CZU 343.7:004.056
DOI: https://doi.org/10.52388/1811-0770.2021.1(243).06

О КРИМИНОЛОГИЧЕСКИХ ПРИЗНАКАХ КРИПТОПРЕСТУПНОСТИ

Evgheni FLOREA
Doctor în drept, conferențiar universitar, Universitatea de Stat din Comrat, or. Comrat, Republica Moldova,
Head of Compliance Department, Quan2um OU cryptoexchange platform, Tallinn, Estonia
e-mail: *florya@yahoo.com*
https://orcid.org/0000-0001-7236-0695

Научно-технический прогресс, помимо неоспоримых преимуществ для развития общества, привел к появлению новых рисков и криминальных угроз. Некоторые инновации находятся на пересечении нескольких научных областей и требуют специальных знаний в каждой из них, чтобы успешно выявлять, регистрировать и расследовать незаконное поведение, связанное с этими технологиями. Одним из таких нововведений является технология блокчейн и концепция цифровой валюты или криптовалюты. Данная статья посвящена анализу криминологических характеристик нового явления, появившегося после развития технологии блокчейн и криптовалют, а именно преступности в сфере криптовалют. Автор анализирует признаки криптопреступности, такие как ее транснациональный характер, виртуальность, организованность, тщательная подготовка совершения деяния с использованием методов и средств кибершпионажа, дисперсность, самодетерминация, использование механизмов блокчейн для легализации незаконно приобретенных средств и др. Выводы автора касаются необходимости вооружить юристов специальными знаниями в области блокчейн и криптовалютных технологий. Это связано с тем, что Молдова может стать благоприятной юрисдикцией для совершения криптопреступлений. Оперативное вмешательство властей в такие угрозы будет способствовать устранению / снижению возможных криминальных рисков.

Ключевые слова: *блокчейн, цифровая валюта, криптовалюта, криптопреступность, признаки криптопреступности, киберпреступность, трансграничная преступность.*

DESPRE SEMNELE CRIMINOLOGICE ALE CRYPTOCRIMINALITĂȚII

Progresul științific și tehnologic, pe lângă avantajele incontestabile pe care le are pentru dezvoltarea societății, a condus la apariția unor noi riscuri și amenințări criminale. Unele inovații se află la intersecția mai multor domenii științifice și necesită cunoștințe speciale în fiecare dintre ele, pentru a identifica cu succes, a înregistra și a investiga comportamentul ilegal asociat acestor tehnologii. O astfel de inovație este tehnologia blockchain și conceptul de monedă digitală sau cryptomonedă. Prezentul articol este dedicat analizei caracteristicilor criminologice ale unui fenomen nou care a apărut în urma dezvoltării tehnologiei blockchain și cryptovalutelor și anume a infracționalității în domeniul cryptovalutar. Autorul analizează semnele cryptocriminalității, precum ar fi caracterul transnațional al acesteia, virtualitatea, caracterul organizat, pregătirea detaliată cu folosirea metodelor și mijloacelor de ciberspionaj, caracterul dispersat, autodeterminarea, folosirea mecanismelor blockchain pentru legalizarea mijloacelor dobândite pe cale ilegală etc. Concluziile autorului abordează necesitatea de a înarma juriștii cu cunoștințe speciale privind tehnologiile blockchain și cryptomoneda. Acest lucru se datorează faptului că Moldova poate deveni o jurisdicție favorabilă pentru cripto-infracțiuni. Intervenția rapidă a autorităților la astfel de amenințari va contribui la eliminarea/reducerea posibilelor riscuri criminale.

Cuvinte-cheie: *blockchain, monedădigitală, cryptovalută, cryptocriminalitate, semnele cryptocriminalității, cibercriminalitate, criminalitate transnațională.*

ABOUT THE CRIMINOLOGICAL SIGNS OF CRYPTOCRIMES

In addition to the undeniable advantages that it has for the development of society, scientific and technological progress, has led to the emergence of new criminal risks and threats. Some innovations are at the intersection of several academic fields and require special knowledge in each of them in order to successfully identify, record and investigate the illegal behavior associated with these technologies. One such innovation is blockchain technology and the concept of digital currency or crypto currency. This article is devoted to the analysis of the criminological characteristics of a new phenomenon that arose as a result of the development of blockchain technology and crypto currencies, namely crime in the field of cryptocurrency. The author analyzes the signs of cryptocrime, such as its transnational character, virtuality, organized character, detailed preparation with the use of methods and means of cyber espionage, dispersed character, self-determination, use of blockchain mechanisms to launder illegally acquired means, etc. The author's conclusions address the need to arm legal practitionerswith special knowledge of blockchain and cryptocurrency technologies. This is due to the fact that Moldova can become a favorable jurisdiction for of cryptocrimes. Rapid intervention by the authorities to such threats will help to eliminate / reduce possible criminal risks.

