УДК: 336.71.078.3
DOI: 10.52531/1682-1696-2022-22-2-33-38
Научная статья

ФИНАНСОВЫЙ МОНИТОРИНГ КРИПТОТРАНЗАКЦИЙ В УСЛОВИЯХ ПРАВОВОЙ НЕОПРЕДЕЛЕННОСТИ ДЕЯТЕЛЬНОСТИ КОНТРАГЕНТОВ

П.И. Бурак[1], В.П. Бауэр[1], Е.В. Чайкина[2]
[1] Институт региональных экономических исследований
[2] ФГАОУ ВО «Севастопольский государственный университет»

В статье выявлены особенности финансовой деятельности контрагентов криптотранзакций в современных условиях финансовой и политической неопределенности. Обоснованы рискориентированные факторы, формирующие неопределенность деятельности контрагентов, выполнен их анализ. Установлено, что большинство контрагентов криптотранзакций с подозрительными операциями функционируют в системах сетевых финансов, что влияет на совершенствование методологии финансового мониторинга и законодательства в области ПОД/ФТ. Развитие российской системы финансового мониторинга необходимо осуществлять как за счет решения теоретических вопросов деанонимизации контрагентов криптовалют, так и за счет внедрения новых инструментальных средств и организационных мероприятий. Направлением перспективных исследований является внедрение в систему российского финансового мониторинга антиотмывочного инструментария, выполняющего деанонимизацию контрагентов криптотранзакций по принципу «знай свои транзакции» («Know Your Transactions» – KYT). В целях совершенствования российского законодательства данный принцип необходимо также внедрить в существующие нормативные и правовые акты в области ПОД/ФТ.

Ключевые слова: *финансовый мониторинг, ПОД/ФТ, AML-сервисы, криптотранзакции, группы рисков криптотранзакций, криптокошелек, контрагенты, принцип «знай своего клиента», принцип «знай свои транзакции».*

Original article

FINANCIAL MONITORING OF CRYPTOTRANSACTIONS UNDER CONDITIONS LEGAL UNCERTAINTY OF ACTIVITIES OF COUNTERPARTS

P.I. Burak[1], V.P. Bauer[1], E.V. Chaikina[2]
[1] Institute of Regional economic research
[2] FGAOU VO «Sevastopol State University»

The article reveals the features of the financial activity of counterparties of crypto transactions in modern conditions of financial and political uncertainty. The risk-oriented factors that form the uncertainty of the counterparties' activities are substantiated, and their analysis is performed. It is established that the majority of counterparties of cryptotransactions with suspicious transactions operate in network finance systems, which affects the improvement of the methodology of financial monitoring and legislation in the field of AML/CFT. The development of the Russian financial monitoring system should be carried out both by solving theoretical issues of deanonymization of cryptocurrency counterparties, and by introducing new tools and organizational measures. The direction of promising research is the introduction of anti-money laundering tools into the Russian financial monitoring system, which performs deanonymization of counterparties of crypto transactions on the principle of «Know Your transactions» («Know Your Transactions» – KYT). In order to improve Russian legislation, this principle should also be implemented.

Keywords: *financial monitoring, AML/CFT, AML services, crypto transactions, risk groups of cryptotransactions, crypto wallet, counterparties, know your customer principle, know your transactions principle.*

ВВЕДЕНИЕ

Статья посвящена совершенствованию финансового мониторинга в области ПОД/ФТ, осуществляемого с использованием современных IT-технологий, предназначенных для выявления, интерпретации, классификации и деанонимизации участников операций с криптовалютами (далее – контрагенты), осуществляемых на основе криптовалютных транзакций (далее – криптотранзакции) в сетевой среде финансовых рынков, коммерческих банков, финансовых посредников и отдельных контрагентов.

