УДК 338
DOI: https://doi.org/10.17816/RJLS642661

Противодействие финансированию децентрализованной диверсионно-террористической деятельности антироссийской направленности

А.Д. Керимов[1], В.В. Красинский[2]

[1] Институт государства и права Российской академии наук, Москва, Россия
[2] Институт финансовых технологий и экономической безопасности, Москва, Россия

АННОТАЦИЯ

В статье рассматривается проблема противодействия финансированию децентрализованной диверсионно-террористической деятельности сетевых структур антироссийской направленности. Авторы рассматривают противоправную деятельность учредителей, координаторов, спонсоров и бенефициаров диверсионно-террористических сетевых движений в онлайн-платформах и интернет-мессенджерах. Дана уголовно-правовая и криминологическая характеристика децентрализованной диверсионно-террористической деятельности. С учетом высокотехнологичного характера современного терроризма, внедрения распределенных механизмов финансирования и ресурсного обеспечения диверсионно-террористической деятельности в работе показаны изменения тактики террористов и современные механизмы финансирования диверсионно-террористической деятельности с использованием криптовалют. Показана связь диверсионно-террористических сетей антироссийской направленности с украинскими спецслужбами и вовлеченность ряда украинских финансовых институтов и провайдеров услуг виртуальных активов в «серые» финансовые схемы, отмывание преступных доходов и финансирование терроризма.

Ключевые слова: децентрализованная диверсионно-террористическая деятельность; диверсионно-террористические сети; финансирование терроризма; теневая финансовая инфраструктура; криптовалюты; виртуальные активы.

Как цитировать
Керимов А.Д., Красинский В.В. Противодействие финансированию децентрализованной диверсионно-террористической деятельности антироссийской направленности // Российский журнал правовых исследований. 2024. Т. 11. № 4. С. 7–13. DOI: https://doi.org/10.17816/RJLS642661

Рукопись получена: 21.10.2024 **Рукопись одобрена:** 07.12.2024 **Опубликована online:** 30.12.2024

DOI: https://doi.org/10.17816/RJLS642661

Countering the financing of anti-Russian decentralized sabotage and terrorism

A.D. Kerimov[1], V.V. Krasinsky[2]

[1] Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia
[2] Institute of Financial Technologies and Economic Security, Moscow, Russia

ABSTRACT

The article discusses the problem of counteracting the financing of anti-Russian decentralized sabotage and terrorist activities of network structures. The authors analyze the illegal activities of founders, coordinators, sponsors, and beneficiaries of sabotage and terrorist network movements in online platforms and Internet messengers. The work provides the criminal and criminological characteristic of decentralized sabotage and terrorist activities. The article presents changes in terrorist tactics and modern mechanisms for financing sabotage and terrorist activities using cryptocurrencies, taking into account the high-tech present-day terrorism, the introduction of distributed financing mechanisms and resource provision of sabotage and terrorist activities. It also demonstrates the relationship between anti-Russian subversive and terrorist networks and Ukrainian special agencies, as well as the involvement of a number of Ukrainian financial institutions and virtual asset service providers in quasi-legal financial schemes, money laundering, and terrorist financing.

Keywords: decentralized subversive and terrorist activities; subversive and terrorist networks; terrorist financing; shadow financial infrastructure; cryptocurrencies; virtual assets.

To cite this article

Kerimov AD, Krasinsky VV. Countering the financing of anti-Russian decentralized sabotage and terrorism. *Russian journal of legal studies.* 2024;11(4):7–13. DOI: https://doi.org/10.17816/RJLS642661

Received: 21.10.2024 **Accepted:** 07.12.2024 **Published online:** 30.12.2024

Актуальность исследования децентрализованной диверсионно-террористической деятельности антироссийской направленности связана с высокотехнологичным характером современного терроризма, распределенными механизмами управления, финансирования и ресурсного обеспечения террористических сетей и диверсионных сообществ (кросс-платформенные мессенджеры, краудфайндинг, DeFi, дропы и др.).

