Научная статья
УДК: 343.985.2

ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ КРИПТОВАЛЮТ В ПРЕСТУПНЫХ ЦЕЛЯХ

Алла Николаевна Колычева[1], Виталий Федорович Васюков[2]
[1]Орловский юридический институт МВД России имени В. В. Лукьянова, г. Орел, Росийская Федерация, allakolycheva87@gmail.com
[2]Московская академия Следственного комитета Российской Федерации имени А. Я. Сухарева, г. Москва, Росийская Федерация, vvf0109@yandex.ru

Аннотация. В статье рассматриваются вопросы противодействия использованию криптовалют в преступных целях. Авторы анализируют отличие криптовалют от традиционных электронных денег, акцентируя внимание на децентрализованном характере блокчейна и отсутствии централизованного управления транзакциями. В работе рассматриваются различные методы, используемые для повышения анонимности транзакций с использованием криптовалют и затруднения их отслеживания, включая смену криптографических ключей, использование «миксеров» и применение альткоинов с улучшенными функциями конфиденциальности. Пристальное внимание авторы обращают на риски, связанные с использованием криптовалют в киберпреступности, подчеркивая, что анонимность, предоставляемая такими криптовалютами, как Monero и ZCash, а также сервисами криптосмешивания, облегчает совершение и сокрытие преступлений.

Ключевые слова: криптовалюта, блокчейн, противодействие преступности, правоохранительные органы

Для цитирования: Колычева А. Н., Васюков В. Ф. Отдельные аспекты противодействия использованию криптовалют в преступных целях // Криминалистика: вчера, сегодня, завтра. 2025. Т. 33. № 1. С. 89–101.

SOME ASPECTS OF COUNTERING THE USE OF CRYPTOCURRENCIES FOR CRIMINAL PURPOSES

Alla N. Kolycheva[1], Vitaly F. Vasyukov[2]
[1]Oryol Law Institute of the MIA of Russia named after V.V. Lukyanov, Oryol, Russian Federation, allakolycheva87@gmail.com
[2]Moscow Academy of the Investigative Committee of the Russian Federation named after A.Ya. Sukharev, Moscow, Russian Federation, vvf0109@yandex.ru

Abstract. The article considers the issues of countering the use of cryptocurrencies for criminal purposes. The authors analyze the difference between cryptocurrencies and traditional electronic money, focusing on the decentralized nature of the blockchain and the lack of centralized transaction management. The paper considers various methods used to increase the anonymity of transactions using cryptocurrencies and complicate their tracking, including changing cryptographic keys, using "mixers" and applying altcoins with improved privacy features. Close attention is paid to the risks associated with the use of cryptocurrencies in cybercrime, emphasizing that the anonymity provided by cryptocurrencies such as Monero and ZCash, as well as crypto-mixing services, makes it easier to commit and conceal crimes.

Keywords: cryptocurrency, blockchain, combating crime, law enforcement

For citation: Kolycheva A. N., Vasyukov V. F. Otdel'nye aspekty protivodejstviya ispol'zovaniyu kriptovalyut v prestupnyh celyah [Certain aspects of combating the use of cryptocurrencies for criminal purposes]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025, vol. 33 no. 1, pp. 89–101 (in Russ.).

Введение

Эскалация ажиотажа вокруг криптовалют инициировала многочисленные дискуссии об их взаимосвязи с преступным миром. Небезосновательно высказываются опасения, что этот платежный инструмент может эксплуатироваться преступниками и террористами для перемещения, сокрытия и «отмывания» доходов от незаконной деятельности в условиях недостаточного контроля со стороны компетентных органов. Уникальное сочетание характеристик, присущих криптовалютам, делает их привлекательными для злоумышленников.

Суть проблемы заключается в том, что криптовалюты, опираясь на алгоритмическую основу своего функционирования, аккумулируют преимущества как электронных, так и наличных денежных средств. Подобно банкноте, монеты (коины) криптовалюты обеспечивают анонимность, не требуя раскрытия информации об идентичности сторон и причинах совершения платежа. Но, в отличие от наличных денег, криптовалюты, будучи представленными в цифровом формате, обладают свойствами делимости и многократного увеличения, что открывает возможность осуществления переводов в любом объеме – от микроплатежей, исчисляемых копейками, до расчетов в рамках масштабных международных торговых операций. Именно этот контраст между анонимностью и возможностью осуществления крупных переводов, как отмечают В. А. Кутырин и А. Г. Волеводз, делает криптовалюты столь привлекательными для преступных схем [1, с. 140].