В 2018 г. FATF ввело новый стандарт рискориентированного подхода к устранению неопреде-

Поступила в редакцию 13.05.2022

ленности в оценке контрагентов криптотранзакций [6]. Положения стандарта требуют перехода от идентификации клиентов финансовой и кредитно-банковской сферы по принципу «знай своего клиента» («Know Your Client» – KYC) к принципу «знай свои транзакции» (KYT), что обеспечивается путем анализа криптотранзакций в целях идентификации криптокошельков и деанонимизации их владельцев. В связи с этим в России возникает необходимость привести действующее законодательство системы оценки данных о клиентах к соответствию международным требованиям [2]. Важно отметить, что впервые аргументированная необходимость внедрения данного решения была обоснована в статье Г.О. Крылова [10]. В ней представлена схема обработки информации системой финансового мониторинга Росфинмониторинга с указанием ее основных недостатков. Показано, что из 4-х базовых задач финансового мониторинга непосредственно автоматизирован только процесс мониторинга, а остальные три задачи замкнуты на экспертов, что существенно задерживает оценку поведения контрагентов финансовых операций на предмет ПОД/ФТ.

Актуальность данной статьи заключается в необходимости выявления возможностей и преодоления ограничений существующих методологий деанонимизации контрагентов криптотранзакций в условиях роста масштабов цифровой экономики и совершенствования методов ПОД/ФТ. Решение данной проблемы становится актуальным в связи с тем, что с 23.08.2021 г. вступили в силу дополнения в Федеральный закон от 7.08.2001г. № 115-ФЗ [7], рекомендующие России выполнения вышеуказанных требований FATF по минимизации рисков отмывания доходов с криптовалютами за счет изменения правил внутреннего контроля путем внедрения программ идентификации не только клиентов, но и их транзакций. В этих целях указанный закон предписывает уполномоченному органу финансового мониторинга (Росфинмониторингу) в целях идентификации и аутентификации контрагентов клиентских финансовых и кредитно-банковских операций взаимодействовать как с Единой системой идентификации и аутентификации (ЕСИА) [14], так и с системой «Знай своего клиента» [16] Банка России. Однако с точки зрения ПОД/ФТ контрагенты подозрительные криптотранзакции могут быть незарегистрированными в указанных системах, поэтому их деятельность априори можно определить правовой категорией «неопределенность» [8]. Характеризуя пространство правовой неопределенности в качестве «серой зоны» [15], можно полагать, что эта зона характерна для контрагентов обращения криптовалют [3], в которой крайне затруднены идентификация криптокошельков и деанонимизация их владельцев [4]. Для решения указанных проблем в статье исследуются вопросы финансового мониторинга в рамках планируемой к созданию для этих целей единой национальной информационно-аналитической системы деанонимизации контрагентов криптотранзакций.

СОДЕРЖАНИЕ ИССЛЕДОВАНИЯ И ЕГО РЕЗУЛЬТАТЫ

Методологическую основу финансового мониторинга формирует необходимость выявления и уточнения информации о контрагентах финансовых и кредитно-банковских сообществ, описываемой наборами труднодоступных сетевых характеристик, в целях их деанонимизации в сложно сформированных гетерогенных сетевых потоках криптотранзакций [9]. В состав контрагентов входят участники финансовых рынков, осуществляющие следующие операции: обмена (конверсии) криптоактивов и фиатных валют; обмена криптоактивов между собой; перевода криптоактивов в качестве платежей; администрирования криптоактивов или соответствующих финансовых инструментов; предоставлении финансовых услуг от выпускающего лица и/или лица, осуществляющего продажу криптоактива. К контрагентам криптотранзакций относятся заказчики услуг по отмыванию криптовалют, субъекты транзитных операций фирм-однодневок, обеспечивающих перевод криптовалют от заказчиков услуг к бенефициарам с корректировкой (при необходимости) сроков исполнения и назначения платежа.

К методологическим особенностям мониторинга криптотранзакций относится ряд требований, характеризующих технологии ПОД/ФТ. Так, для избежания противоправных платежных ситуаций криптовалюту, получаемую от частных лиц, через криптобиржи или из прочих нерегулируемых источников, в соответствии с международными и национальными нормативными и правовыми актами рекомендуется проверять на легитимность. Объясняется это тем, что любая криптовалюта могла быть задействована раньше в мошеннических проектах, в операциях на черном рынке, в финансировании терроризма и других преступных деяниях. Такая криптовалюта, в том числе украденная, например, при взломах криптобирж или DeFi-протоколов, обычно помечается как «грязная». Известно, что блокчейн хранит информацию о каждой криптовалюте или ее доле, начиная с момента их создания майнером. Поэтому, когда контрагент отправляет «грязную» криптовалюту на регулируемую платформу, например, криптобиржу, то соответствующий AML-сервис может определить ее как подозрительную. В связи с этим у контрагента могут возникнуть юридически значимые проблемы. Его биржевый счет будет заблокирован до конца разбирательства платежа, и ему придется доказывать, что он лично не задействован в преступных схемах. Поэтому для идентификации криптоплатежа выделяют три группы рисков криптотранзакций: опасных, подозрительных и безопасных. Рассмотрим их особенности.