Keywords: *blockchain, digital currency, cryptocurrency, cryptocrime, signs of cryptocrime, cybercrime, transnational crime.*

SUR LES SIGNES CRIMINOLOGIQUES DE CRYPTOCRIMES

Le progrès scientifique et technologique, outre les avantages indéniables qu'il a pour le développement de la société, a conduit à l'émergence de nouveaux risques et menaces criminels. Certaines innovations sont à l'intersection de plusieurs domaines scientifiques et nécessitent des connaissances particulières dans chacund'eux, afin de réussir à identifier, enregistrer et enquêter sur le comportement illégal associé à ces technologies. Une de ces innovations est la technologie blockchain et le concept de monnaie numérique ou de crypto-monnaie. Cet article est consacré à l'analyse des caractéristiques criminologiques d'un nouveau phénomène apparu à la suite du développement de la technologie blockchain et des crypto-monnaies, à savoir la criminalité dans le domaine de la crypto-monnaie. L'auteur analyse les signes de la cryptocrime, tels que son caractère transnational, sa virtualité, son caractère organisé, sa préparation détaillée à l'aide de méthodes et de moyens de cyberespionnage, son caractère dispersé, son autodétermination, l'utilisation de mécanismes de blockchain pour légaliser des moyens acquis illégalement, etc. Les conclusions de l'auteur traitent de la nécessité d'armer les experts juridiques avec des connaissances particulières sur les technologies blockchain et crypto-monnaie. Cela est dû au fait que Moldova peut devenir une juridiction favorable pour les crypto-crimes. Une intervention rapide des autorités face à de telles menaces contribuera à éliminer / réduire les risques criminels éventuels.

Mots-clés: *blockchain, monnaie numérique, crypto-monnaie, crypto-criminalité, signes de crypto-criminalité, cybercriminalité, criminalité transnationale.*

Введение

Научно-технический прогресс, стремительно набравший обороты в первые десятилетия XXI века, помимо несомненных плюсов для экономического развития общества, повлёк за собой возникновение новых криминальных рисков и угроз, к которым правоохранительные органы многих государств оказались не вполне готовы. Некоторые инновации находятся на пересечении сразу нескольких научных сфер и требуют специальных познаний в каждой из них для успешной идентификации, регистрации и расследования противоправного поведения, связанного с данными технологиями. Одной из таких инноваций является технология блокчейн и основанная на ней концепция цифровых денег или криптовалюты. Для понимания данного инновационного продукта необходимо иметь представление о таких разных сферах как экономика, финансы, криптография, банкинг, программирование и

технология распределённых реестров. В рамках настоящего исследования мы рассмотрим основные криминологические особенности преступных проявлений в криптовалютной сфере которые неизбежно возникли и развились в сфере цифровых активов и являются своего рода платой общества за научно-технический прогресс. Под ***преступностью в криптовалютной сфере (криптопреступностью)*** мы понимаем вид финансовой киберпреступности, состоящий в совокупности общественно опасных и запрещённых уголовным законом деяний, совершённых при создании, обороте и уничтожении криптоактивов, а также при их использовании как средства совершения преступления.

Криптопреступность, как и любое социально-негативное явление, характеризуется определёнными специфическими свойствами, позволяющими глубже понять природу этого феномена и отделить его от смежных категорий. По нашему мнению, преступные проявления в криптовалютной сфере обладает следующими отличительными свойствами:

Транснациональный (трансграничный) характер

Этот признак означает, что деяния такого рода одновременно затрагивают юрисдикции двух и более государств. Криптопреступникам свойственно игнорирование государственных границ, международного и национального законодательства. Транснациональный аспект криптопреступности может проявляться в следующих формах:

- совершение преступления на территории двух или более государств. Преступник может находиться в одной стране, его жертва – в другой, а полученные в результате совершения преступления средства могут быть обналичены в третьей.