В традиционной денежной системе электронные деньги представляют собой покупательную способность, зарегистрированную на текущем счете, открытом в банке. При осуществлении покупки или банковского перевода в пользу бенефициара физического перемещения денежных средств не происходит, вместо этого баланс покупателя уменьшается, а баланс продавца увеличивается на соответствующую сумму, что отража-

ется простой бухгалтерской записью. Однако «реализация данной схемы предполагает обязательное участие банка, который выполняет ряд функций: проверяет наличие средств на счете покупателя, исполняет платежное поручение, дебетует счет покупателя и зачисляет средства на счет продавца» [2, с. 41].

Таким образом, для функционирования традиционных электронных денег необходимо «централизованное» ведение счетов, требующее участия третьей стороны – банка. Именно банк, располагая информацией, хранящейся на его централизованных и защищенных серверах, осуществляет проверку и подтверждение личности заказчика, наличия средств и правильности кодов безопасности, исполняет операцию и фиксирует ее в бухгалтерском учете.

Основная часть

Принципиальным новшеством, который был предложен разработчиками Биткойна (и других функционирующих конвертируемых криптовалют), является отказ от централизованного управления транзакциями. Система спроектирована таким образом, чтобы ведение счетов распределялось между всеми участниками сети, а не возлагалось на единого оператора. «Бухгалтерская книга», фиксирующая все операции, более не является исключительной прерогативой отдельного банка или банковской системы, а хранится каждым пользователем на персональном устройстве. Реестр, таким образом, не только децентрализован, но и распределен в сети, где ни один «узел» не выполняет центральную роль. Этот распределенный реестр («distributed ledger») получил название «блокчейн» [3, с. 36].

Согласно определению, получившему широкое распространение в научной литературе, блокчейн представляет собой последовательную цепочку блоков (отсюда и название), в каждом из которых регистрируются идентификационные данные плательщика и получателя, а также сумма перевода. Каждый блок содержит информацию обо всех транзакциях, осуществленных в течение примерно десяти минут, и ссылку на предыдущий блок. Следовательно, блокчейн, представляющий собой последовательную цепь блоков, предоставляет в любой момент времени полную и актуальную картину всех транзакций, выполненных с момента запуска системы.

Криптовалюты, такие как Биткойн (Bitcoin), кардинально отличаются от традиционных финансовых систем, упраздняя централизованное управление транзакциями. Вместо концентрации полномочий по проверке и подтверждению операций в едином центре ответственность распределена между всеми участниками сети. Подтверждение транзакций обеспечивается сложным криптографическим механизмом. Когда пользователь инициирует перевод, он предоставляет системе информацию о счете, а также сумме операции. В отсутствие доверенного посредника, которому можно было бы сообщить ключи доступа к счету, система требует, чтобы пользователь передал эти ключи в зашифрованном виде остальным участникам сети [4, с. 22].

В свою очередь майнеры, играющие ключевую роль в обеспечении безопасности сети, для авторизации транзакции должны расшифровать ключ, решив сложную математическую задачу. В качестве стимула первый майнер, успешно расшифровавший код и подтвердивший транзакцию, получает вознаграждение в виде криптовалюты. Подтвержденная

транзакция добавляется в блок, который в свою очередь включается в блокчейн – непрерывную цепочку блоков, содержащую информацию обо всех транзакциях. Этот децентрализованный подход обеспечивает большую прозрачность и безопасность, но также создает новые вызовы для регулирования и правоохранительной деятельности.

В инфраструктуре криптовалют особую роль играют виртуальные кошельки, представляющие собой специализированные программные решения и приложения, предназначенные для обеспечения хранения, аккумулирования и транзакций с использованием как Bitcoin, так и других видов цифровых активов. Функциональность данных сервисов не ограничивается хранением приватных ключей и упрощением взаимодействия пользователей с криптовалютными биржами и онлайн-продавцами; при необходимости поставщики виртуальных кошельков осуществляют взаимодействие с другими участниками рынка, формируя тем самым сложную и взаимосвязанную экосистему цифровых активов [5, с. 150].