Научная основа изучения сетевых диверсионно-террористических движений в настоящее время только формируется. Существующие публикации затрагивают в основном вопросы уголовно-правовой квалификации или частные аспекты обеспечения медиабезопасности [1–4].

С учетом высокой степени общественной опасности сетевых диверсионно-террористических движений, значительного оперативного и боевого потенциала диверсионно-террористических структур, необходимости моделирования, прогнозирования и анализа деятельности децентрализованных диверсионно-террористических сетей антироссийской направленности углубленная теоретическая разработка данного вида преступной деятельности в качестве самостоятельного тематического направления научных исследований представляется обоснованной.

Большинство диверсионно-террористических движений, обеспечивающих координацию, ресурсное и финансовое обеспечение диверсионно-террористических актов, оказание финансовой, материальной либо иной помощи деятельности террористических организаций и диверсионных сообществ на территории Российской Федерации, в социальных медиа действуют как децентрализованные сообщества сетевого типа.

Сетевой характер организации диверсионно-террористической деятельности помимо массовости, узнаваемости, общей идейной платформы антисоциальной направленности позволяет кураторам террористических организаций и диверсионных сообществ обеспечивать систему устойчивой связи и управления, определенную автономность структурных звеньев, рекрутирование единомышленников, кросс-рекламу и финансирование.

Современные диверсионно-террористические движения антироссийской направленности неоднородны и представлены боевыми крыльями сепаратистских структур («Движение за независимость Зеленого Клина», «Зелений Клин — моя батьківщина», «Свободный Идель-Урал», «Малиновый Клин — Независимая Кубань» и др.), террористическими добровольческими этнонациональными незаконными вооруженными формированиями — структурными звеньями «Иностранного легиона ВСУ» («Русский добровольческий корпус», «Легион Свобода России», «Сибирский батальон», «Карельский национальный батальон», «Уральский батальон», «Рота Башкорт» и др.), самостоятельными диверсионно-террористическими организациями («Боевая организация анархо-коммунистов», «Российское движение „Право Силы“», «Черный мост», «Черный мост поддержка», «Экспозиция Революционного Анархизма» и др.).

Антироссийская сепаратистская активность стала развиваться в российском сегменте Интернета и социальных сетях задолго до начала СВО.

Еще в 2008–2010 гг. для популяризации идей национально-государственной автономии и регионального сепаратизма в районах компактного проживания украинцев были созданы псевдоисторические страницы в интернет-энциклопедии Wikipedia.

Малоактивные, «полуспящие» паблики «Зеленый Клин — моя батьківщина», «Малиновый Клин — Независимая Кубань» после начала СВО стали размещать персональные данные российских сотрудников правоохранительных органов, рекламировать террористические организации «Легион Свобода России», «Русский добровольческий корпус», предлагать помогать «партизанским отрядам» в проведении диверсий[1].

В 2018 г. на Украине зарегистрирована сепаратистская организация «Свободный Идель-Урал»[2], главными целями которой провозглашены «развал России и создание на ее руинах новых государств» народами Урала и Поволжья, населяющими Татарстан, Башкортостан, Чувашию, Мордовию, Удмуртию, Марий Эл. После начала СВО модераторы сетевого движения «Идель-Урала» перешли к призывам сторонников сепаратизма к захвату оружейных комнат, арсеналов воинских частей, участию в боевых действиях на стороне Украины, совершению террористических актов и диверсий на российской территории.

Заметной сепаратистской сетевой инициативой является созданная в мае 2022 г. «Лига свободных наций» (League of Free Nations)[3].

Движение ориентировано на привлечение внимания к «дискриминации порабощенных народов в России», консолидацию «антиимперских сил», обретение государственного суверенитета субъектами Российской Федерации.

Идеологи «Лиги свободных наций» представляют ее как общественно-политическую платформу националистических движений башкир, бурят, ингерманландцев, казаков, калмыков, татар и эрзян.

Отмечается повышенная сетевая активность и продвижение в соцсетях и кросс-платформенных интернет-мессенджерах т.н. Форума свободных народов ПостРоссии

[1] Решением Верховного Суда Российской Федерации от 7 июня 2024 г. движения «Зеленый Клин — моя батьківщина» и «Малиновый Клин — Независимая Кубань» признаны экстремистскими и запрещены на территории России.

