

Синкевичс Никита

Вс. iur., студент Рижского университета имени Страдина

ПРОТИВОДЕЙСТВИЯ ПРЕДИКАТНЫМ ПРЕСТУПЛЕНИЯМ, В СОВЕРШЕНИИ КОТОРЫХ ИСПОЛЬЗУЮТСЯ КРИПТОВАЛЮТЫ

В статье в целом рассмотрены правовой статус криптовалют, обозначена актуальность использования криптовалют в предикатных преступлениях, проблематика и возможные методы противодействия предикатным преступлениям, в совершении которых используются криптовалюты.

Ключевые слова: криптовалюта, предикатные преступления, технология “блокчейн”, преступления и криптовалюта.

Sinkevics Nikita

Bc. iur., student of Riga Stradins University

COUNTERACTING PREDICATE OFFENCES WHICH COMMITTED BY USING CRYPTOCURRENCIES

In the article in general considered legal status of cryptocurrencies, determinate cryptocurrencies actuality in predicate offences, problematics and possible methods of counteracting predicate offences which committed by using cryptocurrencies.

Keywords: cryptocurrency, predicate offences, blockchain technology, offences and cryptocurrency.

Существует множество решений, в основе которых лежит технология “блокчейн”. Например, это криптовалюты и “умные” контракты. Данные решения в основном работают на таких популярных платформах (сетях), как “Bitcoin”, “Ethereum”, “Ripple”, “Litecoin”, “BitcoinCash”, “EOS” и др. [1]. Самой популярной криптовалютой является “BTC” (“биткоин”), который действует на платформе “Bitcoin”, рыночная капитализация которого на 29 февраля 2020 года составляет примерно 158 миллиардов американских долларов [2].

Надо отметить, что правовой статус криптовалют в разных государствах отличается либо вообще не определен. Например, в Латвии криптовалюты считаются **виртуальными валютами**, но не фиатными денежными средствами. Согласно второй части 2 статьи 1 Закона предотвращения легализации преступно полученных средств и финансирования пролиферации, виртуальные валюты – цифровое отображение стоимости, которое может быть в цифровом виде отослано, может храниться или продаваться и функционировать как средство обмена, но не признано законным платежным средством, не считается банкнотой и монетой, безналичными деньгами и электронными деньгами, а также не имеет монетарной стоимости, которая накоплена в платежном инструменте [3]. В Латвии использование криптовалюты является договорным способом оплаты [4]. Если предприятие предоставляет какие-либо услуги, связанные с криптовалютами, например, услуги обмена фиатных денежных средств на криптовалютные средства, то на это предприятие распространяются требования Закона предотвращения легализации преступно полученных средств и финансирования пролиферации, то есть, таким предприятиям необходимо быть зарегистрированным как правовым субъектам, подать информацию о сфере деятельности и ответственном лице, создать внутреннюю контрольную систему, сообщать о непростых и подозрительных сделках [5].

Также и в Дании криптовалюты не считаются фиатными денежными средствами, так как криптовалюты не обладают реальной торговой стоимостью [6]. В свою очередь в Германии криптовалюты имеют статус официального средства расчетов [7]. Несмотря на то, что во многих государствах понятие криптовалюты отличается, Целевая группа по финансовым действиям¹ рекомендует на законодательном уровне обязать предприятия, которые оказывают криптовалютные услуги, проводить надлежащую проверку клиентов при установлении деловых отношений или при осуществлении разовых операций [8].

Учитывая общий технический принцип действия технологии “блокчейн”, доступность, простоту и надежность использования

¹ FATF, Financial Action Task Force

криптовалют, криптовалютные операции осуществляются в преступной деятельности, а именно в совершении **предикатных преступлений**. Как указано в учебном пособии Управления Организации Объединенных Наций по наркотикам и преступности, “Отсутствие связи между счетами в виртуальных валютах и реальными людьми в сочетании с возможностью иметь неограниченное множество счетов создает благоприятную почву для создания новых сложных моделей, направленных на сокрытие криминального происхождения средств”[9]. Основное преимущество использования криптовалюты в преступной деятельности – это не привязанность лиц к криптовалютным кошелькам.