Стоит подчеркнуть, что инфраструктура криптовалют включает в себя экосистему независимых разработчиков программного обеспечения и приложений, которые, предлагая широкий спектр сопутствующих услуг, таких как инструменты анализа блокчейна и специализированные решения по обеспечению безопасности, расширяют функциональные возможности системы, действуя как в сотрудничестве с обменниками и поставщиками кошельков, так и автономно.

Довольно значимым аспектом, определяющим потенциальные преступные риски использования виртуальных валют, является их анонимность, или точнее – псевдоанонимность. Блокчейн, согласно замыслу его создателей, является публичным и прозрачным реестром. Любой участник сети может в любой момент времени увидеть информацию обо всех транзакциях: суммы переводов, а также идентификаторы отправителей и получателей. Однако несмотря на это, отследить операции до конкретной личности практически невозможно. Каждая операция идентифицируется с помощью открытого и закрытого ключей. При этом блокчейн фиксирует открытый ключ отправителя и сумму транзакции, в то время как приватный ключ, подобный паролю, остается в распоряжении владельца электронного кошелька. Таким образом, в публичном реестре отображается не реальное имя участника транзакции, а лишь идентификационный номер, соответствующий его открытому ключу [6, с. 241].

В связи с этим в отношении системы блокчейн часто используется термин «псевдоанонимность». Это означает, что, несмотря на открытость реестра транзакций, участники операций идентифицируются не по имени и фамилии, а по номерам, соответствующим их открытым ключам доступа к системе.

Несмотря на вышесказанное, некоторые авторы считают, что такая структура не обеспечивает полной анонимности. Хотя личность пользователя и скрыта, публичность блокчейна позволяет получить исчерпывающую информацию обо всех операциях, связанных с конкретной учетной записью, включая суммы и адреса получателей. В случае выявления подозрительных операций (например, множественных переводов одному контрагенту за короткий

период или единичной транзакции на крупную сумму), компетентные органы могут попытаться установить реального владельца электронного кошелька, используя специализированное программное обеспечение [7, с. 310].

Сказанное позволяет резюмировать, что в криптовалютной инфраструктуре существует сложный баланс между стремлением к приватности и необходимостью обеспечения прозрачности для предотвращения преступной деятельности. Между тем одной из ключевых особенностей биткоина является возможность генерации практически неограниченного числа открытых и соответствующих им закрытых ключей. В силу этого пользователи могут использовать различные идентификаторы для каждой транзакции, что значительно затрудняет выявление закономерностей и подозрительных операций. Как следствие, частая смена криптографических ключей представляет собой серьезное препятствие для обнаружения признаков незаконной деятельности и последующей идентификации пользователей.

Помимо этого отрасль активно разрабатывает сложные программные решения, направленные на повышение конфиденциальности и обход публичной природы блокчейна, что, по мнению ряда международных организаций, специализирующихся на борьбе с отмыванием денег, представляет собой потенциальную угрозу. Данные инструменты становятся все более востребованными среди пользователей, стремящихся сохранить анонимность [8, с. 22].

Одним из наиболее распространенных методов сокрытия транзакций является использование так называемых «миксеров» (от англ. – «mixing»). Подобные сервисы позволяют пользователям буквально запутать историю переводов путем объединения множества платежей в «единый котел» и последующего перемешивания источников и адресатов. Используя услуги по смешиванию, злоумышленник надеется на «анонимное сотрудничество» с другими участниками. Его средства перемешиваются с транзакциями совершенно незнакомых людей, и он не имеет никакого представления о том, кто отправляет средства в обратном направлении. Эта анонимная «игра в прятки» с деньгами делает отслеживание традиционными следственными методами невозможным [9, с. 97].

Вместе с тем следует учитывать, что рынок конвертируемых криптовалют не ограничивается Биткойном. Как известно, он включает в себя множество альтернативных криптовалют, таких как «альткоины», характеризующихся различной степенью распространенности. Несмотря на то, что альткоины, как правило, следуют концептуальной модели, предложенной Биткойном, в ряде случаев они используют алгоритмические решения, направленные на значительное повышение уровня конфиденциальности транзакций[1].

