingov-potreboval-otmenit-prigovor.html>
- 5) Основатель Bitcoin Fog получил более 12 лет за крупномасштабное отмывание денег <https://www.cybersecurity-help.cz/blog/4381.html>
- 6) Роман Стерлингов - последние новости, фото, биография <https://imag.one/news/persons/roman-sterlingov>
- 7) Осужденный на 12,5 лет Стерлингов обратил внимание суда США на упущения в деле https://www.rapsinews.ru/international_news/20260414/311766712.html
- 8) Гражданин России осужден за отмывание \$400 млн <https://www.slavicsac.com/2025/01/21/roman-sterlingov-sentenced/?amp=1>
- 9) Bitcoin Fog: крупнейшая платформа для отмывания биткоинов закрыта, её создатель — в тюрьме <https://rumafia.news/news/33142-bitcoin-fog-krupnejchaja-platforma-dlja-otmyvanija-bitkoinov-zakryta-ee-sozdatelj-v-tjurjme>
- 10) Гражданина России и Швеции приговорили в США к 12,5 годам тюрьмы за отмывание \$400 млн с помощью Bitcoin Fog <https://x-compliance.ru/publications/podft/grazhdanina-rossii-i-shvetsii-prigovorili-v-ssha-k-125-godam-turmy-za-otmyvanie-400-mln-s-pomoschu-bitcoin-fog>
- 11) Федеральный суд не запрещает крипто-миксеры повсеместно <https://phemex.com/ru/news/article/no-federal-appeals-court-ruling-bans-crypto-mixers-universally-13754>
- 12) Регулирование криптовалютного бизнеса в РФ. Период серых зон заканчивается <https://plusworld.ru/advertising/>
- 13) «Это вообще законно?» Гайд по легальному использованию криптовалют в России <https://mspmo.ru/public/eto-voobshche-zakonno-gayd-po-legalnomu-ispolzovaniju-kriptovaljut-v-rossii/>
- 14) Крипторегулирование 2025 — что можно, что нельзя и сколько платить <https://overclockers.ru/blog/Dodzbogdan/show/239515/Kriptoregulirovanie-2025-cto-mozhno-cto-nel-zya-i-skol-ko-platit>
- 15) Постановление Правительства РФ от 09.10.2024 № 1347, редакция действует с 1 июня 2025 <https://www.dirmagazina.ru/npd/doc/docid/1309798259/modid/99>
- 16) Подозрительные сделки с цифровой валютой заблокируют <https://www.pnp.ru/economics/podozritelnye-sdelki-s-cifrovoy-valyutoy-zablokiruyut.html>
- 17) Криптовалюта в России разрешена — но по жёстким правилам <https://investfuture.ru/articles/kriptovalyuta-v-rossii-razreshena-no-po-zhyostkim-pravilam>
- 18) Постановление Правительства РФ от 09.10.2024 N 1347 (ред. от 22.04.2025) https://www.consultant.ru/document/cons_doc_LAW_487919/#utm_campaign=fw&utm_source=archive&utm_medium=email&utm_content=old
- 19) Российские криптотрейдеры испытывают давление из-за новых законов <https://www.mitrade.com/insights/news/live-news/article-3-989365-20250726>
- 20) Законна ли криптовалюта в России: регулирование и соответствие требованиям <https://www.lightspark.com/knowledge/is-crypto-legal-in-russia>

- 21) Создателей криптовалютного миксера Samourai приговорили к тюремному заключению <https://xakep.ru/2025/11/25/samourai-sentenced/>
- 22) Создателям миксера Samourai Wallet пригрозили ... <https://bits.media/sozdatelyam-miksera-samourai-wallet-prigrozili-tyurmoy/>
- 23) Суд в США установил срок заключения соучредителям ... <https://incrypted.com/sud-v-ssha-ustanovyl-srok-zakljuchenyja-souchredyteljam-samourai-wallet-za-otmyvanye-sredstv/>
- 24) Разработчик кошелька Samourai приговорён к 5 годам ... <https://www.coindesk.com/ru/policy/2025/11/06/samourai-wallet-developer-sentenced-to-5-years-in-prison-for-unlicensed-money-transmitting>
- 25) \$237 млн от даркнета и киллеров. Создатели Samourai Wallet получили реальные сроки <https://www.securitylab.ru/news/566377.php>
- 26) Создатели миксера Samourai Wallet признали вину в отмывании \$100 млн <https://id.tradingview.com/news/bitsmedia%3A14f98a3c967b8%3A0/>
- 27) Основателей Samourai Wallet обвинили в сознательном отмывании денег <https://forklog.com/news/osnovatelej-samourai-wallet-obvinili-v-soznatelnom-otmyvanii-deneg/>
- 28) 67-летний разработчик криптокошелька Samourai получил четыре года тюрьмы <https://www.rbc.ru/crypto/news/691ed1409a794751324409d4>
- 29) Основатели Samourai Wallet признают вину: до 25 лет ... <https://hashtelegraph.com/osnovateli-samourai-wallet-priznajut-vinu-do-25-let-tjurmy-za-mikser-kriptoaljut/>
- 30) В США разработчика Samourai Wallet приговорили к 4 годам тюрьмы за нелегализованный сервис переводов <https://www.ossetia.tv/2025/12/09/v-ssha-razrobotchika-samourai-wallet-prigovorili-k-4-godam-tyurmy-za-nelitsenzirovannyj-servis-perevodov/>
- 31) Вы работаете в криптоиндустрии? Если да, то вы являетесь объектом внимания... <https://www.facebook.com/FBIPhoenix/posts/do-you-work-in-the-crypto-industry-if-so-you-are-a-target-of-north-korean-actors/122162201648047590/>
- 32) Вашингтон ввел санкции против 19 организаций, в то время как объем американских транзакций составил 16,6 млрд долларов... https://cryptoslate.com/washington-sanctions-19-entities-while-16-6b-in-us-losses-intensifies-pressure/?_cf_chl_rt_tk=xCoZGKTZGJalhof09IAGJTHC2vatAseNesObTu6D3Fs-1777084504-1.0.1.1-vsmn05CHHigsflpVnmZgLAKdocsWwqIT129EL2eZOPw
- 33) Elliptic: Кроссчейн-технологии используют для ... <https://www.occrp.org/ru/novosti/elliptic-krosscein-technologii-ispolzuiut-dlia-otmyvaniia-nezakonnyx-kriptodoxodov>
- 34) Минфин США признал легальный статус криптомиксеров <https://ru.beincrypto.com/status-kriptomikserov-v-ssha/>
- 35) ФАС выиграла суд по делу об антиконкурентном соглашении <https://pravo.ru/news/?tagId=5256&page=149>
- 36) Тёмная сторона цифровизации: использование новых технологий для отмывания денег и финансирования терроризма <https://jomeam.ru/ru/nauka/article/117158/view>
- 37) За IV кв. 2024 г. в мире было изготовлено 334,5 млн смартфонов <https://www.tssonline.ru/news/archive/2025/03>
- 38) США отменили санкции против трех грузовых судов под российским флагом <https://www.forbes.ru/tegi/minfin-ssha>
- 39) Nvidia будет производить суперкомпьютеры <https://www.coindesk.com/ru/tech/2025/04/16/the-protocol-nvidia-to-manufacture-ai-supercomputers-in-u-s-new-opportunities-for-crypto-miners>
- 40) Каким образом Монеро (XMR) сохраняет приватность при анализе данных в цепочке блоков? <https://www.gate.com/ru/crypto-wiki/article/how-does-monero-xmr-maintain-privacy-in-on-chain-data-analysis-20251118>
- 41) Основы Монеро (XMR): логика whitpaper, варианты использования, технологические инновации и динамика реализации дорожной карты <https://www.gate.com/ru/crypto-wiki/article/what-is-monero-xmr-fundamentals-whitepaper-logic-use-cases-technology-innovation-and-roadmap-progress-explained-20251223>
- 42) Какие преимущества будет иметь Монеро (XMR) в 2025 году по сравнению с другими аналогичными криптовалютами в сфере обеспечения конфиденциальности? <https://web3.gate.com/zh-tw/crypto-wiki/article/how-does-monero-xmr-compare-to-other-privacy-coins-in-2025>
- 43) Новости <https://xmr.ru/categories/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/page/8/>
- 44) Этот сайт требует JavaScript <https://libera.monerologs.net/monero-community/20251123>
- 45) Что такое Монеро (XMR)? Полное введение в мир ведущей криптовалюты для обеспечения конфиденциальности <https://www.bittrue.com/ru/blog/what-is-monero-crypto-xmr>
- 46) Как отследить Монеро (XMR) и другие анонимные криптовалюты <https://bithide.io/blog/ru/all-posts/how-to-trace-monero-and-privacy-coins-2/>

- 47) Монеро усиливает конфиденциальность с обновлением «Fluorine Fermi» для противодействия сетевому наблюдению <https://www.bitget.com/ru/news/detail/12560605010738>
- 48) Шпион в сети не пройдёт: Монеро нашёл способ вычислить тех, кто следит за транзакциями <https://myseldon.com/ru/news/index/336306703?requestId=d33284fc-5fa6-4e0d-bf39-e6295f27e064>
- 49) Монеро - не так безопасно как кажется? <https://bitcointalk.org/index.php?topic=5514626.msg64701987#new>
- 50) Разрешены ли операции с анонимными криптовалютами? <https://belapan.by/cryptocurrency/razresheny-li-operaczii-s-anonimnymi-kriptovalyutami>
- 51) Россия: Регулирование криптовалют (до 20.06.2025) https://teletype.in/@odanoder/W15W32t-DLi?utm_source=teletype&utm_medium=feed_rss&utm_campaign=odanoder
- 52) Законна ли криптовалюта в России? <https://blog.mexc.com/zh-hans/wiki/is-crypto-legal-in-russia/>
- 53) Законна ли Монеро? Как разобраться в правилах XMR и соблюдении требований MiCA <https://baltex.io/ru/blog/ecosystem/is-monero-legal-xmr-regulations-mica-compliance>
- 54) Криптовалюта и закон: что изменилось в России к сентябрю 2025 <https://emcd.io/ru/academy/articles/kriptovalyuta/kriptovalyuta-i-zakon-что-izmenilos-v-rossii-k-sentyabryu-2025/>
- 55) Законна ли Монеро? Что нужно знать в 2025 году <https://baltex.io/ru/blog/ecosystem/is-monero-legal-what-you-need-to-know-2025>
- 56) Представитель Росфинмониторинга отметила рост числа финрасследований, связанных с использованием криптовалют в преступных целях <https://www.fedsfm.ru/releases/8964>
- 57) Росфинмониторинг задействует «Прозрачный блокчейн» в выявлении преступных доходов <https://www.pnp.ru/economics/rosfinmonitoring-zadeystvuet-prozrachnyy-blokcheyn-v-vyavlenii-prestupnykh-dokhodov.html>
- 58) Росфинмониторинг создаст реестр «подозрительных» криптокошельков <https://www.ossetia.tv/2025/12/03/rosfinmonitoring-sozdast-reestr-podozritelnyh-kriptokoshelkov/>
- 59) В Росфинмониторинге назвали мифом анонимность криптовалютных транзакций <https://fomag.ru/news-stream/v-rosfinmonitoringe-nazvali-mifom-anonimnost-kriptovalyutnykh-tranzaktsiy/>
- 60) Профессор Шайхразеева: в России усиливается контроль за цифровыми активами <https://www.osnmedia.ru/ekonomika/professor-shajhrazeeva-v-rossii-usilivaetsya-kontrol-za-tsifrovymi-aktivami/amp/#>
- 61) Росфинмониторинг: Анонимность криптовалют — это иллюзия <https://www.ossetia.tv/2025/12/04/rosfinmonitoring-anonimnost-kriptovalyut-eto-illyuziya/>
- 62) Представители Росфинмониторинга приняли участие в круглом столе Совета Федерации, посвященном регулированию оборота цифровых валют в России <https://eurasiangroup.org/en/rosfinmonitoring-representatives-participated-in-the-federation-council-roundtable-devoted-to-the-digital-currency-turnover-regulation-in-russia>
- 63) В Росфинмониторинге рассказали о росте числа финрасследований, связанных с использованием криптовалют преступниками <https://x-compliance.ru/publications/podft/v-rosfinmonitoringe-rasskazali-o-rote-chisla-finrassledovaniy-svyazannyh-s-ispolzovaniem-kriptovalut-prestupnikami>
- 64) В Росфинмониторинге заявили, что анонимность криптовалютных транзакций россиян — это миф <https://vecherka-spb.ru/2025/05/20/v-rosfinmonitoringe-zayavili-что-anonimnost-kriptovalyutnykh-tranzaktsii-rossiyan--eto-mif>
- 65) Криптовалюта в РФ: стратегии защиты от блокировок счетов <https://companies.rbc.ru/news/ACkd788MuE/kriptovalyuta-v-rf-strategii-zaschityi-ot-blokirovok-schetov/>
- 66) Российская криптобиржа для обхода санкций Garantex продолжила работать под новыми названиями и разрослась в децентрализованную сеть, выяснили ... <https://istories.media/news/2025/09/10/rossiiskaya-kriptobirzha-dlya-obkhoda-sanktsii-garantex-prodolzhila-rabotat-pod-novimi-nazvaniyami-i-razrosilas-v-detsentralizovannuyu-set-transperensi-interneshnl-rossiya/?tztc=1>
- 67) Россия создает подпольную криптосеть после исключения из системы SWIFT <https://www.kucoin.com/ru/news/flash/russia-builds-underground-crypto-network-after-swift-exclusion>
- 68) От Нудра до А7А5: Подпольные потоки России на \$376,3 млрд в блокчейне меняют глобальную финансовую карту <https://www.htx.com/ru-ru/news/327559/>
- 69) FT обнаружила криптоканал обхода санкций против России, через который провели \$9,3 млрд за четыре месяца <https://thebell.io/ft-obnaruzhila-kriptokanal-obkhoda-sanktsiy-protiv-rossii-cherez-kotoryy-proveli-93-mlrd-za-chetyre-mesyatsa>
- 70) Рублевый стейблкоин А7А5: как Россия обходила санкции в 2025 году <https://www.btcc.com/ru-RU/amp/square/BeincryptoRU/1397812>
- 71) Что такое MetaMask и как мы можем его использовать? <https://www.gate.com/zh/post/status/14109685>

72) Криптовалюта в РФ: стратегии защиты от блокировок счетов

<https://myseldon.com/ru/news/index/339938883>

73) Компании из РФ провели \$9,3 млрд через криптобиржу Grinex для обхода санкций

<https://ru.investing.com/news/general-news/article-2806978>

74) Россия создает подпольную криптосеть после запрета SWIFT <https://phemex.com/ru/news/article/russia-develops-underground-crypto-network-postswift-exclusion-43364>

Глава 10. Аппаратные кошельки и конфискация

История криптовалют полна случаев, когда люди теряли целые состояния из-за, казалось бы, банальных вещей: забытый пароль, выброшенный жёсткий диск или, что гораздо прозаичнее, визит сотрудников правоохранительных органов. Когда кто-то говорит «ваши ключи — ваши деньги», многие упускают из виду вторую часть этого правила: к кому в руки попали ключи, тот и владеет деньгами. И если этими руками окажутся сотрудники силовых ведомств, коллекторы или приставы, ваша криптографическая крепость может рухнуть за секунды.

Третья часть нашего разговора о безопасности посвящена самому надёжному способу хранения — аппаратным кошелькам — и самому недооценённому риску: физическому изъятию. К сожалению, 2025-2026 годы показали, что государство всё чаще смотрит на владельцев крипты не просто как на «инвесторов», а как на потенциальных нарушителей, чьи активы можно и нужно конфисковывать.

В этой главе мы разберёмся, как именно приставы и следователи могут добраться до вашего «холодного» кошелька, почему стандартное хранение сид-фразы «смертельно» опасно и, наконец, что нужно делать прямо сейчас и в критический момент, чтобы ваши монеты не стали трофеем силовиков.

Могут ли изъять Ledger или Trezor: правовая реальность 2026 года

Самый частый вопрос, который задают новички при покупке аппаратного кошелька: «Если ко мне придут, смогут ли они его забрать?». Ответ — да, могут. И сделают это на абсолютно законных основаниях. Для этого государственной машине не нужно принимать новый закон — достаточно того, что уже есть в Гражданском процессуальном и Уголовно-процессуальном кодексах.

Здесь важно понимать, кто именно стоит у вашей двери. Это не праздный вопрос — от этого зависит, что именно вам грозит.

Сценарий № 1: Пришли приставы (ОСП)

К вам пришли судебные приставы, чтобы исполнить решение суда о взыскании крупного долга. В этом случае у них на руках есть исполнительный лист и постановление о возбуждении исполнительного производства. Они

действуют в рамках Федерального закона «Об исполнительном производстве».

Приставы имеют право входить в ваше жилое помещение и производить осмотр и арест имущества. А поскольку криптовалюта признана Федеральным законом № 259-ФЗ «иным имуществом», на неё распространяются все те же нормы, что и на золотой слиток или коллекцию картин. Более того, Пленум Верховного суда РФ в 2025 году специально разъяснил, что арест может быть наложен и на цифровую валюту.

Ключевой момент: пристав не обязан взламывать ваш кошелёк. По закону вы, как должник, **обязаны сами** предоставить доступ к своему имуществу для погашения долга. Если вы отказываетесь сообщить пин-код от аппаратного кошелька или пароль к компьютеру, это классифицируется как воспрепятствование законной деятельности пристава. Административный штраф за это — до 2500 рублей и, как показывает практика, повторный визит с гораздо более суровыми последствиями, вплоть до возбуждения уголовного дела за злостное уклонение.

Самое же опасное — что отказ назвать пароль пристав может запротоколировать, суд сочтёт это отягчающим обстоятельством, и ваше финансовое положение будет ухудшаться. При этом в рамках исполнительного производства вас не могут заставить давать показания против себя, но отказаться передать имущество, на которое наложен арест, вы не имеете права.

Сценарий № 2: Пришли с обыском (МВД, ФСБ, СК)

Этот сценарий гораздо серьезнее. Обыск проводится в рамках возбуждённого уголовного дела, и сотрудники действуют на основании постановления следователя. В этой ситуации изымаются любые предметы, содержащие электронную информацию: ноутбуки, телефоны, флешки и, конечно, аппаратные кошельки. Даже если ваш Ledger или Tangem просто лежит в ящике стола, его заберут на экспертизу.

Дальше начинается самое опасное. Хотя Уголовно-процессуальный кодекс формально запрещает требовать от человека пароль к его устройствам, на практике это обходят элементарно. Во-первых, оборудование просто увозится к техническим специалистам, которые обладают необходимыми средствами для взлома или анализа. Во-вторых, во время обыска на вас оказывается колоссальное психологическое давление. Вам могут сказать: «Либо ты называешь пин-код сейчас, либо мы изымаем всё и завтра к тебе

придут уже по статье за госизмену». И в 99% случаев человек, никогда не сталкивавшийся с силовой машиной, плывёт и выдаёт информацию.

Но даже если вы устоите, это не гарантирует сохранность средств. Аппаратные кошельки, особенно старых моделей, не являются на 100% защищёнными от физического взлома. Известны случаи, когда при наличии специального оборудования специалисты считывали данные напрямую с чипов памяти. Ledger и Trezor постоянно исправляют подобные уязвимости в новых прошивках, но если ваша модель не обновлялась несколько лет, вы находитесь в зоне риска. В 2025 году производитель Ledger официально признал наличие векторов атак на старые модели Nano S и рекомендовал пользователям перейти на Nano X или Nano S Plus.

Что изымут точно: список без сюрпризов. При любом сценарии под изъятие попадают: ноутбуки и системные блоки, все мобильные телефоны, аппаратные кошельки (Ledger, Trezor, Tangem, OneKey), флеш-накопители и внешние диски, sim-карты, а также любые бумажные записи с цифрами и буквами. Именно о последнем пункте — бумажных записях — мы сейчас и поговорим.

Как хранить сид-фразу так, чтобы её не нашли

Стандартный совет в интернете звучит примитивно: «Запишите 12 или 24 слова на бумагу и спрячьте в надёжном месте». Однако обыск потому и называется обыском, что сотрудники ищут везде: в книгах, за обоями, в сливном бачке, под половицами. Найти бумажку со случайными словами — их главная цель, потому что это ключ ко всем вашим деньгам.

Как делать нельзя — распространённые ошибки:

- Хранить сид-фразу целиком, в правильном порядке, на одном листе бумаги.
- Хранить бумажку с фразой рядом с аппаратным кошельком. Это всё равно, что оставить ключ в двери банковской ячейки.
- Использовать «бытовой тайник» — в книге, за иконой, в одежде. Это первое, что проверяют.
- Хранить сид-фразу в облаке (Google Диск, Яндекс.Диск, iCloud), в заметках телефона или в черновиках почты. Если ваш телефон изымают, следствие получает доступ и к облаку.

- Гравировать слова на металле без шифрования. Это надёжно против пожара, но бесполезно против обыска — силовики прочитают всё так же легко, как и вы.

Как делать правильно: продвинутые стратегии сокрытия

Стратегия 1: Добавление 25-го слова (passphrase). Большинство современных кошельков (Ledger, Trezor, Tangem) поддерживают функцию passphrase — дополнительного слова или даже целой фразы, которую вы придумываете сами. Без неё стандартная сид-фраза из 24 слов открывает пустой или отвлекающий кошелёк. Именно этот метод мы будем детально разбирать ниже, в технике «душа крипты». Главное преимущество: вы можете спокойно отдать силовикам свою сид-фразу, и они увидят лишь незначительную сумму, в то время как основные активы останутся скрыты за passphrase.

Стратегия 2: Разделение секрета (Shamir's Secret Sharing). Это метод, при котором ваша сид-фраза математически разделяется на несколько частей. Чтобы восстановить кошелёк, нужно собрать определённое количество частей (например, 2 из 3 или 3 из 5). Одну часть вы храните дома, вторую — у доверенного родственника в другом городе, третью — в банковской ячейке. Даже если при обыске найдут одну часть, восстановить по ней кошелёк математически невозможно.

Стратегия 3: Мнемоническое шифрование. Вы записываете сид-фразу, но не в открытом виде, а с помощью личного шифра, известного только вам. Например, вы заменяете каждое слово кодовым обозначением по заранее составленной таблице, либо добавляете к каждому слову фиктивный слог, либо пишете слова в обратном порядке с определённым шагом. Самый простой и элегантный метод — «книжный шифр». Вы берёте конкретную книгу, издание, страницу и заменяете каждое слово сид-фразы на номер строки и позиции в этой строке. Без знания того, какая именно это книга, расшифровать запись невозможно.

Критическое правило: доверенное лицо, у которого хранится часть секрета, не должно знать, где находятся остальные части и что именно оно хранит. Идеально, если это человек, вообще не разбирающийся в криптовалютах.

Техника «душа крипты»: что делать, если вас взяли

Термин «душ крипты» пришёл из англоязычного криптосообщества. Это комплексная стратегия, которая готовится заранее и активируется в момент,

когда вы физически теряете контроль над своими устройствами — будь то задержание, обыск или ограбление.

