



УДК 343.2/7(4/9)
МРНТИ 10.77.51

Д.Б. Кайназарова

*Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан,
г. Косшы, Республика Казахстан*

ОТМЫВАНИЕ ДЕНЕГ В СФЕРЕ ВИРТУАЛЬНЫХ ВАЛЮТ: РИСКИ И РЕГУЛИРОВАНИЕ

Аннотация. Настоящая статья посвящена исследованию масштабов и механизмов отмывания преступных доходов с использованием виртуальных валют, прежде всего криптовалют, в условиях стремительной цифровизации глобальной экономики и трансформации финансовых потоков.

В работе проведен всесторонний анализ правовых, технологических и институциональных рисков, возникающих вследствие использования криптовалют в противоправной деятельности, включая схемы легализации средств, полученных от торговли наркотиками, киберпреступлений, вымогательства, обхода санкций и финансирования терроризма.

Особое внимание уделено ключевым особенностям виртуальных активов, таким как децентрализация, псевдонимность транзакций и технические возможности сокрытия происхождения активов – посредством миксеров, анонимных криптовалют, DeFi-протоколов и NFT.

Подчеркивается роль аналитических платформ в деанонимизации подозрительных транзакций и необходимость институциональной подготовки следователей, прокуроров и аналитиков. Сделан вывод о необходимости комплексной трансформации подходов к финансовому мониторингу, включающей правовое обновление, техническое переоснащение и международную координацию усилий. Предложены рекомендации по созданию национальных центров анализа криптотранзакций, усилению взаимодействия с глобальными регуляторами, сертификации блокчейн-экспертов и стандартизации процессуального обращения с цифровыми доказательствами.

Ключевые слова: криптовалюта; блокчейн; отмывание денег; киберпреступность; преступный доход; анонимная монета; криптоплатформа; децентрализация; токен; транзакция.

Д.Б. Қайназарова

*Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы,
Қосшы қ., Қазақстан Республикасы*

ВИРТУАЛДЫ ВАЛЮТАЛАР САЛАСЫНДАҒЫ АҚШАНЫ ЖЫЛЫСТАТУ: ТӘУЕКЕЛДЕР ЖӘНЕ РЕТТЕУ

Аннотация. Бұл мақала жаһандық экономиканы жедел цифрландыру және қаржы ағындарын трансформациялау жағдайында виртуалды валюталарды, ең алдымен криптовалюталарды пайдалана отырып, қылмыстық кірістерді жылыстатудың ауқымы мен тетіктерін зерттеуге арналған.

Жұмыста есірткі саудасынан, киберқылмыстардан, бопсалаудан, санкцияларды айналып өтуден және терроризмді қаржыландырудан алынған қаражатты заңдастыру схемаларын қоса алғанда, құқыққа қарсы қызметте криптовалюталарды пайдалану нәтижесінде туындайтын құқықтық, технологиялық және институционалдық тәуекелдерге жан-жақты талдау жүргізілді.

Орталықсыздандыру, транзакциялардың бүркеншік аты және активтердің шығу тегін жасырудың техникалық мүмкіндіктері сияқты виртуалды активтердің негізгі ерекшеліктеріне – араластырғыштар, анонимді криптовалюталар, DeFi протоколдары және NFT арқылы ерекше назар аударылады.

Күдікті транзакцияларды анонимизациялаудағы аналитикалық платформалардың рөлі және тергеушілерді, прокурорларды және талдаушыларды институционалдық даярлау қажеттілігі атап өтіледі. Құқықтық жаңартуды, техникалық қайта жарақтандыруды және күш-жігерді халықаралық үйлестіруді қамтитын қаржылық мониторингке тәсілдерді кешенді трансформациялау қажеттілігі туралы қорытынды жасалды. Криптотранзакцияларды талдаудың ұлттық орталықтарын құру, жаһандық реттеушілермен өзара іс-қимылды күшейту, блокчейн-сарапшыларды сертификаттау және цифрлық дәлелдемелермен процессуалдық өңдеуді стандарттау бойынша ұсыныстар ұсынылды.



Түйінді сөздер: криптовалюта; блокчейн; ақшаны жылыстату; киберқылмыс; қылмыстық кіріс; анонимді монета; криптоплатформа; орталықсыздандыру; таңбалауыш; транзакция.