В качестве примера можно привести валюту Monero, выпущенную на рынок в 2014 году. Протокол ее работы предусматривает автоматическую генерацию новых пар ключей для каждой транзакции, а информация о транзакции, включая ее сумму, становится доступной только получателю или третьему лицу, которому отправитель предоставил специаль-

[1] Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets, 2021 // URL: https://biblioteca.gafilat.org/?p=647 (дата обращения: 21.01.2025).

ный «ключ просмотра». В системе Monero реализована функция автоматического смешивания транзакций, доступная всем пользователям, что существенно затрудняет их отслеживание и восстановление деталей. Другая криптовалюта – ZCash, размещенная на криптобиржах в 2016 году, также обладает схожими характеристиками, предоставляя пользователям возможность выбора уровня прозрачности транзакций. Вполне закономерно, что присущая криптовалютам анонимность (или псевдоанонимность) в сочетании с распространением сервисов криптосмешивания и возможностью осуществления быстрых и необратимых трансграничных транзакций вызывает обоснованные опасения в контексте предотвращения и пресечения преступной деятельности [10, с. 69].

Так, одну из наиболее серьезных и непосредственных угроз представляет использование криптовалют киберпреступниками, то есть лицами, совершающими преступления с применением информационных систем. Указанные субъекты, как правило, действуют в организованных группах, характеризующихся четким разделением ролей, где выделяются, например, программисты, разрабатывающие вредоносное программное обеспечение, дистрибьюторы, распространяющие или продающие незаконно полученные данные или товары, а также так называемые «денежные мулы», занимающиеся получением и отмыванием доходов, полученных преступным путем.

Опыт последних лет свидетельствует о том, что деятельность данных групп осуществляется в двух основных направлениях: атаки на компьютеры частных лиц или организаций (государственных или частных) с целью распространения вирусов, кражи или изменения конфиденциальных данных, либо использование информационных систем для совершения общеуголовных преступлений, таких как мошенничество, нелегальные азартные игры, купля-продажа незаконных товаров или услуг[2].

Таким образом, внедрение криптовалют объективно способствовало укреплению существующих схем киберпреступности, повышая их эффективность за счет анонимности транзакций. Подтверждением этому служит в частности информация, представленная в отчете Управления ООН по наркотикам и преступности об угрозах, связанных с транснациональной организованной преступностью, и слиянии кибермошенничества, подпольных банковских операций и технологических инноваций в Юго-Восточной Азии (октябрь, 2024 год), где подчеркивается, что криптовалюты все чаще используются киберпреступниками, а отдельные их виды являются ключевыми инструментами при совершении операций на нелегальных рынках и получении выплат в результате сотен тысяч преступлений различных категорий[3].

Особую обеспокоенность у научного сообщества вызывает участившееся использование криптовалют в так называемых атаках программ-вымогателей. Данный вид киберпре-

[2] FATF Guidance for a risk based approach, Virtual Assets and Virtual Assets Service Providers, June 2019 // URL: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf (дата обращения: 21.01.2025).

[3] Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape // URL: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (дата обращения: 21.01.2025).

ступлений заключается в распространении вредоносного программного обеспечения, шифрующего данные на пораженных системах и требующего выплату выкупа за их дешифровку.

Широко известным примером является масштабная атака WannaCry, произошедшая в мае 2017 года и затронувшая компьютеры под управлением операционной системы Microsoft Windows. Вредоносный вирус, распространяемый злоумышленниками, шифровал файлы на зараженных устройствах и требовал выплаты выкупа в Биткойнах для восстановления доступа к информации. Как следствие, 12 мая 2017 года произошло масштабное заражение информационных систем многих организаций по всему миру. В частности, пострадали такие крупные иностранные компании, как Portugal Telecom, Deutsche Bahn, FedEx, Telefónica, Tuenti, Renault и другие. К 28 мая того же года, по имеющимся данным, более двухсот тридцати тысяч компьютеров в 150 странах стали жертвами вредоносной программы WannaCry, что позволило квалифицировать данную атаку как один из самых масштабных инцидентов в истории киберпреступности.

В этой связи представляется логичным вывод о том, что распространение виртуальных валют, затрудняющих идентификацию бенефициаров кибервымогательств, создает благоприятную среду для совершения подобного рода преступлений. Доказательством тому служит рост числа атак с использованием программ-вымогателей в 2024 году более чем на 50 % по сравнению с предыдущим годом, а также увеличение общей суммы выплат, произведенных пострадавшими компаниями [11, с. 670].