Опасные криптотранзакции. Эти транзакции характерны для криптовалют, платежи которыми 1) связаны с жестоким обращением с детьми или их эксплуатацией, 2) связаны с финансированием терроризма, оборотом наркотиков и прочей незаконной деятельностью, 3) использовались для покупок в ДАРКНЕТЕ, 4) были получены обманным путем, 5) прошли перемешивание с безопасными криптовалютами, 6) были получены путем вымогательства или шантажа, 7) участвовали в торговле на криптобиржах, уличенных в мошенничестве, 8) были различными способами украдены, 9) были связаны с нелицензионными онлайн-играми, 10) осуществляются субъектами, находящимися под санкциями, 11) были получены путем обмана клиентов и т.п.

Подозрительные криптотранзакции. Данные транзакции могут формировать: 1) криптобиржи, которые не используют AML-сервисы или имеют требования на AML-проверки транзакций только в определенных странах, 2) криптобиржи, которые позволяют выводить ежедневно криптовалюту объемом свыше $2000 без KYC/AML, 3) P2P-биржи, которые позволяют выводить более $1000 в криптовалюте ежедневно без KYC/AML, 4) транзакции со смарт-контрактами, в которых токены блокируются для обеспечения ликвидности, 5) криптовалюты, полученные из криптовалютных банкоматов и др.

Надёжные криптотранзакции. Надежными считаются следующие транзакции: 1) те, которые формируют майнеры для еще не отправленной криптовалюты, 2) транзакции с криптовалютой, которая хранится в надежных криптокошельках, 3) транзакции с криптовалютой, которая до этого проверялась AML-сервисами, 4) транзакции с криптовалютой, которая использовалась для оплаты легальной деятельности, 5) транзакции криптобирж, которые прошли идентификации KYC/AML для всех депозитов и/или для снятия средств со счетов, 6) P2P-биржи, требующие идентификации KYC/AML для депозитов и/или снятия средств со счетов, 7) транзакции с криптовалютой, изъятой из оборота правительством и/или надзорными органами и др.

В большинстве случаев проверка криптотранзакций AML-сервисами заключается в отслеживании их контрагентов и криптокошельков. Если значительная часть средств пришла из опасных криптокошельков, то возникает риск того, что платежная система не будет осуществлять данную транзакцию, поскольку криптокошелек контрагента также станет потенциально опасным. Поэтому при проверке криптовалюты на легальность осуществляется анализ и оценка следующих аспектов криптоплатежа: 1) непосредственно сама криптотранзакция, 2) уровень риска данной криптотранзакции, 3) формируется детальная информация об источниках криптовалюты в каждой транзакции, 4) выявляется процентный состав «чистых» и «грязных» криптовалют в данной транзакции, 5) анализируется общая и техническая информация о транзакции, 6) выявляются все предыдущие отправители и получатели криптовалюты этой транзакции, 7) определяется адрес криптокошелька получателя криптовалюты, 8) оценивается уровень риска взаимодействия с данным криптокошельком, 9) собирается детальная информация о том, из каких источников в данный криптокошелек приходят криптовалюты, 10) оценивается статистика использования криптокошелька, 11) оценивается сумма ненадежных криптовалют в криптокошельке, 12) выявляются транзакции, в которых участвовал данный криптокошелек и т.д.

Кроме вышеуказанных мер в Интернете для общедоступного пользования формируется «черный список» сетевых адресов контрагентов, с которыми опасно совершать транзакции. В настоящее время существует шесть источников получения данных адресов: 1) Abuse Report (Отчет о злоупотреблениях) – адреса, по которым есть сведения о злоупотреблениях в Интернете, 2) Ransomware extortionists (Вымогатели выкупа) – адреса, используемые шантажистами для удовлетворения требований по незаконной выплате, 3) OFAC sanctions – адреса, санкционированные Управлением по контролю за иностранными активами (OFAC), 4) DOJ sanctions – адреса, санкционированные Министерством юстиции США (DOJ), 5) Scam или Gainbitcoin scam – адреса, о которых сообщалось как о мошеннических, 6) Banned by contract – адреса контрагентов, занесенных в черный список Ethereum contract. Рассмотрим некоторые подходы к внедрению представленной выше методологии в практику ПОД/ФТ.