Первый и главный компонент этой стратегии — **passphrase (25-е слово)**. Базовая сид-фраза открывает лишь «отвлекающий» кошелёк с небольшой, правдоподобной суммой — например, 0,05 BTC или эквивалент 500 долларов. Основные средства хранятся за passphrase. Если от вас под давлением требуют сид-фразу, вы отдаёте её — и злоумышленник видит именно эту сумму. Он не может знать, существует ли второй кошелёк, потому что сам протокол кошелька не предусматривает счётчика скрытых аккаунтов. Даже если он заставит вас ввести пин-код от устройства, вы введёте пин, привязанный к «чистому» кошельку (на многих устройствах, включая Ledger, можно привязать дополнительный пин-код ко второму аккаунту с passphrase).

Второй компонент — **физический сброс устройства**. Некоторые аппаратные кошельки позволяют настроить автоматический сброс настроек после нескольких неверных попыток ввода пин-кода, либо вы можете в критической ситуации ввести «аварийный» пин-код, при вводе которого устройство мгновенно стирает все данные.

Третий компонент — **юридическая защита**. Он предполагает, что у вас есть контакт проверенного крипто-адвоката, записанный не на бумажке в кошельке, а в памяти. Вы должны помнить, что имеете право хранить молчание и что любое требование назвать пароль вы можете обжаловать через адвоката.

Ключевой принцип «душа крипты»: вы не сопротивляетесь физически, вы не геройствуете перед спецназом, а напротив — подчёркнуто вежливы и готовы сотрудничать.

План действий в момент визита силовиков:

- **Не сопротивляйтесь.** Физическая конфронтация с сотрудниками — это отягчающее обстоятельство и гарантированный привод.
- **Немедленно потребуйте адвоката.** Если у вас нет конкретного контакта, требуйте предоставить адвоката по назначению, но не давайте показаний до его прибытия.
- **Сообщите адвокату о специальном статусе.** Как только адвокат прибыл, сразу же разъясните ему, что изымается криптовалюта и что ситуация требует специальных знаний.

- **Не называйте пароли и пин-коды.** Это ваше конституционное право — не свидетельствовать против себя (статья 51 Конституции РФ).
- **Если обыск уже идёт, следите за протоколом.** В протоколе обыска должны быть перечислены ВСЕ изымаемые предметы. Проследите, чтобы ваш аппаратный кошелёк был записан с указанием модели и серийного номера. Это ваш единственный шанс доказать потом, что изъяли именно его.

Что делать после изъятия:

- **Немедленно переведите остатки.** Как только вы остались одни, переведите все уцелевшие средства с «горячих» кошельков на новый чистый адрес, который не был скомпрометирован.
- **Подайте жалобу.** Если обыск проводился с нарушениями (отсутствие понятых, неправильно оформленный протокол), подавайте жалобу в прокуратуру и в суд в течение 5 дней.

Вывод из Главы 10

Аппаратный кошелёк — это ваш банковский сейф, но даже самый прочный сейф не поможет, если ключ от него приклеен скотчем к дверце. Государство образца 2026 года умеет изымать криптовалюту и делает это всё чаще. Ваша задача — построить такую систему безопасности, которая защитит вас и от цифровой атаки, и от физической силы.

Главные правила:

1. Используйте passphrase (25-е слово) и настройте «отвлекающий» кошелёк.
2. Храните сид-фразу только в разделённом виде, желательно с использованием шифрования.
3. Подготовьтесь к визиту силовиков заранее: знайте свои права и имейте контакт профильного адвоката.
4. В критический момент не геройствуйте, а включайте протокол «душа крипты» — отдавайте то, что угрожают забрать силой, но так, чтобы основные средства остались вне доступа.

Часть 4. Экономика — крипта как спасение или ловушка?

Глава 11. Инфляция, вклады и биткоин

Сбережения россиян в 2026 году оказались между молотом и наковальней. С одной стороны — банковские депозиты со ставками, которые всё ещё высоки, но неумолимо снижаются. С другой — биткоин, который за последние годы показал взрывной рост, но путь этот был усеян обвалами на десятки процентов. К этому добавляется официальная инфляция, пожирающая покупательную способность рубля, и серый рынок криптовалют, где одни теряют всё, а другие зарабатывают состояния. Чтобы понять, что на самом деле происходит с деньгами, давайте обратимся к цифрам.

Биткоин и рубль: американские горки с российской спецификой

2025 год стал для биткоина историческим, но не в том смысле, в каком ожидали многие. В октябре первая криптовалюта достигла абсолютного максимума в \$126,080. Аналитики связывали этот взлёт с приходом на рынок крупных институциональных инвесторов и политикой администрации Дональда Трампа, подписавшей указ о создании стратегического биткоин-резерва США. Однако к концу года картину испортили «киты» — давние держатели биткоина, которые начали массово продавать свои монеты, фиксируя прибыль после многолетнего роста. В результате к концу декабря биткоин откатился примерно до \$89,841, а год закрыл со снижением около 3%.

И вот здесь начинается самое интересное для российского инвестора. Если смотреть на график биткоина в долларах, то после октябрьского пика в \$126,080 началась глубокая коррекция, и к апрелю 2026 года цена ушла в район \$72,700. Падение от хаёв (резкое снижение цены актива с его максимальных исторических или локальных значений) составило примерно 45%. Но если пересчитать ту же динамику в рублях, картина получается иной. В начале 2025 года доллар стоил около 92 рублей. На пике в октябре, когда биткоин достиг \$126,080, его рублёвая стоимость была просто заоблачной. А сейчас, когда биткоин в долларах падает, курс рубля к доллару, согласно апрельскому макроопросу Банка России, укрепляется — аналитики прогнозируют средний курс в 2026 году на уровне 81,2 рубля за доллар. Более крепкий рубль частично компенсирует падение долларовой цены биткоина, но общая рублёвая доходность за последние полгода для тех, кто купил на пике, выглядит удручающе.

Именно этот эффект — резкое укрепление рубля во время коррекции биткоина — и создаёт ту самую «русскую специфику». Если американец потерял 45% от октябрьского максимума, то россиянин мог потерять ещё больше из-за того, что его рубли стали дороже. В этом и заключается главный риск крипты как защитного актива: она растёт быстрее рынка, но и падает так же стремительно.

Банковские вклады: доходность тает на глазах

Пока крипторынок штормит, в банковском секторе наблюдается своя драма. В 2025 году россияне активно несли деньги на депозиты, привлечённые высокими ставками вслед за ключевой ставкой ЦБ. Ещё в декабре 2025 года максимальная ставка по вкладам в топ-10 банков превышала 15,5% годовых. Однако тренд развернулся. Ключевая ставка зафиксировалась на уровне 16,00%, а вслед за ней начали снижаться и проценты по депозитам. Во второй декаде апреля 2026 года средняя максимальная ставка упала до 13,39% — минимума с октября 2023 года.

Люди реагируют на это падение закономерно. Спрос на онлайн-вклады в первом квартале 2026 года сократился на 17% по сравнению с концом предыдущего. Пользователи чаще выбирают вклады с капитализацией процентов и на короткие сроки — три месяца и полгода. И на этом фоне резко, на 24%, взлетел интерес к инвестиционным инструментам.

Почему это происходит, понять несложно. Инфляция в декабре 2025 года составила 5,6%, и аналитики прогнозируют, что в 2026 году она ускорится до 5,5%. Реальная доходность вклада со ставкой 13,39% после вычета инфляции оказывается меньше 8% годовых. А для тех, кто помнит биткоин по \$126,000, банковские проценты не выглядят впечатляющей альтернативой.

Майнинг: битва за рентабельность

2025 год стал первым полным годом легального майнинга в России, и его результаты дают наглядное представление о том, что значит добывать криптовалюту в легальном поле. Россия прочно заняла второе место в мире по объёму добычи, обеспечивая около 16% глобального хешрейта. За год российские майнеры добыли примерно 26 тысяч биткоинов, что по усреднённому курсу декабря (\$88,000) эквивалентно \$2,2 млрд.

Но обратная сторона этой медали — резкое сжатие маржинальности. Сложность сети за год выросла на 35%, что означает падение эффективности

устаревшего оборудования. Одновременно выросли затраты на электроэнергию, которая и составляет основную статью расходов майнера. В начале декабря 2025 года ключевой показатель прибыльности упал до \$35 за петакеш в секунду — на 45% ниже годового пика. При таких цифрах даже компании с дешёвой энергией работают практически в ноль.

Усугубляет ситуацию то, что около 70% оборудования, ввезённого в предыдущие годы по серым схемам, остаётся незарегистрированным в ФНС. Эти машины продолжают работать, но их владельцы не платят налоги, что создаёт неравную конкуренцию легальным майнерам. По оценкам МТС, общее количество майнинговых ферм в России за 2025 год выросло на 44% и достигло 196,9 тысяч. Большинство из них — небольшие, с непрозрачным происхождением и без налоговой истории.

Сколько россиян реально заработали на крипте

Самый сложный вопрос — кто же на самом деле оказался в плюсе. Минфин России оценивает количество держателей криптовалют в стране примерно в 20 миллионов человек. По данным Центробанка, совокупный объём их активов на криптобиржах составляет около 827 млрд рублей, и за год эта цифра выросла на 27%.

Однако здесь важно разделить два понятия: «владеть» и «заработать». 20 миллионов владельцев — это те, у кого есть хоть какая-то сумма в крипте. Но статистика реальной прибыли выглядит иначе. Если биткоин в октябре достиг \$126,000, то в апреле 2026 года он торгуется около \$72,700 — это падение на 45% от пика. Инвесторы, зашедшие на хаях, понесли колоссальные убытки. Те, кто покупал в 2022 году по \$15,000-\$20,000, даже при текущей коррекции остаются в плюсе.

Трейдинговая панель The Block фиксирует, что доходы майнеров от комиссий сети упали до \$210,000 в день — годового минимума. Розничные инвесторы, активно торговавшие на P2P-платформах, столкнулись с массовыми блокировками счетов и «токсичными» рублями в 2025 году. Можно с уверенностью сказать, что реально заработали на крипте за последние два года те, кто придерживался среднесрочной стратегии, а не пытался ловить каждый отскок.

Вывод из Главы 11

Криптовалюта в России 2026 года — это не лотерейный билет и не «тихая гавань». Это высоковолатильный актив, который на коротком горизонте

может принести как +200%, так и -45% за полгода. Банковский вклад даёт предсказуемую, но скромную доходность, едва перекрывающую инфляцию. Майнинг из полуподвального бизнеса превратился в отрасль со сжатой до нуля маржой и жёсткими требованиями к эффективности.

Выбор между биткоином и вкладом — это на самом деле выбор между волатильностью и предсказуемостью. И оба варианта имеют свою цену.

Использованные в главе источники:

- 1) Ключевые показатели <http://www.cbr.ru/key-indicators/>
- 2) Спрос на вклады падает вместе с доходностью по ним <https://www.klerk.ru/buh/news/688791/>
- 3) BTC Wealth <https://in.tradingview.com/chart/BTCUSD/nmjla6HU-BTC-Wealth/>
- 4) How Cryptocurrency Mining Has Changed in Russia. Results of 2025 <https://www.htx.com/news/how-cryptocurrency-mining-has-changed-in-russia-results-of-2-BXLd4ViG/>
- 5) Россия представила дорожную карту регулирования криптовалют с доступом к банковским услугам <https://t.signalplus.com/crypto-news/detail/russia-crypto-regulation-bitcoin-adoption-20m-users?lang=ru-RU>
- 6) Macroeconomic survey of the Bank of Russia
Survey results: April 2026 https://cbr.ru/eng/statistics/ddkp/mo_br/?f-
- 7) МАКСИМАЛЬНАЯ СТАВКА ПО ВКЛАДАМ В РУБЛЯХ В АПРЕЛЕ СНИЗИЛАСЬ ДО 13,39%
<https://urbc.ru/1068144034-maksimalnaja-stavka-po-vkladam-v-rubljah-v-aprele-snizilas-do-1339.html>
- 8) Bitcoin's Least Volatile Year in 2025; K33 Research Predicts New Highs in 2026
<https://www.kucoin.com/news/flash/bitcoin-s-least-volatile-year-in-2025-k33-research-predicts-new-highs-in-2026>
- 9) Russia Eyes Arctic Bitcoin Boom—Miners May Flee South for Frozen Profits <https://www.btcc.com/en-AU/square/decryptCO/363592>
- 10) Минфин: около 20 млн россиян используют криптовалюту <https://www.ntv.ru/novosti/2943111>

Глава 12. Цифровой рубль — самый страшный для крипты конкурент?

С 1 сентября 2026 года в России начинается массовое внедрение цифрового рубля. Крупнейшие банки должны будут обеспечить клиентам возможность открывать цифровые кошельки, проводить переводы и оплачивать покупки. Для криптосообщества это не просто новость из мира финансовых технологий, а событие, способное перекрыть весь ландшафт: может ли государственный цифровой рубль сделать ненужными биткоин и стейблкоины? Или он, наоборот, подтолкнет россиян искать убежище в децентрализованных активах?

Чем цифровой рубль отличается от биткоина (технически и юридически)

На первый взгляд, биткоин и цифровой рубль — явления из параллельных вселенных, и путать их могут только те, кто совсем не разбирается в теме. Но чтобы понять, почему государство так активно продвигает свой цифровой актив, а криптосообщество так настороженно за ним наблюдает, нужно разложить различия по полочкам.

Первое и фундаментальное различие — эмитент. Биткоин не выпускается никаким центральным органом, его эмиссия алгоритмически задана и ограничена 21 миллионом монет, а новые биткоины появляются в результате майнинга, который может осуществлять кто угодно. У цифрового рубля единственный эмитент — Банк России, и он ничем не ограничен в объёмах выпуска. Это классические фиатные деньги, просто в новой технологической обёртке.

Технологически разница не менее принципиальна. Биткоин работает на публичном, децентрализованном блокчейне, где все участники сети равноправны и могут проверять транзакции друг друга. Никто не может заблокировать биткоин-адрес или отменить транзакцию — для этого пришлось бы получить контроль над 51% вычислительной мощности сети. Цифровой рубль использует технологию распределённого реестра, но этот реестр полностью контролируется Центральным банком. Это не децентрализованная сеть, а централизованная база данных, в которой регулятор видит каждую операцию и имеет техническую возможность заблокировать любой кошелёк.

Наконец, юридический статус. Биткоин по российскому закону — имущество, его можно купить, продать, хранить, но нельзя использовать для оплаты товаров и услуг. Цифровой рубль — законное платёжное средство, третья форма национальной валюты наравне с наличными и безналичными. Отказаться принимать его к оплате будет нельзя.

Programmable money: зачем ЦБ вводит «окрашенные» деньги

Самая революционная и одновременно пугающая особенность цифрового рубля — программируемость. В классической финансовой системе деньги обезличены: получая зарплату, вы можете потратить её на что угодно. Цифровой рубль ломает этот принцип.

Смарт-контракты цифрового рубля позволяют государству задавать условия, при которых деньги могут быть использованы. ЦБ уже обсуждает с банками создание платформы для коммерческих смарт-контрактов. Министр финансов Антон Силуанов заявил, что цифровой рубль может использоваться в смарт-контрактах для контроля за целевым расходованием бюджетных средств. Проще говоря, государство сможет выпускать «окрашенные» рубли, которые разрешено потратить только на определённые цели и в определённые сроки.

Предположим, государство выделяет субсидию на строительство. Цифровые рубли поступят подрядчику, но он не сможет обналичить их или перевести в криптовалюту — смарт-контракт разрешит тратить их только на стройматериалы. Или социальное пособие на ребёнка — цифровые рубли можно будет потратить только в детских магазинах.

Для государства это инструмент контроля, который решает сразу несколько задач. Во-первых, бюджетные средства перестанут утекать налево, потому что каждый рубль будет иметь цифровой след. Во-вторых, появляется возможность таргетированной социальной поддержки. В-третьих, цифровой рубль делает практически невозможной всю теневую экономику — серые зарплаты, неучтённые доходы, уход от налогов.

Но для пользователя криптовалют это создаёт принципиально новую реальность. Программируемость означает, что государство получает инструмент тотального контроля над денежными потоками, какого не имело никогда в истории. И это неизбежно повысит привлекательность активов, которые находятся вне этого контроля.

Прогноз: исчезнет ли P2P после полного внедрения цифрового рубля

Главный вопрос, который волнует российское криптосообщество: что станет с P2P-обменниками, через которые сегодня проходит основной объём конвертации рублей в криптовалюту и обратно? Ответ неоднозначен, и многое зависит от того, как именно будет реализован цифровой рубль.

С одной стороны, цифровой рубль действительно может нанести серьёзный удар по привычным P2P-схемам. Сегодня главная проблема P2P — блокировки банковских карт по 115-ФЗ. Цифровой рубль технически позволяет избежать этих блокировок, потому что транзакции проходят напрямую на платформе ЦБ, а не через коммерческий банк, который может расценить перевод как подозрительный. Продавцы на P2P-площадках уже начали добавлять цифровой рубль как способ оплаты именно по этой причине — такие переводы считаются более «чистыми».

Однако более вероятный сценарий — не исчезновение P2P, а его трансформация и выдавливание. Как только цифровой рубль станет обязательным для бюджетников и пенсионеров с сентября 2026 года, а затем и для всех крупных торговых точек, государство получит беспрецедентный уровень видимости денежных потоков. Каждый перевод, каждая операция будет записана в реестре ЦБ. В таких условиях анонимный P2P-обмен станет технически невозможен — каждый цифровой рубль имеет уникальный идентификатор и отслеживается от эмиссии до погашения.

Рынок неизбежно разделится на два параллельных мира. В regulated finance — зарплаты, пенсии, налоги, оплата в магазинах — будет безраздельно править цифровой рубль. В нерегулируемой сфере — криптобиржи, DeFi, стейблкоины, трансграничные переводы — продолжат жить децентрализованные активы. Граница между ними станет жёстче, а переход из одного мира в другой окажется под пристальным вниманием ФНС и Росфинмониторинга.

Региональный менеджер криптобиржи CoinEx в СНГ прогнозирует, что доля USDT в расчётах внутри страны может сократиться на 25-30% уже в первые месяцы работы цифрового рубля. Однако полное вытеснение криптовалют невозможно: пока существует потребность в сбережениях, защищённых от инфляции и девальвации, пока бизнесу нужно рассчитывать с зарубежными партнёрами в обход SWIFT, биткоин и стейблкоины будут востребованы. Цифровой рубль не заменит криптовалюту — он лишь усилит разрыв между контролируруемыми и неконтролируемыми финансами.

Вывод из Главы 12

Цифровой рубль — это не убийца криптовалют, а катализатор размежевания. Он заберёт себе сферу повседневных платежей, государственных выплат и бюджетных расчётов — всё то, что должно быть прозрачным и контролируемым с точки зрения государства. Биткоин и стейблкоины сохраняют позиции там, где нужна свобода от государственного контроля, защита от инфляции и возможность трансграничных переводов.

Для обычного человека это означает, что с сентября 2026 года нужно будет освоить новую финансовую реальность: официальные доходы будут приходить в цифровых рублях, а криптовалюта окончательно переместится в разряд «параллельной» системы, работающей по собственным законам.

Использованные в главе источники:

- 1) Падение в будущее: как цифровой рубль изменит жизнь россиян <https://abnews.ru/news/2025/9/14/padenie-v-budushhee-kak-czifrovoj-rubl-izmenit-zhizn-rossiyan>
- 2) Банки предлагают платформу для коммерческих смарт-контрактов в цифровых рублях <https://interfax.com/newsroom/top-stories/116487/>
- 3) Руководство по российским биржам 2026: Навигация по ликвидности активов в эпоху цифрового рубля <https://www.kucoin.com/ru/blog/pt-2026-russia-exchange-guide-navigating-asset-liquidity-in-the-digital-ruble-era>
- 4) Новое видение инноваций и технологий. Усиление законодательного надзора за виртуальной валютой и устранение незаконной деятельности <https://www.wenweipo.com/a/202601/14/AP6966aae4e4b069b7ebf82a1c.html>
- 5) Российская национальная стратегия стейблкоинов: технико-экономическое обоснование и дедолларизация в 2026 году <http://gate.tv/zh/post/status/18896744>
- 6) Будут ли платить пенсии и зарплаты в цифровых рублях и как их получить <https://tolknews.ru/ekonomika/214981-pensii-i-zarplati-v-tsifrovih-rublyah-blizhayschaya-realnost-chto-izvestno>
- 7) Силуанов: Нужно выбирать пилотные проекты для тестирования инструментов прослеживаемости в цифровых рублях <https://interfax.com/newsroom/top-stories/116814/>
- 8) Цифровой рубль меняет правила игры: что ждёт долларовые стейблкоины и биткоин <https://ru.investing.com/analysis/article-200322547>
- 9) Запреты биткойнов на управление государством на блокчейне: секретная война России за финансовый суверенитет <https://www.russiamatters.org/analysis/bitcoin-bans-blockchain-statecraft-russias-secret-war-financial-sovereignty>
- 10) Влияние цифрового рубля на российскую экосистему безналичных платежей и традиционные финансовые услуги <https://www.ainvest.com/news/digital-ruble-impact-russia-cashless-payments-ecosystem-traditional-financial-services-2601/>

Глава 13. Санкции, SWIFT и стейблкоины

Когда Россию отключили от SWIFT и заморозили золотовалютные резервы, многие предрекали финансовый коллапс. Вместо этого российские компании, предприниматели и обычные граждане нашли лазейку, о которой санкционные стратеги тогда подумали в последнюю очередь. Этой лазейкой стали стейблкоины — цифровые токены, привязанные к курсу реальных валют.

К 2026 году стейблкоины превратились для России в полноценный дублер банковской системы для внешних расчетов. Но этот инструмент оказался обоюдоострым. Эмитенты стейблкоинов подчиняются западным регуляторам и в любой момент могут заморозить средства на любом адресе. Как Россия пытается решить эту проблему, и какие альтернативы просматриваются на горизонте?

Почему USDT стал для России фактически второй валютой

После отключения российских банков от SWIFT и ухода из страны Visa и Mastercard трансграничные расчеты превратились в квест. Банковский перевод в долларах или евро стал невозможен, а схемы с промежуточными юрисдикциями занимали недели и стоили до 15% комиссии. На этом фоне USDT (Tether) — стейблкоин, привязанный к доллару 1:1, — стал идеальным суррогатом. Его можно перевести в любую точку мира за минуты с комиссией в пределах одного доллара.

Россияне начали использовать USDT в трёх основных сценариях. Первый — внешнеторговые расчеты: оплата параллельного импорта, переводы за услуги иностранным контрагентам. Второй — фриланс и работа на зарубежных компании. Оплата в USDT стала стандартом де-факто, потому что не требует банков-корреспондентов и не привязана к географии. Третий сценарий — сбережения: в условиях волатильности рубля USDT воспринимается как «цифровой доллар под матрасом».

Масштабы впечатляют: по данным ЦБ, совокупный объём криптоактивов россиян на биржах достигает 827 млрд рублей. Львиная доля этой суммы номинирована именно в стейблкоинах.