[2] В феврале 2022 г. общественная организация «Свободный Идель-Урал» (Украина) признана нежелательной на территории Российской Федерации, в июне 2024 г. признана экстремистской.

[3] Зарегистрированная в Литве «Лига свободных наций» 17 февраля 2023 г. признана в Российской Федерации нежелательной организацией, 7 июня 2024 г. признана экстремистским объединением.

(ФСНПР)[4], учрежденного гражданами Польши, Украины, Великобритании и США.

Для реализации сепаратистской программы разрушения федерализма и территориальной целостности Российской Федерации используется главным образом тактика террористических действий, которая предполагает различные формы и методы антигосударственной борьбы.

Функционеры ФСНПР призывают к вооруженной борьбе с «режимом», акциям гражданского неповиновения, а также формируют на этнической основе антироссийские воинские формирования для «защиты коренных народов и порабощенных регионов». В программных документах ФСНПР закреплена цель силового захвата власти с использованием национал-сепаратистского подполья.

Установленные участники ФСНПР причастны к совершению в 2022–2024 гг. серии преступлений террористической направленности, предусмотренных ст. 205, 205.1, 205.2, 205.3, 205.4 УК РФ.

Большинство участников специализированных диверсионно-террористических движений («Роспартизан», Российское движение «Право Силы», «Черный мост», «Экспозиция Революционного Анархизма») помимо агитационной работы и осуществления самостоятельных диверсионно-террористических акций сотрудничают с украинскими спецслужбами и вооруженными формированиями. Через систему чат-ботов ведется набор добровольцев для вступления в т.н. «Иностранный легион» ВСУ. Часть средств диверсионно-террористических движений перечисляется на нужды террористических организаций (например, «Легиона Свобода России» или «Русского добровольческого корпуса»).

Следует учитывать, что участие российских граждан в вооруженном конфликте в составе непосредственно противостоящих Российской Федерации вооруженных формирований Украины образует состав государственной измены в форме перехода на сторону противника (ст. 275 УК РФ).

Помимо разового осуществления терактов и диверсий на идейной основе кураторы децентрализованной сетевой диверсионно-террористической деятельности призывают к систематическому совершению диверсионно-террористических акций на материальной основе, в качестве постоянного источника преступного дохода. Таким образом в их действиях содержатся признаки организации финансирования терроризма и диверсий, что влечет более строгое уголовное наказание.

Новым элементом финансирования экстремистской, сепаратистской и диверсионно-террористической деятельности является широкое использование криптовалют[5] [5].

Наблюдается изменение тактики сбора пожертвований. Если ранее (до 2023 г.) привлечение средств осуществлялось открыто, через закрепы в профилях или в ссылках, то теперь финансовые реквизиты направляются заинтересованным лицам в личном сообщении.

Фиксируется использование криминальных сервисов блокчейн-аналитики (AML-бот, сервис Antinalysis и др.), которые дают возможность анализировать применение транзакций с точки зрения правоохранительных органов. Пользователь получает скоринг-оценку вероятности маркировки его транзакций как подозрительных и блокировки его криптовалютных активов [6]. Таким образом преступники получили возможность протестировать свои методы ОД/ФТ.

Растет уровень конспирации — в качестве мер усиления безопасности практикуется смена сетевых адресов аккаунтов координаторов преступной деятельности и размещение проверочных QR-кодов.

При проведении финансовых транзакций предлагается использовать VPN и безопасный режим работы браузера.

Распространено использование дропперских услуг (оформление карт на третьих лиц) с покупкой идентификаторов (электронной почты, телеграм-аккаунтов), прохождением проверки в платежных системах и на криптобиржах, выводом средств на криптокошельки в различных валютах и обналичиванием через «серые» обменники.