Вместе с тем, помимо кибервымогательств, криптовалюты, в частности Bitcoin, Monero и ZCash, все чаще используются при осуществлении атак типа DDoS (аббр. от англ. “denial-of-service attack” – «отказ в обслуживании»), направленных на преднамеренный вывод из строя информационных систем, предоставляющих услуги клиентам, путем исчерпания их ресурсов.

Наряду с этим следует учитывать, что жертвами киберпреступников нередко становятся и сами держатели виртуальных валют. Злоумышленники осуществляют целенаправленные атаки на криптовалютные биржи и поставщиков кошельков с целью получения несанкционированного доступа к приватным ключам и последующего хищения средств. Подтверждением тому является инцидент с гонконгской биржей Bitfinex, где в августе 2016 года было похищено криптовалюты на общую сумму 72 миллиона долларов США. Еще более масштабным стало хищение 744 408 биткойнов, эквивалентных 350 миллионам долларов США, у биржи Mt-Gox, в свое время являвшейся одной из крупнейших в мире [12, с. 7–8].

Не менее показательным является случай атаки на краудфандинговый проект «The Dao», в результате которой хакеры похитили более 152 миллионов долларов США во время первичного размещения монет (ICO), представляющего собой первую публичную продажу новой виртуальной валюты.

Следует отметить, что криптовалюты не только используются в преступных схемах, но и создают новые риски для потребителей, приобретающих товары и услуги за криптоактивы. Ключевой особенностью транзакций является их необратимость,

что в сочетании с анонимностью, присущей криптовалютам, создает благоприятную среду для мошеннических действий. Так, в случае неполучения оплаченного товара или получения контрафактной продукции отмена платежа становится невозможной, а идентификация недобросовестного продавца – крайне затруднительной.

Помимо этого существуют риски, связанные с мошенничеством в отношении лиц, вкладывающих в криптовалюты инвестиции. Есть много примеров финансовых операторов, использующих так называемую «схему Понци», заманивая потенциальных инвесторов в специализированных блогах обещаниями высоких доходов, которые поступают не от реальной торговой деятельности, а от новых ничего не подозревающих инвесторов. Более того, нередки случаи внезапного исчезновения криптовалютных бирж, владельцы которых присваивают себе все депозиты, принадлежащие их клиентам [13, с. 131].

В дополнение к обозначенным криминогенным аспектам следует отметить, что криптовалюты, конвертируемые в фиатные валюты, представляют повышенную опасность с точки зрения легализации преступных доходов и финансирования международного терроризма. Ключевым фактором, обусловливающим эти риски, является возможность абсолютно анонимного финансирования преступной деятельности.

Значительное число пользователей криптовалют реализуют их, размещая объявления в Интернете, блогах или на специализированных платформах, минуя посредничество бирж и других организаций, потенциально подлежащих контролю со стороны регулирующих органов. Оплата в таких случаях может осуществляться различными способами, включая пополнение предоплаченных и дебетовых карт [14, с. 33].

Непосредственный характер криптовалютных транзакций создает условия для ее покупки за наличные средства при личной встрече. Потенциальному покупателю достаточно создать цифровой кошелек, связаться с продавцом, встретиться с ним в общественном месте, передать наличные средства и дождаться осуществления перевода с использованием, например, специального приложения, установленного на мобильном телефоне.

В связи с этим становится очевидным, что лицо, обладающее значительными средствами, полученными незаконным путем (например, уклонения от уплаты налогов), может без особого труда связаться с частным лицом, желающим продать свои токены, и анонимно приобрести их на «открытом рынке», не оставляя никаких следов этой сделки [15, с. 53].

Таким образом, владелец электронного кошелька, пополненного доходами, полученными преступным путем, получает возможность конфиденциально распоряжаться этими средствами, приобретая товары и услуги, не раскрывая своей личности. Как уже отмечалось, система виртуальных валют приобрела глобальный масштаб, что позволяет беспрепятственно осуществлять транснациональные переводы криптовалют, переправляя значительные капиталы в страны со слаборазвитым или отсутствующим законодательством в сфере противодействия легализации преступной деятельности.