Риски заморозки USDT: ваш кошелёк может стать тыквой

Удобство USDT имеет обратную сторону — централизацию. Tether Inc. полностью контролирует смарт-контракт и может в одностороннем порядке заморозить средства на любом адресе. Механизм заморозки реализован через функцию `freeze()`, которой нет в децентрализованных активах вроде биткоина.

2026 год показал, что это не теоретический риск, а реальный инструмент санкционной политики. В конце апреля 2026 года Tether заморозил более \$340 млн в USDT после прямых запросов от американских правоохранительных органов. В компании заявили, что действуют в рамках координации с 340 правоохранительными агентствами из 65 стран и что общий объём замороженных средств уже превысил \$4,4 млрд. Глава Tether Паоло Ардино подчеркнул, что «USDT не является убежищем для незаконной деятельности» и компания действует при обнаружении «достоверных связей с санкционированными лицами, преступными сетями или иной незаконной активностью».

Самый громкий прецедент, затронувший россиян напрямую, — блокировка USDT на \$2,5 млрд на счетах криптобиржи Garantex в 2025 году. После этого держатели USDT в России осознали: их кошельки уязвимы, если они хоть как-то связаны с адресами, попавшими под санкции OFAC.

Альтернативы для обычного пользователя

На фоне санкционной войны вокруг стейблкоинов у российского пользователя остаётся несколько опций, каждая со своими рисками:

DAI. Децентрализованный стейблкоин от протокола MakerDAO, обеспеченный не фиатными резервами, а криптовалютым залогом. Его преимущество — невозможность заморозки центральным эмитентом. Недостаток — более низкая ликвидность на P2P-рынках и сложность использования для новичков.

BUSD (Binance USD). Упомянутый в названии главы как «умирающий» — и действительно, после давления регуляторов США на Paxos в 2024 году эмиссия BUSD была прекращена. На начало 2026 года этот стейблкоин практически не используется.

Рублёвые стейблкоины (A7A5, RUBx). Россия начала выстраивать собственную инфраструктуру стейблкоинов, неподконтрольную западным

регуляторам. Ключевой проект здесь — A7A5, рублёвый стейблкоин, запущенный в начале 2025 года. Токен функционирует на блокчейнах Tron и Ethereum. Формально он выпущен под юрисдикцией Киргизии, но его финансовая стабильность обеспечена рублёвыми депозитами в российском банке. Основные пользователи A7A5 — российские компании, которым нужны трансграничные расчеты в обход западной банковской системы. Общий объём транзакций менее чем за год превысил \$100 млрд. Ежедневные объёмы торгов на пике достигали \$1,5 млрд.

Рост A7A5 не остался незамеченным. В октябре 2025 года 19-й пакет санкций ЕС ввёл запрет на транзакции с A7A5, а также внёс в санкционные списки связанные с ним компании. В апреле 2026 года 20-й пакет санкций ЕС пошёл ещё дальше. В санкционные списки добавили ещё один рублёвый стейблкоин — RUBx. Результат этих мер — двукратное падение дневных объёмов A7A5 (с \$1,5 млрд до примерно \$500 млн) после того, как крупные децентрализованные биржи вроде Uniswap добавили токен в свои блок-листы, а связанные с A7A5 кошельки начали замораживаться.

Вывод из Главы 13

Санкционная реальность разделила рынок стейблкоинов на два уровня. Верхний — долларовые стейблкоины (USDT, USDC) — остаётся основным рабочим инструментом для внешних расчётов. Нижний — рублёвые стейблкоины вроде A7A5 — формирует параллельную инфраструктуру для обхода западного контроля.

Для пользователя это означает, что выбор стейблкоина сегодня — не только вопрос удобства и комиссий, но и вопрос геополитического риска. Хранение крупных сумм в USDT несёт риск блокировки. Использование рублёвых стейблкоинов — риск санкций для ваших иностранных партнёров. Поэтому в 2026 году ключевой стратегией становится диверсификация: не держать все яйца в одной корзине, распределять активы между разными инструментами и тщательно проверять контрагентов.

Использованные в главе источники:

- 1) Как криптовалюта финансирует российскую войну <https://cepa.org/article/how-crypto-funds-russias-war/>
- 2) Новости криптовалют сегодня: Tether замораживает USDT на 340 миллионов долларов, поскольку давление на соблюдение требований по обеспечению соблюдения криптовалют в США усиливается <https://www.analyticsinsight.net/news/crypto-news-today-tether-freezes-340m-usdt-as-us-crypto-enforcement-pressure-widens>
- 3) Несмотря на международные санкции, рублёвый стейблкоин A7A5 в прошлом году обогнал USDT и USDC <https://www.coindesk.com/zh/markets/2026/01/09/a-ruble-stablecoin-outpaced-market-leaders-last-year-despite-international-sanctions>

- 4) ЕС нацелен на криптовалюты, уклоняющиеся от санкций, и союзников России по 20-му пакету санкций <https://www.mittrade.com/insights/news/live-news/article-3-1664668-20260424>
- 5) Фриланс и USDT в 2026 году: как получать оплату в крипте и не получить бан от банка <https://wellcrypto.io/ru/blog/frilanser-usdt-oplata-2026-nalogi-blokirovki/>
- 6) Криптовалюты: способ избежать санкций? <https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-evade-sanctions>
- 7) Министерство финансов США вводит санкции против связанных с Ираном криптокошельков и замораживает цифровые активы на сумму 344 млн долларов <https://www.tronweekly.com/us-treasury-targets-iran-linked-crypto/>
- 8) Объем российского стейблкоина A7A5, обеспеченного рублем, превышает 90 миллиардов долларов, опережая USDT и USDC <https://www.kucoin.com/news/flash/russia-s-ruble-stablecoin-a7a5-supply-surpasses-90-billion-outpaces-usdt-and-usdc>
- 9) ЕС ударил по российской криптовалюте полным запретом CASP и блокировкой цифрового рубля <https://coinmarketcap.com/community/articles/69eb611e720dcb27e41c2cc3/>
- 10) Сеть «Овальный флаг»: сеть российских криптоплатформ для обхода санкций <https://www.gate.com/zh-tw/post/status/18947906>

Часть 5. Стратегии выживания и процветания

Глава 14. Как легально завести крипту в Россию

После всего, что мы обсудили в предыдущих главах — блокировок карт, уголовных дел, санкционных рисков и «грязной» ликвидности — может сложиться впечатление, что единственный безопасный способ работать с криптовалютой в России — это не работать с ней вовсе. Но это не так.

С 1 июля 2026 года вступает в силу новый закон «О цифровой валюте и цифровых правах», который кардинально меняет правила игры. Вместо «серой зоны», где каждый сам за себя, государство создает легальную инфраструктуру: с лицензированными посредниками, налогами и защитой прав. Теперь завести крипту в Россию можно полностью «в белую» — и в этой главе мы разберем, как именно.

Работа через операторов ЦФА (пошаговая инструкция)

Самый понятный и прозрачный способ войти в легальный крипторынок — использовать платформы операторов цифровых финансовых активов (ЦФА). На апрель 2026 года в реестре Банка России уже 20 таких операторов. Давайте разберем, как это работает и с чего начать.

Шаг 1. Выберите оператора ЦФА. Список лицензированных площадок обширен: Сбербанк, Альфа-Банк, Т-Банк, Газпромбанк, платформа «Атомайз», «Лайтхаус», «Мастерчейн» и другие. Все они имеют лицензию ЦБ, что означает: государство признает их деятельность законной, а ваши инвестиции — защищенными. При выборе обратите внимание на три параметра: удобство интерфейса, комиссии, какие именно активы доступны.

Шаг 2. Откройте счет и пройдите идентификацию. Процедура та же, что и при открытии брокерского счета: паспорт, ИНН, подтверждение личности. Никакой анонимности, но и никаких блокировок «по подозрению» — все операции прозрачны для регулятора, а значит, не вызовут вопросов у банка.

Шаг 3. Приобретите ЦФА, привязанные к криптовалютам. Здесь есть важный нюанс: ЦФА — это не сама криптовалюта, а токенизированный актив, привязанный к ее курсу. Вы покупаете цифровой финансовый актив, который отражает стоимость биткоина или эфира, но с юридической точки зрения это полностью регулируемый инструмент. Для неквалифицированных

инвесторов доступны только те криптовалюты, что прошли российский листинг — на данный момент это Bitcoin и Ethereum.

Шаг 4. Соблюдайте лимиты. Для неквалифицированных инвесторов установлен годовой лимит на покупку криптовалют — до 300 тысяч рублей через одного посредника. Квалифицированные инвесторы таких ограничений не имеют. Перед первой сделкой нужно пройти бесплатное тестирование (аналог того, что проходят инвесторы перед покупкой сложных финансовых инструментов) и подписать уведомление о рисках.

Шаг 5. Уплатите налоги. Доход от операций с ЦФА облагается НДФЛ по прогрессивной шкале от 13% до 22%, как и любой другой инвестиционный доход.

Важное предупреждение для всех держателей криптовалют

С 1 июля 2026 года валютные резиденты РФ будут обязаны уведомлять ФНС о зарубежных криптокошельках в течение 30 дней с момента открытия. Но формы уведомления на момент написания книги не существует.

Дело в том, что обязанность уведомлять ФНС о зарубежных криптокошельках появится только с 1 июля 2026 года, и сам законопроект об этом всё ещё находится на стадии рассмотрения.

Что говорят источники?

Информация из проверенных деловых и правовых изданий однозначна:

1. **Обязанность ещё не вступила в силу.** Все источники сходятся во мнении, что уведомлять ФНС о криптокошельках нужно будет только с **1 июля 2026 года**. Эта норма содержится в правительственном законопроекте №1194929-8, который на данный момент (конец апреля — начало мая) только прошёл первое чтение в Госдуме.
2. **Нет утверждённой формы.** Законопроект устанавливает саму обязанность, но **порядок и форма** подачи уведомления ещё не разработаны. Этим будет заниматься Правительство РФ по согласованию с ЦБ. Поэтому скачать официальный бланк с сайта ФНС сейчас действительно невозможно.
3. **Нет санкций.** Пока в законодательстве отсутствует ответственность (штрафы) за неуведомление о кошельках.

Поэтому единственная рабочая рекомендация на сегодня — это следить за обновлениями на официальном портале ФНС (nalog.gov.ru) в июне-июле 2026 года. Как только закон заработает, форма появится именно там.

Экспериментальный налоговый режим для майнеров

Майнинг в 2026 году — полностью легальный бизнес. С января 2025 года доход от майнинга официально стал объектом налогообложения. Вот главное, что нужно знать майнеру.

Обязательная регистрация в реестре ФНС для всех, кто превышает лимит энергопотребления в 6000 кВт·ч в месяц. Для этого заходите на портал rmo.nalog.gov.ru через личный кабинет налогоплательщика, подаете заявление со списком оборудования (модели ASIC-майнеров, серийные номера) и адресом площадки. Срок рассмотрения — до 15 рабочих дней.

Налог возникает дважды: в момент зачисления криптовалюты на кошелек (доход от майнинга) и при продаже. Юридические лица платят налог на прибыль по ставке 25%. Индивидуальные предприниматели и физические лица — НДФЛ по прогрессивной шкале от 13% до 22%. Для ИП на УСН майнинг официально запрещен.

Из дохода можно вычесть документально подтвержденные расходы: электричество по счетчику, стоимость оборудования при наличии чеков и накладных, аренду помещения, интернет, ремонт и обслуживание.

Важный момент: региональные ограничения. В Дагестане, Чечне, Ингушетии, остальном Северном Кавказе и новых регионах майнинг запрещен полностью до 2031 года. В **Иркутской области** — **сезонный запрет** на осенне-зимний период. В **Бурятии и Забайкальском крае** — **круглогодичный запрет** (с 1 апреля 2026 года, до 15 марта 2031 года).

Покупка криптовалюты у юрлиц на СПБ Бирже

Московская и Санкт-Петербургская биржи официально заявили о готовности запустить торги криптовалютами, как только появится соответствующее регулирование. С 1 июля 2026 года такой запуск становится возможным. Торги будут проходить через брокеров с хранением активов в цифровых депозитариях — специальных организациях под надзором ЦБ.

Для частного инвестора это будет выглядеть как обычная покупка ценных бумаг: вы открываете брокерский счет, пополняете его рублями и даете поручение на покупку. Биржа выступает организатором торгов, брокер —

посредником, а депозитарий — хранителем актива. Неквалифицированным инвесторам будут доступны только Bitcoin и Ethereum с лимитом до 300 тысяч рублей в год. Квалифицированные инвесторы смогут покупать без ограничений.

Важный нюанс: вывод криптовалюты за пределы российского депозитария — только на счет лицензированной иностранной биржи. Вывод на личный кошелек законопроектом не предусмотрен, а ЦБ вправе устанавливать лимиты на вывод вплоть до полной блокировки.

Вывод из Главы 14

Легальный вход в криптовалюту для российского инвестора в 2026 году существует — и он станет еще доступнее. Три основных канала: через операторов ЦФА (уже работает, 20 лицензированных площадок), через биржевые торги (запуск с 1 июля 2026 года) и через легальный майнинг (с регистрацией в реестре ФНС). Главное, что объединяет все три способа — полная прозрачность для государства и, как следствие, отсутствие риска блокировок и уголовного преследования.

Мы вступаем в новую эру: из «серой зоны» криптовалюта в России переходит в регулируемое русло. И это хорошая новость для тех, кто готов платить налоги и спать спокойно.

Использованные в главе источники:

- 1) Мосбиржа рвется в крипту. Что нам с этого? <https://blogs.crypto.ru/mosbirzha-rvyotsya-v-kriptu/>
- 2) Налог на майнинг в 2026 году: реестр, отчетность и декларация без штрафов <https://companies.rbc.ru/news/NuaqbArSKX/nalog-na-majning-v-2026-godu-reestr-otchetnost-i-deklaratsiya-bez-shtrafov/>
- 3) Банк Уралсиб получил возможность выпускать цифровые финансовые активы <https://kras.mk.ru/economics/2026/04/24/bank-uralsib-poluchil-vozmozhnost-vypuskat-cifrovye-finansovye-aktivy.html>
- 4) Как запустить обращение криптовалютой в РФ и что даст стране новый рынок <https://expert.ru/analitika/kak-zapustit-obrashchenie-kriptovalyutoy-v-rf-i-cto-dast-strane-novyy-rynok/>
- 5) Законопроект о регулировании цифровых валют прошел I чтение в Госдуме <https://www.interfax-russia.ru/moscow/news/zakonoproekt-o-regulirovanii-cifrovyyh-valyut-proshel-i-chtenie-v-gosdume>
- 6) Прорвало сразу после ЦБ: Мосбиржа и "СПБ биржа" готовы запустить торги криптовалютами https://www.tbank.ru/invest/social/profile/Victoria_Business/17da57d5-a51b-4366-afb1-fc035dc7d192/?author=profile
- 7) Криптовалюта и налоги 2026: как не попасть на НДФЛ, блокировки и уголовку <https://www.klerk.ru/user/1963286/687416/>
- 8) Реестр операторов ЦФА расширился до 20 участников <https://ru.beincrypto.com/reestr-operatorov-czfa-20/>
- 9) Правительство РФ одобрило инициативу о легализации обращения цифровых валют <https://www.garant.ru/news/2039158/>
- 10) В России вводят комплексное регулирование крипторынка через лицензированных посредников <https://www.tks.ru/reviews/2026/03/31/0001/>

- 11) Налоговый дайджест от 06.04.2026 г.: новости, законы, контроль ФНС <https://www.pgplaw.ru/analytics-and-brochures/tax-reviews/tax-news-digest-06-04-26/>
- 12) Резидентов РФ могут обязать уведомлять ФНС об иностранных криптокошельках с 1 июля <https://www.interfax.ru/business/1081570>
- 13) Резидентов РФ могут обязать уведомлять ФНС об иностранных криптокошельках <https://iz.ru/2071255/2026-04-02/rezidentov-rf-mogut-obiazat-uedomliat-fns-ob-inostrannykh-kriptokoshelkakh>
- 14) Россиян планируют обязать уведомлять о зарубежных криптокошельках <https://78.ru/news/2026-04-02/v-rossii-planiruyut-obiazat-grazhdan-uedomlyat-o-zarubezhnih-kriptokoshelkah>
- 15) Резидентов РФ могут обязать уведомлять ФНС об иностранных криптокошельках <https://expert.ru/amp/news/rezidentov-rf-mogut-obiazat-uedomlyat-fns-ob-inostrannykh-kriptokoshelkakh/>
- 16) Резидентов РФ обяжут уведомлять налоговую о зарубежных криптокошельках с 1 июля 2026 года <https://www.klerk.ru/buh/news/686195/>
- 17) Резиденты РФ обязаны уведомлять ФНС об иностранных криптокошельках с 1 июля 2026 года <https://www.univ-tours.fr/annuaire/m-jean-philippe-lafontaine?live-news-1819391-2026-04-02-ezidentov-mogut-obiazat-uedomlat-ob-inostrannyh-kriptokosel-kah-s-1-iula-oskva-2>
- 18) Резиденты РФ должны будут сообщать налоговой об иностранных криптокошельках <https://www.x-compliance.ru/publications/podft/rezidenty-rf-dolzheny-budut-soobschat-nalogovoy-ob-inostrannyh-kriptokoshelkah>
- 19) Правительство предложило российским резидентам уведомлять ФНС об иностранных криптокошельках https://www.kommersant.ru/doc/8553529?from=horisontal_lenta
- 20) Учет блокчейн-кошельков в налоговой <https://www.nalogoved.ru/news/16429.html>

Глава 15. Как вывести крипту в рубли без потерь и блокировок

Вы купили биткоин, добыли его в майнинг-пуле, получили оплату от иностранного заказчика в USDT или просто хранили криптовалюту несколько лет, и теперь она стоит в разы дороже. Но пока это лишь цифры на экране. Чтобы превратить их в реальные деньги, нужно решить главную задачу: как вывести криптовалюту в рубли, не потеряв счет, не нарвавшись на блокировку и, тем более, не став фигурантом уголовного дела.

В 2026 году правила игры изменились кардинально. С 1 июля вступает в силу новый закон «О цифровой валюте и цифровых правах», который вводит лицензированных посредников и поэтапно запрещает нелегальный P2P-обмен. Одновременно ФНС и Росфинмониторинг усилили контроль: нейросети «Прозрачного блокчейна» круглосуточно сопоставляют банковские переводы с данными криптобирж.

В этой главе мы разберем, как безопасно и законно превратить крипту в наличные рубли. Все способы разделены по уровням сложности, риска и легальности: от быстрых малых сумм до полностью прозрачных схем с уведомлением государства.

Сценарий № 1: Использование малых сумм (до 600 тысяч рублей в месяц), чтобы не привлекать внимания банков

Для большинства обычных людей, чьи обороты не превышают 600 тысяч рублей в месяц, самым доступным и гибким инструментом вывода остаются P2P-площадки. Несмотря на то, что с 1 июля 2026 года «серый» P2P начнут постепенно выдавливать, у пользователей есть переходный период до 1 июля 2027 года, чтобы адаптироваться.

Однако уже с 1 июля 2026 года заработает механизм блокировки платежей в пользу площадок, не входящих в реестр ЦБ. Поэтому главное правило: **работать только через площадки, где соблюдается хотя бы минимальный KYC, и избегать одноранговых сделок в Telegram.**

Механика вывода. Вы регистрируетесь на бирже, поддерживающей P2P-торговлю с рублем (Bybit, OKX, MEXC, Bitget, KuCoin), переводите туда криптовалюту, размещаете ордер на продажу, выбираете покупателя с высоким рейтингом (десятки тысяч завершенных сделок) и получаете рубли на свою банковскую карту или через СБП.

Почему P2P до сих пор работает и остается популярным. Во-первых, комиссия минимальна или вообще отсутствует. Во-вторых, сделки защищены системой эскроу: крипта не перейдет покупателю, пока продавец не подтвердит получение рублей. В-третьих, есть гибкость — можно использовать разные способы оплаты и договариваться о курсе.

Пять правил безопасности, которые защитят вас от блокировки:

1. **Используйте отдельную карту.** Никогда не принимайте переводы от P2P-сделок на зарплатную или кредитную карту. Заведите отдельную дебетовую карту в банке из топ-10. Если ее заблокируют, вы не останетесь без средств к существованию.
2. **Никаких крипто-терминов в назначении платежа.** Слова «биткоин», «USDT», «крипта» в комментарии к переводу — это мгновенный красный флаг для банковского робота.
3. **Выбирайте только проверенных контрагентов.** Ориентируйтесь на пользователей с десятками тысяч успешных сделок, верифицированными аккаунтами и рейтингом выше 99%. Курс у них может быть чуть ниже рыночного, но это плата за безопасность.
4. **Разбивайте крупные суммы.** Продажа 5000 USDT в один заход — это риск. Лучше разбить на пять сделок по 1000 USDT с разными проверенными трейдерами в разные дни. Это снижает внимание банковских алгоритмов.
5. **Всегда фиксируйте подтверждения.** Скриншоты ордера, переписка с контрагентом, выписка из банка о поступлении средств — этот пакет документов при блокировке станет вашим единственным доказательством законности происхождения денег.

Важнейший нюанс, который нужно помнить всегда: **как только совокупный оборот по всем вашим криптокошелькам за год приближается к 600 тысячам рублей, вы обязаны подать отчет в ФНС.** Это требование валютного контроля, и его игнорирование ведет к серьезным штрафам.

Сценарий № 2: Полностью легальный путь через самозанятость и договоры с физлицами

С 1 января 2025 года самозанятым официально запретили легализовывать доходы от операций с криптовалютой через режим налога на профессиональный доход (НПД). Налоговая четко разъяснила: доход от продажи криптовалюты не подпадает под НПД. Следовательно, схема «зарегистрироваться как самозанятый и платить 4-6% с крипто-доходов» в 2026 году больше не работает.

Вы имеете право продать криптовалюту как физическое лицо, и это будет законно. Но доход от этой продажи облагается налогом на доходы физических лиц (НДФЛ) по прогрессивной шкале от 13% до 22%, в зависимости от вашего совокупного годового дохода.

При расчете налога вы можете уменьшить налогооблагаемую базу на сумму документально подтвержденных расходов на приобретение криптовалюты. Например, если вы купили биткоин за 1 млн рублей, а продали за 3 млн рублей, налог вы заплатите не со всей суммы, а с разницы — с 2 млн рублей прибыли.

Легализация через договор купли-продажи. Чтобы обезопасить себя, оформите сделку через стандартный договор купли-продажи имущества (криптовалюта по закону — это именно имущество, а не средство платежа). Необходимо указать в договоре паспортные данные обеих сторон и адрес кошелька. В договоре обязательно пропишите, что цена выражена в рублях. Это позволит в случае необходимости подтвердить происхождение средств в банке и ФНС. После продажи подается декларация 3-НДФЛ, и с полученной прибыли уплачивается налог по ставке 13-15%.

Альтернативный легальный путь для бизнеса. Если ваши обороты значительны, вы можете зарегистрироваться как ИП на общей системе налогообложения (ОСН) и платить налог на прибыль по ставке 25%. Это имеет смысл при оборотах свыше нескольких миллионов рублей в год, заменяя собой устаревшую схему с УСН (Доходы 6% или Доходы минус расходы 15%), которая часто привлекала внимание ФНС как «непрофильная» для крипто-сделок.