- преступление совершается в одном государстве, а действия по его подготовке, планированию и организации – в другом;

- преступное деяние совершается в одном государстве, а его последствия (материальный ущерб, дезорганизация нормальной деятельности предприятия, учреждения, организации) наступают в другом;

- члены преступной организации (преступного сообщества) могут действовать координированно, находясь на территории различных государств.

Транснациональная специфика Интернет-пространства, его глобальный характер, требуют оперативного взаимодействия правоохранительных органов различных стран в целях предупреждения преступной деятельности в данной сфере. Однако, приходится констатировать, что у преступности, действующей в сети интернет, существует явное преимущество перед органами правопорядка. Как правило, из-за бюрократических преград координация работы правоохранительных органов различных стран требует значительного времени. Иногда это занимает месяцы или даже годы. Если в странах разная нормативная база, то такое сотрудничество ещё более усложняется. В случае, когда необходимо взаимодействие представителей правоохранительных органов трёх и более юрисдикций, то результативность такого сотрудничества стремится к нулю. В свою очередь, члены преступной группы из разных стран общаются в реальном времени.

Кроме того, представители криминалитета умело используют политические противоречия между государствами. Так, например, специалисты по кибербезопасности отмечают, что многие российские киберпреступники перебираются на Украину, а украинские – в Россию. Российские хакеры, находясь на территории Украины, совершают преступления против российских финан-

совых учреждений, а украинцы, в свою очередь, находясь на территории РФ, атакуют украинские финансовые учреждения. При этом, и те, и другие остаются безнаказанными [1; с. 124].

Виртуальность

Признак наличия физической дистанции между преступником и его жертвой. Это свойство открывает новые горизонты для криминалитета и создаёт значительные психологические преимущества для правонарушителей, которые не существуют для них в реальном мире. Если мы говорим о социальной инженерии, то, в случае разоблачения, злоумышленник, действующий в киберпростанстве, легко прекращает контакт с потенциальной жертвой без каких-либо негативных последствий для себя. При непосредственном контакте с потерпевшим существует целый ряд рисков, которые потенциальному преступнику нужно учитывать:

– даже при «удачном» стечении обстоятельств, злоумышленника могут запомнить в лицо либо он может попасть на камеру видеонаблюдения;

– не исключено вмешательство третьих лиц, которые помешают совершению преступления;

- разоблачение может привести к непредсказуемой реакции, вплоть до насилия в отношении мошенника как со стороны жертвы, так и третьих лиц.

Все эти сложности совершения преступления в реальном мире не имеют никакого значения в сети Интернет. Как отмечают психологи, в виртуальном пространстве теряет свое значение ряд барьеров общения, связанных с полом, возрастом, социальным статусом, внешней привлекательностью или непривлекательностью, а также невербальной составляющей коммуникативной компетентности партнеров; возникает возможность создавать о себе любое впечатление по своему выбору, при этом обогащаются возможности ... конструирования образа по своему выбору» [2; с. 60].

В этом контексте, необходимо упомянуть технологию Deepfake, которая, по мнению IT-аналитиков, может стать самой опасной в цифровой сфере за последние десятилетия. Данная технология применяет возможности искусственного интеллекта для синтеза человеческого изображения, она объединяет несколько снимков, на которых человек запечатлён с разных ракурсов и с разным выражением лица, и делает из них видеопоток [3].

Первое время большинство случаев использования Deepfake выглядело просто как шалость – они представляли собой видеоматериалы, созданные с использованием бесплатных инструментов и содержавшие лица знаменитых людей, наложенные на порнографические ролики. Однако через несколько лет данная технология развилась настолько, что создаваемые с её помощью материалы стали пугающе убедительными. Широкую известность она получила после того, как один из пользователей социальной сети Reddit разместил видео, где лицо актрисы из порнофильма правдоподобно заменили на лицо известной американской актрисы Галь Гадот [3]. Вне всяких сомнений, технология Deepfake представляет серьёзную криминальную угрозу, выходящую далеко за пределы безопасности криптовалютных операций. Уже появились случаи дискредитации знаменитостей, фото которых легко отыскать в интернете. Технология Deepfake может быть использована в политике с целью дискредитации отдельных деятелей и целых партий, чтобы манипулировать общественным мнением, влиять на выборы или даже на финансовый рынок. Одно сообщение в Twitter, сделанное Илоном Маском, подняло почти на 30% стоимость одной из криптовалют [4]. Именно по этой причине не следует исключать, что такой инструмент, как техноло-

гия Deepfake, заинтересует криминальные структуры, которые захотят использовать его в своих целях. Отметим, что самая популярная программа в этой сфере, вместе с демонстрацией своих возможностей (DeepFaceLab) находится в свободном доступе в сети Интернет [5].

