Вопросы применения новых технологий в противодействии кибертерроризму*

*Антонян Е. А.***

Ключевые слова: *киберугрозы, блокчейн-технологии, система предупреждения, использование компьютеров, компьютерная информация, международный уровень, нормативные акты.*

Аннотация. *В статье рассматриваются новые технологии противодействия кибертерроризму, который направлен на дестабилизацию общественного порядка, масштабное нарушение работы коммуникационных систем, устрашение путем навязывания своей воли, в том числе, властным структурам и, в целом, представляет повышенную угрозу национальной и информационной безопасности государства. Особое внимание уделено блокчейн-технологии, которая позволяет скрыть средства, направленные на финансирование террористической деятельности, в том числе, в информационном пространстве.*

DOI: 10.21681/2226-0692-2020-1-51-55

В современный период в целом сформировалась общая система нормативных правовых актов в сфере противодействия киберэкстремизму и кибертерроризму. Прежде всего, следует отметить важность основополагающих документов Организации Объединенных Наций (далее — ООН), определяющих основы сотрудничества в сфере предупреждения преступности в целом. При этом подчеркнем, что «ООН со времени своего основания активно участвует в разработке и распространении признанных на международном уровне принципов в области предупреждения преступности и уголовного правосудия»[1].

К документам, определяющим основные положения (принципы) предупреждения преступности и международного сотрудничества, следует отнести: Декларацию ООН о преступности и общественной безопасности (резолюция 51/60 Генеральной Ассамблеи от 12 декабря 1996 г); Венскую декларацию о преступности и правосудии: ответы на вызовы XXI века (резолюция 55/59 Генеральной Ассамблеи ООН от 4 декабря 2000 г.; Руководящие принципы для предупреждения преступности (резолюция 2002/13 Экономического и Социального Совета от 24 июля 2002 г.); Бангкокскую декларацию о взаимодействии и ответных мерах: стратегические союзы в области предупреждения преступности и уголовного правосудия (резолюция 60/177 Генеральной Ассамблеи ООН от 16 декабря 2005 г.); Салвадорскую декларацию о комплексных стратегиях для ответа на глобальные вызовы: система предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире (резолюция 62/230 Генеральной Ассамблеи ООН от 21 декабря 2010 г.) и др. Вообще, на различных мероприятиях ООН многие годы находят обсуждение вопросы, связанные с угрозой киберпреступности. Так, начиная с XIII Конгресса ООН по предупреждению преступности и обращению с правонарушителями в 1990 г. эта организация занимается рассмотрением различных процессов в сферах, связанных с использованием компьютеров, но до настоящего времени ООН не разработан и не принят документ, который бы был посвящен именно противодействию киберпреступности в современных условиях, т. е. отвечал бы потребностям современного общества и новым вызовам преступности.

Советом Европы, авторитетной международной региональной организацией, принят ряд документов, устанавливающих основополагающие положения в сфере борьбы с преступностью; наиболее важным из этих документов является Конвенция о преступности в сфере компьютерной информации (Будапешт, 2001 г.), где подчеркивается важность укрепления сотрудничества между государствами, нацеленного на защиту общества от преступности в сфере компьютерной информации.

[1] Сборник стандартов и норм Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, Нью-Йорк, 2016 г. С. 5.

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16175 «Блокчейн-технологии противодействия рискам кибертерроризма и киберэкстремизма: криминолого-правовое исследование».

** ***Антонян Елена Александровна***, доктор юридических наук, профессор, профессор кафедры криминологии и уголовно-исполнительного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация,
E-mail: antonyaa@yandex.ru

СНГ, региональной международной организацией, также приняты документы, определяющие основы предупреждения преступности и сотрудничества, в том числе в сфере компьютерной информации. В частности, Соглашение о сотрудничестве государств-участников Содружества Независимых государств в борьбе с преступностью 1998 г. и Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации.

Очевидно, что именно на международном уровне необходимо развивать правовую базу с учетом современных реалий, глобальных угроз мировому сообществу, которыми являются киберпреступность, кибертерроризм, киберэкстремизм. Учеными предлагаются новые подходы к пониманию роли права в условиях киберугроз и киберрисков, которые детерминируют создание новой киберреальности, требующей своевременного правового регулирования [1, 2, 4, 8, 9].

В Российской Федерации действует ряд нормативных правовых актов в сфере противодействия киберпреступности, кибертерроризму и киберэкстремизму. Вместе с тем отсутствует единый нормативный правовой акт, регулирующий данный вид правоотношений, что свидетельствует об отсутствии единых подходов, целей, задач в сфере противодействия киберугрозам. Прежде всего, укажем на Федеральные законы «О противодействии терроризму» от 6 марта 2006 г. № 35-ФЗ (в ред. от 18.04.2018 г.) и «О противодействии экстремистской деятельности» от 25 июля 2002 г. № 114-ФЗ (в ред. от 28.11.2018 г.), в которых установлены основные принципы противодействия терроризму и экстремизму, правовые и организационные основы профилактики терроризма и экстремизма.