Учитывая осведомленность координаторов о наличии открытых баз блокчейнов криптовалют и успешной практике деанонимизации правоохранительными органами участников криптовалютных транзакций, кураторы сетевых движений предлагают использовать для сбора донатов криптовалюты повышенной анонимности (в первую очередь, Monero) и теневую финансовую инфраструктуру (серые криптообменники, миксеры, теневые кроссчейновые мосты).

Необходимо отметить, что финансирование деятельности нежелательных в Российской Федерации организаций, экстремистских объединений и движений, финансирование террористической деятельности и диверсий являются составами преступлений (ч. 2 ст. 284.1 УК РФ «Осуществление деятельности иностранной или международной организации, в отношении которой принято решение о признании нежелательной на территории Российской Федерации ее деятельности», ст. 282.3 УК РФ «Финансирование экстремистской деятельности», ст. 205.1 УК РФ «Содействие террористической деятельности» и ст. 281.1 УК РФ «Содействие диверсионной деятельности»).

При этом законодателем предусмотрено специальное основание освобождения от уголовной ответственности по данным статьям, если лицо содействовало предотвращению или пресечению преступления, которое оно финансировало или совершению которого содействовало, если в его действиях не содержится иного состава преступления. Для освобождения от ответственности при финансировании экстремистской деятельности (ст. 282.3 УК РФ)

[4] Форум свободных народов ПостРоссии 22 ноября 2024 г. признан террористической организацией и запрещен в России.

[5] Social Media and Terrorism Financing. Asia/Pacific Group on Money Laundering / Middle East and North Africa Financial Action Task Force. January 2019. P. 6, 11-14. URL: www.apgml.org (дата обращения: 01.12.2024).

должно выполняться условие — совершение преступления впервые.

В целях криминологического изучения механизма финансирования децентрализованной сетевой диверсионно-террористической деятельности рассмотрим данные открытых блокчейнов о финансировании некоторых диверсионно-террористических движений, полученные с помощью общедоступных инструментов мониторинга криптовалютных транзакций.

Криминологическое значение и доказательная база находящихся в публичном доступе графов криптовалютных транзакций сетевых диверсионно-террористических движений заключается в документировании преступной деятельности всех ее участников и их связей. Децентрализованная база блокчейна обеспечивает надежную и стабильную запись любых финансовых операций, в том числе подозрительных и криминальных, с использованием криптовалют. Зарегистрированные в блокчейне данные невозможно удалить или изменить (блоки связаны системой криптографических доказательств, для потенциального изменения данных требуются огромные вычислительные мощности).

Так, анализ транзакций находящегося в свободном доступе криптокошелька экстремистского движения «Лига свободных наций» показывает вывод средств на украинскую криптобиржу Whitebit, серый обменник криптовалют «Обменка SU», а также криминальные даркнет-площадки Mega DarkMarket и OMG, используемые для незаконного сбыта наркотиков и продажи криминальных услуг.

Особенностью телеграм-канала «Свободная Чувашия — Волжская Булгария» (движение признано экстремистским), осуществляющего сбор средств на нужды ВСУ и террористических организаций (ЛСР, РДК) является его коммерческая ориентация. Администрация канала постоянно рекламирует т.н. «чувашскую криптовалюту».

Планируется создание системы личных кабинетов, где доступ к контролю криптовалюты можно будет получить, подтвердив чувашское происхождение (знание языка или документы) либо заплатив определенную сумму токенами. Те, кто прошел данную верификацию, могут принимать участие в голосовании по распределению токенов либо делегировать свой голос представителю. Криптовалюта будет направляться в «Фонд освобождения Чувашии» для «деоккупации родины».

Проект напоминает частную финансовую криптовалютную пирамиду этнически ориентированного характера с признаками нелегального участника финансового рынка (отсутствие лицензий регулятора, декларируемые гарантии доходности, невозможность защиты прав потребителей финансовых услуг в случае их нарушения).

С размещенного в открытом телеграм-канале криптокошелька диверсионно-террористического движения «Роспартизан» средства выводятся на дубайскую биржу Bybit и украинскую биржу Kuna (в нарушение стандартов ФАТФ и антиотмывочного законодательства провайдер не требует обязательной верификации участника транзакции).