В настоящее время за рубежом и в России существуют многочисленные компании, разрабатывающие конкурирующие между собой AML-сервисы, осуществляющие мониторинг криптотранзакций: SAS AML, Oracle Mantas AML, Nice Actimize AML, Norkom Technologies AML, Whale Alert и др. К числу наиболее известных фирм-провайдеров данных сервисов являются следующие компании: AML Technology, Bitfury Crystal, Chainalisis, CipherTrace, Citi, Elliptic, Lendingblock, Payler, Kaspersky Fraud prevention, Контур.призма, ФБ Консалт и ряд других.

AML-сервисы осуществляют отслеживание информации о перемещениях криптовалют и передачу ее в соответствующие аналитические структуры и ведомства. Пользователи не видят этих процедур и не участвует в них, мониторинг и передача информации происходят в автоматическом режиме. Анализ функций ряда AML-сервисов показывает, что в них используются следующих методы анализа криптотранзакций и, соответственно, их контрагентов: методы непосредственного онлайн-мониторинга; методы анализа маскирования адресации контрагентов в киберпространстве; методы анализа идентификации объектов в киберпространстве на основе сигнатурных, эвристических и комбинированных методов; ме-

тоды глубокого анализа трафиков транзакций; методы глубокого машинного обучения; методы использования нейросетей для анализа трафиков транзакций и выявления преступных криптосообществ; методы интеллектуальной поддержки принятия решений; методы технологий облачных и туманных вычислений; методы технологий установления цифровой идентичности; методы компьютерной технологической и конкурентной разведки; методы экономической разведки и промышленного шпионажа; методы внешней разведки; методы разработки антифрод-систем; методы управления безопасностью SIEM-систем; методы выявления компьютерных угроз и обеспечения информационной безопасности; методы расследования инцидентов; методы создания инструментов компьютерной криминалистики; методы разработки, функционирования и эксплуатации безопасных, надёжных и эффективных систем, основанных на искусственном интеллекте; методы анализа жизненных циклов устойчивого развития информационных и социально-экономических систем; методы подготовки и реализации хакерских атак и др.

В качестве инструмента создания транзакций криптовалют наиболее подробно изучен блокчейн [13] и формируемые на его основе криптокошельки, которые выполняют функции хранения, отправки и получения криптовалюты [5]. В связи с этим Росфинмониторинг в целях совершенствования системы финансового мониторинга криптотранзакций реализовал с участием таких стран, как Финляндия, Люксембург, Лихтенштейн, Белоруссия и Мальта международную научно-прикладную программу «Прозрачный блокчейн» [1]. Сущность реализованного коллективом специалистов подхода к решению данной проблемы содержится в патентах, защищающих результаты данной программы [17, 12] позволяющих осуществлять анализ транзакций в сети Интернет-2, включающей частные сети I2P, RetroShare, Freenet, GNUnet и др.

Кратко рассмотрим представленный во втором патенте алгоритм поиска криптокошельков. Алгоритм анализирует социальные сети, WEB-магазины, мессенджеры, сайты, содержащие информацию о пожертвованиях, сборах средств на благотворительные цели и др. Для формирования сведений, найденных в Интернете, используется анализ HTML-страниц и прилегающих к ним второстепенных скриптовых и стилевых файлов. Под анализом HTML-страниц понимается процесс поиска по заранее заданным сигнатурам для установления статуса криптографического кошелька: опасный, подозрительный, безопасный. Для этого предлагается исследовать структуру изучаемых HTML-страниц на предмет наличия потенциально опасных слов и фраз, которые содержатся в заранее заданных сигнатурах. Присвоение статуса опасности осуществляется на основе анализа HTML-страниц данных, содержащихся в машиночитаемом носителе, а именно: сигнатур и записи о криптографических кошельках, содержащие журнал транзакции кошелька и различные сведения, содержащие упоминание о кошельке, например, HTML-страницы или файлы. После этого блок принятий решений возвращает данные с пометкой о статусе кошелька в машиночитаемый носитель. Система идентификации кошельков на основе анализа транзакций предусматривает регулярное обновление данных о кошельках, которое происходит в заданные промежутки времени и осуществляется блоком мониторинга данных, получаемых из машиночитаемого носителя, с одновременным осуществлением проверки о наличии новых сведений о транзакциях и ссылок на HTML-страницы, находящиеся в распределенной базе данных.