Помимо подделки изображения, появились и технологии подделки голосов, построенные по такому же принципу. Они способны, при наличии образца, достоверно имитировать голос того или иного человека. Уже были случаи использования этой технологии в преступных целях, а именно для того, чтобы путём обмана убедить жертву-сотрудника компании осуществить какие-то действия в пользу злоумышленника – перевести деньги, отправить документы, передать банковские реквизиты и т.д. (т.н. целевой фишинг - англ. *spearphishing*) [6].

Организованный характер

Совершение криптопреступления – сложная многоэтапная деятельность, требующая значительного времени на подготовку, планирование и реализацию преступной цели. Это вызывает необходимость создания иерархической структуры, функционального распределения ролей и согласования общей стратегии преступного объединения. Для осуществления такой деятельности потребуются обширные познания в сфере систем безопасности и контроля, электронных и криптофинансов, программирования, психологии и социальной инженерии. Подобные «криминальные проекты» осуществляет не случайная группа преступников, а хорошо подготовленные организации, имеющие своих генеральных и локальных менеджеров, аналитиков, технарей, шпионов. По сути, речь идёт о корпоративном сетевом криминальном бизнесе со всеми его атрибутами и свойствами. Поэтому в одиночку совершить такого рода преступления очень непросто. Согласно докладу исследовательской компании Chainalysis, всего две группы хакеров, обозначенные в исследовании как «Альфа» и «Бета», провели 60% всех зарегистрированных взломов криптобирж и суммарно похитили криптовалюты на сумму более $1 миллиарда [7]. Следует также отметить нацеленность организованных киберкриминальных корпораций на сверхприбыль. По данным того же доклада, хакеры из названных групп в среднем крадут криптоактивы на $90 миллионов за раз, но увеличилось и количество «незначительных краж» на $20−$30 миллионов [7]. Поэтому и традиционная организованная преступность, видя повышенную «прибыльность» криминальной деятельности в киберпространстве по сравнению с офлайн способами криминального обогащения, переходит в Интернет-пространство или расширяется за счёт него.

Тщательная подготовка с использованием способов и средств кибершпионажа

Также и называемый *e-espionage,* кибершпионаж используется с целью поиска потенциальных жертв, сбора персональной и иной информации об объектах криминального интереса. Причём следует констатировать значительное усовершенствование такой подготовки. Наравне с несанкционированным доступом к личным данным потенциальной жертвы, предполагающим использование вредоносных и шпионских программ, применяются и более тонкие способы получения необходимой злоумышленникам информации. В частности, криминалом активно используется ***киберразведка*** (cyber intelligence или open source intelligence – OSINT), состоящая в изучении и анализе информации из открытых источников. Такие данные, как поведение лица в социальных сетях, его публичная активность, могут многое рассказать о потенциальной жертве. Объём информации, который можно получить в сети Интернет из

открытых источников, весьма значителен. Можно узнать о ближайшем окружении жертвы, её привычках, психологических особенностях, распорядке дня, наличии кредитов, географическом расположении, контактных данных и т.д. [8] В открытом доступе существует программное обеспечение, позволяющее, собрать вместе все данные с вебсайта компании. Например, программа Maltego позволяет собрать в единую систему IP-адреса, домены, электронные адреса, телефоны всех сотрудников фирмы. Результат предоставляется в виде дерева, позволяющего увидеть важные взаимосвязи и сделать необходимые выводы [9]. Другая, находящаяся в открытом доступе программа, – Spyse – предоставляет пользователю техническую информацию о вебсайте, в том числе об его уязвимостях [9].

В отличие от кибершпионажа, являющегося противозаконным, изучение информации из открытых источников, само по себе, в отрыве от будущего преступления, чрезвычайно проблематично инкриминировать злоумышленникам. В целом прослеживается очевидная тенденция стирания грани, размывания различий, между допустимым и незаконным сбором информации в сети о тех или иных физических лицах или компаниях. Представляется, что главным критерием, позволяющим разграничить правомерные и противоправные действия в этой плоскости, являются цели сбора такой информации. Если преследуются преступные цели, то сбор информации даже из открытых источников подпадает под признаки подготовительной деятельности к преступлению.