Предикатное преступление – это корыстное преступление, в результате совершения которого, получают средства (преступные), которые в дальнейшем могут быть подвергнуты легализации [10]. Согласно статье 1 подпункта “е” Конвенции об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности, предикатное преступление – это любое уголовное преступление, в результате которого получены доходы, которые могут стать предметом уголовно-наказуемого деяния, которое определено в статье 6 настоящей Конвенции [11]. Как указывает Ляскало А. Н., “легализация (отмывание) преступно приобретенных денежных средств и иного имущества является логическим продолжением первичного (предикатного) преступления” [12] Например, предикатным преступлением может считаться наркоторговля, мошенничество, легализация денежных средств и другие преступления, в совершении которых используются криптовалюты. Также, надо отметить, что после совершения предикатного преступления, полученные не законные средства, могут быть подвергнуты легализации с использованием тех же криптовалют.

Как указывает Зиновьева Н. С., “Один из самых популярных способов оборота криптовалюты в преступных целях осуществляется через криптовалютные биржи” [13]. Криптовалютные биржи – это специальные сетевые платформы – сайты, на которых можно производить обмен фиатных денежных средств на криптовалютные средства, и соответственно наоборот.

Существует множество таких криптовалютных обменных или биржевых систем, например такие, как “Bitok”, “Netex24”, “Wunderbit”, “Binance” и др.

В Латвии, согласно пункту 7 части 1 статьи 11 Закона предотвращения легализации преступно полученных средств и финансирования пролиферации, правовые субъекты, которые осуществляют сделки с виртуальной валютой обязаны производить исследование своего клиента [3], то есть должны придерживаться принципу “знай своего клиента”. Учитывая, что множество криптовалютных обменных или биржевых систем действуют в разных юрисдикциях, не всегда возможно данное требование распространить на все сетевые обменники или биржи.

Например, в правилах использования криптовалютной обменной системы “Bitok”, которая доступна по адресу “bitok.cc”, в подпункте 3 подпункта 1 пункта 3, указано, что “Bitok.cc обязуется: **не хранить** информацию (адреса, суммы, время, идентификационные данные (персональные данные) и т.д.) по обменным операциям Клиентов и предоставлять её по первому требованию Клиентов, к которым она относится.” В свою очередь, в подпункте 6 подпункта 4 пункта 3, указано, что “Bitok.cc обязуется: не разглашать информацию по обменным операциям, а также личные данные Клиентов Bitok.cc третьим лицам, за исключением следующих ситуаций: по законному запросу компетентных органов по месту нахождения владельца сервиса Bitok.cc” [14].

На самом сайте, в том числе в правилах использования, этой криптовалютной обменной системы не указаны данные, о том, какой правовой субъект предоставляет криптовалютные услуги, а также какие-либо контактные данные для связи. Единственное, что указано, это название предприятия – “BITOK.CC LLP”, возле символа копирайта, в нижней части сайта, хотя не понятно, где данное предприятие зарегистрировано, какой у него регистрационный номер. Также надо отметить, что зона доменных имен “CC” – это национальный домен верхнего уровня для Кокосовых островов [15]. В свою очередь, сам сервер сайта расположен в Германии [16]. Поэтому не ясна юрисдикция действия данной криптовалютной обменной системы.

Надо отметить, что в сети множество криптовалютных обменных систем с неопределенной юрисдикцией. Вследствие чего, возможно, что такие сервисы используются или могут быть использованы в преступной деятельности.

Также надо отметить, что активно криптовалюты как расчетные средства используются в сети “DarkNet”, то есть скрытой сети, в которой данные передаются в зашифрованном виде. В такой сети множество площадок – сайтов, на которых осуществляется незаконная деятельность. Например, в феврале 2019 года в скрытой сети действовало примерно 2.5 тысяч магазинов наркотических и психотропных веществ [17], в которых расчеты осуществляются с помощью криптовалютных средств.