Отсутствие централизованного управления в криптовалютной сфере лишает уполномоченные органы надежного контрагента для взаимодействия, что значительно усложняет

их деятельность. Важно подчеркнуть, что характерные особенности системы приводят к тому, что транзакции с виртуальными валютами затрагивают организации, расположенные в различных юрисдикциях. Это, с одной стороны, затрудняет определение территориальной юрисдикции компетентных органов по борьбе с отмыванием денег, а с другой – исключает возможность установления лиц, которым можно адресовать, например, запросы о предоставлении информации о бенефициарном владельце криптовалютного кошелька при расследовании уголовного дела. Все вышеизложенное свидетельствует о необходимости разработки новых подходов к противодействию использованию криптовалют в преступных целях.

Выводы и заключение

Подводя итог нашему исследованию, следует отметить, что трансграничный характер инфраструктуры криптовалют обуславливает потребность в международной координации усилий правоохранительных органов, поскольку фрагментация нормативно-правового регулирования и различия в подходах к идентификации пользователей создают благоприятную среду для перемещения активов, полученных преступным путем, между юрисдикциями, что затрудняет выявление и пресечение финансовых преступлений.

Развитие интернет-технологий является неотъемлемым элементом прогрессивного общества, и попытки его сдерживания вряд ли приведут к снижению связанных с ним рисков. Основная сложность заключается в недостаточной изученности и комплексном характере феномена криптопреступности. Тем не менее проблема использования криптовалют для совершения противоправных деяний требует оперативного внедрения эффективных регуляторных механизмов и их дальнейшей оптимизации, особенно в сфере административного контроля, во избежание формирования нерегулируемой среды, благоприятствующей активизации цифровых преступлений, связанных с криптовалютами.

При надлежащем правовом регулировании и эффективном контроле технология блокчейн, лежащая в основе криптовалют, может быть трансформирована в инструмент для выявления и пресечения различных видов финансовой преступности, включая уклонение от уплаты налогов и легализацию доходов, полученных преступным путем.

СПИСОК ИСТОЧНИКОВ

1. *Кутырин В. А., Волеводз А. Г.* Место электронных денег в системе денежных инструментов: некоторые данные к оценке рисков оборота криптовалюты и изучению проблем ее правовой регламентации // Библиотека криминалиста. Научный журнал. 2016. № 3 (26). С. 138–147.

2. *Волеводз А. Г.* Противодействие легализации (отмыванию) доходов от преступлений, совершенных с использованием криптовалюты: правовые основы международного сотрудничества в сфере уголовного судопроизводства // Использование криптовалют в противоправных целях и методика противодействия : мат-лы Междунар. науч.-практ. «круглого

стола» / Москва, 25 апреля 2019 года, Московская академия Следственного комитета Российской Федерации. М., 2019. С. 38–45.

3. *Шушкевич Ю. А.* Возможности использования криптовалют в интересах стабилизации и развития финансовых рынков и национальных денежных систем // Вестник современных цифровых технологий. 2019. № 1. С. 35–45.

4. *Осипов Н. Р., Кротова Е. Л.* Блокчейн – платформа для инноваций // Вестник УрФО. Безопасность в информационной сфере. 2017. № 4 (26). С. 21–24.

5. *Ермакова А. Л., Чаплыгина В. Н.* Фишинг как распространенное киберпреступление современности // Закон и право. 2022. № 2. С. 149–151.

6. *Морозова Н. В.* Некоторые особенности расследования компьютерных преступлений // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования : сб. матлов междунар. науч.-практ. конф., посв. 100-летию принятия УПК РСФСР 1922 г., 20-летию действия УПК РФ. В 2-х частях. Орел, 2022. С. 240–245.

7. *Каширгов А. Х., Семенов Е. А.* Некоторые вопросы противодействия преступлениям, совершенным с использованием IT-технологий // Евразийский юридический журнал. 2021. № 9 (160). С. 309–310.

8. *Волеводз А. Г., Цыплакова А. Д.* Цифровые доказательства в уголовном процессе государств – членов совета сотрудничества арабских государств персидского залива: правовой статус и процедуры признания // Вестник экономической безопасности. 2024. № 2. С. 21–29.

9. *Liu M., Dong B.* Analysis of Cryptocurrencies Mixing Services and Its Regulatory Mechanism // International Conference on Blockchain and Trustworthy Systems. Singapore : Springer Nature Singapore, 2024. P. 95–110.