Дисперсность (политаргетированность)

Указанный признак связан с нацеленностью преступлений на неопределённо широкий круг потерпевших. В первую очередь это относится к таким видам криптопреступности как фишинг (phishing) и мошенничество, связанное с первичным размещением валют (ICO). Как в первом, так и во втором случае, злоумышленники не знают своих потенциальных жертв. При фишинге рассылка, призывающая пользователя перейти на сайт преступника и ввести данные своего счёта (кошелька), рассылается на максимальное количество электронных адресов. Обман, связанный с ICO, как правило, имеет признаки финансовой пирамиды под формой публичного привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют. Следует заметить, что при фишинге представители преступного мира стали больше использовать «личностный подход» в плане выбора жертвы атаки. Это требует больше усилий и подготовки, однако криминальные дивиденды оказываются значительно выше. Поэтому простой фишинг всё чаще вытесняется спирфишингом (*spearphishing*), т.е. вредоносные сообщения рассылаются не всем подряд, а заранее определённой и тщательно изученной группе лиц, которые представляют интерес для преступников. В данном случае речь идёт о держателях криптовалютных кошельков, либо сотрудниках компаний, работающих с криптоактивами. Указанному виду преступлений в большинстве случаев предшествует кража персональных данных потенциальных жертв.

Самодетерминация

Это свойство криминальных проявлений в криптовалютной сфере означает их способность к самовоспроизводству. Криптопреступность – не просто множество совершаемых за определённый промежуток времени и на определённой территории преступлений. Как уже подчёркивалось, это явление характеризуется едиными системными свойствами [10; с. 87]. В свою очередь, данная система характеризуется способно-

стью к самовоспроизводству и самосохранению. Профессор А.И. Долгова, говоря о самодетерминации преступности, отмечает, что «это признак системы, заключающийся в воссоздании структур и связей между ними; постоянный процесс поддержания равновесия системы с окружающей средой. Это базовое свойство системы, без которого она прекратила бы свое существование» [11; с. 8]. Следовательно, криптопреступность, являющаяся сегментом общей преступности, – это не временное явление, а закономерный, естественный побочный продукт бурного развития новых технологий, негативная сторона этого процесса, которая будет существовать, развиваться и изменяться вместе и параллельно с существованием, развитием и изменением блокчейн-технологий в сфере криптовалют.

Главными внутренними источниками воспроизводства криптопреступности следует признать:

- гиперлатентность, формирующая ощущение безнаказанности у лиц, совершающих криптопреступления. В криминологии известно понятие так называемого «криминального куража», т.е. психологической закономерности, согласно которой одно удачно совершённое и нераскрытое преступление порождает ещё одно или несколько последующих нарушений уголовного закона, причём, как правило, более дерзких, наносящих больший ущерб и с вовлечением большего числа преступников.

- необходимость совершения так называемых предикатных преступлений для того, чтобы были созданы необходимые условия реализации преступного замысла. К данной категории следует отнести создание вредоносных программ, кражу личных данных, взлом компьютеров и компьютерных сетей.

- конвейерный характер совершаемых преступлений, когда они превращаются в главный, а иногда единственный, источник дохода для лиц, вовлечённых в этот вид криминальной деятельности [12; с. 9].

Постоянный мониторинг и оперативное внедрение новейших цифровых технологий

Научно-технический прогресс – объективное явление, которое нельзя остановить. Однако отсутствие должного контроля за доступом к инновациям, либо неспособность государства предвидеть негативные последствия, которые могут вызвать те или иные технологии, провоцируют рост преступлений с использованием новейших достижений научно-технического прогресса. Свободный доступ к таким технологиям, как Deepfake, Maltego, Spyce и многим другим, появляющимся практически каждый день разработкам, представляет реальную угрозу для безопасности общества. По всей видимости, следует признать криминологической аксиомой принцип, согласно которому, в гонке за инновациями криминалитет всегда будет впереди органов, призванных бороться с преступностью. Преступники, в отличие от тех, кто должен им противостоять, не обременены бюрократическими, организационными, юрисдикционными барьерами и преградами, поэтому они быстрее осваивают новейшие технологии. Такая технологическая адаптированность, характерная не только для криптопреступности, но и для всей киберпреступности, влечёт за собой постоянное совершенствование путей и способов извлечения криминальных доходов, причём интервал времени, необходимый преступникам для освоения и использования новейших технологий заставляет говорить о практически моментальной «перезагрузке» [13; с. 10] преступности, которая с каждым разом становится менее уязвимой и более опасной.