Эксперты из Королевского колледжа Лондона в 2016 году пришли к выводу, что 57% из доступных площадок в скрытой сети посвящены уголовной деятельности, в свою очередь, 15% – покупке и продаже наркотических и психотропных веществ [17].

Большого всего в 2019 году преступлений с использованием криптовалют было совершено в сфере сетевого мошенничества [18].

Как уже упоминалось, криптовалютные операции считаются анонимными потому, что адреса криптовалютных кошельков, как правило, не связаны с конкретным лицом. Однако, сама цепочка транзакций, которая связана с конкретным кошельком, не является анонимной. При необходимости, конкретная цепочка транзакций может быть подвергнута анализу, в результате которого есть доля вероятности идентифицировать лицо, которому принадлежит конкретный криптовалютный кошелек по связям с другими адресами в цепочке.

Однако, существуют системы, которые позволяют сохранить криптовалютные транзакции конфиденциальными. Например, сетевая система “Blender”, которая доступна по адресу “blender.io”. Данная система предоставляет услугу скрытия адресов криптовалютных кошельков, с которых были получены криптовалютные средства. Это достигается тем, что сумма, которую необходимо “замаскировать”, делится на части и отправляется на адреса криптовалютных кошельков, которые созданы для клиента и не связаны с первым (основным)

адресом криптовалютного кошелька, где средства хранились изначально [19], что в результате запутывает следы происхождения средств. Также, как указано на сайте сетевой системы “Blender”, у системы достаточное количество резерва криптовалютных средств, что позволяет клиенту получить свои средства с начала цепочки блоков [20], и поэтому происхождения средств не будет где-либо отображаться. Сетевая система “Blender” не хранит информацию о обработанных транзакциях, все связанные данные с транзакциями стираются после того, как все криптовалютные средства отправлены на целевые адреса криптовалютных кошельков [21]. Также, надо отметить, что не ясно, какой конкретно правовой субъект обеспечивает данную услугу, так как на сайте сетевой системы “Blender” не опубликованы условия использования системы, название и регистрационный номер предприятия, адрес или какая-либо другая контактная или юридическая информация, кроме адреса электронной почты.

Основная проблема в предотвращении использовании криптовалюты в предикатных преступлениях заключается в технической трудности идентификации лица или группы лиц, которые осуществляют криптовалютные операции в незаконных целях. Такие цели могут быть направлены на легализацию денежных средств, то есть сокрытие их незаконного происхождения, совершение платежей в скрытой сети, организацию различных мошеннических схем, взломов информационных систем и другие преступления.

Поэтому, учитывая техническую специфику действия криптовалютных операций, а также упомянутые технические возможности “маскировки” происхождения криптовалютных средств, необходимо развитие способов исследования **следообразования**, выработки алгоритма установления и закрепления криминалистически значимых сведений для данного типа преступлений [22]. Для достижения упомянутого, необходима гармонизация права в этом направлении. Транзакции в сетях технологии “блокчейн” анонимны по отношению к пользователям как лицам, но не анонимны по отношению к самим транзакциям. Поэтому, сети технологии “блокчейн” с множеством транзакций могут быть подвергнуты целост-

ному и взаимосвязанному анализу, что дает возможность борьбе с предикатными преступлениями. Для совершения такого анализа необходимы специальные знания и **специальное программное обеспечение**.