ЗАКЛЮЧЕНИЕ

В статье исследованы подходы к деанонимизации контрагентов криптотранзакций, осуществляемых в AML-сервисах финансового мониторинга при переходе от обслуживания клиентов по принципу KYC к принципу KYT в рамках единого информационного и программно-технического контура деанонимизации контрагентов криптотранзакций. Для этого изучены способы отмывания криптовалют, включающие три основных этапа: размещения криптовалюты (ввод в финансовую систему), «наслоение» криптовалюты (путем «перемешивания» валюты в целях сокрытия связи между криптовалютой и преступниками) и получение вместо «грязной» криптовалюты «чистой». Изучены принципы и функционал работы AML-сервисов, создаваемых для финансовых организаций и организаций кредитно-банковской сферы в следующих целях: для использования при разработке антиотмывочного программного обеспечения; для осуществления финансового и системного риск-менеджмента; для внедрения IT-комплаенса; для обнаружения фактов мошенничества и др.

В условиях роста масштабов цифровой экономики полученные результаты позволят: 1) усовершенствовать по принципу «Прозрачные Транзакции» процессы деанонимизации контрагентов криптотранзакций и принятия решений на основе адаптированных к специфике задач деанонимизации AML-сервисов; 2) осуществить комплексирование ряда существующих в Росфинмониторинге, Банке России и банковском сообществе информационных систем анализа онлайн- и оффлайн информации финансового мониторинга и на основе этого предпринять совместные усилия для создания в России в области ПОД/ФТ единого «регуляционного периметра» криптотранзакций; 3) создать в России единый информационный и программно-технический контур, минимизирующий ряд существующих в настоящее время организационных и управленческих издержек при выявлении причастности к противоправной деятельности участников транзакций с криптовалютами.

Результаты исследований позволяют сделать вывод о том, что Росфинмониторингу и Банкау России целесообразно создать в России единый информационный и программно-технический AML-контур антиотмывочного инструментария в области ПОД/ФТ, состоящий из AML-сервисов, предназначенных для анализа контрагентов криптотранзакций и поддержки принятия безопасных решений в сфере финансовой и межбанковской деятельности. Создание AML-контура позволит российским финансовым и кредитно-банковским учреждениям выявлять в сфере обращения криптовалют новые вызовы и угрозы до их официального опубликования Банком России и Росфинмониторингом, с упреждением планировать и оптимизировать свою кредитно-финансовую деятельность и за счет этого занимать в развивающейся цифровой экономике проактивную риск-ориентированную позицию [11].