Использование особых блокчейн-механизмов для легализации незаконно полученных средств

Для некоторых технологий блокчейн-индустрии анонимность является главным приоритетом. Это обеспечивает защищённость персональных данных и конфиденциальность финансовых сделок, но, с другой стороны, неизбежно порождает повышенные криминальные риски, связанные с отмыванием преступных средств и финансированием терроризма. Например, такие криптомонеты как Monero, Zcash, Dash используют специальные криптографические протоколы, которые значительно усложняют отслеживание данных транзакций. Адрес кошелька такой валюты может раскрыть только его непосредственный владелец [14]. Проблема существует и в сфере обмена криптовалют. Если крупные площадки находятся в правовом поле, а значит соблюдают KYC (*know your customer* – знай своего клиента) и AML (*anti-money laundering* – противодействие отмыванию денег) требования регуляторов, то децентрализованные биржи (*Decentralized Exchange* - DEX), бум на которые начался в 2020 году, не требуют верификации клиентов и, в целом, практически не поддаются контролю [15]. Наконец, серьёзной головной болью для структур, отслеживающих незаконные финансовые потоки, являются Bitcoin-миксеры [16] или Bitcoin-тумблеры, которые дробят криптовалютный поток клиента на огромное количество «ручейков» и пропускают его через тысячи адресов, смешивая с чужими средствами, чтобы потом снова соединить его в одном месте. На выходе клиент получает ту же сумму за вычетом небольшой комиссионной платы. Очевидно, что определение реального владельца денежных средств после прохождения такой процедуры практически невозможно.

Чрезвычайно высокий уровень латентности (гиперлатентность)

Данное свойство преступлений в криптовалютной сфере имеет как объективные, так и субъективные причины. Главная объективная причина состоит в том, что жертвы криптопреступлений не видят смысла обращаться в правоохранительные органы, поскольку сомневаются в том, что могут получить необходимую защиту. По данным некоторых специалистов, в случае обычных преступлений пострадавшие обращаются в полицию в 80–90% случаев, тогда как при компьютерных преступлениях этот показатель составляет примерно 15–20% случаев [17; с.130].

Субъективный характер латентности криптопреступлений обусловлен недостаточной квалификацией правоохранительных структур в сфере кибербезопасности. Для регистрации, расследования и раскрытия криптопреступлений необходима специальная подготовка. Без знаний специфики функционирования продуктов блокчейн-технологии весьма сложно противостоять этой угрозе. На сегодняшний день в мире практически нигде нет системной подготовки специалистов по борьбе с криптопреступностью. Поэтому существует острая нехватка профессионалов по обнаружению и расследованию преступлений такого рода, отсутствуют методики расследования IT преступлений, нет эффективных и современных информационно-аналитических разработок. Всё это весьма красноречиво отражают цифры, озвученные в докладе The Global Risks Report 2020, согласно которому вероятность привлечения к уголовной ответственности киберпреступников в США составляет 0.05% [18]. С учётом того, что Соединённые Штаты являются одним из мировых технологических лидеров, то едва ли в других государствах ситуация в этом плане намного лучше.

Выводы

Явление, которое рассматривается в настоящем исследовании, относится к категории ультрасовременных высокотехнологичных преступных проявлений. В мире уже сформировался объёмный рынок поставщиков и потребителей услуг и продуктов глобальной криптовалютной индустрии, которыми активно пользуются не только законопослушные граждане, но и криминалитет. Республика Молдова не является исключением из этого вывода, о чём свидетельствуют конкретные примеры [19]. Представляется необходимым в рамках подразделений правоохранительных органов, занимающихся выявлением и расследованием киберпреступлений, обеспечить подготовку специалистов, имеющих специальные знания в сфере блокчейн-технологий и криптовалют. На данном этапе, ввиду отсутствия национальной законодательной базы и разработанных техник по противодействию преступности данного вида, Молдова может стать благоприятной юрисдикцией для совершения криптопреступлений. Своевременная реакция властей на возникшую угрозу позволит если не полностью устранить возможные криминальные риски, то, по меньшей мере, снизить на порядок их уровень.

Библиография

1. Выступление генерального директора компании Group-IB Ильи САЧКОВА на заседании круглого стола *Высокотехнологичная преступность: новые вызовы для общества, государства и бизнеса* // Индекс безопасности. Научно-практический журнал ПИР-центра (Центра политических исследований *Р*оссии). № 1-2 (116-117), Том 22. Москва, 2016.