Например, одно из таких программных обеспечений это “Crystal”, которое принадлежит Нидерландскому предприятию “Bitfury Group”. Данное программное обеспечение способно выявлять и отслеживать незаконную деятельность в сетях технологии “блокчейн” [23], а именно способно следующее: выявить преступную деятельность на блокчейне (позволяет определить, связан ли кошелек с системами, которые активно используются в незаконной деятельности, например, в скрытой сети, системах “маскировки” происхождения средств и так далее); выдать доказательства сделок подозреваемого (указав все адреса кошельков, которые связаны с подозреваемым, возможно определить любые попытки скрыть источник или место назначения незаконных средств); ускорить расследование киберпреступности (позволяет автоматизировано отследить наиболее подозрительных участников сети, исключив время, которое будет потрачено на ручные распутывающие транзакций и следуя неопределенным указаниям) и т.д. Упомянутое предприятие свое программное решение предлагает для правоохранительных органов и других организаций [27]. Надо отметить, что программное обеспечение “Crystal” не ограничивает свои возможности только анализом криптовалютной сети, но и способно находить и группировать информацию об адресах и сущностях сети из других источников, таких как форумов и других сайтов. Благодаря такому комплексному подходу программное обеспечение “Crystal” может раскрыть не только адрес объекта, но и его реальное имя в реальном мире [28]. Программное обеспечение “Crystal” используется в Азии, США, Европе и СНГ как финансовыми организациями, так и правоохранительными органами [29]. Примером успешной работы упомянутого программного обеспечения является борьба с вирусом “WannaCry”, в результате были отслежены платежи от жертв вируса, и установлена сущность, вымогающая платежи [27].

Существуют также и другие программные обеспечения, например, “Chainalysis”, “CipherTrace”, “CryptoFinance” и др. В основном,

задачи и функции данных программных обеспечений схожи, возможно, отличается их алгоритм анализа и получения данных [24- 26, 30]. В любом случае, учитывая, что существуют программные обеспечения, способные производить комплексный и систематизированный анализ в криптовалютной сети, а также то, что существуют реальные примеры противодействия данным программам преступной деятельности, их необходимо по мере возможности и необходимости применять в расследованиях. Также, учитывая, что расследования данной категории преступлений требует специальных знаний, необходимо осваивать и тестировать данные программы со специалистами в соответствующей области.

Надо отметить, что в случае раскрытия предикатного преступления и констатации преступных средств в виде криптовалюты, стоит вопрос в аресте, а также в дальнейшей конфискации данных криптовалютных средств. Однако, для решения этого вопроса приходится сталкиваться, как с правовыми, так и с техническими трудностями.

На данный момент нет единого правового регулирования, которое предусматривало бы порядок ареста или конфискации криптовалютных средств. Также пока что не ясно, как арестовать или конфисковать криптовалютные средства, если правоохранительным органам не известен приватный цифровой ключ криптовалютного кошелька правонарушителя.

Возможно, правонарушитель помнит и знает свой приватный цифровой ключ, однако разглашать его это не в интересах правонарушителя. Поэтому, если следствию известно, что конкретному лицу принадлежит криптовалютный кошелек с преступными криптовалютными средствами, без содействия самого правонарушителя технически арест или конфискация невозможна.

В случае невозможности ареста или конфискации криптовалютных средств, адреса криптовалютных кошельков, используемые в незаконной деятельности, можно вносить в “черные” списки, как например это делает Департамент казначейства США. Они создали “черный” список адресов криптовалютных кошельков пользователей для внедрения санкций. Дейв Мюррей экс-советник заместителя

Министра финансов США считает: “Несмотря на то, что пользователи, скорее всего, не будут использовать свои адреса после их отметки, они могут быть просто необходимы для различных финансовых институтов” [31].

Однако бывают случаи, когда криптовалютный кошелек привязан к какой-либо криптовалютной биржевой системе, тогда есть возможность обратиться с запросом правовому субъекту, который обслуживает данную криптовалютную биржевую систему, с просьбой выдать данные либо произвести арест или конфискацию, например, переведя средства правонарушителя на другой для ареста или конфискации созданный криптовалютный кошелек. Но, надо отметить, что как ранее упоминалось, не все криптовалютные биржевые системы публикуют свою контактную информацию, а также информацию о своем правовом статусе, что в результате не дает возможности обращения. Также, не всегда определена юрисдикция деятельности таких предприятий.