Литература

1. В России создали сервис для отслеживания транзакций с криптовалютой URL: https://www.vedomosti.ru/finance/news/2021/02/19/858677-v-rossii-sozdali-servis-dlya-otslezhivaniya-tranzaktsii-s-kriptovalyutoi.
2. **Ващекина И.В., Ващекин А.Н.** Международные меры противодействия отмыванию нелегальных доходов пятого поколения – правовые условия укрепления безопасности финансового рынка // Вестник университета. 2021. № 1. С. 126–133. DOI: 10.26425/1816-4277-2021-1-126-133.
3. **Гордеев А.Ю., Лащенко Р.А.** Правовая компаративистика криптовалют // Проблемы правоохранительной деятельности. 2019. № 2. С. 25–31.
4. Деанонимизация (деанон) – нарушение анонимности, заключающееся в публикации персональных данных (настоящих ФИО, места проживания или работы и др.) участника Интернета, в частности: википроектов, блогов, форумов и т.д. URL: http://wikireality.ru/wiki/%D0%94%D0%B5%D0%B0%D0%BD%D0%BE%D0%BD%D0%B8%D0%BC%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F.
5. **Джабраилов Ю.М.** Биткоин-кошелек. Как завести, настроить и обезопасить // Экономика. Бизнес. Информатика. 2017. Т. 3. № 5. С. 417–425.
6. Директива 2018/843/EU Европейского Парламента и Совета Европейского Союза о внесении поправок в Директиву 2015/849/EU о предотвращении использования финансовой системы для отмывания денег и финансирования терроризма, а также о внесении поправок в Директивы 2009/138/EC и 2013/36/EU. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.156.01.0043.01.ENG&toc=OJ:L:2018:156:TOC.
7. Закон от 07.08.2001 № 115-ФЗ (в действующей редакции от 24.02.2021) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // http://ivo.garant.ru/#/document/12123862/paragraph/92387:0.
8. **Иванцов С.В., Сидоренко Э.Л., Спасенников Б.А., Берёзкин Ю.М., Суходолов Я.А.** Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // Всероссийский криминологический журнал // 2019. Т. 13, № 1. С. 85–93. DOI 10.17150/2500-4255.2019.13(1).85-93.
9. **Каратаев М.В.** Особенности экономической модели теневого сектора на современном этапе и предложения по автоматизации контрольной среды // Система ПОД/ФТ в глобальном мире: риски и угрозы мировой экономики: сборник тезисов докладов участников V Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ. 14-15 ноября 2019 г. М.: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2020. С. 138–141.
10. **Крылов Г.О.** Совершенствование процессов принятия решений при обработке больших данных в Росфинмониторинге // Современная математика и концепции инновационного математического образования. 2020. Т. 7. № 1. С. 143–152.
11. **Магомедов Ш.М., Каратаев М.В.** Концепция риск-ориентированного подхода в системе финансового мониторинга // Вестник Московского финансово-юридического университета. 2019. № 4. С. 67–77.
12. **Михайлов Д.М., Гроусов А.М., Проничкин А.С., Лебедев Ф.В.** Система и способ идентификации криптографических кошельков на основе анализа транзакций. Патент на изобретение RU 2693314 C1, 02.07.2019. Заявка № 2018128055 от 01.08.2018.
13. **Молокин А.С., Севанько А.М.** Блокчейн как инструмент транзакций в системах криптовалют // Финансы, деньги, инвестиции. 2016. № 2(58). С. 29–36.
14. Регламент информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства. Версия 2.15 (приложение 18 к протоколу заседания Подкомиссии по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 13.05.2016 № 168пр). URL: https://www.garant.ru/products/ipo/prime/doc/71744346/.
15. **Савин Л.В.** Концепция «серой зоны» // Информационные войны. 2020. № 2 (54). С. 5–17.
16. Федеральный закон от 21 декабря 2021 г. № 423-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». URL: https://www.garant.ru/products/ipo/prime/doc/403165654/.

17. **Юров А.А., Демкин К.В., Михайлов Д.М.** Прототип программно-аналитического комплекса для мониторинга криптовалют «Прозрачный блокчейн». Свидетельство о регистрации программы для ЭВМ 2020619277, 14.08.2020. Заявка № 2020618748 от 07.08.2020.