Сценарий № 3: Полностью легальный выход через уведомление ФНС

Для тех, кто хочет абсолютной прозрачности и полной защиты от любых претензий, существует путь полного декларирования. С 1 июля 2026 года он станет не просто добровольным, а обязательным для многих.

О чём именно нужно уведомлять.

- **О зарубежных криптокошельках.** С 1 июля 2026 года все валютные резиденты РФ обязаны уведомлять ФНС об открытии и закрытии блокчейн-кошельков в иностранных системах. Срок — не позднее одного

месяца со дня открытия или закрытия. Пока не уточняется, нужно ли сообщать о кошельках, открытых до 1 июля 2026 года.

- **О годовом обороте.** Как только совокупный оборот по всем вашим зарубежным криптокошелькам превысит 600 тысяч рублей в год, вы обязаны ежегодно подавать в ФНС специальный отчет о движении средств.
- **О владении криптовалютой.** В рамках ежегодной декларационной кампании (до 30 апреля следующего года) вы обязаны задекларировать доход от продажи криптовалюты, подав форму 3-НДФЛ.

Порядок действий для полной легализации:

1. **Уведомление ФНС об иностранном криптокошельке.** Форма уведомления утверждена Приказом ФНС. В ней указываются: ваши ФИО, ИНН, адрес кошелька (публичный ключ), наименование цифровой валюты, дата открытия кошелька и наименование оператора информационной системы (например, [Blockchain.com](https://blockchain.com), Tron, Ethereum).
2. **Подача ежегодного отчета о движении средств.** Если оборот по кошельку превысил 600 тысяч рублей, вы обязаны подать отчет, в котором детализируете все входящие и исходящие транзакции за отчетный период.
3. **Подача налоговой декларации 3-НДФЛ.** В декларации вы указываете доход от продажи криптовалюты, применяете налоговые вычеты (например, имущественный вычет по расходам на приобретение) и рассчитываете сумму НДФЛ к уплате по прогрессивной ставке от 13% до 22%.

О статусе уведомления в ФНС

На момент написания книги закон об обязательном уведомлении о зарубежных криптокошельках находится на стадии принятия. Ожидается, что он вступит в силу с 1 июля 2026 года. Конкретная форма уведомления и порядок ее подачи будут утверждены ФНС отдельным приказом. До появления официального бланка рекомендуем использовать образец договора купли-продажи криптовалюты (см. Приложение 1) как основной документ для подтверждения законности происхождения средств.

Вывод из Главы 15

Вывод криптовалюты в рубли в 2026 году — это не просто техническая операция, а юридически значимый шаг, который может иметь серьезные налоговые и правовые последствия. Государство планомерно создает

систему тотального контроля, где «серая зона» сжимается, а цена ошибки постоянно растет.

Три главных правила для безопасного вывода:

1. **Не храните крупные суммы на биржах и транзитных картах.** Вывели деньги — сразу перевели их на основной счет или сняли наличными.
2. **Платите налоги.** Декларация 3-НДФЛ с уплаченным налогом — это не просто обязанность, а ваша страховка от обвинений в незаконном предпринимательстве или отмывании денег.

Будьте готовы к переходу на полностью легальные каналы. С 1 июля 2026 года начинается новая эра регулирования. P2P-обмен без посредника будет окончательно запрещен с 1 июля 2027 года. Чем раньше вы освоите работу через лицензированные платформы или наладите прямой документальный обмен, тем спокойнее будет ваша жизнь.

Использованные в главе источники:

- 1) Новый закон о крипте от 1 апреля 2026: что изменится для обычных людей уже этим летом <https://www.klerk.ru/user/2551474/687356/>
- 2) Законопроект о регулировании цифровых валют прошел I чтение в Госдуме <https://www.interfax-russia.ru/moscow/news/zakonoproekt-o-regulirovanii-cifrovyyh-valyut-proshel-i-chtenie-v-gosdume>
- 3) Крипта под контролем 2026: налоги, блокировки счетов и безопасный вывод денег <https://www.klerk.ru/blogs/exchagent/684223/>
- 4) Криптовалюта в России с 1 июля 2026 года: что известно о новом законопроекте <https://riamo.ru/articles/shpargalki/kriptovaljuta-v-rossii-s-1-ijulja-2026-goda-chto-izvestno-o-novom-zakonoproekte/>
- 5) Госдума одобрила в первом чтении законопроект о цифровых валютах <https://nbi.ru/news/gosduma-odobrila-v-pervom-chtenii-zakono/72989/>
- 6) В Госдуму внесли новую инициативу по криптовалютам в России <https://news.ru/amp/vlast/v-gosdumu-vnesli-zakon-o-kontrole-za-kriptovalyutoj>
- 7) Госдума приняла в первом чтении пакет законопроектов по легализации обращения цифровых валют https://www.akm.ru/news/gosduma_prinyala_v_pervom_chtenii_paket_zakonoproektov_po_legalizatsii_obrashcheniya_tsifrovyykh_valyut/
- 8) Крипту легализуют, но не для всех: новые правила доступа для инвесторов <https://www.fd.ru/news/64529-kriptu-legalizuyut-no-ne-dlya-vseh-novye-pravila-dostupa-dlya-investorov>
- 9) Согласно новым предложениям, россиянам будет запрещено обменивать криптовалюту на наличные деньги <https://coinmarketcap.com/community/articles/69d8f2fd4601924793d61006/>
- 10) Россиянам не будет разрешено обменивать криптовалюту на наличные согласно новым предложениям <https://www.mittrade.com/au/insights/news/live-news/article-3-1624878-20260410>
- 11) Может ли самозанятый в 2026 г работать с криптовалютой и платить налог на профессиональный доход? <https://vc.ru/id1377271/2708235-samozanyatye-i-kriptoaluta-v-2026-godu>
- 12) Налог на криптовалюту в России: что нужно знать в 2026 году <https://habr.com/ru/articles/1004046/>
- 13) Как самозанятому платить налог с продажи USDT в 2026 году <https://pravoved.ru/question/4799523/>
- 14) Самозанятые в 2026 году: изменения, ставки, налоги, как перейти <https://www.glavbukh.ru/art/390747-samozanyatye-v-2026-godu-izmeneniya-stavki-nalogi-kak-pereyti-s-1-yanvarya>
- 15) Налогообложение криптовалюты в разных странах мира <https://iworld.com/ru/blog/tax-cryptocurrency>

- 16) Изменения в налогах на майнинг и криптовалюты: что ждет в 2026 году <https://companies.rbc.ru/news/q9qPMm1mvn/izmeneniya-v-naloga-na-majning-i-kriptovalyutyi-cto-zhdet-v-2026-godu/>
- 17) ИП, криптовалюта и ФНС в 2026 году: как выстроить работу с криптовалютой и платить налоги на УСН в новых реалиях? <https://vc.ru/id1377271/2700711-rabota-ip-s-kriptovalyutoy-i-nalogi-na-usn-v-2026-godu>
- 18) Глобальное руководство по налогообложению ... <https://www.cryptopolitan.com/ru/global-crypto-tax-guide-2026/>
- 19) Руководство по налогам на криптовалюту в 2026 году <https://www.bittrue.com/ru/blog/crypto-tax-guide-2026-investors-key-to-profit>
- 20) КРИПТОВАЛЮТА и НАЛОГИ | Полный анализ 2026 г. <https://www.youtube.com/watch?v=Jp-6N7Vs5oE>
- 21) Отчет по майнингу цифровой валюты: сроки сдачи в ФНС для ИП и юрлиц в 2026 году <https://www.business.ru/article/5891-otchet-po-mayningu-tsifrovoy-valyuty>
- 22) Криптовалюта и налоги 2026: как не попасть на НДФЛ, блокировки и уголовку <https://www.klerk.ru/user/1963286/687416/>
- 23) Резиденты РФ обязаны уведомлять ФНС об иностранных криптокошельках с 1 июля 2026 года <https://www.univ-tours.fr/annuaire/m-jean-philippe-lafontaine?live-news-1819391-2026-04-02-ezidentov-mogut-obazat-vedomlat-ob-inostrannyh-kriptokosel-kah-s-1-iula-oskva-2>
- 24) Налоговый дайджест от 06.04.2026 г.: новости, законы, контроль ФНС <https://www.pgplaw.ru/analytics-and-brochures/tax-reviews/tax-news-digest-06-04-26/>
- 25) Криптовалюту приравнивают к валютным ценностям <http://m.vkirove.ru/news/2026/04/21/prirovnyat-kriptovalyutu-k-valyutnym-tsennostyam-predlozhilo-pravitelstvo-zakonoproekt-v-gosdume.html>
- 26) Валютных резидентов РФ могут обязать уведомлять ФНС об иностранных криптокошельках <https://nebohod.media/nashi-smi/moscow-post-su-valyutnyh-rezidentov-rf-mogut-obyazat-vedomlyat-fns-ob-inostrannyh-kriptokoshelkah-199335/>
- 27) Россия требует декларировать зарубежные криптокошельки и отчитываться перед налоговыми органами <https://t.signalplus.com/crypto-news/detail/russia-report-foreign-crypto-wallets-fns?lang=zh-CN>
- 28) Резиденты РФ должны будут сообщать налоговой об иностранных криптокошельках <https://www.x-compliance.ru/publications/podft/rezidenty-rf-dolzny-budut-soobschat-nalogovoy-ob-inostrannyh-kriptokoshelkah>
- 29) Представить в ИФНС сведения о майнинге цифровой валюты <https://spmag.ru/events/789>
- 30) Российских резидентов обяжут уведомлять ФНС об иностранных криптокошельках <https://www.rzn.info/news/2026/4/2/rossijskih-rezidentov-obyazhut-vedomlyat-fns-ob-inostrannyh-kriptokoshelkah-341752.html>
- 31) Как вывести криптовалюту в рубли легально в 2026 году: способы, законы и риски <https://1000bankov.ru/wiki/kak-vyvesti-kriptovalyutu-v-rubli-legalno-v-2025-godu-sposoby-zakony-i-riski/>
- 32) P2P-обменники: прямые сделки с криптовалютой и ключевые аспекты выбора <https://companies.rbc.ru/news/YBJXnL7nUH/p2p-obmenniki-pryamye-sdelki-s-kriptovalyutoy-i-klyuchevye-aspekty-vyibora/>
- 33) Как вывести крипту с Trust Wallet через P2P — 2026 <https://rutube.ru/video/9c602646d58749c47b6a97eb1620ef31/>
- 34) Основные криптовалютные биржи, поддерживающие вывод средств на банковские карты <https://www.gt-io.com/zh/crypto-wiki/article/the-best-cryptocurrency-exchanges-with-card-withdrawal-options-20260201>
- 35) Путеводитель по российским биржам на 2026 год: управление ликвидностью активов в эпоху цифрового рубля <https://www.kucoin.com/zh-hant/blog/id-2026-russia-exchange-guide-navigating-asset-liquidity-in-the-digital-ruble-era>
- 36) Путеводитель по российской бирже на 2026 год: Навигация по ликвидности активов в эпоху цифрового рубля <https://www.kucoin.com/blog/en-2026-russia-exchange-guide-navigating-asset-liquidity-in-the-digital-ruble-era>
- 37) Top 5 P2P Crypto Platforms in Russia: Safe Bitcoin Buying Guide (2026) <https://bingx.com/es-la/learn/article/top-p2p-crypto-platforms-in-russia-buy-bitcoin-safely>
- 38) CactusPay — моментальный приём оплат и выплаты в USDT! Без верификации и блокировок <https://forum.kurs.expert/threads/cactuspay-momentalnyj-prijom-oplat-i-vyplaty-v-usdt-bez-verifikacii-i-blokirovok.8946/page-2#post-102629>
- 39) Руководство по российским биржам 2026: Навигация по ликвидности активов в эпоху цифрового рубля <https://www.kucoin.com/ru/blog/pt-2026-russia-exchange-guide-navigating-asset-liquidity-in-the-digital-ruble-era>
- 40) ЦБ предлагает разрешить банкам и брокерам получать лицензии криптообменников в уведомительном порядке <http://www.finmarket.ru/currency/news/6573410>

- 41) Лицензия для криптообменников будет несложной, если они не работают с рынком ценных бумаг <http://www.finmarket.ru/database/news/6547891?fid=7471&fs=T&ref=AnketaOrg>
- 42) ЦБ предложил ввести уголовную ответственность за криптодеятельность без лицензии <https://iz.ru/2076137/2026-04-09/tcb-predlozhit-vvesti-ugolovnuu-otvetstvennost-za-kriptodeiatelnost-bez-litsenzii#main-content>
- 43) ЦБ предложил наделить банки функциями криптообменников <https://expert.ru/finance/kripta-ishchet-vykhod/>
- 44) ЦБ и Минфин определили правила работы крипторынка <https://pravo.ru/news/262555/>
- 45) Регулирование криптовалют в России в 2026 году: новые законы, лицензирование и налоги https://www.klerk.ru/blogs/exchagent/677827/?srsltid=AfmBOor8kiBpXrgInZOdY4GwduZApoM8zPF_Er63j7c7S6L_e967Fo0zZ
- 46) Полный контроль ЦБ: согласован новый закон о регулировании крипторынка <https://mспmo.ru/news/polnyy-kontrol-tsb-soglasovan-novyj-zakon-o-regulirovanii-kriptyrynka/>
- 47) Криптообменники в России начнут работать по новым правилам <https://legalacademy.ru/sphere/post/kriptoobmenniki-v-rossii-nachnut-rabotat-po-novym-pravilam>
- 48) ЦБ и Минфин договорились о регулировании криптоотрасли <https://ru.investing.com/news/general-news/article-3125266>
- 49) ЦБ и Минфин разработали правила регулирования криптоотрасли <https://plusworld.ru/advertising/>
- 50) Новые правила игры навсегда изменили рынок цифровых активов в России <https://argumenti.ru/society/2026/04/993610/amp>
- 51) «Прозрачный блокчейн»: эксперт пояснил, почему анонимность крипты кончилась <https://mosregtoday.ru/news/sec/prozrachnyj-blokchejn-ekspert-pojasnii-pochemu-anonimnost-kripty-konchilas/>
- 52) Легальна ли криптовалюта в России? Законы, ограничения и обновления 2026 года <https://westafricatradehub.com/crypto/is-crypto-legal-in-russia/>
- 53) Розничные лимиты: неквалифицированным инвесторам грозит годовой лимит покупки в размере 300 000 рублей (~ 3800 долларов США) <https://www.binance.bh/en-IN/square/post/308555793938801?sqb=1>
- 54) Эксперт: кому грозит тюремный срок за майнинг и покупку криптовалюты https://vfokuse.mail.ru/articles/69616585-ekspert-komu-grozit-tyuremnyj-srok-za-majning-i-pokupku-kriptoalyuty/?utm_partner_id=969
- 55) Криптовалюта в РФ будет приравнена к банковским вкладам <https://www.hill.ru/press-center/kriptoalyuta-v-rf-budet-pripravnena-k-bankovskim-vkladam/>
- 56) Интересует вопрос о налоговом законодательстве в сфере криптовалюты <https://d0.pravoved.ru/question/4875246/>
- 57) Налоги и крипта: что нужно знать российскому инвестору <https://investfuture.ru/articles/nalogi-i-kripta-cto-nuzhno-znat-rossiyskomu-investoru>
- 58) Риски операций с криптовалютой для физлиц и ИП в России: налоги, банки, законы в 2026 году <https://amp.spark.ru/user/265425/blog/292141/riski-operatsij-s-kriptoalyutoj-dlya-fizlits-i-ip-v-rossii-nalogi-banki-zakoni-v-2026-godu>
- 59) Регуляция крипты 2026: что изменится для держателей цифровых активов с 1 января <https://finbazar.ru/hashtag/%d0%bd%d0%b0%d0%bb%d0%be%d0%b3%d0%b8%d0%bd%d0%ba%d1%80%d0%b8%d0%bf%d1%82%d1%83>
- 60) Криптовалюта по правилам: как новый закон разделит российских инвесторов на своих и чужих https://nbj.ru/pubs/kriptoalyuta_po_pravilam_kak_novyj_zakon_72686/
- 61) Лимит на покупку криптовалют для «неквалов» в 300 тыс. руб. - не финальный вариант <http://www.finmarket.ru/news/6547605>
- 62) Минфин поддержал идею допустить неквалифицированных инвесторов к торгам криптой <https://expert.ru/news/minfin-podderzhal-ideyu-dopustit-nekvalifitsirovannykh-investorov-k-torgam-kriptom/>
- 63) Минфин: Лимит на покупку криптовалют для «неквалов» в 300 тыс. руб. - не финальный вариант, цифру можно обсуждать <https://rusbonds.ru/news/20260122141900939216>
- 64) Аналитик Смирнов: интерес россиян к криптовалюте упадет из-за лимита операций https://mt.gazeta.ru/blog/43508207971/Analitik-Smirnov-interes-rossiyan-k-kriptoalyute-upadet-iz-za-limita-operatsij?utm_referrer=mirtesen.ru
- 65) В ЦБ объяснили причины допуска россиян к криптовалютам и лимиты на них https://news.mail.ru/society/70515112/?utm_partner_id=969
- 66) ЦБ и Госдума готовят правила для безопасной покупки криптовалют россиянами <https://ura.news/news/1053062870>
- 67) Центробанк определил условия доступа россиян к рынку криптовалют <https://vecherka-spb.ru/2026/01/26/tsentrobank-opredelil-usloviya-dostupa-rossiyan-k-rinku-kriptoalyut>

- 68) «Казино»: Лимит на покупку криптовалют не спасет инвесторов от разорения
<https://nsn.fm/society/kazino-limit-na-pokupku-kriptoalut-ne-spaset-ot-razoreniya>
- 69) В Минфине готовы дальше обсуждать годовой лимит на покупку криптовалют для «неквалов»
<https://m.interfax.ru/1068996>
- 70) Эксперты опасаются ухода владельцев криптовалют в серую зону из-за новых законов
<https://www.vedomosti.ru/finance/news/2026/04/22/1192102-eksperti-opasayutsya-uhoda?from=newsline>
- 71) Законопроект о регулировании цифровых валют прошел I чтение в Госдуме
<https://www.interfax.ru/business/1085154>
- 72) Ограничить и защитить: рынок криптовалют в России выводят из серой зоны
<https://www.ntv.ru/novosti/2977135>
- 73) Пакет законопроектов о регулировании криптовалютного рынка РФ Госдума рассмотрит 21 апреля
<http://www.finmarket.ru/news/6602092>
- 74) Владельцев тайных криптокошельков в России начнут штрафовать
Источник: <https://deita.ru/article/583761> © DEITA.RU <https://deita.ru/article/583761>
- 75) Госдума поддержала легализацию криптовалюты в России <https://kprfnsk.ru/inform/news/48673/>
- 76) Первое чтение законопроектов о регулировании крипторынка намечено на 21 апреля
<https://www.interfax.ru/russia/1084558>
- 77) В России вводят комплексное регулирование крипторынка через лицензированных посредников
<https://www.tks.ru/reviews/2026/03/31/0001/>

Глава 16. Чек-лист «Нулевой риск»

Эта глава отличается от всех предыдущих. Если раньше мы подробно разбирали каждый закон, каждую схему и каждый риск, то здесь я собрала для вас три самых практических алгоритма действий. Это та глава, которую стоит перечитать дважды, сохранить в закладках, а раздел о блокировке счета — держать под рукой на отдельном листе.

Три главные темы, которые мы разберем:

1. Как проверить контрагента, чтобы не получить «грязные» рубли или криптовалюту.
2. Правило «трех кошельков» — как организовать хранение, чтобы даже под физическим давлением сохранить основной капитал.
3. Что делать (конкретно, по шагам), если банк всё-таки заблокировал ваш счет.

Проверка контрагента по базе ФНС и сервисам блокчейн-разведки

Любая сделка с криптовалютой — это встреча с незнакомцем. Вы не знаете, откуда у него деньги, не знаете, не находится ли он под санкциями, не знаете, не числится ли его кошелек в «серых списках» Росфинмониторинга. Но вы можете это проверить. Инструменты проверки делятся на два эшелона: блокчейн-аналитика (для крипто-адресов) и государственные реестры (для фиатных контрагентов).

Блокчейн-аналитика: как проверить чистоту криптовалютного адреса. Блокчейн — это открытая база данных, в которой каждая транзакция записана навсегда. Специализированные компании — Chainalysis, Crystal, Elliptic — анализируют цепочки переводов и помечают адреса по категориям: биржа, миксер, азартные игры (gambling), даркнет, мошенничество, санкционный адрес. Важно понимать: AML-проверка не только защищает от проблем с законом, но и служит индикатором благонадежности контрагента. Если кошелек имеет связи с ненадежными или опасными источниками, это повод отказаться от сделки.

Сервисов для проверки множество, от бесплатных до корпоративных. Приведем основные:

- **AMLBot** — популярный сервис, доступный через веб-интерфейс и Telegram-бота. Поддерживает более 22 блокчейнов, стоимость проверки от 0,3 до 3 долларов США.
- **GetBlock** — еще один удобный инструмент с собственным Telegram-ботом, поддерживает 8 блокчейнов.
- **Matbea** — сервис от известного в прошлом обменника, стоимость проверки от 0,12 евро.
- **MistTrack** — бесплатная разовая проверка адресов с риск-оценкой.
- **Cryptomus** — мультичейн-сервис с полностью бесплатной разовой проверкой для физических лиц.

Важнейший инструмент для российского пользователя — **AML-анализатор BestChange**. С апреля 2026 года он работает с данными шести провайдеров, а стоимость проверки варьируется от 0 до 4,5 долларов в зависимости от количества задействованных сервисов. BestChange поддерживает более 80 криптовалют и токенов, включая BTC, ETH, USDT, USDC и DAI в различных сетях.

На что обращать внимание в результатах проверки? Адреса, связанные с миксерами, даркнетом, украденными монетами, замороженными юридическими лицами и санкционными площадками (например, Garantex, Tornado Cash), получают «красные метки». Даже единичный переход через такой адрес повышает ваш уровень риска и может привести к заморозке средств на бирже.

Государственные реестры: проверка фиатного контрагента. С крипто-адресом разобрались. Но если вы заключаете договор купли-продажи с физическим лицом или компанией, вам нужен второй эшелон проверки — через государственные базы данных. Главный инструмент здесь — **сервис ФНС России «Прозрачный бизнес»**, доступный по адресу pb.nalog.ru. Этот сервис бесплатно и в онлайн-режиме предоставляет комплексную информацию о юридических лицах и индивидуальных предпринимателях.

Что можно узнать через «Прозрачный бизнес»:

- Реквизиты и систему налогообложения контрагента;
- Численность сотрудников и финансовые показатели;
- Участие в других организациях;
- Задолженность перед бюджетом;
- Наличие налоговых правонарушений;
- Признаки массовой регистрации по юридическому адресу.