В случае, если правонарушитель оказывает содействие или удастся другими способами выяснить приватный цифровой ключ криптовалютного кошелька правонарушителя, самым разумным является перевод приступных криптовалютных средств на другой для ареста или конфискации созданный криптовалютный кошелек, так как оставлять средства на текущем криптовалютной кошельке нельзя. В противном случае, криптовалютные средства могут быть переведены на другие криптовалютные кошельки без ведома правоохранительных органов.

В результате можно сделать вывод, что различный и неопределённый правовой статус криптовалют в разных государствах, не способствует укреплению мер по борьбе с предикатными преступлениями. Проблематика использования криптовалют в незаконной деятельности – это проблематика не одного государства или двух, а проблематика на международном уровне, так как криптовалютные операции совершаются посредством глобальной сети “Интернет”, у которой нет каких-либо территориальных и юрисдикционных границ. Поэтому при отсутствии единого международного правового регулирования придется сталкиваться с про-

блемами определения юрисдикции действия, например, сетевых криптовалютных обменных или биржевых систем. Резюмируя, необходима разработка и создание единого международного правового регулирования криптовалют и с ними связанных операций.

Сетевые криптовалютные обменные или биржевые системы, а также другие системы, на которых оказываются какие-либо криптовалютные услуги, которые не опубликовывают на своих сайтах юридическую информацию, например, название и регистрационный номер предприятия, контактную информацию и т.д. – это системы, которые, по сути, осуществляют свою деятельность скорее всего незаконно, так как скрывают юридическую информацию о себе, или вовсе осуществляют хозяйственную деятельность не зарегистрировавшись надлежащим образом. Упомянутое, затрудняет, при необходимости, правоохранительным органам адресовать запросы в такие неопределенные организации. Возможно, что такие не добросовестные системы необходимо, по возможности, блокировать или добавлять в специальные “черные” списки.

Благодаря тому, что существует множество аналитических программных обеспечений, которые способны осуществлять комплексные анализы криптовалютных сетей, появляется больше возможностей раскрытия предикатных преступлений, в совершении которых используются криптовалюты. Поэтому тот факт, что адреса криптовалютных кошельков не связаны с конкретными лицами, не означает, что предикатные преступления, в совершении которых используются криптовалюты, не раскрываемы. Наоборот, они раскрываемы и об этом свидетельствуют множество примеров, когда в статье упомянутые программные обеспечения смогли, как идентифицировать лиц, совершивших преступление, так и отследить поток незаконных криптовалютных средств. Поэтому, рекомендуется правоохранительным органам использовать в работе такие программные обеспечения.

Также надо отметить, что решение в статье упомянутой проблемы института ареста и конфискации незаконно полученных криптовалютных средств требует международного правового подхода.

Резюмируя, поскольку, транзакции в криптовалютных сетях не анонимны, и могут быть подвергнуты комплексному анализу, а также благодаря специальным программным обеспечениям и другим методам, есть возможности противодействовать предикатным преступлениям, в совершении которых используются криптовалюты.

ЛИТЕРАТУРА

1. Reiff N. The 10 Most Important Cryptocurrencies Other Than Bitcoin. Investopedia. URL: <https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/>.

2. Top 100 Cryptocurrencies by Market Capitalization. CoinMarketCap. URL: <https://coinmarketcap.com/>.

3. Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums: Latvijas Republikas likums. *Latvijas Vēstnesis*, № 116.

4. Lībenzons A. Bitcoin un Kriptovalūtas Latvijā. Valsts ieņēmumu dienests. URL: http://www.liaa.gov.lv/files/liaa/attachments/kriptovalutas_seminars_30.01_arnis_libenzons_vid_prezentacija_par_kriptovalutam_latvija.pdf.

5. Kriptovalūtas. Valsts ieņēmumu dienests. URL: <https://www.vid.gov.lv/iv/kriptovalutas>.

6. Regulation of Bitcoin in Selected Jurisdictions. Denmark. The Library of Congress. Bitcoin Survey. URL: <http://www.loc.gov/law/help/bitcoin-survey/#denmark>.