D.B. Kainazarova

*The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan,
Kosshi, the Republic of Kazakhstan*

MONEY LAUNDERING IN VIRTUAL CURRENCIES: RISKS AND REGULATION

Abstract. This article is devoted to the study of the scale and mechanisms of laundering crime proceeds using virtual currencies, primarily cryptocurrencies, in the context of rapid digitalization of the global economy and transformation of financial flows.

The paper provides a comprehensive analysis of the legal, technological and institutional risks arising from the use of cryptocurrencies in illegal activities, including schemes for legalization of funds derived from drug trafficking, cybercrime, extortion, sanctions circumvention and terrorist financing.

Special attention is paid to key features of virtual assets, such as decentralization, transaction pseudonymity and technical possibilities to conceal the origin of assets – through mixers, anonymous cryptocurrencies, DeFi protocols and NFT.

The role of analytical platforms in de-anonymizing suspicious transactions and the need for institutional training of investigators, prosecutors and analysts are emphasized. It is concluded that there is a need for a comprehensive transformation of approaches to financial monitoring, including legal updating, technical re-equipment and international coordination of efforts. Recommendations are offered to establish national crypto-transaction analysis centers, strengthen cooperation with global regulators, certify blockchain experts, and standardize the procedural treatment of digital evidence.

Keywords: cryptocurrency; blockchain; money laundering; cybercrime; criminal proceed; anonymous coin; crypto platform; decentralization; token; transaction.

DOI: 10.52425/25187252_2025_37_82

Введение. Виртуальные валюты, в особенности криптовалюты, функционирующие на основе технологии распределенного реестра (блокчейн), стали важным элементом глобальной финансовой системы. С момента появления биткойна в 2009 году данный класс цифровых активов претерпел эволюцию от маргинального эксперимента до признанного инвестиционного и транзакционного инструмента. Их технологические характеристики, такие как децентрализация, отсутствие посредников, быстрые трансграничные переводы и верификация операций по алгоритмическим протоколам, обеспечили высокую привлекательность криптовалют для широкого круга пользователей. Однако эти же свойства превратили криптовалюты в удобный инструмент легализации доходов, полученных преступным путем, что вызывает беспокойство не только национальных регуляторов, но и международного сообще-

ства.

Как подчеркивает Н.А. Егорова, именно правовая неустойчивость статуса криптовалют и отсутствие универсального правового режима «создают благоприятную среду для латентной финансовой преступности и трансграничного отмывания средств» [1, 47 стр.].

По оценкам Управления ООН по наркотикам и преступности (UNODC), ежегодно в мире отмывается порядка 2-5% глобального ВВП, что составляет до 2 трлн долларов США¹. Растущая доля этих средств перемещается посредством цифровых активов, что существенно усложняет традиционные механизмы выявления и отслеживания финансовых потоков. Организация экономического сотрудничества и развития (ОЭСР) указывает, что криптовалюты все чаще используются в схемах финансирования

¹ UNODC: Illicit money: how much is out there? [Электронный ресурс] – Режим доступа: <https://financialtransparency.org/unodc-illicit-money-how-much-is-out-there> (дата обращения: 28.08.2025).



терроризма, торговли людьми, наркотрафика и обхода санкционных режимов. Например, в отчетах World Economic Forum за 2023 год подчеркивается, что виртуальные валюты «перерастают в альтернативную параллельную финансовую систему, не подчиняющуюся традиционным регуляторным правилам»².

В условиях глобальных кризисов последних лет, таких как пандемия COVID-19, рост киберпреступности, обострение геополитической напряженности, наблюдается ускоренная цифровизация преступной деятельности. Криптовалюты становятся средством ухода от традиционного контроля: от использования в схемах вымогательства (ransomware) до вывода активов за пределы юрисдикции при корпоративных мошенничествах.

При этом значительное число сервисов, включая микшеры, DeFi-протоколы, NFT-маркетплейсы и платформы выпуска стейблкоинов, действуют вне зоны регулирования либо подчиняются лишь формальным требованиям AML/KYC.