Поиск можно вести по ИНН, ОГРН, наименованию компании, юридическому адресу и ФИО руководителя. Если вы имеете дело с физическим лицом — запросите его ИНН, это нормальная практика при заключении договора на крупную сумму. Для предпринимателей доступны расширенные инструменты: «1СПАРК Риски» и «1С:Контрагент».

Правило «трех кошельков»: архитектура безопасности

В Главе 10 мы подробно разбирали, как работают аппаратные кошельки, passphrase и техника «душа крипты». Теперь соберем это в единую архитектуру хранения, которая защитит вас и от цифровой атаки, и от физического принуждения.

Горячий кошелек — для повседневных операций. Это программный кошелек на телефоне или в браузере (Trust Wallet, MetaMask, Cake Wallet), который подключен к интернету. На нем хранится сумма, необходимая для текущих расходов — условно, не более 10% от вашего крипто-капитала. Эти деньги вы используете для обмена, оплаты или быстрых переводов. Скомпрометирован горячий кошелек — вы теряете не все, а лишь оперативный запас.

Холодный кошелек — ваш основной банковский сейф. Аппаратное устройство (Ledger, Trezor, Tangem, OneKey), которое хранит приватные ключи офлайн. На нем находится основная сумма — 70-80% вашего капитала. Сид-фраза хранится в разделенном виде в разных физических локациях, с использованием одного из методов, описанных в Главе 10. Холодный кошелек вы достаете только тогда, когда нужно пополнить горячий или зафиксировать крупную покупку.

«Смертный» кошелек — ваша страховка на черный день. Это самый специфический, но в российских реалиях 2026 года критически важный инструмент. Концепция «смертного» (duress) кошелька в том, что это кошелек, который вы спокойно отдадите злоумышленнику под физическим давлением — и он увидит там правдоподобную сумму (например, 0,05 BTC или эквивалент \$500), в то время как основные средства останутся скрытыми. Технически это реализуется через passphrase, кодовую фразу, которая разблокирует скрытый кошелек. Без этой фразы стандартная сид-фраза открывает пустой или отвлекающий кошелек.

Некоторые аппаратные кошельки, например Coldcard, позволяют настроить отдельный Duress PIN: при его вводе устройство работает нормально, но открывает совершенно отдельный кошелек, отличный от вашего основного.

Эта технология была разработана для защиты в ситуациях физического принуждения. Вы можете настроить свой собственный «смертный» кошелек с помощью функции `passphrase` на любом современном аппаратном кошельке. Важно: на «смертном» кошельке должна лежать правдоподобная сумма — не ноль (это вызовет подозрения), но и не миллион долларов. Сумма, которую вам психологически не жалко потерять.

Итоговая архитектура:

- Горячий кошелек: до 10% средств, для оперативных нужд.
- Холодный кошелек с `passphrase`: 70–80% средств, основной капитал.
- «Смертный» кошелек (холодный кошелек БЕЗ `passphrase`): правдоподобная сумма на случай физического давления.

Если банк всё-таки заблокировал счет: алгоритм действий

Мы детально разбирали механизмы 115-ФЗ и 161-ФЗ в Главе 3. Теперь — чистый алгоритм действий. Когда счет заблокирован, главное — не паниковать и не совершать резких движений. Действуйте по этой схеме.

Шаг 1. Установите причину блокировки. Первым делом нужно обратиться в службу поддержки банка, чтобы выяснить конкретную причину блокировки. Банк обязан сообщить вам, на каком основании введены ограничения. С 25 марта 2026 года ЦБ РФ рекомендовал банкам самостоятельно связываться с клиентами сразу же после приостановки операций для разъяснения причин. Банк должен указать, на каких правовых основаниях установлена блокировка, а также разъяснить пошаговый порядок действий для снятия ограничений.

Помните о принципиальной разнице между двумя законами, которую мы разбирали в Главе 3. Блокировка по 115-ФЗ действует только в конкретном банке. Блокировка по 161-ФЗ — это централизованный реестр Банка России, и счета блокируются одновременно во всех банках страны. Определите, по какому закону вас заблокировали — от этого зависит дальнейшая стратегия.

Шаг 2. Зафиксируйте все доказательства. Сделайте скриншоты всех уведомлений, СМС, push-сообщений из приложения банка. Запросите письменный перечень операций и оснований ограничений с указанием конкретных норм закона. Соберите документы, подтверждающие законность происхождения средств: договоры купли-продажи, скриншоты P2P-ордеров, переписку с контрагентом, выписки из криптокошелька, банковские выписки о поступлении средств, налоговую декларацию (если операция уже

задекларирована). Если у вас есть уплаченный налог с дохода от продажи криптовалюты — это ваш главный козырь.

Шаг 3. Пройдите реабилитацию на уровне банка. Предоставьте собранные документы в банк вместе с объяснительной запиской, детально описывающей экономический смысл операций. Если банк ограничил операции по собственной инициативе (а не на основании присвоенного ЦБ уровня риска), вы можете подать заявление о снятии ограничений в любое время, количество обращений неограниченно. Срок рассмотрения — от одного до десяти дней, в зависимости от политики банка и убедительности представленных документов.

Шаг 4. Если банк отказал — обжалуйте через Межведомственную комиссию ЦБ. Если банк мотивированно отказывается снимать ограничения, клиенту должны быть разъяснены процедуры обжалования. Обжаловать саму блокировку можно только в Межведомственной комиссии Центробанка (МВК). Сделать это нужно в течение 6 месяцев со дня, когда вы получили от банка сообщение о блокировке. Обращение в МВК — обязательный досудебный порядок: если эта процедура не пройдена, суд не будет рассматривать ваше обращение.

Параллельно вы можете подать жалобу в интернет-приемную Банка России и в Росфинмониторинг (если банк мотивирует блокировку 115-ФЗ). Шаблоны заявлений доступны на сайте ЦБ.

Шаг 5. Если МВК не помогла — обращайтесь в суд. Судебная практика по таким делам постепенно формируется в пользу добросовестных клиентов. Помните: операция с криптовалютой не равна правонарушению. Как мы неоднократно подчеркивали, прямого запрета на владение и продажу криптовалюты для физических лиц в России нет.

Важное обновление 2026 года, о котором нужно знать

С 1 января 2026 года приказ ЦБ удвоил перечень признаков подозрительных операций по 161-ФЗ — с 6 до 12. К типовым триггерам для физических лиц теперь относятся: переводы самому себе от 200 тысяч рублей с последующим переводом третьему лицу в течение суток, резкий рост оборотов, несоразмерный обычным доходам, получение большого количества переводов от разных лиц, переводы на клиентов из «серых списков» ЦБ, а также операции с цифровым рублем по новым риск-признакам.

Кроме того, ЦБ и Минцифры прорабатывают механизм разблокировки карт через портал «Госуслуги». Это означает, что в ближайшее время процесс может стать более прозрачным и быстрым. Но пока система работает в прежнем режиме, и ваша главная защита — документальная готовность.

Итоговый чек-лист «Нулевой риск»

- 1. Перед каждой сделкой проверяйте контрагента.** Кripto-адрес — через AML-анализатор (AMLBot, GetBlock, BestChange). Фиатного контрагента — через «Прозрачный бизнес» ФНС.
- 2. Разделите хранение на три кошелька.** Горячий (до 10%), холодный с passphrase (основной капитал), «смертный» (правдоподобная сумма на случай давления).
- 3. Храните сид-фразу отдельно.** Не на одном листе, не рядом с устройством, не в облаке.
- 4. Документируйте каждую сделку.** Скриншоты P2P-ордеров, переписка с контрагентом, выписка по кошельку — всё сохранять.
- 5. Платите налоги.** Декларация с уплаченным НДФЛ — ваш главный аргумент в споре с банком и ФНС.
- 6. При блокировке счета:** Спокойствие → Запрос причины → Сбор документов → Банк → МБК ЦБ → Суд.
- 7. Никаких крипто-терминов в назначении платежа.** И никаких сделок с подозрительным курсом.
- 8. Следите за новостями.** Регуляторная база меняется ежемесячно. То, что безопасно сегодня, может стать рискованным завтра.

Использованные в главе источники:

- 1) AML-проверка Биткоина в 2026 году - сервисы проверки чистоты <https://blog.proinvest.com/2025/11/aml-proverka-bitcoin-v-2025-godu-servisy-proverki-chistoty.html>
- 2) Проверка на отмывание (AML) кошелька в 2026: 7 этапов анализа, которые спасут ваши активы <https://vc.ru/crypto/2801185-aml-proverka-koshelka-7-etapov-analiza>
- 3) Криптообменники онлайн: какие сервисы работают стабильно в 2026 году <https://dtf.ru/flood/4850961-kriptobednik-online-nadezhnie-servisy-2026>
- 4) AML-проверка кошелька и криптовалют в 2026 году <https://crypto.ru/aml-proverka/>
- 5) Как проверить USDT на AML в 2026: Топ сервисов и пошаговое руководство <https://vc.ru/crypto/2622941-kak-proverit-usdt-na-aml>
- 6) Сайты для AML-проверки криптовалюты в 2026 году: лучшие скоринг-сервисы и почему их нужно использовать <https://proinvestment.com/sites-checking-cryptocurrencies/>
- 7) ТОП 10 платных и бесплатных AML-сервисов для проверки криптовалют в 2026 году <https://blog.proinvest.com/2025/11/reiting-aml-servisov-dlya-proverki-kriptovalyut.html>
- 8) AML Check Bot | AML проверка криптокошелька бесплатно <https://trusteeglobal.com/ru/aml-checker/>
- 9) Как проверить чистоту средств с помощью AML-сервиса BestChange? Инструкция <https://forklog.com/exclusive/kak-proverit-chistotu-sredstv-s-pomoshhyu-aml-servisa-bestchange-instruktsiya/>
- 10) AML проверка криптокошелька: лучшие сервисы для анализа транзакций и адресов <https://dtf.ru/howto/4555238-aml-proverka-kriptokoshelka>
- 11) Оценить надежность контрагентов поможет сервис ФНС России https://snezhnoe-r897.gosweb.gosuslugi.ru/dlya-zhiteley/novosti-i-reportazhi/novosti_3486.html

- 12) Сервис налоговой службы «Прозрачный бизнес» помогает проверить контрагентов https://taishet.irkmo.ru/news/?ELEMENT_ID=199615
- 13) GitHub - atomno-labs/mcp-fns-check: MCP-сервер для проверки российских контрагентов через открытые данные FNS (EGRUL/EGRIP, EFRSB, KAD, FSSP) <https://github.com/atomno-labs/mcp-fns-check>
- 14) Проверить себя и контрагента поможет электронный сервис «Прозрачный бизнес» <https://sp-inzer.ru/news/2025/03/7361/>
- 15) Проверить себя и контрагента поможет электронный сервис «Прозрачный бизнес» <https://podlubovo.ru/2025/03/7469/>
- 16) Где можно найти информацию о контрагенте? https://its.1c.ru/db/content/newsclar/src/487441.htm#_print
- 17) Проверить себя и контрагента поможет электронный сервис «Прозрачный бизнес» - Николаевский сельсовет Башкортостан Кармаскалинский район <https://nikolaevosp.ru/news/2025/03/2555/>
- 18) Сервис «Прозрачный бизнес» помогает оценить благонадежность контрагентов <https://korenovsk.ru/servis-prozrachnyj-biznes-pomogaet-ocenit-blagonadezhnost-kontragentov/>
- 19) Сервис "Прозрачный бизнес" дает возможность проверить контрагентов <https://volchansk-adm.ru/govinfo/govinfofns/media/2025/4/4/servis-prozrachnyj-biznes-daet-vozmozhnost-proverit-kontragentov/>
- 20) Сервис "Прозрачный бизнес" дает возможность проверить контрагентов <https://kgo66.ru/ekonomika/gm-eco-fns/servis-prozrachnyj-biznes-daet-vozmozhnost-proverit-kontragentov>
- 21) PIN-код COLDCARD Duress PIN — расширенная функция безопасности для аппаратных кошельков <https://coldcard.com/duress-pin>
- 22) Deus Wallet представляет режим принуждения: революционное решение для безопасности криптовалют <https://www.binance.me/de/square/post/17771612990138>
- 23) Deus Wallet представляет режим сотрудничества: революционное решение для безопасности криптовалют <https://bravenewcoin.com/es/interconexi%C3%B3n/Deus-Wallet-presenta-el-modo-de-coacci%C3%B3n%3A-la-soluci%C3%B3n-revolucionaria-para-la-seguridad-de-las-criptomonedas>
- 24) Deus Wallet представлен Duress Mode: новым революционным решением для криптовалют <https://www.binance.com/uk-UA/square/post/17771615519241>
- 25) Deus Wallet запускает Force Mode, инновационное решение для безопасности криптовалют <https://bravenewcoin.com/ko/%ED%86%B5%EC%B0%B0%EB%A0%A5/deus-%EC%A7%80%EA%B0%91--%EC%95%94%ED%98%B8%ED%99%94%ED%8F%90-%EB%B3%B4%EC%95%88%EC%9D%84-%EC%9C%84%ED%95%9C-%ED%98%81%EC%8B%A0%EC%A0%81%EC%9D%B8-%EC%86%94%EB%A3%A8%EC%85%98%EC%9D%B8-%27%EA%B0%95%EC%A0%9C-%EB%AA%A8%EB%93%9C%27-%EC%B6%9C%EC%8B%9C>
- 26) КОШЕЛЕК DEUS ВВЕДЕНИЕ <https://www.binance.me/en/square/post/17784641497330>
- 27) Deus Wallet представляет режим принуждения: революционное решение для безопасности криптовалют <https://www.binance.com/cs/square/post/1777450472746>
- 28) Физическая безопасность: Кошелёк на случай угрозы на Ledger и Trezor https://academy.exmon.pro/ru/fiziceskaia-bezopasnost-koselek-na-slucui-ugrozy-na-ledger-i-trezor?_cf_chl_rt_tk=p3Bje8Kui0TOG.svZWgKu2SXh2NvR0vg2I3nR_i6uQ-1777265156-1.0.1.1-GHELfXTnjqpnH5tmVMd6NncU70AaPqOOV6702Ylo2Ms
- 29) Deus Wallet представляет режим принуждения — революционное решение для безопасности криптовалют <https://www.bitget.com/news/detail/12560604435779>
- 30) Почему банки массово блокируют счета и как не попасть под ограничения <https://companies.rbc.ru/amp/news/dd05b46d-a998-4654-846d-3cc697f82834/>
- 31) Локировка расчетного счета в 2026 году: что делать бизнесу <https://www.klerk.ru/blogs/akbars/681734/?srsltid=AfmBOooWmqZJCGkG5TOH4fr4ZOW5hCqI-eADquKOCAYKbOMmoQAZ4uwq>
- 32) Заблокировали карту по 161-ФЗ из-за подозрений в мошеннических операциях. Почему так происходит и как снять блокировку https://www.intellectpro.ru/press/commenters/blokirovka_po_161_fz_glavnoe/
- 33) Почему банки массово блокируют счета и как не попасть под ограничения <https://myseldon.com/ru/news/index/341134995>
- 34) Счет заблокирован: что делать, если банк приостановил операции по счету компании <https://www.if24.ru/schet-zablokirovan/>
- 35) Как снять блокировку по 161-ФЗ: пошаговый алгоритм https://e-kontur.ru/enquiry/2660/blokirovka-po-161-fz#articleNavigation_3
- 36) Снять блокировку счетов по ФЗ-161 можно, только вернув деньги вместо мошенников? <https://www.bfm.ru/news/603966>
- 37) Банк заблокировал мою дебетовую карту НКО ЮМАНИ, по статье о мошенничестве, из-за одного перевода <https://100yuristov.com/q/497567/>

- 38) Три сценария «блокировки»: почему нельзя говорить «заблокировали счет» <https://astral.ru/aj/elem/115-fz-i-161-fz-pochemu-bank-ogranichivaet-operatsii-po-schetu/>
- 39) Полное руководство по блокировкам по 161-ФЗ: новые правила 2026 года и инструкция по защите своих прав <https://shupikov.com/fz-161/polnoe-rukovodstvo-po-blokirovkam-po-161-fz-novyie-pravila-2026-goda>
- 40) 115-ФЗ и криптовалюта: почему банки блокируют счета и как это предотвратить <https://pod-ft.ru/baza-znaniy/115-fz-i-kriptoalyuta-pochemu-banki-blokiruyut-scheta-i-kak-eto-predotvratit/>
- 41) Крипта под контролем 2026: налоги, блокировки счетов и безопасный вывод денег <https://www.klerk.ru/blogs/exchagent/684223/>
- 42) При переводе с криптокошелька на банковскую карту допустил ошибку в номере карты <https://harant.ru/questions/q-144864/>
- 43) Запрет криптообменников в России: к чему на самом деле надо готовиться <https://cryptorank.io/ru/news/feed/ce464-zapret-kriptoobmennikov-v-rossii-k-chemu-na-samom-dele-nado-gotovitsya>
- 44) ЦБ уточнил порядок блокировок по 161-ФЗ и ввел новые правила <https://companies.rbc.ru/news/F55mAHxcYx/tsb-utochnil-poryadok-blokirovok-po-161-fz-i-vvel-novyie-pravila/>
- 45) Что будет с регулированием рынка криптовалют в России в 2026 году <https://www.htx.com.pk/feed/community/17886967/?back=1>
- 46) Что делать, если банк ограничил операции из-за обмена криптовалюты https://finuslugi.ru/navigator/news/novosti_bankovskoj_otrasli/chto_delat_esli_bank_ogranichil_operatsii_iz_za_obmena_kriptoalyuty_zampred_tsb
- 47) Криптовалюта и налоги 2026: как не попасть на НДФЛ, блокировки и уголовку <https://tenchat.ru/media/5195961-kriptoalyuta-i-nalogi-2026-kak-ne-popast-na-ndfl-blokirovki-i-ugolovku>
- 48) Крипта и закон: как не нарваться на блокировку счета в 2026 году https://pikabu.ru/story/kripta_i_zakon_kak_ne_narvatsya_na_blokirovku_scheta_v_2026_godu_13625237
- 49) ЦБ РФ призвал банки в инициативном порядке информировать о блокировках операций <https://www.garant.ru/news/2030159/>
- 50) ЦБ РФ: надо активнее информировать клиентов о причинах блокировки карт и шагах для снятия ограничений <http://www.finmarket.ru/database/news/6585627?fid=7471&fs=T&ref=AnketaOrg>
- 51) Банкам рекомендовано информировать клиентов о причинах блокировки карт и счетов <https://ab-express.ru/news/bankam-rekomendovano-informirovat-klientov-o-prichinah-blokirovki-kart-i-schetov/>
- 52) Банкам следует проактивно и понятно информировать клиентов о блокировках и шагах для снятия ограничений <https://base.garant.ru/413953620/>
- 53) ЦБ рекомендовал банкам сообщать о блокировках и шагах по их снятию <https://bosfera.ru/press-release/cb-rekomendoval-bankam-soobshchat-o-blokirovkah-i-shagah-po-ih-snyatiyu>
- 54) ЦБ обязал банки сообщать клиентам о блокировках и шагах для их снятия <https://www.vedomosti.ru/finance/news/2026/03/25/1185377-soobshchat-o-blokirovkah>
- 55) За что могут заморозить перевод или карту: новые правила Банка России <https://www.gazprombank.ru/pro-finance/safety/za-chto-mogut-zamorozit-kartu/>
- 56) Банкам рекомендовали сообщать клиентам о блокировках до их обращения https://profile.ru/news/economy/bankam-rekomendovali-soobshhat-klientam-o-blokirovkah-do-ih-obrashheniya-1839105/?utm_from=must-amp
- 57) В начале 2026 года банки могли заблокировать до 3 млн карт и счетов физлиц <https://nbi.ru/news/v-nachale-2026-goda-banki-mogli-zablokir/71791/>
- 58) Эксперт призвал ЦБ дать более четкие рекомендации против мошенничества <https://1prime.ru/20260119/ekspert-866670049.html>
- 59) Что делать, если банк ввел ограничения <https://e.gazeta-unp.ru/1177692>
- 60) ЦБ призывает банки оперативно информировать клиентов о блокировках счетов <https://investfuture.ru/articles/ts-b-prizyvaet-banki-operativno-informirovat-klientov-o-blokirovkakh-schetov-f0c2e5e58d9d904043258dc50033c62f>
- 61) Блокируют банковскую карту? 3 шага для разблокировки по новым правилам ЦБ <https://kubnews.ru/panorama/2026/01/21/blokiruyut-bankovskuyu-kartu-3-shaga-dlya-razblokirovki-po-novym-pravilam-tsb/>
- 62) Блокировка счетов в России: нововведения и как защитить свои права <https://tver-news.ru/society/2026/02/26/46076.html>
- 63) ЦБ требует от банков понятных объяснений блокировок и быстрых ответов на обращения <https://xn----dtbeec7ak4ay9j.xn--p1ai/news/tsb-trebuot-ot-bankov-ponyatnykh-obyasneniy-blokirovok-i-bystrykh-otvetov-na-obrashcheniya/#comments>

64) Что делать, если банк заблокировал счёт или карту: советы экспертов

<https://www.gazetametro.ru/articles/cto-delat-esli-bank-zablokiroval-schet-ili-kartu-sovety-ekspertov-23-01-2026>

65) Блокировка счета в 2026: причины и как себя защитить <https://biznesinalogi.ru/lenta/post/54367/>

Часть 6. Жизненные ситуации: крипта в наследстве, разводе и бизнесе

Глава 17. Крипта и наследство — как не похоронить свои монеты вместе с собой

Это самая недооценённая проблема в криптосообществе. Люди тратят годы на накопление биткоинов, но ноль времени — на то, чтобы эти монеты не исчезли после их смерти.

Цифра, которая должна вас напугать

По оценкам аналитической компании Chainalysis, **от 20% до 30% всех существующих биткоинов уже потеряны навсегда**. Значительная часть этих потерь — монеты умерших владельцев, которые не оставили доступа к кошелькам.

Один из громких кейсов: владелец биткоин-кошелька на 500 миллионов долларов умер в 2019 году, не оставив паролей. Его состояние заморожено навсегда.

Почему обычное завещание не работает для крипты

Проблема	Почему это критично
Сид-фразу нельзя записать в завещании	Завещание становится публичным документом после открытия наследства. Ваша сид-фраза окажется у нотариуса, в суде — и теоретически может быть скомпрометирована.
Нотариусы не работают с криптой	У них нет процедуры «перезаписи» криптокошелька. Они могут зафиксировать факт наличия актива, но не передать доступ.
Холодный кошелёк может быть физически утерян	Флешка, Ledger, бумажка с сид-фразой — наследники могут просто не знать, где это искать.
Биржи не отдадут доступ без документов	Если монеты лежат на Binance или Bybit, наследникам придётся проходить долгую юридическую процедуру с нотариусом, а биржа может отказать.

Решение: система «цифрового завещания» для крипты

Вот пошаговый план, который используют опытные криптоинвесторы.

Шаг 1. Разделите сид-фразу на части (схема Shamir Secret Sharing)

Это криптографический метод, который позволяет разделить секрет (сид-фразу) на несколько частей. Для восстановления нужны не все части, а только пороговое количество (например, 3 из 5).