7. Шавина Е., Каленов О., Кукушкин С. Может ли криптовалюта стать альтернативой традиционным валютам? *Экономика знаний: теория и практика*. 2017. № 4 (4). с. 93–95.

8. Руководство по применению рискориентированного подхода. Виртуальные валюты. ФАТФ / ОЭСР. 2015. URL: https://eurasiangroup.org/files/FATF_docs/ROP_Virtualnye_valuty.pdf.

9. Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют. UNODC. 2014. URL: https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_RU_Print.pdf

10. Соловьев, И. Н. Налоговые преступления. Специфика выявления и расследования. 2-е издание. 2015. Москва: Издательство “Проспект”, 226 с.

11. Konvencija par noziedzīgi iegūtu līdzekļu legalizācijas novēršanu, meklēšanu, izņemšanu un konfiskāciju. Starptautisks dokuments. *Latvijas Vēstnesis*. Nr.308/312, 23.10.1998.

12. Ляскало А. Н. Спорные вопросы соотношения предикатных преступлений и легализации (отмывания) преступных доходов. *Законодательство*. 2014. № 3. с. 51-57.

13. Зиновьева Н. С. Возможности блокчейн-технологии в раскрытии и расследовании преступлений в интернет-пространстве. *Вестник Восточно-Сибирского института МВД России*. 2018. №3 (86), с.185-190.

14. Правила использования. Bitok. URL: <https://bitok.cc/privacy.html>.

15. Доменное имя CC. HOSTLINE. URL: <https://hostline.ru/zona-cc.html>.

16. Who is hosting bitok.cc? WhoisHostingThis. URL: <https://www.whoishostingthis.com/#search=bitok.cc>.

17. Сошников А. Россия бьет рекорд за рекордом в даркнете. Что происходит? Би-би-си. URL: <https://www.bbc.com/russian/news-49007476>.

18. The Chainalysis Crypto Crime Report is Here. Download to Learn Why 2019 Was the Year of the Ponzi Scheme. Chainalysis Team. URL: <https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report>.

19. Blender.io - Advanced privacy for Bitcoin transactions (mixer). Bitcoin Forum. URL: <https://bitcointalk.org/index.php?topic=5052876.msg47020787>.

20. How does it work? Blender. URL: <https://blender.io/how>.

21. FAQ. Blender. URL: <https://blender.io/faq>.

22. Родивилин И. П., Родивилина В. А. Получение криминалистически значимой информации при расследовании преступлений, совершенных с использованием криптовалют. *Эксперт-криминалист*. 2019. №1. ISSN: 2072-442X. с. 27-29.

23. Блокчейн. Bitfury. URL: <https://bitfury.com/ru/blockchain>.

24. Petrova M., Dimitrov G. E-правосудие – гарантия эффективной судебной системы. Инициативы в Болгарии. In: *Revista Națională de Drept*. 2011, № 10-11(134), p. 169-172. ISSN 1811-0770. URL: https://ibn.idsi.md/ro/vizualizare_articol/10731

25. Petrova M., Hristov Hr. Proactive publication of information about judicial cases and acts of the court of justice. *Administrative and Criminal Justice*, Riga, 2018, Vol. 1, № 82 (2018), p. 91-109 URL: <http://journals.rta.lv/index.php/ACJ/article/view/2853/3287>

26. Petrova M. M. (2015). E-Justice system in Bulgaria: Electronic tools for E-Justice in development, *Administrative and Criminal Justice*, Riga, VOL. 4, № 73 (2015), p. 48-53, DOI: <http://dx.doi.org/10.17770/acj.v4i73.4358>

27. Crystal Clear Crypto Compliance. Crystal. URL: <https://crystalblockchain.com/>.

28. The Bitfury Group. Bitfury Launches Crystal — A Blockchain Investigative Tool for Law Enforcement and Financial Institutions. Medium. URL: <https://>

medium.com/meetbitfury/bitfury-launches-crystal-a-blockchain-investigative-tool-for-law-enforcement-and-financial-3d7712dd5dce.