Особое значение имеет рост использования частных криптовалют, таких как Monero и Zcash, где архитектура блокчейна намеренно исключает возможность отслеживания транзакций [2]. Данные монеты позволяют злоумышленникам выстраивать сложные схемы «расщепления» активов, исключая возможность их деконструкции даже с помощью современных аналитических платформ.

На этом фоне становится очевидной необходимость комплексного переосмысления правового и институционального подходов к проблеме отмывания доходов через виртуальные валюты. Наблюдается смещение парадигмы: от исключительно финансового регулирования к междисциплинарному взаимодействию, охватывающему уголовно-правовой, процессуальный, криминалистический и технический уровни.

Целью настоящего исследования является

комплексный научный анализ рисков, связанных с использованием виртуальных валют в противоправной деятельности, а также критическая оценка существующих механизмов регулирования с акцентом на национальный и международный опыт. В фокусе рассмотрения – не только правовые инструменты (FATF, MiCA, OFAC, FinCEN), но и практические кейсы, а также институциональные и кадровые дефициты, затрудняющие эффективное противодействие отмыванию доходов в цифровой среде. Особое внимание уделяется казахстанской правоприменительной практике, отражающей как достижения, так и системные уязвимости в данной сфере.

Материалы и методы. В настоящем исследовании применен комплексный междисциплинарный подход, сочетающий правовой, эмпирический, сравнительно-правовой и экспертно-аналитический методы. Такое сочетание обусловлено необходимостью многоплоскостного анализа феномена отмывания преступных доходов через виртуальные валюты, который охватывает как сферу цифровых технологий, так и финансового регулирования, уголовной юстиции, криминалистики и международного публичного права.

Правовой метод позволил последовательно проанализировать эволюцию нормативных основ, регулирующих обращение виртуальных активов и деятельность поставщиков соответствующих услуг. В поле рассмотрения попали обновленные рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (FATF) 2019-2023 гг., с акцентом на применимость «правила путешествия» (travel rule), а также Регламент ЕС MiCA (2023), который устанавливает универсальные стандарты лицензирования и KYC/AML-практик в рамках Евросоюза³.

Особое внимание уделено законодательным актам Республики Казахстан (далее – РК): Закону «О цифровых активах» (2023), нормам, регулирующим

² Pathways to the Regulation of Crypto-Assets: A Global Approach // Geneva: World Economic Forum, 2023. – 36 p. [Электронный ресурс] – Режим доступа: https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf (дата обращения: 22.08.2025).

³ Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. – Paris: FATF, 2023 [Электронный ресурс] – Режим доступа: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html> (дата обращения: 22.08.2025).



деятельность криптобирж на базе МФЦА, и подзаконным актам Агентства по регулированию и развитию финансового рынка⁴. Проведен также обзор практики административных и уголовных производств, включающих обращения цифровых активов, с учетом постановлений Верховного Суда РК.

Сравнительно-правовой подход дал возможность соотнести национальную правовую модель с аналогичными системами других юрисдикций: США, стран ЕС, Объединенных Арабских Эмиратов, России и Сингапура. Анализ показал существенные различия в уровне институциональной зрелости подходов к регулированию криптоиндустрии, при этом опыт Эстонии, Литвы и Южной Кореи признан перспективным для адаптации в казахстанском контексте. Отдельно выделено участие Казахстана в инициативе FATF-style regional bodies (FSRB) через ЕАГ (Евразийская группа по противодействию легализации преступных доходов).

Кейс-метод использован для анализа реальных уголовных и санкционных дел, ставших репрезентативными для понимания механизмов отмывания через виртуальные валюты. Среди них: дело Bitzlato (2023), дело Tornado Cash (2022), Bitcoin Fog (Sterlingov), коллапс FTX, а также кейсы, зарегистрированные в Казахстане в 2022-2024 гг., включая попытки вывода криптоактивов за рубеж и обход ограничительных мер.

Контент-анализ применен к материалам специализированных аналитических платформ: Chainalysis, TRM Labs, Elliptic, CipherTrace и RUSI. Изучались ежегодные отчеты по криминальной активности в блокчейне, обзоры эффективности FATF, пресс-релизы правительственных ведомств – OFAC, FinCEN, SEC, Europol, а также казахстанских агентств (АППФР, АФМ РК).