2. ЖИЧКИНА, А. *Социально-психологические аспекты общения в Интернете*. Цит. по КУЗНЕЦОВА, Ю. М., ЧУДОВА, Н. В. *Психология жителей Интернета*. – М.: Издательство ЛКИ, 2008.

3. ПАНАСЕНКО, А. *Технологии Deepfake как угроза информационной безопасности*//Anti-Malware.ru – 08.04.2020 [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/Deepfakes-as-a-information-security-threat (дата обращения: 01.02.2021).

4. *После твита Илона Маска цена Dogecoin выросла почти на 30%* // РосБизнесКонсалтинг – 21.12.2020. [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/crypto/news/5fe055c99a79476879ca33a9 (дата обращения: 01.02.2021).

5. iperov/DeepFaceLab//GitHub. [Электронный ресурс]. – Режим доступа: https://github.com/iperov/DeepFaceLab (дата обращения: 01.02.2021).

6. ПАНАСЕНКО, А. *Технологии Deepfake как угроза информационной безопасности* // Anti-Malware.ru – 08.04.2020 [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/Deepfakes-as-a-information-security-threat (дата обращения: 01.02.2021).

7. *Crypto Crime Series: Decoding Hacks*//Chainalysis – 28.01.2019. [Электронный ресурс]. – Режим доступа: https://blog.chainalysis.com/reports/crypto-crime-hacks (дата обращения: 01.02.2021).

8. BAZZELL, M. *Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information*. Eighth Edition. Createspace Independent Publishing Platform, US, California. 2021.

9. KORZUN, V. *Навыки OSINT (Интернет-разведки) в кибербезопасности* // Proglib – 14.11.2020. [Электронный ресурс]. – Режим доступа: https://proglib.io/p/navyki-osint-internet-razvedki-v-kiberbezopasnosti-2020-11-14 (дата обращения: 04.02.2021).

10. 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.

11. ДОЛГОВА, А. И. *Криминологические оценки организованной преступности и коррупции, правовые баталии и национальная безопасность.* Москва: Российская криминологическая ассоциация, 2011.

12. МАКАРОВ, В. В. *Криминологическое исследование самодетерминации преступности.* Автореф. дис. ... канд. юрид. наук. М., 2014.

13. КОРЧАГИН, А. Г., ЯКОВЕНКО, А. А. — *Криминогенная роль криптовалюты* // Юридические исследования. – 2020. – № 2. [Электронный ресурс]. – Режим доступа: https://nbpublish.com/library_read_article.php?id=32096 (дата обращения: 04.02.2021).

14. ДЖИГИЛО, И. *Лучшие анонимные криптовалюты в 2021 году* // Cryptonisation.ru – 07.02.2021. [Электронный ресурс]. – Режим доступа: https://cryptonisation.ru/luchshie-anonimnye-kriptovalyuty/ (дата обращения: 07.02.2021).

15. *Что такое децентрализованные финансы (DeFi)?* // ForkLog – 29.07.2020. [Электронный ресурс]. – Режим доступа: https://forklog.com/chto-takoe-detsentralizovannye-finansy-defi/ (дата обращения: 07.02.2021).

16. *Биткойн-миксер* // Wikipedia – 19.11.2020. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82%D0%BA%D0%BE%D0%B9%D0%BD-%D0%BC%D0%B8%D0%BA%D1%81%D0%B5%D1%80 (дата обращения: 07.02.2021).

17. Выступление эксперта расширенной рабочей группы по реформированию МВД Елены Лариной на заседании круглого стола *Высокотехнологичная преступность: новые вызовы для общества, государства и бизнеса*//Индекс безопасности. Научно-практический журнал ПИР-центра (Центра политических исследований *Р*оссии). № 1-2 (116-117), Том 22. Москва, 2016.

18. *The Global Risks Report 2020.* 15th Edition. World Economic Forum. Geneva. - P.63. [Электронный ресурс]. – Режим доступа: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (дата обращения: 07.02.2021).

19. *В Молдове за мошенничество с биткоинами арестованы члены ОПГ* // ForkLog – 12.03.2021. [Электронный ресурс]. – Режим доступа: https://forklog.com/v-moldove-za-moshennichestvo-s-bitkoinami-arestovany-chleny-opg/ (дата обращения: 14.03.2021).