29. BitfuryRussia. Bitfury Crystal: как работает и где используется наш инструмент для отслеживания подозрительных крипто-транзакций. Хабр. URL: <https://habr.com/ru/company/bitfury/blog/434282/>.

30. Petrova M. M. (2017). Integration of the information processes. Automation and unification of the judicial system, Simon Kuznets Kharkiv National University of Economics, «*Economics of Development*», ISSN 1683-1942. 2017. № 2 (82), p. 50-59.

31. Примула А. Департамент казначейства США создает список адресов криптовалютных кошельков пользователей черного списка для внедрения санкций. BITGID. URL: <https://bitgid.com/sshazavedetchernyj-spisok-polzovatelej-kriptokoshelkov/>.

REFERENCES

1. Reiff, N. The 10 Most Important Cryptocurrencies Other Than Bitcoin. Investopedia. URL: <https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/> [In English].

2. Top 100 Cryptocurrencies by Market Capitalization. CoinMarketCap. URL: <https://coinmarketcap.com/> [In English].

3. Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums: Latvijas Republikas likums. *Latvijas Vēstnesis, I/16* [In Latvian].

4. Lībenzons, A. Bitcoin un Kriptoalūtas Latvijā. Valsts ieņēmumu dienests. URL: http://www.liaa.gov.lv/files/liaa/attachments/kriptoalutas_seminars_30.01_arnis_libenzons_vid_prezentacija_par_kriptoalutam_latvija.pdf [In Latvian].

5. Kriptoalūtas. Valsts ieņēmumu dienests. URL: <https://www.vid.gov.lv/lv/kriptoalutas> [In Latvian].

6. Regulation of Bitcoin in Selected Jurisdictions. Denmark. The Library of Congress. Bitcoin Survey. URL: <http://www.loc.gov/law/help/bitcoin-survey/#denmark> [In English].

7. Shavina, E., Kalenov, O., Kukushkin, S. (2017). Mozhet li kriptoalyuta stat alternativoy traditsionnym valyutam? *Ekonomika znaniy: teoriya i praktika – Economics of knowledge: theory and practice*, 4 (4), 93–95 [In Russian].

8. Rukovodstvo po primeneniyu riskoriyentirovannogo podkhoda. Virtualnyye valyuty. (2015). FATF. OESR. URL: https://eurasiangroup.org/files/FATF_docs/ROP_Virtualnye_valyuty.pdf [In Russian].

9. Bazovoye posobiye po vyyavleniyu i rassledovaniyu otmyvaniya prestupnykh dokhodov. sovershennogo posredstvom virtualnykh valyut. (2014).

UNODC. URL: https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_RU_Print.pdf [In Russian].

10. Solovyev, I. N. (2015). Nalogovyye prestupleniya. Spetsifika vyyavleniya i rassledovaniya. Moskva: Izdatelstvo “Prospekt” [In Russian].

11. Konvencija par noziedzīgi iegūtu līdzekļu legalizācijas novēršanu, meklēšanu, izņemšanu un konfiskāciju. Starptautisks dokuments. *Latvijas Vēstnesis*, 308/312 [In Latvian].

12. Lyaskalo, A. N. (2014). Spornyye voprosy sootnosheniya predikatnykh prestupleniy i legalizatsii (otmyvaniya) prestupnykh dokhodov. *Zakonodatelstvo – Legislation*, 3, 51–57 [In Russian].

13. Zinovyeva, N. S. (2018). Vozmozhnosti blokcheyn-tehnologii v raskrytii i rassledovanii prestupleniy v internet-prostranstve. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii – Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia*, 3 (86), 185–190 [In Russian].