Экспертно-аналитический компонент реализован через анализ авторских выступлений, интервью и публикаций признанных специалистов, таких как Майкл Гронагер (Chainalysis), Кэтрин Уэстмор (RUSI), Джонатан Левин (TRM Labs), а также

казахстанских экспертов в сфере финансового мониторинга. Данные материалы использовались для формирования независимых оценок институциональной зрелости подходов противодействия отмыванию в криптосекторе.

Эмпирическая база охватывает период с 2018 по 2024 гг. и включает более 40 кейсов, отраженных в публичных и полупубличных источниках, в т.ч. данные из регуляторных отчетов, пресс-релизов правоохранительных органов, аналитических бюллетеней и судебных решений.

Таким образом, комплексное применение указанных методов позволило не только проанализировать действующие правовые механизмы, но и выявить системные уязвимости институционального, процессуального и экспертного характера, что создает основу для предложений по реформированию практик AML в условиях цифровой экономики.

Результаты, обсуждение. Отмывание доходов, полученных преступным путем с использованием виртуальных валют, является одной из наиболее острых проблем цифровой экономики. Особенность криптовалют как формы электронных активов заключается в их децентрализованном и, зачастую, анонимном характере. Это делает криптовалюты привлекательными как для легального использования, так и для сокрытия незаконных денежных потоков.

Преступные группировки адаптировали классические схемы легализации доходов под новые реалии блокчейн-технологий, применяя криптовалютные кошельки, DeFi-инструменты, приватные монеты и NFT как инструменты «расслоения» денежных потоков. По данным Chainalysis, в 2022 году объем криптовалют, полученных в результате противоправной деятельности, составил свыше 20 млрд долларов США. Эта сумма включает доходы от мошенничества, взломов, вымогательства, торговли наркотиками и оружием, а также средства, выведенные в обход санкций.

Ключевым фактором риска при

⁴ О цифровых активах в Республике Казахстан: закон Республики Казахстан от 6 февр. 2023 г. № 193-VII (с изм. и доп. от 07.01.2025 г.) [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=33689356 (дата обращения: 07.08.2025).



использовании криптовалют в отмывании денег является псевдонимность транзакций. Хотя блокчейн прозрачен и каждая операция фиксируется в публичной цифровой книге, адреса кошельков не содержат информации о личностях их владельцев. Это позволяет злоумышленникам создавать множество анонимных цепочек для расщепления средств и запутывания следов. Особенно эффективно такие схемы работают при использовании миксеров, например Tornado Cash, которые автоматически перераспределяют средства между множеством пользователей. В 2022 году Министерство финансов США ввело санкции против Tornado Cash, обвинив платформу в содействии отмыванию более 7 млрд долларов, включая 455 млн, связанных с северокорейской хакерской группировкой Lazarus Group.

Другим важным звеном схем отмывания стали приватные криптовалюты. В частности, монеты Monero и Zcash используют технологии конфиденциальности на уровне протокола, такие как zk-SNARK и ring signatures. Эти криптовалюты фактически исключают возможность отслеживания транзакций, что делает их предпочтительным средством «обеления» преступных доходов [2]. Платформы, предлагающие услуги по их обмену или конверсии в более ликвидные активы, зачастую работают вне регулируемого поля, особенно в оффшорных юрисдикциях.

В числе знаковых кейсов последних лет можно выделить дело Bitzlato – обменной платформы, зарегистрированной в Гонконге, которая, по информации FinCEN, обслуживала транзакции, связанные с даркнетом, ransomware и обходом санкций. По приблизительным подсчетам, через Bitzlato было отмыто более 700 млн долларов. В январе 2023 года платформа была заблокирована в рамках международной операции с участием Europol, FBI и Минюста США.

Еще один пример – процесс против российского гражданина Романа

Стерлингова, обвиненного в управлении сервисом микширования Bitcoin Fog. Прокуратура США утверждает, что через данный ресурс было отмыто более 335 млн долларов. Дело Стерлингова продемонстрировало, что при наличии надлежащих аналитических инструментов и трансграничного сотрудничества даже «глубоко анонимные» сервисы могут быть идентифицированы и заблокированы.