References

1. A service was created in Russia to track transactions with cryptocurrency. URL: https://www.vedomosti.ru/finance/news/2021/02/19/858677-v-rossii-sozdali-servis-dlya-otslezhivaniya-tranzaktsii-s-kriptovalyutoi (In Russian).
2. **Vashchekina I.V., Vashchekin A.N.** International measures to combat the laundering of illegal incomes of the fifth generation – legal conditions for strengthening the security of the financial market. *Vestnik universiteta*. 2021;(1): 126–133. DOI: 10.26425/1816-4277-2021-1-126-133 (In Russian).
3. **Gordeev A.Yu., Lashchenko R.A.** Legal comparison of cryptocurrencies. *Problemy pravookhranitel'noy deyatel'nosti*. 2019; (2): 25-31. (In Russian).
4. Deanonymization (deanon) is a violation of anonymity, which consists in the publication of personal data (real name, place of residence or work, etc.) of an Internet participant, in particular: wikis, blogs, forums, etc. URL: http://wikireality.ru/wiki/. (In Russian).
5. **Dzhabrailov Yu.M.** Bitcoin wallet. How to start, configure and secure. *Ekonomika. Biznes. Informatika*. 2017; 3(5): 417–425. (In Russian).
6. Directive 2018/843/EU of the European Parliament and of the Council of the European Union amending Directive 2015/849/EU on the prevention of the use of the financial system for money laundering and terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.156.01.0043.01.ENG&toc=OJ:L:2018:156:TOC. (In Russian).
7. Law No. 115-FZ of August 7, 2001 (as amended on February 24, 2021) «On countering the legalization (laundering) of proceeds from crime and the financing of terrorism». URL: http://ivo.garant.ru/# /document/12123862/paragraph/92387:0. (In Russian).
8. **Ivantsov S.V., Sidorenko E.L., Spasennikov B.A., Berezkin Yu.M., Sukhodolov Ya.A.** Crimes related to the use of cryptocurrency: main criminological trends // Vserossiyskiy kriminologicheskiy zhurnal. 2019; 13(1): 85–93. DOI 10.17150/2500-4255.2019.13(1).85–93. (In Russian).
9. **Karataev M.V.** Features of the economic model of the shadow sector at the present stage and proposals for automation of the control environment. The AML / CFT system in the global world: risks and threats to the world economy: a collection of abstracts of the participants of the V International Scientific and Practical Conference of the International Network Institute in the field of AML / CFT. November 14-15, 2019 M.: FGBOU VO "PRUE named after. G.V. Plekhanov". 2020: 138–141. (In Russian).
10. **Krylov G.O.** Improving decision-making processes in processing big data in Rosfinmonitoring. *Sovremennaya matematika i kontseptsii innovatsionnogo matematicheskogo obrazovaniya*. 2020; 7(1): 143–152. (In Russian).
11. **Magomedov Sh.M., Karataev M.V.** The concept of a risk-based approach in the system of financial monitoring. *Vestnik Moskovskogo finansovo-yuridicheskogo universiteta*. 2019; (4): 67–77. (In Russian).
12. **Mikhailov D.M., Grousov A.M., Pronichkin A.S., Lebedev F.V.** System and method for identifying cryptographic wallets based on transaction analysis. Patent for invention RU 2693314 C1, 02.07.2019. Application N 2018128055 dated 08/01/2018. (In Russian).
13. **Molokin A.S., Sevanko A.M.** Blockchain as a transaction tool in cryptocurrency systems. *Finansy, den'gi, investitsii*. 2016; 2(58): 29–36. (In Russian).
14. Regulations for the information interaction of the Participants with the ESIA Operator and the Operator for the operation of the e-government infrastructure. Version 2.15 (Appendix 18 to the minutes of the meeting of the Subcommittee on the use of information technologies in the provision of state and municipal services of the Government Commission on the use of information technologies to improve the quality of life and business conditions dated May 13, 2016 N 168pr). URL: https://www.garant.ru/products/ipo/prime/doc/71744346/. (In Russian).
15. **Savin L.V.** The concept of the «grey zone». *Informatsionnyye voyny*. 2020; 2 (54): 5–17. (In Russian).
16. Federal Law N 423-FZ of December 21, 2021 «On Amendments to Certain Legislative Acts of the Russian Federation». URL: https://www.garant.ru/products/ipo/prime/doc/403165654/. (In Russian).
17. **Yurov A.A., Demkin K.V., Mikhailov D.M.** The prototype of the software-analytical complex for monitoring cryptocurrencies «Transparent Blockchain» Certificate of registration of the computer program 2020619277, 14.08.2020. Application N 2020618748 dated 08/07/2020. (In Russian).

Бурак Петр Иосифович, д.э.н., профессор, директор Института региональных экономических исследований
тел: +7 (499) 241-04-18, **e-mail:** irei@irei.ru
ORCID: 0000-0003-0709-2449
Бауэр Владимир Петрович, д.э.н., доцент, г.н.с. Института региональных экономических исследований»
119002, г. Москва, пер. Сивцев Вражек, д. 29/16
119002, Moscow, per. Sivtsev Vrazhek, 29/16
тел.: +7 (916) 355-80-29, **e-mail:** bvp09@mail.ru
ORCID: 0000-0002-6612-3797
Чайкина Елена Васильевна, к.э.н., доцент, зав. кафедрой финансов и кредита ФГАОУ ВО «Севастопольский государственный университет»
299053, г. Севастополь, ул. Университетская, д. 33
299053, Sevastopol, st. Universitetskaya, 33
тел.: +7 (978) 834-09-38, **e-mail:** lena_chaykina@list.ru
ORCID: 0000-0003-4413-3414