

ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТ В СОВЕРШЕНИИ КИБЕРПРЕСТУПЛЕНИЙ: УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ И СЛЕДСТВЕННАЯ ПРАКТИКА

*Дусматов Дурбек Рустамжон оглы, прокурор отдела в сфере
Противодействия теневой экономики прокуратуры города
Ташкента, юрист 2-класса*

КИБЕРЖИНОЯТЛАРНИ СОДИР ЭТИШДА КРИПТОВАЛЮТАЛАРДАН ФОЙДАЛАНИШ: ЖИНОЯТ-ХУКУКИЙ ТАҲЛИЛ ВА ТЕРГОВ АМАЛИЁТИНИНГ ХУСУСИЯТЛАРИ

*Дўсматов Дурбек Рустамжон ўгли, Тошкент шаҳар
прокуратураси Яширин иқтисодиётга қарши курашиш соҳасида
назорат бўлими прокурори, 2-даражали юрист*

USE OF CRYPTOCURRENCIES IN COMMITTING CYBERCRIMES: CRIMINAL LAW ANALYSIS AND INVESTIGATIVE PRACTICE

*Dusmatov Durbek Rustamjon ugli, Tashkent City Prosecutor's Office
Prosecutor of the Department in the field of counteraction shadow
economy, 2nd class lawyer*

Аннотация: В статье рассматриваются особенности использования криптовалют при совершении киберпреступлений, включая их роль в легализации преступных доходов и финансировании противоправной деятельности. Проведен уголовно-правовой анализ действующего законодательства, выделены ключевые проблемы квалификации и доказывания преступлений с применением цифровых активов. Отдельное внимание уделено следственной практике и международным подходам к правовому регулированию оборота криптовалют. Представлены предложения по совершенствованию уголовного законодательства и правоприменительной практики.

Ключевые слова: криптовалюта, киберпреступность, отмывание доходов, уголовное право, биткойн, блокчейн, электронные доказательства.

Аннотация: Мақолада кибержиноятларни содир этишда криптовалютадан фойдаланишнинг ўзига хос жиҳатлари, жумладан, жинойий йўллар билан олинган даромадларни легаллаштириш ва ноқонуний фаолиятни молиялаштиришдаги роли кўриб чиқилади. Амалдаги қонунчиликка нисбатан жиноят-хуқуқий таҳлил ўтказилган, рақамли активлардан фойдаланилган ҳолда содир этилган жиноятларни квалификация қилиши ва исботлашдаги асосий муаммолар ажратиб кўрсатилган. Тергов амалиёти ва криптовалюталар муомаласини ҳуқуқий тартибга солишда халқаро ёндашувларга алоҳида эътибор қаратилган. Жиноят қонунчилиги ва ҳуқуқни қўллаш амалиётини такомиллаштириш бўйича таклифлар илгари сурилган.

Калит сўзлар: криптовалюта, кибержиноятчилик, даромадларни ювиш, жиноят ҳуқуқи, биткойн, блокчейн, электрон далиллар.



<https://orcid.org/0009-0007-0038-4832>

e-mail:
bk179971@gmail.com



Abstract: *The article examines the specific features of using cryptocurrencies in the commission of cybercrimes, including their role in the legalization of criminal proceeds and the financing of unlawful activities. A criminal law analysis of the current legislation is conducted, highlighting key issues related to the qualification and proof of crimes involving digital assets. Particular attention is paid to investigative practices and international approaches to the legal regulation of cryptocurrency circulation. The article also presents proposals for improving criminal legislation and law enforcement practices.*

Keywords: *cryptocurrency, cybercrime, money laundering, criminal law, bitcoin, blockchain, electronic evidence.*