Среди инструментов, способствующих деанонимизации таких схем, стоит выделить аналитические платформы Chainalysis Reactor, TRM Labs и Elliptic Lens. Они позволяют отслеживать движение криптовалют по публичному блокчейну, строить графовые модели, выявлять кластеры адресов, связанных с киберпреступностью. Например, Chainalysis в своем отчете за 2023 год подчеркивает, что почти 68% криминальных транзакций были сконцентрированы на пяти крупных платформах, что делает их уязвимым звеном для правоприменительных мер⁵.

Нарастающим вызовом стали кроссчейн-технологии, включая агрегаторы ликвидности и мосты между блокчейнами. Использование протоколов THORChain, Anyswap и Rubic позволяет злоумышленникам мгновенно перемещать активы между экосистемами Ethereum, Bitcoin, Monero и другими, обходя известные точки мониторинга. Подобные операции фиксируются как основа для новых схем отмывания через мультичейн-инфраструктуру, требующую модернизации аналитических инструментов.

В международной нормативной плоскости важнейшее значение имеет деятельность FATF, которая еще в 2019 году внедрила так называемое правило путешествия (travel rule) в отношении поставщиков услуг виртуальных активов. Согласно этому правилу, обменные платформы и кошельки обязаны собирать и передавать информацию об отправителе и получателе криптовалютной транзакции, если ее сумма превышает установленный порог. Однако по данным на конец 2023 года, лишь около 30 стран в полном объеме имплементировали

⁵ Crypto Money Laundering: Four Exchange Deposit Addresses Received Over \$1 Billion in Illicit Funds in 2022. – Chainalysis [Электронный ресурс] – Режим доступа: <https://www.chainalysis.com/blog/crypto-money-laundering-2022> (дата обращения: 22.08.2025).



данную норму. Европейский союз утвердил регламент MiCA, вступающий в силу в 2024 году. Он предусматривает лицензирование всех поставщиков криптоуслуг, обязательную проверку клиентов (KYC), идентификацию эмитентов стейблкоинов, а также разработку единых стандартов отчетности. В США надзор за криптовалютами осуществляют сразу несколько ведомств: SEC, FinCEN, IRS, OFAC. Каждый из них осуществляет надзор в рамках своей юрисдикции: SEC регулирует выпуск токенов как ценных бумаг, FinCEN отслеживает схемы отмывания, OFAC применяет санкции, а IRS контролирует налогообложение⁶.

Реакция частного сектора на вызовы отмывания неоднозначна. Так, CEO JPMorgan Джейми Даймон в 2021 году охарактеризовал биткойн как «валюту преступников», отметив, что его основное применение – это обход санкций, шантаж и финансирование терроризма [3]. В то же время крупные институциональные игроки, такие как Fidelity, Mastercard и BlackRock, интегрируют криптовалютные активы в свою инфраструктуру, выдвигая требование к прозрачности, KYC и сотрудничеству с регуляторами.

В Казахстане с 2022 года реализуется правовой эксперимент в рамках МФЦА, где криптовалютные биржи работают на основании лицензий Агентства по регулированию и развитию финансового рынка. Принят Закон «О цифровых активах», в котором установлены нормы AML/KYC, определена ответственность поставщиков криптоуслуг и предусмотрена возможность блокировки операций, вызывающих подозрения в отмывании. Однако остаются вызовы, в т.ч. нехватка экспертов по блокчейн-экспертизе, ограниченные возможности аналитических служб, отсутствие подключений к международным системам мониторинга. Кроме того, судебная практика по криптовалютам в РК остается фрагментарной и требует систематизации.

Как справедливо отмечает Б.Ж. Кулибаев,

«уголовно-правовая политика Республики Казахстан в отношении виртуальных активов все еще находится в стадии становления, что обуславливает высокие риски правоприменительной неопределенности» [4, 83 стр.].

В последние годы также проявляются новые механизмы: легализация через NFT, игровые токены, приватные ICO и DAO-протоколы. Эти направления требуют оперативной доктринальной оценки и включения в состав правовой экспертизы. Как отмечает К. Уэстмор из RUSI, «технических инструментов недостаточно – их нужно сопровождать процессуально грамотной правоприменительной практикой, иначе собранные данные не будут приняты судом как доказательства» [5]. Примером успешной практики в странах ЕС служат решения, где блокчейн-аналитика признана допустимым доказательством благодаря сертификации экспертов и стандартизации методик⁷.