Как это выглядит на практике:

- Вы создаёте 5 частей вашей сид-фразы
- 1 часть храните в банковской ячейке
- 1 часть у надёжного друга/родственника
- 1 часть у вашего адвоката
- 1 часть в сейфе дома
- 1 часть в облачном хранилище (зашифрованную)

В завещании вы указываете: *«Для доступа к криптокошельку необходимо собрать 3 из 5 фрагментов, которые находятся у следующих лиц: ...»*

Ни один из хранителей не имеет полного доступа. Даже если кто-то из них скомпрометирован — ваши монеты в безопасности.

Шаг 2. Составьте «письмо наследникам» (не в завещании)

Это отдельный документ, который не подаётся в суд, но хранится у адвоката или в банковской ячейке. В нём содержится:

- **Где искать сид-фразу** (или её части)
- **Какие кошельки у вас есть** (список публичных адресов)
- **На каких биржах лежат монеты** (логины без паролей)
- **К кому обратиться за помощью** (контакты криптоюриста, который разбирается в вопросе)

Это письмо **не является завещанием** в юридическом смысле. Оно не имеет обязательной силы, но даёт наследникам дорожную карту.

Шаг 3. Назначьте «цифрового душеприказчика»

В завещании вы можете указать человека, который будет отвечать за цифровые активы. Это может быть тот же душеприказчик, что и по обычному наследству, или отдельный — технически подкованный.

Душеприказчик:

- Получает доступ к инструкциям после вашей смерти
- Помогает наследникам восстановить доступ к кошелькам
- Контролирует, чтобы крипта не была украдена в процессе передачи

Шаг 4. Используйте сервисы отложенной передачи (с осторожностью)

Существуют смарт-контракты и сервисы, которые автоматически переводят крипту наследникам после подтверждения смерти (например, Safe Haven, наследственные смарт-контракты на блокчейне).

В России эти сервисы не имеют юридической силы. Но их можно использовать как техническое решение в дополнение к завещанию.

Важное предупреждение: никогда не доверяйте полностью автоматическим сервисам. Ошибка в смарт-контракте может привести к потере всех монет.

Что делать, если близкий умер, а вы не знаете пароль от его кошелька

Ситуация: вы нашли Ledger или записку с непонятными словами, но доступ получить не можете.

1. **Не пытайтесь подобрать пароль брутфорсом.** От 5 до 10 неверных попыток — и аппаратный кошелек самоуничтожится.
2. **Найдите профессионалов.** В РФ есть компании (и частные эксперты), которые занимаются восстановлением доступа к криптокошелькам по заказу наследников. Проверяйте их через адвоката — много мошенников.
3. **Подайте заявление нотариусу о включении криптовалюты в наследственную массу.** Нотариус не даст вам пароль, но зафиксирует, что актив существует. Это важно, если вы потом найдёте доступ — у вас будут документы, что монеты не украдены, а унаследованы.
4. **Если монеты лежат на бирже** — обращайтесь на биржу с нотариальным свидетельством о праве на наследство. Binance, Bybit и другие крупные

биржи имеют процедуру для таких случаев (хотя она может занять месяцы).

Чего делать категорически нельзя

Не делайте	Почему
Не записывайте сид-фразу в завещание	Завещание станет публичным — любой сможет украсть монеты
Не доверяйте сид-фразу одному человеку	Он может умереть раньше вас, потерять запись или украсть монеты
Не храните сид-фразу только в голове	При травме головы, инсульте или деменции доступ потерян навсегда
Не используйте облачные менеджеры паролей как единственное хранилище	Взлом, блокировка аккаунта, банкротство сервиса — и всё пропало

Чек-лист «Криптонаследство за 30 минут»

- Записал сид-фразу на металлической пластине (не на бумаге)
- Разделил сид-фразу на 3-5 частей по схеме Shamir
- Назначил доверенных лиц, у каждого — одна часть
- Составил «письмо наследникам» с инструкциями
- Обсудил с наследниками (не в деталях, но сам факт) — чтобы они знали, что крипта есть и где искать инструкции
- Указал в завещании душеприказчика с доступом к инструкциям
- Сделал копию инструкции (у адвоката или в банковской ячейке)

Глава 18. Крипта и развод — как делятся криптоактивы при разделе имущества

Развод — это стресс. Развод с криптовалютой — это стресс в квадрате. Судьи до сих пор не всегда понимают, что такое блокчейн, а ваша бывшая половина может требовать половину кошелька, о котором она даже не знала.

Главный принцип: крипта — это имущество

Верховный Суд РФ последовательно придерживается позиции: **криптовалюта является имуществом**, если она имеет экономическую ценность и может быть оценена в рублях.

Это означает, что при разводе криптоактивы подлежат разделу наравне с квартирами, машинами и акциями.

Правовая база:

- Семейный кодекс РФ, ст. 34 — совместно нажитое имущество
- Ст. 38 СК РФ — раздел имущества
- Судебная практика: определения Верховного Суда РФ по делам с участием криптовалюты (с 2021 года появляются регулярно)

Что считается совместно нажитым, а что — личным

Ситуация	Считается совместным	Считается личным
Купили крипту в браке на общие деньги	Да	Нет
Купили крипту до брака	Нет	Да (но прибыль от продажи в браке — уже общая)
Получили крипту в дар или наследство в браке	Нет (если дарственная или завещание — только на вас)	Да
Майнили в браке (на общем оборудовании и электричестве)	Да	Нет
Получили крипту как зарплату в браке	Да	Нет
Купили крипту на деньги от продажи добрачной квартиры	Нет (если можете доказать происхождение денег)	Да

Ключевая проблема: доказать происхождение криптовалюты. Если вы купили биткоин в 2025 году, а брак расторгается в 2026-м — по умолчанию суд исходит из того, что это совместное имущество, пока вы не докажете обратное.

Как суды узнают о существовании криптокошелька

Самый страшный сценарий для криптоинвестора при разводе — это не потеря половины монет, а **необходимость раскрыть факт их существования**. Вот как суд может узнать о вашей крипте:

1. **Вторая сторона сама знает** (вы рассказывали, показывали кошелёк, обсуждали покупки)
2. **Банковские выписки** (вы заводили рубли на биржу — остаются следы)
3. **Запросы в криптобиржи** (по решению суда Binance, Bybit и другие обязаны предоставить информацию)
4. **Блокчейн-аналитика** (редко для гражданских дел, но теоретически возможно)
5. **Налоговая декларация** (вы подали 3-НДФЛ с указанием доходов от криптовалюты)
6. **Переписки в мессенджерах** (если суд запрашивает переписку, а вы обсуждали крипту)

Что требует бывшая супруга (бывший супруг)

Закон даёт право требовать не только сами монеты, но и:

- **Информацию о наличии криптокошельков** (адреса, биржи, объёмы)
- **Доступ к кошельку для оценки** (на практике — суд назначает эксперта)
- **Денежную компенсацию вместо выдела монет** (если выделить половину кошелька технически сложно)

Суды, как правило, не заставляют переводить половину биткоинов на кошелёк бывшей половины. Вместо этого назначается **оценка криптовалюты в рублях**, и владелец выплачивает денежную компенсацию.

Стратегии защиты (законные)

1. Оценка криптовалюты — ключевая битва

Стоимость криптовалюты определяется на **дату оценки, назначенную судом**. Это может быть:

- Дата подачи иска
- Дата вынесения решения
- Любая другая дата по усмотрению суда

Разница в цене биткоина между этими датами может составлять десятки процентов. **Ваша задача — добиться оценки на наиболее выгодную для вас дату.**

2. Доказывание личного происхождения

Если вы купили криптовалюту до брака или на личные деньги:

- Сохраняйте **выписки из банка** о движении денег
- Храните **договоры купли-продажи** криптовалюты
- Ведите **учёт операций** (дата, сумма, кошелек отправителя)

Без документов суд решит в пользу общей совместной собственности.

3. Соглашение о разделе имущества (до суда)

Это лучший вариант. Вы с супругой/супругом можете договориться о том, что криптовалюта остаётся вам, а взамен вы отдаёте другое имущество (квартиру, машину, наличные).

Важно: соглашение должно быть нотариально удостоверено. В тексте можно указать, что вторая сторона не имеет претензий к криптоактивам, даже если они вырастут в цене после развода.

4. Что делать, если вы не хотите раскрывать криптовалюту

Это скользкая тема. Юридически **сокрытие имущества при разводе — это нарушение**. Если суд узнает, что вы скрыли криптовалюту, в последствии могут быть:

- Признание брачного договора или соглашения недействительным
- Присуждение компенсации в двойном размере
- В отдельных случаях — уголовная ответственность (ст. 159 УК — мошенничество, если скрыли крупную сумму)

Реалистичный совет: не скрывайте, но и не выкладывайте всё на стол. Ответьте на прямой вопрос суда. Не лгите под присягой. Если не спрашивают — не говорите лишнего.

5. Технические меры до брака (идеальный вариант)

Если вы только собираетесь жениться и у вас уже есть крипто:

1. **Составьте брачный договор.** Укажите в нём, что добрачная крипто и вся прибыль от неё — ваше личное имущество.
2. **Переведите крипто на отдельный кошелёк,** который не пополняется в браке из общих денег.
3. **Никогда не смешивайте.** Как только вы добавили на этот кошелёк рубль из общего бюджета — вся крипто на нём может стать совместной.

Реальный кейс из практики

Дело: г. Москва, 2023 год. Мужчина купил 2 BTC в 2020 году (до брака). В браке (2021-2022) продал их, выручил 6 млн рублей и купил машину. При разводе супруга потребовала половину от 2 BTC, которые к тому моменту стоили уже 10 млн рублей.

Решение суда: Монеты были добрачными — супруга не имеет права на них. Но! Прибыль от продажи (6 млн рублей) была получена в браке и признана совместным имуществом. Машина (купленная на эти 6 млн) подлежит разделу. А потенциальный рост стоимости биткоина после развода (до 10 млн) супругу не касается — это уже актив мужа.

Вывод: время продажи и форма хранения критически важны.

Чек-лист «Крипто и развод: что сделать прямо сейчас»

- Если вы в браке и у вас есть крипто — сделайте скриншоты всех кошельков с текущими балансами
- Сохраните выписки банка о том, откуда пришли деньги на покупку крипто

- Если крипта добрачная — соберите доказательства (чеки, договоры, скрины до даты брака)
- Рассмотрите возможность брачного договора (даже сейчас, в браке — это законно)
- Если развод неизбежен — не переводите крипту между кошельками в спешке. Суд может расценить это как сокрытие имущества
- Наймите адвоката с опытом в крипто-разделах (обычные семейные юристы часто не в теме)

Главный вывод

При разводе крипта делится так же, как квартира. Но доказать её происхождение и оценить — сложнее.

Лучшая защита — брачный договор и чистое разделение кошельков: «добрачный» и «совместный». В идеале — вообще не хранить крупные суммы в крипте, если вы не готовы раскрыть их при разводе.

Глава 19. Бизнес на крипте в РФ + НОВОЕ: Законопроект о цифровой валюте (апрель 2026)

Рынок на пороге больших перемен

Российский рынок криптовалют долгие годы оставался вне правового поля. По оценкам экспертов, нелегальный майнинг ежегодно наносит экономике ущерб на сумму более 10 млрд рублей из-за потерь в энергосекторе и до 9,6 млрд рублей из-за уклонения от уплаты налогов. Чтобы изменить эту ситуацию, весной 2026 года российские власти инициировали пакет системных законопроектов, призванных перевести отрасль в легальное русло.

Сегодня государство последовательно выводит криптовалютный рынок из серой зоны — вводятся чёткие правила для бизнеса, лицензирование для посредников и понятные условия для инвесторов.

Главный запрет: расплачиваться криптой нельзя

Это положение остаётся краеугольным камнем государственной политики.

Законопроект «О цифровой валюте и цифровых правах» (№ 1194918-8) прямо устанавливает **запрет на использование цифровой валюты в качестве средства платежа** на территории Российской Федерации. Расплачиваться ею за товары, работы, услуги, ценные бумаги, цифровые права и результаты интеллектуальной деятельности внутри страны нельзя. Российский рубль остаётся единственным законным платёжным средством.

Что можно: условия для инвесторов и бизнеса

Законопроект вводит легальные каналы для операций с криптовалютой. Купить или продать криптовалюту можно будет **только через лицензированных посредников**. Это могут быть:

- Организаторы торговли (биржи)
- Брокеры
- Доверительные управляющие
- Лицензированные криптообменники, включённые в реестр ЦБ.
- Для клиентов — физических лиц — устанавливаются два статуса.

Неквалифицированные инвесторы:

- Обязательное **бесплатное тестирование** на понимание рисков.
- Годовой лимит на покупку — **не более 300 000 рублей в год через одного посредника**.
- Доступ к покупке только самых ликвидных криптовалют из специального перечня Банка России.

Квалифицированные инвесторы:

- Статус присваивается по правилам ст. 51.2 закона «О рынке ценных бумаг».
- Отсутствие лимитов по суммам покупки, более широкий выбор активов.

Организовывать обращение цифровой валюты и цифровых прав смогут только те компании, которые прямо указаны в законе.

НОВОЕ: Покупать криптовалюту можно будет только через посредников — обменники из реестра ЦБ, брокеров и доверительных управляющих. Прямые переводы с российских счетов на личные (некастодиальные) кошельки будут запрещены.

Исключение для внешнеэкономической деятельности (ВЭД)

Законопроект делает важное исключение для бизнеса. При расчётах с иностранными контрагентами криптовалюту использовать **можно**.

НОВОЕ: Юридические лица и индивидуальные предприниматели смогут применять цифровую валюту в расчётах по внешнеторговым контрактам, в том числе через некастодиальные кошельки. Благодаря этому можно существенно минимизировать санкционные риски при международных расчётах.

Это долгожданное послабление, которое открывает новые возможности для экспортёров и импортёров, столкнувшихся с ограничениями в традиционных банковских каналах.

Лицензирование криптобизнеса

Закон предусматривает строгую модель регулирования. Ключевые даты нового регулирования:

- **1 сентября 2026 года** — вступление в силу основных статей законопроекта и запуск механизма блокировки платежей в пользу нелегализованных площадок.
- **1 июля 2027 года** — вступление в силу требования об обязательной работе только через лицензированных посредников.

НОВОЕ:

- **С 1 сентября 2026 года** начнут блокироваться платежи в пользу криптобирж, не акцептованных ЦБ РФ.
- **С 1 июля 2027 года** прямая P2P-торговля без участия лицензированного посредника будет признана незаконной.
- **С 1 июля 2027 года** вводится уголовная ответственность за нелегальный оборот криптовалют.

Требования к криптообменникам:

- Регистрация компании в Российской Федерации.
- Включение в специальный реестр Банка России.
- Соблюдение требований по капиталу.
- Получение отдельной лицензии на осуществление деятельности.

Стартапы и инновации — где есть возможности

Законопроект создаёт новую правовую среду и для технологических проектов.

ЦФА в открытых сетях:

Законопроект предусматривает выпуск и оборот цифровых прав в публичных блокчейн-сетях, а не только в закрытых системах операторов. Это открывает путь для привлечения инвестиций из-за рубежа напрямую, создавая мост между российским регулируемым рынком и глобальной криптоинфраструктурой.

Цифровые депозитарии:

Вводится новый институт **цифровых депозитариев**, поднадзорных ЦБ. Они будут учитывать переход прав на цифровую валюту, открывать и вести счета и предоставлять доступ к адресам-идентификаторам. Это новая ниша для бизнеса.

Экспериментальный правовой режим (ЭПР):

Действующие банки, брокеры и участники экспериментального правового режима ЦБ РФ смогут получить доступ к новым видам деятельности по упрощённой процедуре.

Налогообложение криптобизнеса

Новый закон не меняет базовых принципов, но вводит уточнения.

Вид деятельности	Налог и сборы	Особенности
Юридические лица и ИП	Налог на прибыль / по УСН	Операции с криптовалютой облагаются на общих основаниях как реализация имущества
Резиденты	—	Теперь обязаны уведомлять ФНС об открытии, закрытии и изменении реквизитов криптокошельков за рубежом — точно так же, как о зарубежных счетах в банках
Физические лица (инвесторы)	НДФЛ 13-15%	Налогом облагается положительная разница между ценой продажи и ценой покупки актива

Риски и ответственность для бизнеса

Новое регулирование предусматривает жёсткую ответственность за нарушение установленных требований.

Нарушение	Ответственность
Осуществление деятельности без лицензии ЦБ (с 1 июля 2027 года)	Уголовная ответственность: лишение свободы на срок до 7 лет .
Нарушение правил майнинга (работа в запрещённых регионах)	Административная ответственность: для граждан — до 150 тысяч рублей ; для должностных лиц — до 800 тысяч рублей ; для юрлиц — до 2 млн рублей (все суммы с конфискацией оборудования). За повторное нарушение — до 10 млн рублей .
Незаконный майнинг без регистрации	Штрафы: для граждан — до 150 тысяч рублей ; для юрлиц — до 500 тысяч рублей
Майнинг в регионах, где он запрещён (отдельные районы Бурятии и Забайкалья, республики Северного Кавказа, новые регионы)	Действует круглогодичный запрет до 15 марта 2031 года .

Пошаговая инструкция: как легально запустить криптобизнес в 2026 году

Если вы планируете открыть криптообменник или иной бизнес на рынке, вот план действий.

Шаг 1. Дождитесь принятия закона.

Законопроект № 1194918-8 прошёл первое чтение в Госдуме 21 апреля 2026 года. Ожидается его принятие до конца весенней сессии.

Шаг 2. Определитесь с моделью.

Закон выделяет несколько типов лицензируемой деятельности:

- Организатор торговли (криптовбиржа)
- Брокер
- Доверительный управляющий
- Цифровой депозитарий
- Криптообменник

Шаг 3. Подайте заявку на лицензию в ЦБ РФ (после вступления закона в силу).

Банк России будет выступать главным надзорным органом и выдавать лицензии на организацию обращения цифровых валют.

Шаг 4. Выстройте комплаенс (ПОД/ФТ).

Это критически важно. Ваша компания обязана будет мониторить операции клиентов на предмет признаков отсутствия добровольного согласия. В случае нарушений — обязана возместить сумму сделки. К системе «Прозрачный блокчейн» будут подключены все банки.

Шаг 5. Настройте учёт и налоги.

Отражайте все операции с криптовалютой в бухгалтерском и налоговом учёте.

Шаг 6. Подготовьтесь к блокировке P2P-трафика.

С 1 июля 2027 года все операции должны будут проходить через вас, если у вас есть лицензия. Клиентам, которые торгуют напрямую, будет грозить ответственность, а их платежи будут блокироваться.

Чек-лист «Бизнес на крипте — что сделать прямо сейчас»

Пока законопроект находится в стадии доработки, можно заняться подготовкой.

- **Изучить финальную версию законопроекта № 1194918-8**, когда она будет принята.
- **Подготовить пакет документов** для регистрации ООО (требование к резидентам РФ).
- **Продумать бизнес-модель:** какой тип лицензии подходит?
- **Найти команду с опытом в комплаенс (ПОД/ФТ).**
- **Подписаться на официальные обновления Банка России** по вопросам регулирования криптовалют.
- **Перестать продвигать оплату криптовалютой внутри России.**
- **Подготовить уведомления в ФНС** об открытых кошельках за рубежом для себя и сотрудников.

Этот закон — не запрет, а легализация и структурирование огромного рынка. Те, кто подготовится заранее, получат конкурентное преимущество в новой реальности. P2P-обменники и нелегальные «серые» схемы уходят в прошлое, уступая место прозрачному и регулируемому рынку.

Использованные в главе источники:

- 1) Регулирование криптовалютного бизнеса в РФ. Период серых зон заканчивается <https://plusworld.ru/articles/detail.php?CODE=regulirovanie-kriptoalyutnogo-biznesa-v-rf-period-serykh-zon-zakanchivaetsya>
- 2) Оплата криптовалютой https://www.consultant.ru/law/podborki/oplata_kriptoalyutoj/
- 3) ЦБ предложил разрешить банкам и брокерам получать лицензии криптообменников в уведомительном порядке <https://www.vep.ru/news.html?id=17197>
- 4) Банком России предложено установить специальный экспериментальный правовой режим для регулирования инвестиций в криптовалюты <https://www.consultant.ru/law/hotdocs/88620.html>
- 5) Российские банки и регуляторы планируют многоуровневый доступ к криптовалюте <https://coinpaprika.com/ja/news/roshianoyin-xing-togui-zhi-dang-ju-gafei-zi-ge-tou-zi-jia-xiang-kenojie-ceng-de-naan-hao-akusesuwoji-hua/>
- 6) ЦБ подготовил концепцию по регулированию криптовалют в России <https://expert.ru/news/tsb-podgotovil-kontseptsiyu-po-regulirovaniyu-kriptoalyut-v-rossii/>
- 7) Криптовалюта для граждан РФ: что можно, а что нельзя в 2025 г. <https://kudaev-and-partners.ru/publications/kriptoaluta-dlya-grazhdan-rf-cto-mozhno-a-cto-nelzya-v-2025-g>
- 8) В ЦБ рассказали, с какой ответственностью столкнутся нелегальные криптообменники <https://x-compliance.ru/publications/podft/v-tsb-rasskazali-s-kakoy-otvetstvennostyu-stolknutsya-nelegalnye-kriptoobmenniki>
- 9) Может ли стать реальностью обращение криптовалют в России <https://nbj.ru/publs/mozhet-li-stat-realnostyu-obrashchenie-kri/69879/>
- 10) Перспективы рынка криптовалют: предложения Банка России <http://bulldog.bankodrom.ru/eng/press/event/?id=28215>

Глава 20. Чек-лист для начинающего — пошаговый план «Купил первую крипту — что делать, чтобы не попасть»

Вы купили первую криптовалюту. Поздравляю. Теперь самое главное — не потерять деньги и не получить проблемы с законом.

Этот чек-лист — пошаговая инструкция для новичка в России. Выполняйте пункты последовательно.

Этап 0. До покупки (или сразу после)

0.1. Понять главное правило

Криптовалюта в России — **не платёжное средство**. Нельзя расплачиваться ей в магазине, кафе или за услуги. Можно только **владеть, покупать и продавать**.

0.2. Выбрать безопасный способ покупки (по убыванию безопасности)

Способ	Безопасность	Комментарий
ЦФА через оператора	Высокая	Полностью легально, но мало монет
Крупная биржа с KYC (Bybit, HTX, Binance)	Средняя	Риск блокировки карты при выводе
P2P через биржу	Средняя	Можно, но соблюдать правила (см. ниже)
P2P через Telegram/чат	Низкая	Очень рискованно
Обменник «на улице»/наличные	Очень низкая	Почти гарантированные проблемы

Вывод для новичка: покупайте на крупной централизованной бирже с KYC (Bybit, HTX, Binance). Это не идеально, но лучшее из доступного.

0.3. Не хранить крипту на бирже

Правило «not your keys — not your coins» работает везде, включая Россию. Биржа может быть взломана, заблокирована, а может просто заморозить ваши деньги.

Купили → сразу выведите на свой кошелёк.