ВВЕДЕНИЕ. Стремительное развитие цифровых технологий привело к трансформации экономических и правовых отношений. Одним из наиболее значимых явлений в цифровом пространстве стала криптовалюта — децентрализованная цифровая валюта, не подконтрольная государственным институтам. Несмотря на ряд преимуществ, криптовалюты широко используются в преступных целях: для отмывания доходов, финансирования терроризма, сбыта наркотиков, оплаты за хакерские услуги и прочие преступления в киберпространстве. При этом, появление криптовалют (Bitcoin, Ethereum и др.) [1] существенно трансформировало сферу финансовых и цифровых технологий, но одновременно создало новые риски в виде анонимных, трансграничных и трудноотслеживаемых транзакций, тем самым способствуя росту преступлений — мошенничеству, хакерским атакам, финансированию терроризма и отмыванию денег.

ОБСУЖДЕНИЕ. Мошенничество с криптовалютами может принимать различные формы. Одной из наиболее распространённых схем является фишинг, когда преступники с помощью ложных сайтов или сообщений пытаются получить доступ к кошелькам пользователей и украсть их средства. Также часто встречаются мошенничества с инвестициями: создание фальшивых криптовалютных фондов или платформ для “быстрого” обогащения, на которых граждане теряют свои деньги. Примером таких схем является так называемая “пирамида” — когда деньги новых инвесторов используются для выплаты прибыли старым.

Отмывание преступных доходов осуществляется посредством мультиадресных кошельков, миксеров, обменников, а также через NFT и DeFi-платформы. В международной практике подобные действия квалифицируются как отмывание денежных средств и часто сопровождаются дополнительными составами. Принимая во внимание криминогенную ситуацию в Республике Узбекистан, эмпирические данные показывают, что в 2024 году зарегистрировано 58 800 киберпреступлений (против 863 в 2019), что на 27,1 % больше, чем в 2023 году [7]. Уровень преступности составил 35,6 случаев на 10 000 человек, что рекордно за 4 года, тем самым количество кибератак за 5 лет выросло в 68 раз, доля киберпреступлений выросла с 6,2 % (2023) до 44,4 % (2024) от общего числа, а ущерб граждан превысил 1,9 трлн. сумов (≈180 млн. USD) за период с 2021 по 2024 года.

Одним из главных преимуществ криптовалют является их анонимность. Преступники активно используют криптовалюты для отмывания денег. Транзакции с криптовалютами позволяют скрывать следы преступной деятельности, так как они не привязаны к традиционным финансовым системам. Через децентрализованные биржи, а также с помощью анонимизаторов транзакций, таких как миксеры (обменники криптовалют, которые “смешивают” деньги других пользователей, делая их происхождение трудноотслеживаемым), можно скрывать реальные источники средств.

Криптовалюты также могут использоваться для финансирования терроризма. Анонимность и отсутствие

государственного контроля делают их идеальными для перевода средств на счета террористических организаций. Криптовалюты помогают обходить санкции и международные регуляции, что делает их привлекательным инструментом для террористов. Использование криптовалютных кошельков позволяет избежать отслеживания финансовых потоков, а транзакции между различными странами упрощают процесс перевода средств.

Что касается проблем квалификации и пробелов в законодательстве, то несомненно одной из ключевых трудностей в уголовно-правовом регулировании использования криптовалют является отсутствие единого понятия криптовалюты в уголовном и финансовом праве. Возникают следующие проблемы, неясность правовой природы криптовалют (имущество, финансовый инструмент, цифровой актив), сложность квалификации преступлений с их использованием, правовая неопределенность в части конфискации криптовалют.

В Узбекистане криптоактивы определены в ряде нормативных актов, но в Уголовный кодекс пока не внедрено четкое регулирование в этой сфере. В то же время преступные схемы становятся всё изощрённее. Основная схема, то есть 98 % киберпреступлений связаны с банковскими картами: хищение через вредоносные ссылки или SMS-фишинг, из них 60 % – контроль над картой/устройством, 16 % – получение SMS-кода, 4 % – онлайн-кредиты, 11 % – мошенничество на торговых платформах. Например, в 2024 году и в текущем годах, 12 человек привлечены за незаконный оборот криптовалют, в основном через Binance – административные аресты и штрафы до 100 БРВ, повторно – лишение свободы до 5 лет [8]. Или, например, в Ферганской и Кокандской областях выявлены нелегальные майнинговые фермы (совокупный ущерб, нанесенный государству выявленными майнерами, составил 1,3 млрд. сумов).