Таким образом, в результате анализа выявляется необходимость переосмысления подходов к противодействию отмыванию, с учетом не только нормативных пробелов, но и институционального уровня готовности правоохранительных и судебных структур. Требуется целостная трансформация системы мониторинга, включающая правовое обновление, техническое переоснащение, международную координацию и кадровую профессионализацию.

Заключение. Проведенное исследование подтвердило, что отмывание преступных доходов с использованием виртуальных валют представляет собой не просто разновидность финансовых преступлений, а системную угрозу, характеризующуюся высокой адаптивностью, трансграничностью и технологической устойчивостью. Криптовалютная среда порождает параллельную финансовую инфраструктуру, которая, оставаясь вне традиционного контроля, подрывает эффективность существующих механизмов противодействия легализации преступных доходов и

⁶ U.S. Securities and Exchange Commission. Framework for “Investment Contract” Analysis of Digital Assets [Электронный ресурс] – Режим доступа: <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets> (дата обращения: 22.08.2025).

⁷ Italy affirms legal effectiveness of DLTs and smart contracts [Электронный ресурс] – Режим доступа: <https://www.linklaters.com/de-lu/insights/blogs/fintechlinks/2019/fintech-italy-affirms-legal-effectiveness-of-distributed-ledger> (дата обращения: 22.08.2025).



финансированию терроризма.

Современные схемы отмывания средств с использованием DeFi-протоколов, кроссчейн-технологий, NFT и анонимных монет демонстрируют стремление преступных субъектов к постоянному усложнению конфигураций и уходу от прямой идентификации. При этом даже самые совершенные технические средства мониторинга становятся неэффективными без развитой нормативной базы, институциональной готовности правоохранительных органов и согласованных международных усилий. Это доказывают кейсы Tornado Cash, Bitzlato, Bitcoin Fog, а также эпизоды обналичивания через NFT и игровые токены.

Несмотря на наличие международных стандартов, включая рекомендации FATF, регламент MiCA и действия OFAC, их имплементация носит фрагментарный характер. Многие государства – особенно в развивающихся регионах – сталкиваются с дефицитом кадров, отсутствием процессуального признания блокчейн-экспертиз, недостаточной интеграцией в глобальные информационные базы и устаревшими уголовно-процессуальными рамками. В результате это формирует глобальную асимметрию правового реагирования на криптовалютные угрозы.

В казахстанском сегменте сделаны важные шаги: принятие Закона «О цифровых активах», запуск лицензирования криптобирж в МФЦА, формирование подходов к AML/KYC в сфере виртуальных активов. Однако эффективность этих мер ограничена отсутствием систематизированной судебной практики, методик оценки цифровых рисков, сертифицированной блокчейн-экспертизы и целостной криминалистической доктрины в отношении виртуальных активов.

Научная новизна исследования состоит в комплексном, междисциплинарном анализе схем и механизмов отмывания в криптовалютной среде с интеграцией

уголовно-правового, процессуального, технического и международно-правового компонентов. Впервые в рамках казахстанской академической дискуссии системно проанализированы примеры отмывания через NFT, DeFi и мультчейн-платформы, а также выявлены нормативные лакуны и институциональные риски, препятствующие правоприменению.

С практической точки зрения результаты статьи направлены на разработку рекомендаций по совершенствованию уголовного законодательства, внедрению блокчейн-аналитики в судебную практику и формированию кадрового потенциала в сфере криптокриминалистики.

По итогам исследования предлагается следующее:

- системное обновление уголовно-процессуальных норм, предусматривающее признание блокчейн-экспертизы как доказательства;
- создание института сертифицированных цифровых криминалистов и внедрение образовательных программ для следователей, прокуроров, судей и экспертов;
- учреждение национального центра анализа криптотранзакций с доступом к международным платформам и базам данных;
- обязательное внедрение KYC/AML-протоколов и travel rule на всех криптоплатформах, работающих в юрисдикции РК;
- развитие международного сотрудничества по обмену информацией о подозрительных криптоактивах, в т.ч. в рамках ЕАГ и FATF.