Изучение транзакции с кошелька «Роспартизана» от 23.06.2024 позволяет установить транзитный сетевой адрес, с которого деньги поступают как для диверсионно-террористического движения «Роспартизан», так и для террористической организации «Легион Свобода России».

Анализ финансовых операций с кошелька сбора донатов диверсионно-террористического движения «Черный мост поддержка» свидетельствует об использовании участниками транзакций высокорискового миксера Coin Join Mixer, транзите криптовалюты через кошелек польской организации «Гражданский совет» (признана нежелательной в Российской Федерации) и выводе средств на украинскую биржу Kuna, нарушающую законодательство о противодействии финансированию терроризма и отмыванию преступных доходов.

Представляет интерес и эфировский сетевой адрес криптокошелька «Черный мост поддержка». В схеме финансовых операций зафиксирован вывод средств на теневой кроссчейновый мост, где произошел обмен криптовалют. Анализаторы эфиров фиксируют обмен биткоинов на лайткоины, а также использование автоматического криптообменника EXch, поддерживающего мультивалютные операции с биткоинами, лайткоинами, эфирами и монеро. На этом примере мы видим использование в целях финансирования террористической деятельности аналога цифровой системы «хавала».

Движение средств с криптокошелька террористической организации «Русский добровольческий корпус» идет в том числе на зарегистрированную в США учетную запись Hotwallet (аналог корреспондентского счета), что свидетельствует о том, что один из ее кураторов/координаторов находится на территории Соединенных Штатов. Таким образом, американские регуляторы и провайдеры криптоуслуг, которые наложили санкции на российские системы платежей и обмена финансовыми сообщениями, а также заморозили криптоаккаунты и счета российских граждан, закрывают глаза на заведомое финансирование террористической деятельности в Российской Федерации.

Значительное число аккаунтов, относящихся к украинской криптовалютной индустрии и зарегистрированных в соответствующей юрисдикции, вовлечены или прямо обслуживают теневую и криминальную финансовую деятельность. Примером может служить украинский онлайн-обменник BTCBank (https://btcbank.com.ua). Данная финансовая площадка долгое время специализировалась на обеспечении крупнейших торговых площадок продажи наркотиков RAMP и HYDRA, транзите, обналичивании и легализации преступных доходов от сетевого бесконтактного сбыта наркотиков и психотропных веществ, а также геймблинга (задокументирована связь с 16 410 криминальными транзакциями).

DOI: https://doi.org/10.17816/RJLS642661

Базы блокчейнов показывают 1288 транзакций на 74,13 биткоинов из BTCBank на RAMP и 44 транзакции из RAMP в BTCBank на сумму 34,1 биткоина. Зафиксированы 3022 транзакции объемом 23,9 биткоина из BTCBank на HYDRA, а также 220 транзакций из HYDRA в BTCBank на 51,6 биткоина. Из BTCBank на сервис онлайн-казино 999.Dice[6] перечислено 92,3 биткоина (3922 транзакции). В свою очередь, на BTCBank переведено 93,7 биткоина (2667 транзакций).

Аналогичная структура финансовых потоков характерна для украинских обменников CoCO-Pay (задокументирована связь с 5216 криминальными транзакциями) и MINE.exchange. Графы криптовалютных транзакций показывают вывод с CoCO-Pay 35,9 биткоинов на HYDRA, а также вывод 9,62 биткоинов на Mega. На сервис онлайн-казино 1XBET[7] перечислено 12,22 биткоина.

С MINE.exchange можно отследить перечисления на HYDRA 3209 биткоинов (119 919 транзакций). В свою очередь, с площадки HYDRA на MINE.exchange проведено 11 586 транзакций на 707 биткоинов.

Анализ финансовых операций свидетельствует, что криптообменники BTCBank, CoCO-Pay и MINE.exchange не осуществляют комплаенс-контроль соблюдения антиотмывочных норм и выступают технической обнальной и легализационной площадкой для организованной преступности.