10. *Васюков В. Ф., Старжинская А. Н.* Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют // Российское право: образование, практика, наука. 2024. № 4. С. 68–78.

11. *Gajjar V. R., Taherdoost H.* Cybercrime on a global scale: trends, policies, and cybersecurity strategies // 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI). IEEE, 2024. Pp. 668–676.

12. *Liang R. et al.* Ponziguard: Detecting ponzi schemes on ethereum with contract runtime behavior graph (crbg) // Proceedings of the 46th IEEE/ACM International Conference on Software Engineering. 2024. Pp. 1–12.

13. *Wu B., Wu B.* Bitcoin: the future of money //Blockchain for Teens: With Case Studies and Examples of Blockchain Across Various Industries. Berkeley, CA : Apress, 2022. Pp. 77–134.

14. *Dumas J. G., Jimenez-Garces S., Şoiman F.* Risk analyses of the crypto-market: A literature review //12th International Conference on Complexity, Informatics and Cybernetics (IMCIC 2021). 2021. Т. 1. С. 30–37.

15. *Цыплакова А. Д.* Риски отмывания (легализации) активов, полученных преступным путем, и финансирования терроризма в сфере гейминга // Актуальные вопросы обеспечения национальной безопасности : мат-лы II Междунар. науч.-практ. конф., Санкт-Петербург, 07 декабря 2023 года. Санкт-Петербург, 2024. С. 50–55.

REFERENCER

1. *Kutyrin V. A., Volevodz A. G.* Mesto elektronnyh deneg v sisteme denezhnyh instrumentov: nekotorye dannye k ocenke riskov oborota kriptovalyuty i izucheniyu problem ee pravovoj reglamentacii [The place of electronic money in the system of monetary instruments: some data on assessing the risks of cryptocurrency turnover and studying the problems of its legal regulation]. Biblioteka kriminalista. Nauchnyj zhurnal. – Library of a criminalist. Scientific journal. 2016, no. 3(26), pp. 138–147. (in Russian).

2. *Volevodz A. G.* [Counteracting the legalization (laundering) of proceeds from crimes committed using cryptocurrency: legal basis for international cooperation in criminal proceedings]. Ispol'zovanie kriptovalyut v protivopravnyh celyah i metodika protivodejstviya. Materialy Mezhdunarodnogo nauchno-prakticheskogo «kruglogo stola» [Use of cryptocurrencies for illegal purposes and methods of counteraction. Materials of the International scientific and practical round table (Moskow, 5 aprelya 2019 goda)]. Moscow Academy of the Investigative Committee of the Russian Federation. M., 2019, pp. 38-45. (in Russian).

3. *Shushkevich Yu. A.* Vozmozhnosti ispol'zovaniya kriptovalyut v interesah stabilizacii i razvitiya finansovyh rynkov i nacional'nyh denezhnyh sistem [Possibilities of using cryptocurrencies in the interests of stabilization and development of financial markets and national monetary systems]. Vestnik sovremennyh cifrovyh tekhnologij – Vestnik of modern digital technologies. 2019, no. 1, pp. 35–45. (in Russian).

4. *Osipov N. R., Krotova E. L.* Blokchejn - platforma dlya innovacij [Blockchain - a platform for innovations]. Vestnik UrFO. Bezopasnost' v informacionnoj sfere – Vestnik of the Ural Federal District. Security in the information sphere. 2017, no. 4 (26), pp. 21-24. (in Russian).

5. *Ermakova A. L., Chaplygina V. N.* Fishing kak rasprostranennoe kiberprestuplenie sovremennosti [Phishing as a widespread cybercrime of our time]. Zakon i pravo – Law and Order. 2022, no. 2, pp. 149–151. (in Russian).

6. *Morozova N. V.* [Some features of the investigation of computer crime]. Sovremennoe ugolovno-processual'noe pravo — uroki istorii i problemy dal'nejshego reformirovaniya. Sbornik materialov mezhdunarodnoj nauchno-prakticheskoj konferencii, posvyashchennoj 100-letiyu prinyatiya UPK RSFSR 1922 g., 20-letiyu dejstviya UPK RF. V 2-h chastyah. [Modern criminal procedural law - lessons of history and problems of further reform. Collection of materials of the international scientific and practical conference dedicated to the 100th anniversary of the adoption of the Criminal Procedure Code of the RSFSR in 1922,

the 20th anniversary of the Criminal Procedure Code of the Russian Federation]. Orel, 2022, pp. 240–245. (in Russian).