Этап 1. Кошелёк и безопасность (сразу после покупки)

1.1. Установить некастодиальный кошелёк

Варианты для начинающих:

- **Trust Wallet** (мобильный, простой)
- **MetaMask** (для Ethereum и совместимых сетей)
- **Exodus** (деSKTOPный, красивый)

Не используйте кошельки, которые требуют регистрации по паспорту — это не кошельки, а те же биржи.

1.2. Записать сид-фразу правильно

Сид-фраза (12 или 24 слова) — это **все ваши деньги**. Потеряли фразу — потеряли крипту.

Правильное хранение:

- Запишите фразу **от руки** на листе бумаги
- Сделайте **вторую копию** и храните в другом месте
- **Никогда** не храните сид-фразу в телефоне, заметках, облаке, скриншотах
- **Никогда** не вводите сид-фразу на сайтах, в мессенджерах, по просьбе «поддержки»

Для крупных сумм (от 100 тысяч рублей):

- Выберите сид-фразу на металлической пластине (продаются на Ozon/WB)
- Храните в сейфе или банковской ячейке

1.3. Включить двухфакторную аутентификацию (2FA)

На бирже, где вы покупали — обязательно. Используйте Google Authenticator или Authy, **не SMS** — сим-карты подменяют.

1.4. Разобраться с сетями (чтобы не потерять перевод)

Если переводите USDT — проверьте, в какой сети (TRC-20, ERC-20, BEP-20). Кошелёк получателя должен поддерживать ту же сеть. Ошибка → потеря денег навсегда.

Этап 2. Налоги и ФНС (до первой продажи)

2.1. Запомнить, когда возникает налог

Вы **обязаны заплатить налог** в двух случаях:

1. Вы **продали** крипту за рубли (или обменяли на другую крипту)
2. Вы **получили** крипту (майнинг, подарок, зарплата)

Просто купили и держите — налога нет.

2.2. Посчитать налог правильно

- **Ставка:** 13% (до 2.4 млн рублей дохода в год), 15% (сверх)
- **База:** разница между ценой продажи и ценой покупки

Пример: купили за 100 тысяч рублей, продали за 150 тысяч рублей → налог 13% с 50 тысяч рублей = 6500 рублей.

2.3. Заполнить 3-НДФЛ (до 30 апреля следующего года)

Продали крипту в 2025 году → подаёте декларацию до 30 апреля 2026 года.

Где взять данные для декларации:

- Выписка с биржи (можно скачать в личном кабинете)
- Скриншоты операций (если биржа не даёт выписку)

2.4. Заплатить налог (до 15 июля)

Оплатить можно через сайт ФНС, в приложении «Налоги ФЛ» или в банке.

Что будет, если не платить?

ФНС получает данные от банков (движение по картам) и от бирж (по запросу). Рано или поздно узнают.

Последствия:

- Штраф 20-40% от неуплаченной суммы
- Пени за каждый день просрочки
- Блокировка счетов (при крупных долгах)
- Уголовное дело (от 2.5 млн рублей неуплаты)

2.5. Уведомление о зарубежных кошельках. С 1 июля 2026 года вступает в силу требование об уведомлении ФНС об открытии криптокошельков в иностранных информационных системах. Форма уведомления пока не утверждена — отслеживайте ее появление на nalog.gov.ru. Для текущих операций используйте договор купли-продажи из Приложения 1.

Этап 3. Продажа и вывод в рубль

3.1. Помнить про порог 600 тысяч рублей

Если зачисляете на карту **более 600 тысяч рублей за раз или за короткий период** — банк автоматически уведомляет Росфинмониторинг.

Это **не значит**, что вы нарушитель. Это значит, что вашу операцию проверят.

Как снизить риск:

- Не продавайте крупные суммы разом
- Не выводите на карту, которая не использовалась для крипты раньше
- Держите сумму на вывод в пределах 200-300 тысяч рублей за раз

3.2. Использовать P2P безопасно (если выбираете этот способ)

Правила безопасного P2P:

- Только на крупных биржах (Bybit, HTX, Binance) с системой эскроу
- Проверяйте рейтинг продавца (не ниже 98%, много сделок)
- Не соглашайтесь на перевод «частями» от разных людей
- Не переходите в Telegram/WhatsApp — всё внутри биржи
- Сохраняйте скриншоты и чек-лист подтверждения оплаты

Что делать после P2P:

- Не снимайте деньги сразу со счета
- Не переводите на другие карты в тот же день
- Пусть деньги «отлежатся» 1-2 дня

3.3. Подготовить объяснение для банка (заранее)

Если банк спросит: «Откуда деньги на карте?» — нужно ответить правдоподобно и без крипты.

Варианты ответа:

- «Продал личные вещи» (для сумм до 200 тысяч рублей)
- «Вернул долг знакомый» (можно подтвердить перепиской)
- «Получил подарок от родителей» (для сумм до 500 тысяч рублей)

Не говорите: «Продал крипту». Для банка это красный флаг.

Но помните: если дело дойдёт до серьёзной проверки, ложь только ухудшит положение.

3.4. Что делать, если карту заблокировали (кратко)

Полная инструкция — в **Главе 16**. Кратко:

1. Не паниковать
2. Позвонить в банк, узнать причину
3. Собрать документы (скрины, переписку, договор)
4. Подать заявление на разблокировку
5. Если не помогают — жалоба в ЦБ

Этап 4. Долгосрочное хранение и безопасность

4.1. Перевести крупные суммы на холодный кошелёк

Если у вас крипты на сумму **более вашего 3-месячного дохода** — пора задуматься о холодном (аппаратном) кошельке.

- **Популярные:** Ledger, Trezor, Safepal.

- **Плюсы:** сид-фраза генерируется и хранится на устройстве, никогда не контактирует с интернетом.
- **Минусы:** стоит денег (5-15 тысяч рублей).

4.2. Сделать резервную копию сид-фразы

Одна копия — дома. Вторая — у доверенного лица или в банковской ячейке.

4.3. Не хранить все монеты в одном месте

Разделите крипту:

- **«Горячий» кошелёк** (в телефоне) — небольшая сумма для операций
- **«Холодный» кошелёк** — основное хранение
- **Биржа** — только то, что вы торгуете прямо сейчас

4.4. Быть осторожным с DeFi

Децентрализованные приложения (Uniswap, Aave, PancakeSwap) — мощный инструмент, но:

- Огромные риски взлома смарт-контрактов
- Риск переплатить газ (комиссию сети)
- В России — серая зона, налоговая не поймёт ваши операции

Для новичка: сначала разобраться, потом использовать.

4.5. Никогда никому не доверять (золотое правило)

- Не сообщайте сид-фразу
- Не переходите по ссылкам от «поддержки биржи»
- Не вводите пароли на сайтах, которые пришли в письме
- Не верьте в «бесплатную раздачу монет»
- 99% проблем новичков — из-за доверчивости.

Этап 5. Чрезвычайные ситуации

5.1. Если потеряли доступ к кошельку

- Нет сид-фразы? Деньги потеряны навсегда. Никто не восстановит.

- Сид-фраза есть? Восстанавливаете кошелёк в любом приложении, которое поддерживает эту же сеть.

5.2. Если отправили крипту не туда

- На неверный адрес (но адрес существует) — ничего не сделать, если только владелец не вернёт (почти никогда).
- В неверную сеть (например, USDT ERC-20 на адрес TRC-20) — иногда биржа/сервис могут вернуть за комиссию, но шанс низкий.

5.3. Если взломали кошелёк

- Мгновенно выводите оставшиеся средства на новый кошелёк
- Меняйте пароли от бирж и почты
- Подайте заявление в полицию (шанс найти вора в России ненулевой)

5.4. Если пришли сотрудники (допрос, обыск)

Полный чек-лист — в **Главе 10**. Коротко:

- Молчать до адвоката
- Не подписывать ничего без адвоката
- Не сопротивляться
- Запоминать, что изымают

Итоговый чек-лист на одной странице (можно распечатать и повесить на стену)

Этап	Действие	Сделано
0	Купил первую крипту на крупной бирже	
1	Вывел на свой Trust Wallet / MetaMask	
2	Записал сид-фразу от руки (2 копии)	
3	Включил 2FA на бирже	
4	Запомнил, что налог — 13% с прибыли	
5	Узнал про порог 600 000 ₽ для банков	
6	Понял, что P2P — это риск	
7	Не храню всё на бирже	
8	Не даю сид-фразу никому	
9	При продаже готов объяснить для банка	
10	Знаю, что делать при обыске (молчать + адвокат)	

Главный вывод для начинающего

Крипта — это просто, если соблюдать правила.

Ошибки новичков почти всегда одинаковые: не сохранили сид-фразу, поверили мошенникам, вывели на левую карту, не заплатили налог.

Сделайте первые шаги медленно и внимательно. Не спешите. Сохраните чек-лист.

Глава 21. Список реальных судебных дел — за что сажают на самом деле

Теория — это хорошо. Но лучший способ понять, как работает правосудие в России в отношении крипты, — посмотреть на **реальные приговоры**.

В этой главе — подборка актуальных уголовных дел 2024-2025 годов. Имена изменены или оставлены как в открытых источниках. Выводы — за вами.

1. Мошенничество (ст. 159 УК РФ) — самый частый состав

Дело № 1. «Битмама» — 2,2 млрд рублей

Фигурант: Валерия Федякина (известная как «Битмама»)

Суд: Пресненский районный суд г. Москвы

Приговор: 7 лет колонии общего режима (июнь 2025 года)

Суть: Федякина предлагала инвесторам вкладываться в криптовалюту с обещанием высокой доходности. На деле она присваивала деньги: получала наличные, конвертировала в крипту и отправляла через криптокошельки в ОАЭ. Ущерб — 2,2 млрд рублей. Один из клиентов передал ей 6,7 млрд рублей наличными, после чего понял, что деньги не вернут, и обратился в полицию.

Квалификация: ч. 4 ст. 159 УК РФ (мошенничество в особо крупном размере)

Вывод: Обещания «супердоходности» + сбор денег физических лиц = почти гарантированный срок, если что-то пойдёт не так.

Дело № 2. Фейковое приложение для заработка токенов — 2,5 млн рублей

Фигуранты: Трое жителей Татарстана (Калимуллин, Позднышев, Саушин)

Суд: Красногорский городской суд

Приговор: от 1,5 до 3,5 лет колонии + штрафы (октябрь 2025)

Суть: Калимуллин разработал мобильное приложение — платформу коротких видео с системой вознаграждения токенами. В июле 2023 года объявил акцию: продажа внутренней валюты по сниженной цене. Пользователи инвестировали крипту, после чего участники группы вывели её через биржи на подконтрольные кошельки, а приложение закрыли. Ущерб — 2,5 млн рублей.

Квалификация: ч. 4 ст. 159 УК РФ (мошенничество)

Вывод: Криптостартапы без реальной бизнес-модели и сбора денег с пользователей — это не инновации, а статья.

Дело № 3. Инвестиции с доходностью 360% — 1,7 млн рублей

Фигурант: 25-летний гражданин ближнего зарубежья

Суд: Республика Мордовия

Приговор: 2 года колонии общего режима (сентябрь 2025)

Суть: Осуждённый предлагал знакомым инвестировать в криптобиржу, обещая доходность около 360% годовых. Пятеро его соотечественников и один житель Мордовии передали ему от 100 до 450 тысяч рублей — всего более 1,7 млн рублей. Часть денег он потратил на выплату «процентов» для создания видимости успеха, остальное — на личные нужды. Когда один из инвесторов потребовал подтверждений, а затем возврата денег, оказалось, что их нет.

Квалификация: ст. 159 УК РФ

Вывод: «Свои» и «знакомые» — не гарантия. Обещание 360% годовых — гарантия проблем.

2. Легализация (отмывание) криптовалюты (ст. 174 и 174.1 УК РФ)

Дело № 4. Обмен биткоинов от наркоторговли — перевод на карту

Суть (из обзора судебной практики Верховного Суда РФ): Осуждённый получил биткоины в качестве оплаты за наркотические средства. Затем произвёл финансовые операции на торговой площадке по обмену криптовалютой на рубли с последующим переводом на счёт в российском банке. Суд указал, что последовательность этих операций свидетельствует о цели придания правомерного вида владению, пользованию и распоряжению деньгами.

Квалификация: ч. 1 ст. 174.1 УК РФ

Вывод из постановления Верховного Суда: «Способ получения денежных средств путём совершения последовательных финансовых и банковских операций свидетельствует о наличии у осуждённого цели придания правомерного вида их владению, пользованию и распоряжению».

Дело № 5. Мошенничество + отмывание на 6 млн рублей — Хакасия

Фигурант: 28-летний житель Хакасии

Суд: Абаканский городской суд

Приговор: 3 года 6 месяцев колонии общего режима (август 2025)

Суть: В составе организованной группы похищал деньги граждан на криптоплатформе — списывал на подконтрольные банковские счета. Потерпевших — 13 человек, ущерб — более 1,7 млн рублей. Кроме того,

легализовал более 6 млн рублей через финансовые операции на бирже и переводы на банковские счета.

Квалификация: ч. 4 ст. 159 УК РФ + пп. «а», «б» ч. 4 ст. 174.1 УК РФ (легализация в составе организованной группы)

Вывод: Организованная группа + крипта + отмыwanie через банки = реальный срок. Причём за отмыwanie могут добавить так же серьёзно, как и за само хищение.

3. Дела о вымогательстве крипты

В этой части — дела о **вымогательстве криптовалюты (ст. 163 УК РФ)**, а также случаи, когда жертвами становятся обычные пенсионеры.

Дело № 6. Вымогательство через Telegram-канал — биткоины на 16,8 млн рублей

Фигуранты: два участника организованной группы

Суд: Подольский городской суд Московской области (дело направлено в суд в декабре 2025 года)

Статья: п. «а», «б» ч. 3 ст. 163 УК РФ (вымогательство, совершенное организованной группой)

Суть: Организатор группы создал тематический Telegram-канал, в котором публиковалась заведомо ложная информация о финансовых операциях компаний, якобы связанных с запрещёнными интернет-казино.

Схема работала так:

1. Один из обвиняемых был администратором канала.
2. Второй отвечал за «чарджбэк-процедуры» — массовые жалобы на организации с целью отмены платежей и возврата денег.
3. Злоумышленники угрожали представителям компаний распространением порочащих сведений.
4. Под угрозой сотрудники коммерческой организации перевели вымогателям биткоины на сумму более **16,8 млн рублей**.

Период преступной деятельности: апрель-сентябрь 2024 года.

Обвиняемые свою вину не признали. Уголовное дело направлено в суд для рассмотрения по существу.

Вывод: Вымогательство криптовалюты через репутационные угрозы — растущий сегмент киберпреступности. Организованные группы используют Telegram для анонимности, но это не спасает их от уголовного преследования.

Дело № 7. Похищение криптоинвестора с вывозом в лес — 5,6 млн рублей

Фигуранты: четверо жителей Алтайского края

Суд: Екатеринбург

Приговор: Частичное оправдание присяжными (октябрь 2025 года)

Суть преступления: Житель Алтайского края собрал банду из шести человек для похищения криптоинвестора из Екатеринбурга. Цель — получить доступ к криптокошелькам на сумму около **500 млн рублей**.

Схема:

- Бизнесмена вывезли в лес.
- Под угрозой заставили раскрыть пароли от криптокошельков.
- Похитили около **5,6 млн рублей** в криптовалюте.

Результат рассмотрения: Коллегия присяжных заседателей единогласно признала недоказанным совершение преступления по пп. «а», «б» ч. 3 ст. 163 УК РФ (вымогательство). Двое фигурантов — Александр Герасимов и Дмитрий Атаманов — оправданы по обвинению в пособничестве в разбое. Атаманов также оправдан по ч. 2 ст. 209 и п. «а» ч. 4 ст. 174.1 УК РФ (легализация).

Вывод: Дела о насильственном завладении криптовалютой сложны в доказывании. Присяжные могут не признать состав преступления, если доказательства недостаточны. Однако сам факт возбуждения дела — серьёзный сигнал: крипту начали отнимать силой, и правоохранители это фиксируют.

4. Жертвы — пенсионеры: самые уязвимые цели мошенников

Криптомошенники всё чаще нацелены на пожилых людей. Пенсионеры доверчивы, имеют накопления и не разбираются в технологиях. Результат — потерянные кредиты и сбережения.

Дело № 8. Пенсионерка из Новосибирской области — кредиты на 257500 рублей

Потерпевшая: пенсионерка

Суд: Советский районный суд г. Орска (рассмотрение в октябре 2025 года)

Статья: ч. 3 ст. 159 УК РФ (мошенничество)

Суть: В марте 2024 года неизвестные позвонили пенсионерке через мессенджер и предложили улучшить финансовое положение путём купли-продажи биткоинов. Женщина согласилась.

Для «инвестиций» она взяла кредиты в нескольких банках и перевела деньги на различные счета, указанные мошенниками. Общая сумма ущерба — **257500 рублей**.

В ходе следствия установлено, что часть денег (99500 рублей) была перечислена на расчётный счёт жителя Орска. Прокурор потребовал взыскать с него неосновательное обогащение в пользу пенсионерки.

Вывод: Типичная схема «инвестиции в биткоины» с использованием телефонных звонков и кредитных средств. Даже если дроппер (владелец счёта) не участвовал в обмане, он обязан вернуть деньги — как неосновательное обогащение.

Дело № 9. Пенсионер из Крыма — 145 000 рублей на «инвестиции»

Потерпевший: пенсионер, Ленинский район Республики Крым

Решение суда: иск прокурора удовлетворён (октябрь 2025 года)

Суть: В июне 2025 года пенсионеру позвонили и убедили инвестировать накопления в криптовалюту. Он перечислил на указанный счёт более **145000 рублей**.

В ходе расследования установлена личность дроппера — жителя Республики Башкортостан. Прокуратура обратилась в суд с иском о взыскании неосновательного обогащения. Суд требования удовлетворил.

Вывод: Дропперов вычисляют и привлекают к гражданской ответственности. Даже если уголовное дело против них не возбуждено, деньги придётся вернуть.

Дело № 10. Пенсионер из Томской области — 2,1 млн рублей на крипто-трейдинге

Потерпевший: пожилой мужчина, Кривошеинский район Томской области

Суд: Марьяновский районный суд Омской области

Статья: ч. 4 ст. 159 УК РФ (мошенничество в особо крупном размере)

Суть: Пенсионер заинтересовался торговлей криптовалютой, заполнил анкету на интернет-сайте, оставив персональные данные и номер телефона. Ему позвонил «консультант» и убедил вложить в цифровую валюту **более 2,1 млн рублей**.

Деньги были переведены на счёт жителя Омской области (дроппера). Прокуратура потребовала вернуть средства, и суд иск удовлетворил.

Вывод: Анкеты на сайтах «инвестиционных компаний» — прямой путь к мошенникам. Никогда не оставляйте данные на подозрительных сайтах.

Дело № 11. Пенсионерка-мошенница из Заречного — 4 млн рублей ущерба

Фигурант: 77-летняя жительница Заречного Пензенской области

Суд: Зареченский городской суд

Приговор: 3 года колонии общего режима (июль 2025 года)

Суть (зеркальная ситуация): Пожилая женщина сама была мошенницей. Она входила в доверие к людям, использовала специальную финансовую лексику и предлагала «разбогатеть на биткоине». Одним обещала высокую доходность, у других просила деньги для выгодного вложения.

Общий ущерб — **4058773 рубля**. Похищенные деньги пенсионерка тратила на себя: красивую одежду, продукты, концерты.

На момент преступления у женщины уже была судимость. Суд назначил наказание — 3 года колонии общего режима.

Вывод: Мошенничество с криптовалютами не зависит от возраста. Пожилые люди могут быть как жертвами, так и преступниками. Суд относится к ним так же строго.

5. Дело о хищении через «инвестиционный проект» — 6 лет колонии

Дело № 12. Евгений Васильев — биткоины с криптокошельков

Фигурант: Евгений Владимирович Васильев

Суд: Пресненский районный суд Москвы

Приговор: 6 лет колонии общего режима (февраль 2025 года)

Статья: ч. 4 ст. 159 УК РФ (мошенничество в особо крупном размере)

Суть преступления: Васильев разработал преступный план по хищению денежных средств и криптовалюты BTC. Он предлагал потерпевшим участие в финансовом проекте, обещая выгодные инвестиции.

Убедив жертв вложить деньги и крипту в специально созданные кошельки (которые он контролировал), Васильев неправомерно менял пароли, получал доступ к кошелькам и распоряжался криптовалютой по своему усмотрению.

Суд частично удовлетворил гражданские иски потерпевших.

Вывод: Классическая схема «инвестиционного проекта» с обещанием сверхдоходности. Всегда проверяйте, кому вы переводите крипту. Никто не даст гарантированный доход.

6. Верховный Суд РФ о криптовалюте в уголовных делах

На Петербургском международном юридическом форуме судья Верховного Суда России Евгений Рудаков сделал важное заявление: «За последние годы судами рассмотрено более 20 уголовных дел по преступлениям, связанным с посягательством на принадлежащую гражданам криптовалюту или цифровую валюту. Так, судами города Москвы в 2023-2024 годах рассмотрено 7 таких уголовных дел, судами Московской области — 4 дела».

Ключевые выводы Верховного Суда:

1. **Квалификация преступлений:** Действия чаще всего квалифицируются по нормам УК об ответственности за преступления против собственности.
2. **Способы хищения:** Криптовалюту похищают путём обмана (под видом оказания услуг по обмену или инвестиционной деятельности), а также тайного хищения (кражи) или присвоения.
3. **Насильственные способы:** В последнее время активно применяется насилие с целью завладения криптовалютой — такие действия квалифицируются как вымогательство, грабёж и разбой.
4. **Пример из практики Мособлсуда:** По одному из дел лица обвинялись в похищении человека с целью завладения криптовалютой. Они заставили потерпевшего сообщить данные для доступа к криптокошелькам и похитили 81 единицу криптовалюты, эквивалентную **50 млн рублей**.

7. Общие выводы по судебной практике

Что чаще всего фигурирует в приговорах:

Статья УК РФ	Типичные ситуации	Наказание
159 (мошенничество)	Инвестиционные проекты, фейковые обменники, обещания сверхдоходности	до 10 лет
163 (вымогательство)	Угрозы через Telegram, похищение людей с требованием паролей	до 15 лет
174/174.1 (легализация)	Обналичивание «грязной» крипты, переводы через	до 7 лет
159 (в отношении пенсионеров)	Телефонные звонки, «инвестиции в биткоины»	от 3 до 6 лет

Ключевые риски, которые выявили дела:

1. **Дропперов вычисляют и привлекают к ответственности** — даже если они «просто дали карту». Суды взыскивают суммы как неосновательное обогащение.
2. **Telegram не спасает от вымогательства** — правоохранители находят администраторов каналов и соучастников.
3. **Пенсионеры — лёгкая цель** — и самый частый источник ущерба в криптомошенничестве.

4. **Насильственное завладение криптой растёт** — и суды квалифицируют это по полной программе (похищение человека + вымогательство).
5. **Крипта стала полноценным объектом уголовно-правовой защиты** — Верховный Суд это прямо признал.