ВЫВОДЫ

Большинство современных антироссийских сепаратистских и диверсионно-террористических движений возникло задолго до СВО. Данные сетевые движения курируются украинскими спецслужбами. На это указывают учредители сепаратистских и диверсионно-террористических проектов (парламентские объединения и комиссии Верховной Рады Украины, координация со стороны Офиса Президента), место регистрации сепаратистских организаций, сетевые адреса аккаунтов и пабликов, платежные реквизиты.

Все сепаратистские и диверсионно-террористические сети используют криптовалюты (в первую очередь, коины повышенной анонимности), украинскую теневую финансовую инфраструктуру, нарушающую антиотмывочные стандарты, и прибегают к услугам криминальных обменников (OMG, Mega, RAMP и др.) [7, 8].

В большинстве схем финансирования терроризма и экстремизма прослеживается четкая аналогия с подозрительными финансовыми операциями в сфере незаконного сетевого сбыта наркотиков (фиксируются многочисленные, не имеющие очевидного экономического смысла запутанные операции с длинными цепочками промежуточных транзакций). Для выявления организаторов и пособников диверсионно-террористической деятельности требуется анализ финансовых связей исполнителей данных преступлений.

Парсинг данных соцсетей и макроанализ ряда украинских финансовых институтов и провайдеров услуг виртуальных активов (Приватбанк, цифровой банк Monobank, криптообменники BTCBank, MINE.exchange и CoCO-Pay, криптобиржа Kuna и др.) указывают на их вовлеченность в серые финансовые схемы и определенную специализацию в отмывании преступных доходов и финансировании терроризма. Это является достаточным основанием для номинации Украины в санкционные списки ФАТФ.

Независимо от идеологической окраски и профиля деятельности любые радикальные сетевые движения заинтересованы в рекламе, брендировании и финансировании, поэтому эксплуатируют разнообразную тематику и в силу установок кураторов / главных спонсоров / конечных бенефициаров и коньюнктурной заинтересованности могут сотрудничать по широкому спектру направлений.

Для документирования децентрализованной диверсионно-террористической деятельности правоохранительным органам нужно доказывать причастность фигурантов к сетевому движению: сходство целей, использование бренда, названия, аббревиатуры, символики, кросс-рекламу и финансирование, кросс-постинг, одинаковых учредителей и выгодополучателей.

Большинство специализированных диверсионно-террористических движений («Роспартизан», Российское движение «Право Силы», «Черный мост», «Черный мост поддержка», «Экспозиция Революционного Анархизма») до сих пор не запрещены на территории Российской Федерации и не признаны террористическими, что требует адекватного реагирования со стороны государства. Не признаны террористическими и курирующие их спецорганы Украины (Главное управление разведки и Служба безопасности Украины).

При подготовке исковых заявлений о запрете целесообразно применение наиболее широкого диапазона альтернативных наименований структуры. Это позволяет выявлять, документировать и пресекать разнообразные звенья и организационные формы преступной сети. Участие в подобных сетевых движениях преступного характера должно квалифицироваться по более тяжким составам УК РФ.

Кроме того, приведенные факты и анализ активности сетевых диверсионно-террористических движений могли бы использоваться Россией на международных площадках антиотмывочного (ФАТФ, региональные группы по ее типу, Группа «Эгмонт») и антитеррористического характера (профильные комитеты ООН, РАТС ШОС, АТЦ СНГ) в качестве аргументации для отвода претензий коллективного Запада и отстаивания наших национальных интересов.

[6] Social Media and Terrorism Financing. Asia/Pacific Group on Money Laundering /Middle East and North Africa Financial Action Task Force. January 2019. P. 6, 11-14. URL: www.apgml.org (дата обращения: 01.12.2024).

[7] Ресурс 1XBET включен в реестр заблокированных сайтов ФНС России.