Таким образом, противодействие отмыванию доходов в криптоэкономике требует не просто нормативной адаптации, а глубокой институциональной перестройки, где технологии, право и компетенции должны действовать синхронно, подчиняясь единой архитектуре цифровой законности и глобальной ответственности.

Список использованной литературы:

1. Егорова, Н.А. Правовые основы противодействия легализации преступных доходов в цифровой экономике / Н.А. Егорова, А.В. Захаров. – М.: Проспект, 2020. – 232 с.



2. Зыгин, А.Ю. Проблемы анонимности в блокчейн-сетях: на примере Monero и Zcash / А.Ю. Зыгин, М.С. Головин // Информационная безопасность. – 2021. – № 3 (27). – С. 18-24.
3. J. Cox. Jamie Dimon lashes out on crypto: “If I was the government, I’d close it down” // CNBC. – 06.12.2023 [Электронный ресурс] – Режим доступа: <https://www.cnn.com/2023/12/06/jamie-dimon-lashes-out-on-crypto-if-i-was-the-government-id-close-it-down.html> (дата обращения: 22.08.2025).
4. Кулибаев, Б.Ж. Уголовно-правовая политика Республики Казахстан в отношении виртуальных активов: тенденции и проблемы правоприменения / Б.Ж. Кулибаев // Уголовное право и криминология. – 2024. – № 2 (18). – С. 83-92.
5. K. Westmore. Anti-Money Laundering Supervision of the Professions in the UK: Four Key Challenges and How to Address Them. – London: Royal United Services Institute, 2023. [Электронный ресурс] – Режим доступа: <https://www.rusi.org/explore-our-research/publications/policy-briefs/anti-money-laundering-supervision-professions-uk-four-key-challenges-and-how-address-them> (дата обращения: 23.08.2025).

References:

1. Egorova, N.A. Pravovye osnovy protivodejstviya legalizacii prestupnyh dohodov v cifrovoj jekonomike / N.A. Egorova, A.V. Zaharov. – M.: Prospekt, 2020. – 232 s.
2. Zygin, A.Ju. Problemy anonimnosti v blokchejn-setjah: na primere Monero i Zcash / A Ju. Zygin, M.S. Golovin // Informacionnaja bezopasnost'. – 2021. – № 3 (27). – S. 18-24.
3. J. Cox. Jamie Dimon lashes out on crypto: “If I was the government, I’d close it down” // CNBC. – 06.12.2023 [Jelektronnyj resurs] – Rezhim dostupa: <https://www.cnn.com/2023/12/06/jamie-dimon-lashes-out-on-crypto-if-i-was-the-government-id-close-it-down.html> (data obrashhenija: 22.08.2025).
4. Kulibaev, B.Zh. Uголовно-правовая политика Respubliki Kazahstan v otnoshenii virtual'nyh aktivov: tendencii i problemy pravoprimenenija / B.Zh. Kulibaev // Uголовное право i kriminologija. – 2024. – № 2 (18). – S. 83-92.
5. K. Westmore. Anti-Money Laundering Supervision of the Professions in the UK: Four Key Challenges and How to Address Them. – London: Royal United Services Institute, 2023. [Jelektronnyj resurs] – Rezhim dostupa: <https://www.rusi.org/explore-our-research/publications/policy-briefs/anti-money-laundering-supervision-professions-uk-four-key-challenges-and-how-address-them> (data obrashhenija: 23.08.2025).

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Дариға Болатқызы Қайназарова – Қазақстан Республикасы Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының Кәсіптік оқыту институтының қылмыстық қудалау және жедел-ізвестіру қызметі кафедрасының доценті, заң ғылымдарының кандидаты, e-mail: dariga.76@list.ru.

Қайназарова Дариға Болатовна – доцент кафедрасы уголовного преследования и оперативно-розыскной деятельности Института профессионального обучения Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, кандидат юридических наук, e-mail: dariga.76@list.ru.

Kainazarova Dariga Bolatovna – Associate Professor of the Department of Criminal Prosecution and Operational Investigative Activities of the Institute of Professional Training of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Candidate of Law, e-mail: dariga.76@list.ru.