Так как, криптовалюты являются децентрализованными и не привязаны к какой-

либо конкретной стране, расследование киберпреступлений, связанных с криптовалютами, часто сталкивается с проблемами юрисдикции. Преступники могут использовать криптовалюты для перевода средств в страны с более мягким законодательством или даже скрываться за анонимными биржами, которые работают без явного контроля со стороны государственных органов.

РЕЗУЛЬТАТЫ. Следственная практика и электронные доказательства. Расследование преступлений с использованием криптовалют требует нового уровня компетенции от следователей, оперативных сотрудников и экспертов. На практике возникают следующие трудности: невозможность отследить цепочку операций без специальных инструментов (Chainalysis, Crystal и др.), отсутствие доступа к иностранным криптобиржам, низкий уровень подготовки правоохранителей, трудности в получении и закреплении цифровых доказательств (лог-файлы, blockchain-история, скриншоты и пр). Сложности усиливаются при отсутствии международного правового сотрудничества и договоренностей с криптоплатформами.

На международном уровне успешно внедряются практики по контролю за криптовалютами, например в Соединённых Штатах Америки, криптобиржи обязаны соблюдать правила KYC/AML, в Евросоюзе принят Регламент MiCA и расширяются полномочия AML-агентств, в России на данный момент инкриминируются статьи о цифровых финансовых активах в ГК и УК РФ.

При этом, для Узбекистана целесообразно ввести отдельную уголовно-правовую норму, предусматривающую ответственность за использование криптовалют в преступных целях, наделить следственные органы доступом к специализированным блокчейн-аналитическим инструментам, заключить международные соглашения с крупными криптобиржами и правоохранительными органами.

Использование криптовалют в киберпреступлениях — вызов для современной уголовной юстиции. Необходимы комплексные меры: уточнение правового статуса криптоактивов, адаптация законодательства, подготовка специалистов, международное сотрудничество. Только сочетание уголовно-правовых и криминологических подходов позволит эффективно противостоять данной угрозе. Эмпирический анализ показывает, что Узбекистан переживает резкий рост криптокриминала — рост почти в 70 раз за 5 лет, значительный экономический ущерб и преобладающий характер финансовых схем.

ЗАКЛЮЧЕНИЕ. Криптовалюты, несмотря на свою полезность и перспективность, представляют серьёзную угрозу для безопасности. Их анонимность и децентрализованная природа предоставляют преступникам возможности для совершения широкого спектра правонарушений, от мошенничества до финансирования терроризма. В связи с этим, необходимо продолжать развивать законодательные и технические меры

по борьбе с киберпреступностью. Только при комплексном подходе, включающем улучшение законодательства, использование новых технологий и международное сотрудничество, можно эффективно противодействовать угрозам, связанным с использованием криптовалют в преступных целях.

СПИСОК ЛИТЕРАТУРЫ:

1. Блокчейн и криптовалюта: правовой анализ / под ред. И.Л. Бачило. – М.: НОРМА, 2021.
2. Государственная служба финансового мониторинга Республики Узбекистан: методические рекомендации по выявлению криптовалютных операций, 2023.
3. FATF Report: Virtual Assets and AML/CFT, 2022.
4. MiCA Regulation (EU) 2023/1114 of the European Parliament and of the Council.
5. Уголовный Кодекс Республики Узбекистан.
6. Абдурахмонов А.Ш. Киберпреступность и электронные доказательства. – Т.: Академия МВД, 2022.
7. Chainalysis Crypto Crime Report 2024.
8. Данные МВД Узбекистана (статистика 2024–2025 гг).