14. Pravila ispolzovaniya. Bitok. URL: <https://bitok.cc/privacy.html> [In Russian].

15. Domennoye imya CC. HOSTLINE. URL: <https://hostline.ru/zona-cc.html> [In Russian].

16. Who is hosting bitok.cc? Who is Hosting This. URL: <https://www.whoishostingthis.com/#search=bitok.cc> [In English].

17. Soshnikov, A. Rossiya byet rekord za rekordom v darknete. Chto proiskhodit? Bi-bi-si. URL: <https://www.bbc.com/russian/news-49007476> [In Russian].

18. The Chainalysis Crypto Crime Report is Here. Download to Learn Why 2019 Was the Year of the Ponzi Scheme. Chainalysis Team. URL: <https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report> [In English].

19. Blender.io - Advanced privacy for Bitcoin transactions (mixer). Bitcoin Forum. URL: <https://bitcointalk.org/index.php?topic=5052876.msg47020787> [In English].

20. How does it work? Blender. URL: <https://blender.io/how> [In English].

21. FAQ. Blender. URL: <https://blender.io/faq> [In English].

22. Rodivilin, I. P., Rodivilina, V. A. (2019). Polucheniye kriminalisticheski znachimoy informatsii pri rassledovanii prestupleniy. sovershennykh s ispolzovaniyem kriptovalyut. *Ekspert-kriminalist – Expert criminalist*, 1, 27-29, ISSN: 2072–442X [In Russian].

23. Blokcheyn. Bitfury. URL: <https://bitfury.com/ru/blockchain> [In Russian].

24. Petrova, M., Dimitrov, G. (2011). E-pravosudiye – garantiya effektivnoy sudebnoy sistemy. Initsiativy v Bolgarii. In: Revista Na?ional? de Drept. 10-

11(134), 169-172. ISSN 1811-0770. URL: https://ibn.idsi.md/ro/vizualizare_articol/10731 [In Russian].

25. Petrova, M., Hristov, Hr. (2018). Proactive publication of information about judicial cases and acts of the court of justice. *Administrative and Criminal Justice*, Riga, Vol. 1, 82 (2018), 91-109. URL: <http://journals.rta.lv/index.php/ACJ/article/view/2853/3287> [In English].

26. Petrova, M. M. (2015). E-Justice system in Bulgaria: Electronic tools for E-Justice in development, *Administrative and Criminal Justice*, Riga, Vol. 4, 73 (2015), 48-53, DOI: <http://dx.doi.org/10.17770/acj.v4i73.4358> [In English].

27. Crystal Clear Crypto Compliance. Crystal. URL: <https://crystalblockchain.com/> [In English].

28. The Bitfury Group. Bitfury Launches Crystal – A Blockchain Investigative Tool for Law Enforcement and Financial Institutions. Medium. URL: <https://medium.com/meetbitfury/bitfury-launches-crystal-a-blockchain-investigative-tool-for-law-enforcement-and-financial-3d7712dd5dce> [In English].

29. BitfuryRussia. Bitfury Crystal: kak rabotayet i gde ispolzuyetsya nash instrument dlya otslezhivaniya podozritelnykh kripto-tranzaktsiy. Khabr. URL: <https://habr.com/ru/company/bitfury/blog/434282/> [In Russian].

30. Petrova, M. M. (2017). Integration of the information processes. Automation and unification of the judicial system, Simon Kuznets Kharkiv National University of Economics, «*Economics of Development*», ISSN 1683-1942, 2 (82), 50–59 [In English].

31. Primula, A. Departament kaznacheystva SSHa sozdayet spisok adresov kriptovalyutnykh koshelkov polzovateley chernogo spiska dlya vnedreniya sanktsiy. BITGID. URL: <https://bitgid.com/ssha-zavedet-chernyj-spisok-polzovatelej-kriptokoshelkov/> [In Russian].

Токарева Катерина Олеівна

кандидат юридичних наук, старший науковий співробітник НДІ правового забезпечення інноваційного розвитку НАПрН України, доцент кафедри правоохоронної діяльності та поліціїстики Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ПРО ДЕРЖАВНЕ ФІНАНСУВАННЯ ІННОВАЦІЙ В УКРАЇНІ