Заключение главы 21

Судебная практика по криптовалюте в России уже сформирована.

За 2023-2025 годы рассмотрены десятки дел. Суды:

- Признают криптовалюту имуществом
- Квалифицируют её хищение по статьям о краже, мошенничестве и вымогательстве
- Взыскивают похищенное через дропперов
- **Назначают реальные сроки (от 3 до 7 лет колонии)**

Если вы думаете, что «крипта — это серо и никто не узнает» — ошибаетесь. Узнают, найдут, осудят.

Использованные в главе источники:

- 1) Подборка наиболее важных документов по запросу Криптовалюта цифровая валюта https://www.consultant.ru/law/podborki/kriptovalyuta_cifrovaya_valyuta/#link-to-assistant
- 2) В Хакасии вынесен приговор по уголовному делу о мошенничестве при проведении операций с криптовалютой <https://epp.genproc.gov.ru/ru/gprf/mass-media/news/archive/e5867113/>
- 3) Прокуратура Московской области направила в суд уголовное дело о вымогательстве криптовалюты https://epp.genproc.gov.ru/ru/proc_50/mass-media/news/main/e8305548/
- 4) Подборка наиболее важных документов по запросу Виртуальные активы https://www.consultant.ru/law/podborki/virtualnye_aktivy/
- 5) В Подмосковье приговор вынесли 3 участникам ОПГ, обвиняемым в хищении криптовалюты <https://riamo.ru/news/proisshestiya/v-podmoskove-prigovor-vynesli-3-uchastnikam-opg-obvinjaemym-v-hischenii-kriptovaljuty/>
- 6) Пенсионерка хотела приобрести биткоины, но стала жертвой мошенников https://sovetsky--orb.sudrf.ru/modules.php?name=press_dep&op=1&did=956
- 7) Общественный совет при УФНС России по Московской области <https://www.rsnmo.ru/index.php?id=97184>
- 8) Обвиняемые в вымогательстве криптовалюты на 16,8 млн руб предстанут перед судом https://rapsinews.ru/judicial_news/20251210/311422273.html
- 9) Суд вынес приговор Битмаме <https://news.rambler.ru/incidents/54881490-sud-vynes-prigovor-bitmame/>
- 10) Перед судом в Хакасии предстанет один из организаторов мошеннической схемы по продаже криптовалюты https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/%D1%83%D0%B1%D0%BA/Publikacii_i_vistuplenija/item/66453501/?year=2025&month=7&day=7
- 11) Советский районный суд г. Орск Оренбургской области https://sovetsky--orb.sudrf.ru/modules.php?name=press_dep&op=1&did=956
- 12) Прокуратура Московской области направила в суд уголовное дело о вымогательстве криптовалюты https://epp.genproc.gov.ru/ru/proc_50/mass-media/news/main/e8305548/
- 13) Фигурант дела о мошенничестве с криптовалютами получил 6 лет колонии https://krasnogvardeiskiy--krm.sudrf.ru/modules.php?name=press_dep&op=1&did=142

- 14) В Ленинском районе прокуратура защитила права пенсионера, пострадавшего от действий телефонных мошенников https://epp.genproc.gov.ru/ru/proc_91/mass-media/news/main/e6245801/
- 15) В Екатеринбурге вынесли вердикт по делу ОПГ из Сибири <https://ura.news/news/1053022631>
- 16) Верховный Суд Республики Башкортостан
https://vs.bkr.sudrf.ru/modules.php?name=press_dep&op=1&did=50
- 17) Зареченский городской суд Пензенской области
https://zarechensky.pnz.sudrf.ru/modules.php?name=press_dep&op=4&did=29
- 18) Прокуратура Кривошеинского района Томской области в судебном порядке взыскала с дроппера денежные средства, похищенные дистанционными мошенниками https://volodinskoe-r69.gosweb.gosuslugi.ru/dlya-zhiteley/novosti-i-reportazhi/novosti_531.html
- 19) В Подмоскowie полиция задержала администратора Telegram-канала по подозрению в вымогательстве
<https://en.mvd.ru/news/item/61521378/>
- 20) Барун-Хемчикский районный суд Республики Тыва https://barun-hemchikskiy.tva.sudrf.ru/modules.php?name=press_dep&op=1&did=56

Заключение

Мы прошли долгий путь. От юридического лабиринта до судебных приговоров, от наследства до развода, от чек-листа для новичка до стратегий для бизнеса.

Пришло время собрать всё воедино и заглянуть в будущее.

Три главных вывода из книги

1. Крипта в России не запрещена, но и не свободна.

Вы можете владеть биткоинами, покупать их, продавать, дарить, наследовать. Но вы не можете расплачиваться ими в магазине. Вы обязаны платить налоги с прибыли. И вы находитесь под колпаком блокчейн-аналитики — каждый ваш перевод виден.

2. «Серая зона» заканчивается.

С 2026 года в России начнёт работать легальный рынок криптовалют: лицензированные обменники, спецдепозитарии, доступ для квалифицированных инвесторов. Те, кто не легализуется, после 2027 года попадут под уголовные статьи.

3. Ваша безопасность — в ваших руках (и в правильном хранении сид-фразы).

90% проблем с криптой — это потеря доступа, мошенничество или незнание законов. Аппаратный кошелёк, две копии сид-фразы, понимание налогов — это не паранойя, это базовая гигиена.

Что будет дальше? Прогноз на 2026–2028 годы

2026 год:

- Принятие базового закона о криптовалютах (статус валютной ценности)
- Запуск лицензирования криптообменников
- Начало работы системы «Прозрачный блокчейн» во всех банках
- ЦФА в открытых блокчейн-сетях (мост с глобальной криптоинфраструктурой)

2027 год:

- Полный запрет нелегальных криптообменников (уголовная ответственность)
- Массовый выход легальных игроков на рынок
- Рост рынка ЦФА и стейблкоинов
- Появление первых российских криптофондов

2028 год:

- Интеграция крипты в традиционные банковские продукты
- Возможность для неквалифицированных инвесторов (с лимитами)
- Развитие DeFi в российском правовом поле (осторожно, но он будет)

Что останется неизменным?

- Запрет на оплату товаров и услуг криптовалютой внутри РФ
- Обязанность платить налоги
- Контроль со стороны Росфинмониторинга и ФНС

Последний совет автора

Криптовалюта — это инструмент. Как нож: можно нарезать хлеб, а можно порезаться. Или даже получить срок, если использовать его не по назначению.

В России крипта — не способ обогащения за месяц и не способ спрятать деньги от государства. Это высокорисковый инвестиционный актив, который требует знаний, осторожности и уважения к закону.

Если вы готовы учиться, платить налоги и хранить ключи правильно — крипта может стать частью вашего портфеля.

Если вы ищете лёгких денег, анонимности или способа обойти закон — эта книга предупредила вас. Дальше вы сами.

И помните: в блокчейне нет анонимности. Есть только псевдонимность. И она снимается в тот момент, когда вы выходите в реальный мир — к банку, бирже или налоговой.

Спасибо, что дочитали. Берегите сид-фразу.

Приложение 1. Образец договора купли-продажи криптовалюты

ДОГОВОР КУПЛИ-ПРОДАЖИ КРИПТОВАЛЮТЫ № ____

г. _____ « ____ » _____ 20__ г.

Гражданин РФ _____,
паспорт серии _____ № _____, выдан _____
_____ « ____ » _____ 20__ г.,
зарегистрированный по адресу: _____

именуемый в дальнейшем «**Продавец**», с одной стороны, и

Гражданин РФ _____,
паспорт серии _____ № _____, выдан _____
_____ « ____ » _____ 20__ г.,
зарегистрированный по адресу: _____

именуемый в дальнейшем «**Покупатель**», с другой стороны, совместно
именуемые «**Стороны**», заключили настоящий договор о нижеследующем:

1. Предмет договора

1.1. Продавец передает в собственность Покупателя, а Покупатель принимает и оплачивает следующее имущество: **цифровую валюту (криптовалюту)** в количестве и ассортименте, указанном ниже.

1.2. Наименование цифровой валюты: _____
(*USDT (TRC-20), Bitcoin (BTC), Ethereum (ETH)*)

1.3. Количество цифровой валюты: _____
_____ (цифрами и прописью).

1.4. Адрес кошелька Продавца, с которого будет осуществлен перевод: _____.

1.5. Адрес кошелька Покупателя, на который будет осуществлен перевод: _____.

2. Цена и порядок расчетов

2.1. Цена договора составляет _____
_____ рублей (цифрами и прописью).

2.2. Оплата производится Покупателем в рублях путем перевода на банковский счет Продавца по следующим реквизитам:

Банк-получатель: _____

Номер счета: _____

ФИО получателя: _____

2.3. Моментом исполнения обязательств по оплате считается момент зачисления денежных средств на счет Продавца.

3. Передача цифровой валюты

3.1. Продавец обязуется осуществить перевод цифровой валюты на адрес кошелька Покупателя, указанный в п. 1.5, в течение ____ часов с момента поступления оплаты.

3.2. Моментом передачи цифровой валюты считается момент подтверждения транзакции в блокчейне (количество подтверждений сети: ____).

4. Подтверждение сделки

4.1. Стороны признают юридическую силу следующих доказательств совершения сделки:

- Скриншотов переписки в мессенджерах (Telegram, WhatsApp и др.);
- Скриншотов P2P-ордера с указанием ID сделки;
- Хеша транзакции в блокчейне (TxID);
- Выписок из банковских приложений о движении средств.

5. Ответственность сторон

5.1. В случае неисполнения или ненадлежащего исполнения обязательств по настоящему договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

6. Реквизиты и подписи сторон

Продавец

Покупатель

ФИО: _____

ФИО: _____

Паспорт: _____

Паспорт: _____

Телефон: _____

Телефон: _____

Подпись: _____

Подпись: _____

Приложение 2. Форма заявления в банк о разблокировке счёта

Генеральному директору (Управляющему)

_____ (наименование банка)

от _____

_____ (ФИО полностью)

Паспорт РФ: серия _____ № _____

Выдан: _____

Дата выдачи: «___» _____ 20__ г.

Адрес регистрации: _____

Телефон: _____

E-mail: _____

ЗАЯВЛЕНИЕ

о снятии ограничений на распоряжение банковским счетом

Я, _____, являюсь клиентом _____ (наименование банка), на мое имя открыт счет № _____ «___» _____ 20__ г. банком были введены ограничения на распоряжение моими денежными средствами (заблокированы дистанционный доступ к счету, операции по картам и переводам).

Полагаю данные ограничения незаконными по следующим основаниям. Источником происхождения денежных средств, вызвавших подозрение банка, является доход от продажи принадлежащего мне на праве собственности имущества — **цифровой валюты (криптовалюты)**, что подтверждается следующими документами:

1. Договор купли-продажи криптовалюты № ___ от «___» _____ 20__ г.
2. Скриншоты P2P-ордера (ID сделки: _____)/хеш транзакции (TxID: _____).
3. Выписка из криптокошелька о движении средств.
4. Налоговая декларация по форме 3-НДФЛ за 20__ г. с отметкой о приеме (при наличии).

В соответствии с Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах...» цифровая валюта признается имуществом. Действующим законодательством Российской Федерации не установлен запрет на совершение физическими лицами сделок купли-продажи цифровой валюты.

Прошу снять ограничения на распоряжение моим банковским счетом в течение установленного законом срока. В случае отказа прошу предоставить мотивированный письменный ответ.

Приложения:

1. Копия договора купли-продажи на ____ л.
2. Копии скриншотов сделки на ____ л.
3. Копия выписки из криптокошелька на ____ л.
4. Копия налоговой декларации на ____ л.

« ____ » _____ 20__ г. _____ / _____
(подпись) (расшифровка)

Приложение 3. Гайд по восстановлению доступа к кошельку без сид-фразы

Потеря сид-фразы (12 или 24 случайных слов) — это самая страшная ситуация для владельца криптовалюты. В отличие от банка, здесь нет кнопки «Забыли пароль?» и офиса с паспортом. Вероятность успешного восстановления без резервной копии зависит только от того, насколько у вас сохранился «технический след», то есть доступ к самому приложению или его остаткам.

Важное предупреждение: Остерегайтесь мошенников! Ни один добросовестный специалист по кибербезопасности не может гарантировать 100% восстановление и не должен брать предоплату. Все, кто пишет в личные сообщения «Я хакер, восстановлю ваш кошелек» — это скамеры.

Этап 1. Восстановление через приложение (если кошелек еще открыт)

Если приложение кошелька запускается и вы помните пин-код для входа (но потеряли сид-фразу для восстановления на новом устройстве), сделайте следующее немедленно:

- **Немедленно создайте новый кошелек.** Установите на другое устройство новый кошелек (например, Trust Wallet или MetaMask), безопасно сохраните новую сид-фразу на бумаге и сфотографируйте ее на телефон, который физически находится в безопасном месте.
- **Переведите все активы.** Срочно отправьте все токены с уязвимого кошелька на адрес нового. Не ждите и не оставляйте даже небольшие суммы — приложение может обновиться, телефон может потеряться или сломаться в любой момент.

Этап 2. Поиск сид-фразы в файловой системе (для опытных пользователей и специалистов)

Этот этап требует привлечения профессионала по восстановлению данных. Самостоятельно копаться в файлах смертельно опасно для ваших средств.

- **Мобильные кошельки (Trust Wallet, MetaMask и др.)**

На Android-устройствах данные приложений хранятся в защищенной директории/data/data/. Для доступа обычно нужны root-права. Файл конфигурации часто представляет собой зашифрованный JSON-файл. Например, в Trust Wallet файл может называться trustwallet.json или config.json. Для его расшифровки потребуются пароль, который вы вводили при создании кошелька. Если у вас есть root-доступ и вы помните пароль, специалист может попытаться расшифровать этот файл и извлечь сид-фразу.

- **Браузерные расширения (MetaMask)**

Данные расширения хранятся в папке профиля браузера. В Windows путь обычно выглядит как C:\Users\[Имя]\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn. Файлы зашифрованы, а ключ шифрования хранится в связке ключей операционной системы (например, Keychain в macOS). Без доступа к этой связке ключей расшифровать данные невозможно.

Этап 3. Если кошелек уже удален

- **Экстренное восстановление данных с диска**

Немедленно выключите устройство (телефон или компьютер), чтобы избежать перезаписи секторов памяти. Обратитесь в лабораторию по форензике (криминалистическому восстановлению данных). Специалисты могут снять дампы памяти и попытаться найти остатки конфигурационных файлов. Шансы есть, если устройство использовалось недолго и память не перезаписывалась новыми данными.

- **Поиск резервных копий**

Проверьте все облачные хранилища (Google Диск, Яндекс.Диск, iCloud), мессенджеры, черновики электронной почты и заметки, физические записи в книгах и блокнотах. Сделайте полный обыск своего рабочего места.

Этап 4. Новые технологии на вашей стороне

Некоторые новые кошельки внедряют механизмы социального восстановления или резервного копирования через MPC (Multi-Party Computation), которые позволяют восстановить доступ без классической сид-фразы. Если вы только выбираете кошелек, рекомендуем обратить внимание на этот класс решений, чтобы в будущем минимизировать риск безвозвратной потери средств.

Приложение 4. Лимиты и риски (сводная таблица)

Операция	Лимит / Порог	Период	Для кого действует	Санкция за нарушение
Майнинг без регистрации в реестре	6000 кВт·ч	месяц	Физические лица	Штраф до 150 тысяч рублей + конфискация
Покупка криптовалюты (неквалы, ЦФА)	300-600 тысяч рублей	год	Неквалифицированные инвесторы	Отказ в проведении операции
Обязательная подача отчета в ФНС	600 тысяч рублей	год	Владельцы зарубежных кошельков	Штраф по валютному законодательству
Уголовная ответственность за незаконный майнинг	3,5 млн рублей	разово / накопленный доход	Все категории	До 5 лет лишения свободы
Крупный размер в уголовных делах	3,5 млн рублей	разово	Все категории	Наступление квалифицирующего признака
Особо крупный размер в уголовных делах	13,5 млн рублей	разово	Все категории	Наступление квалифицирующего признака
Обязанность уведомить ФНС о кошельке	Любой факт открытия	30 дней с даты открытия	Валютные резиденты РФ	Уточняется
Блокировка по 115-ФЗ	Любая сумма	—	Все владельцы банковских карт	Блокировка конкретного счета
Блокировка по 161-ФЗ	Любая сумма	—	Все владельцы банковских карт	Блокировка всех счетов во всех банках

Важно: Таблица отражает состояние законодательства на апрель 2026 года. Лимиты 300-600 тысяч рублей для неквалифицированных инвесторов обсуждаются и могут измениться ко второму чтению законопроекта. Следите за обновлениями.

Приложение 5. Регионы с запретом майнинга (по состоянию на апрель 2026 года)

Постановлением Правительства РФ № 1869 от 23 декабря 2024 года установлен перечень регионов с полным запретом майнинга на период с **1 января 2025 года по 15 марта 2031 года**.

Регионы с полным запретом майнинга:

- Республика Дагестан
- Республика Ингушетия
- Кабардино-Балкарская Республика
- Карачаево-Черкесская Республика
- Республика Северная Осетия — Алания
- Чеченская Республика
- Донецкая Народная Республика
- Луганская Народная Республика
- Запорожская область
- Херсонская область

Регионы с круглогодичным запретом (с 1 апреля 2026 года):

- Республика Бурятия (заменен сезонный запрет на круглогодичный)
- Забайкальский край (заменен сезонный запрет на круглогодичный)

Регионы с сезонным запретом (осенне-зимний период):

- Отдельные районы Иркутской области (перечень районов уточняется постановлением Правительства РФ)

Важно: В указанных регионах майнинг запрещен полностью, включая физических лиц в пределах лимита 6000 кВт·ч. Любая деятельность влечет административную (ст. 15.50 КоАП РФ) или уголовную (ст. 171.6 УК РФ) ответственность.

Актуальный перечень всегда доступен на официальном портале Правительства РФ (<http://government.ru/>).

Приложение 6. Полезные информационные ресурсы

Официальные государственные ресурсы:

1. **Центральный банк Российской Федерации** <https://www.cbr.ru/> (раздел «Противодействие нелегальной деятельности» содержит актуальные списки компаний с признаками нелегальной деятельности)
2. **Федеральная налоговая служба** <https://www.nalog.gov.ru/> (здесь публикуются формы деклараций 3-НДФЛ и образцы заполнения для операций с криптовалютой)
3. **Сервис «Прозрачный бизнес»** <https://pb.nalog.ru/> (для проверки контрагентов по ИНН)
4. **Росфинмониторинг** <https://www.fedsfm.ru/> (реестр организаций и лиц, причастных к экстремистской деятельности и терроризму)
5. **Портал государственных услуг** <https://www.gosuslugi.ru/> (через него планируется запустить механизм оспаривания блокировок по 161-ФЗ)

AML-сервисы для проверки криптоадресов:

1. **AMLBot** <https://amlbot.com/> (проверка через веб-интерфейс и Telegram-бота. Поддерживает более 22 блокчейнов)
2. **GetBlock** <https://getblock.net/aml> (AML-проверка адресов с собственным Telegram-ботом. Поддерживает 8 блокчейнов)
3. **BestChange (AML-анализатор)** <https://www.bestchange.ru/aml> (проверка с использованием данных шести провайдеров. Поддерживает более 80 криптовалют)
4. **MistTrack** <https://misttrack.io/> (бесплатная разовая проверка адресов с оценкой риска)
5. **Chainalysis** <https://www.chainalysis.com/> (профессиональный инструмент для расследований)

Онлайн-сервисы для поиска юристов:

- «Правовед» <https://pravoved.ru/> (раздел «Криптовалюта»)
- «Харант» <https://harant.ru/> (поиск по городам)

Глоссарий

115-ФЗ — Федеральный закон о противодействии легализации (отмыванию) доходов. Основание для блокировки счетов банками.

161-ФЗ — Федеральный закон «О национальной платежной системе». Основание для внесения клиента в «черный список» ЦБ РФ.

KYC (Know Your Customer) — процедура проверки личности клиента (по паспорту или другим документам).

AML (Anti-Money Laundering) — меры по противодействию отмыванию денег. AML-проверка кошелька показывает, связан ли он с преступной деятельностью.

DeFi (Decentralized Finance) — децентрализованные финансовые сервисы, работающие без посредников на основе смарт-контрактов.

P2P (Peer-to-Peer) — прямые сделки между пользователями без участия посредников.

Адрес (Wallet Address) — уникальная строка символов в блокчейне, на которую можно получить криптовалюту. Аналог номера банковской карты.

Блокчейн (Blockchain) — децентрализованная база данных, состоящая из цепочки блоков, в которых записаны все транзакции. Невозможно изменить или удалить.

Горячий кошелек (Hot Wallet) — программный кошелек, постоянно подключенный к интернету. Удобен для частых операций, но уязвим для взлома.

Дроппер (Дроп) — лицо или его банковская карта, используемые для транзита и «разрыва» цепочки переводов. Часто дропперами становятся добросовестные участники P2P-сделок, сами того не подозревая.

Кастодиальный кошелек (Custodial Wallet) — кошелек, где приватные ключи хранятся у третьей стороны (например, биржи). Вы не контролируете свои средства полностью.

Криптовалюта (Цифровая валюта) — децентрализованное цифровое средство учета, не имеющее единого эмитента. Признается имуществом в РФ.

Майнинг (Mining) — процесс решения математических задач с помощью вычислительного оборудования для создания новых блоков в блокчейне и получения вознаграждения.

Миксер (Mixer / Tumbler) — сервис для смешивания и анонимизации транзакций. В России находится под пристальным надзором.

Некастодиальный кошелек (Non-custodial Wallet) — кошелек, где приватные ключи хранятся только у владельца. Вы полностью контролируете свои средства.

Неквал — это жаргонное сокращение, обозначающее частное лицо на фондовом рынке, не имеющее подтвержденного статуса квалифицированного инвестора.

Приватный ключ (Private Key) — секретный криптографический код, дающий право распоряжаться криптовалютой на определенном адресе. Его потеря означает безвозвратную потерю доступа к средствам.

Публичный ключ (Public Key) — криптографический код, который генерируется из приватного ключа и служит адресом для получения средств.

Сид-фраза (Seed Phrase) — последовательность из 12 или 24 случайных слов, с помощью которой можно восстановить доступ к кошельку и всем связанным с ним приватным ключам.

Смарт-контракт (Smart contract) — программа, выполняющаяся в блокчейне автоматически при наступлении заранее определенных условий.

Стейблкоин (Stablecoin) — токен, привязанный к курсу реального актива (например, доллара). Обеспечивает стабильность.

Транзакция (Transaction) — операция по переводу криптовалюты с одного адреса на другой, записанная в блокчейн.

Фиат (Fiat) — традиционные, выпущенные государством деньги (рубли, доллары, евро).

Холодный кошелек (Cold Wallet) — способ хранения приватных ключей на устройстве, физически не подключенном к интернету. Максимальная защита от взлома.

ЦФА (Цифровые финансовые активы) — токенизированные версии традиционных финансовых инструментов (акций, облигаций), выпущенные в соответствии с Федеральным законом №259-ФЗ. Являются регулируемым инструментом.