7. *Kashirgov A. H., Semenov E. A.* Nekotorye voprosy protivodejstviya prestupleniyam, sovershennym s ispol'zovaniem IT-tekhnologij [Some issues of counteracting crimes committed using IT technologies]. Evrazijskij yuridicheskij zhurnal. – Eurasian Law Journal. 2021, no. 9 (160), pp. 309–310. (in Russian).

8. *Volevodz A. G., Cyplakova A. D.* Cifrovye dokazatel'stva v ugolovnom processe gosudarstv - chlenov soveta sotrudnichestva arabskih gosudarstv persidskogo zaliva: pravovoj status i procedury priznaniya [Digital evidence in criminal proceedings of the member states of the Cooperation Council for the Arab States of the Gulf: legal status and recognition procedures]. Vestnik ekonomicheskoj bezopasnosti – Economic Security vestnik. 2024, no 2, pp. 21–29. (in Russian).

9. *Liu M., Dong B.* Analysis of Cryptocurrencies Mixing Services and Its Regulatory Mechanism. International Conference on Blockchain and Trustworthy Systems. – Singapore : Springer Nature Singapore, 2024, pp. 95–110.

10. *Vasyukov V. F., Starzhinskaya A. N.* Ob operativno-rozysknyh i sledstvennyh merah protivodejstviya legalizacii prestupnyh dohodov s ispol'zovaniem kriptovalyut [On operational-search and investigative measures to combat the legalization of criminal proceeds using cryptocurrencies]. Rossijskoe pravo: obrazovanie, praktika, nauka – Russian law: education, practice, science. 2024, no. 4, pp. 68–78. (in Russian).

11. *Gajjar V. R., Taherdoost H.* Cybercrime on a global scale: trends, policies, and cybersecurity strategies. 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI). IEEE, 2024, pp. 668–676.

12. *Liang R. et al.* Ponziguard: Detecting ponzi schemes on ethereum with contract runtime behavior graph (crbg). Proceedings of the 46th IEEE/ACM International Conference on Software Engineering. 2024, pp. 1–12.

13. *Wu B., Wu B.* Bitcoin: the future of money //Blockchain for Teens: With Case Studies and Examples of Blockchain Across Various Industries. Berkeley, CA : Apress, 2022, pp. 77–134.

14. *Dumas J. G., Jimenez-Garces S., Şoiman F.* Risk analyses of the crypto-market: A literature review.12th International Conference on Complexity, Informatics and Cybernetics (IMCIC 2021). 2021, vol. 1, pp. 30–37.

15. *Cyplakova A. D*. [Risks of laundering (legalization) of assets obtained by criminal means and financing of terrorism in the field of gaming]. Aktual'nye voprosy obespecheniya nacional'noj bezopasnosti : materialy II Mezhdunarodnoj nauchno-prakticheskoj konferencii [Actual issues of ensuring national security: materials of the II International scientific and practical conference]. Sankt-Peterburg, 2024, pp. 50-55. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Колычева Алла Николаевна, кандидат юридических наук, старший преподаватель кафедры криминалистики и предварительного расследования в ОВД. Орловский юридический институт МВД России имени В. В. Лукьянова. 302027, Российская Федерация, г. Орел, ул. Игнатова, 2.

Васюков Виталий Федорович, доктор юридических наук, профессор, главный научный сотрудник научно-исследовательского отдела Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева. 125080, Российская Федерация, г. Москва, ул. Врубеля, 12.

INFORMATION ABOUT THE AUTHORS

Alla N. Kolycheva, Candidate Law, Senior Lecturer of the Department of Criminalistics and Preliminary Investigation in the Department of Internal Affairs.e Oryol Law Institute of the MIA of Russia named after V.V. Lukyanov. 2, Ignatov St., Oryol, Russian Federation, 302027.

Vitaly F. Vasyukov, Doctor of Law, Professor, Chief Researcher of the Research Department. Moscow Academy of the Investigative Committee of the Russian Federation named after A.Ya. Sukharev. 12, Vrubel St., Moscow, Russian Federation, 125080.