СПИСОК ЛИТЕРАТУРЫ

1. Давитадзе М.Д. Уголовная ответственность за диверсию // Вестник Московского университета МВД России. 2020. № 3. С. 169–173. EDN: SOYWGE doi: 10.24411/2073-0454-2020-10163

2. Лисовский Д.Г., Моисеенко Е.Е. Уголовно-правовая и социальная сущность диверсии // E–Scio. 2022. № 4(67). С. 181–185. EDN: IRAREM

3. Тутуков А.Ю., Татаров Л.А. Правильная квалификация террористического акта и его отграничение от диверсии // Пробелы в российском законодательстве. 2018. № 6. С. 166–170. EDN: YPOQYX

4. Хрусталев М.А. Диверсионно-террористическая война как военно-политический феномен // Международные процессы. 2003. Т. 1, № 2(2). С. 55–67. EDN: OIPOIP

5. Dr. Teichmann F., Park E. Terrorismusfinanzierung durch Kryptowaehrungen // ZRFC. 2018. № 2. doi: 10.37307/j.1867-8394.2018.02.05

6. Красинский В.В. Противодействие финансированию терроризма с использованием криптовалют // Современное право. 2022. № 9. С. 108–115. EDN: LDHFOO doi: 10.25799/NI.2022.58.84.018

7. Красинский В.В, Леонов П.Ю., Морозов Н.В. Применение искусственного интеллекта в сфере противодействия отмыванию денег и финансированию тероризма // Современное право. 2024. № 5. С. 75–82. EDN: SWGQID

8. Красинский В.В., Норкина А.Н. Криминологические исследования блокчейнов криптовалют в российской антиотмывочной системе // Современное право. 2024. № 8. С. 88–94. EDN: BRTINO doi: 10.25799/NI.2024.43.93.017

REFERENCES

1. Davitadze MD. Criminal liability for sabotage. *Bulletin of the Moscow university of the ministry of internal affairs of Russia.* 2020;(3):169–173. EDN: SOYWGE doi: 10.24411/2073-0454-2020-10163

2. Lisovskij DG, Moiseenko EE. The criminal-legal and social essence of sabotage. *E-Scio.* 2022;(4):181–185. EDN: IRAREM

3. Tutukov AYu, Tatarov LA. The correct qualification of act of terrorism and its distinction from diversion. *Gaps in Russian Legislation.* 2018;(6):166–170. EDN: YPOQYX

4. Hrustalev MA. Sabotage and terrorist warfare as military and political phenomenon. *International Trends.* 2003;(2):55–67. EDN: OIPOIP

5. Teichmann F., Park E. Terrorismusfinanzierung durch Kryptowaehrungen. *ZRFC.* 2018;(2). doi: 10.37307/j.1867-8394.2018.02.05

6. Krasinsky VV. Countering the financing of terrorism using cryptocurrencies. *Modern Law.* 2022;(9):108–115. EDN: LDHFOO doi: 10.25799/NI.2022.58.84.018

7. Krasinsky VV, Leonov PYu, Morozov NV. Criminological research of cryptocurrency blockchains in the russian anti-laundering system. *Modern Law.* 2024;(5):75–82. EDN: SWGQID

8. Krasinsky VV, Norkina AN. The use of artificial intelligence in the field of countering money laundering and terrorist financing. *Modern Law.* 2024;(8):88–94. EDN: BRTINO doi: 10.25799/NI.2024.43.93.017

ОБ АВТОРАХ

Александр Джангирович Керимов, д-р юрид. наук, профессор, главный научный сотрудник;
eLibrary SPIN: 7041-9829; e-mail: 8017498@mail.ru
***Владислав Вячеславович Красинский,** д-р юрид. наук, доцент; ORCID: 0000-0001-6354-4644;
eLibrary SPIN: 9577-6810; e-mail: VVkrasinskii@mephi.ru

AUTHOR INFO

Alexander Dzh. Kerimov, Dr. Sci. (Jurisprudence), professor, chief researcher; eLibrary SPIN: 7041-9829;
e-mail: 8017498@mail.ru
***Vladislav V. Krasinsky,** Dr. Sci. (Jurisprudence), associate professor; ORCID: 0000-0001-6354-4644;
eLibrary SPIN: 9577-6810; e-mail: VVkrasinskii@mephi.ru

* Автор, ответственный за переписку / Corresponding author