К настоящему времени отсутствуют, прежде всего на международном уровне, нормативные правовые акты, которые бы отражали проблему киберпреступности в целом и кибертерроризма и киберэстремизма в частности. Именно в международных правовых актах должны быть предусмотрены комплексные и эффективные меры по противодействию им, которые должны быть реализованы в национальном законодательстве различных государств, включая международное сотрудничество. Следует учитывать и трансдисциплинарный подход, при которой происходит качественное изменение правовой политики [10, с. 92].

В течение последних лет происходящие в мире процессы цифровизации и глобализации позволили почти каждому человеку пользоваться инновационными явлениями современности. Это значительно облегчило взаимодействие людей в обществе, однако одновременно с этим современные технологические достижения человечества используются и в целях нарушения законодательства, создав в мире новые технологии преступной деятельности. Опора на достоинства информационно-цифровых технологий, как главный признак новых форм преступных деяний, закономерно потребовала от систем национальной безопасности стран мира новых форм противодействия.

Одной из таких угроз совершенно нового типа является, например, применение криптовалюты в целях финансирования террористических и экстремистских организаций. Криптовалюта — это полностью виртуальная валютная единица, не имеющая физических эквивалентов и реализованная сегодня в форме «биткойна». Биткойн полностью независим от государств и банковских систем. Особенным элементом этой платежной системы является базовая программа-клиент. Запущенные на множестве компьютеров программы-клиенты соединяются между собой в одноранговую сеть, и никто не может ее арестовать даже временно, а отследить финансовые операции крайне сложно. При этом отправка биткойна с одного кошелька на другой полностью анонимна. Не удивительно, что эта технология легла в основу современной экономики запрещенных организаций. Еще в 2017 году на совещании по криптовалютам Президент Российской Федерации В. В. Путин отметил: «Прежде всего это [использование криптовалют] возможность отмывания капиталов, полученных преступным путем, ухода от налогов и финансирование даже терроризма, ну и, конечно, распространение мошеннических схем, жертвами которых, безусловно, могут стать рядовые граждане»[2].

Формирование принципиально новой технологической среды на базе современных цифровых технологий, вне всяких сомнений, оказывает существенное влияние на экономику, политику и социальные процессы, да и вообще на все общественные отношения современного мира [6, с. 25]. Киберпространство и использование в нем новых технологий на базовом принципе распределенного (децентрализованного) реестра (blockchain tech) привело к созданию принципиально нового инструментария: умные контракты, электронно-цифровые подписи, базовые технологические патенты, стандарты и правила и т.д. [7, с. 19], что детерминирует необходимость выработки новых форм противодействия преступлениям в данной сфере. Важнейшим аспектом новых форм противодействия преступлениям является деанонимизация пользователей анонимных систем прокси-серверов. И если раньше органы безопасности еще имели доступные «лазейки» для прямого выхода на IP адрес пользователя, то теперь все стало намного сложнее и необходим комплексный анализ трафика того или иного пользователя.

В Российской Федерации основным инструментом для борьбы с такими формами преступлений является СОРМ-3. Эта система обеспечивает контроль части VPN-серверов, прослушивает в режиме реального времени спутниковую связь, мессенджеры, хранит метаданные о звонках, Интернет-сессиях, позволяет получить данные из внутренних систем оператора[3].

Эта технология способна почти гарантированно пресечь любую попытку террористической активности. И если в условиях развитого Интернета перед органами безопасности могли возникнуть проблемы шифровки сообщений между преступниками через виртуальную

[2] Путин заявил о криптовалютных рисках. [Электронный ресурс]: РБК. URL: https://www.rbc.ru/finances/ 10/10/2017/59dce47c9a7947e49a203b49 (дата обращения: 08.10.2019).

[3] Как устроен СОРМ? [Электронный ресурс]: Интернет-журнал "РСпектр". URL: https://www.rspectr.com/ articles/515/kak-ustroen-sorm (дата обращения: 10.10.2019).

частную сеть (VPN), то эта система решает эту проблему. Возможность мониторинга мессенджеров, таких, как Telegram — безусловно, ключевая ценность этой уникальной системы, так как именно мессенджеры используют террористы и экстремисты для коммуникации.

В Российской Федерации преступления все чаще совершаются с использованием высоких технологий [5], и это требует от государственной безопасности особой реакции. Однако практика применения нашей системы СОРМ-3 как новой формы противодействия преступности минимальна. Технологический потенциал органов безопасности РФ, несомненно, высок, но для точечного пресечения особо технологически изощренных преступных деяний, связанных с криптовалютами и анонимными прокси-серверами, недостаточен. Поскольку имеются сложности с государственным контролем блокчейн-криптооборота, то для того, чтобы обезопасить страну от финансового усиления запрещенных организаций, следует внести дополнение в статью 172 Уголовного кодекса Российской Федерации[4], определив криптовалюту (биткойн) как предмет преступления. Прочие меры, направленные на развитие новых форм противодействия преступности, невозможны без совместной правоохранительной реакции на международную сеть преступности (наркоторговля, криптофинансирование запрещенных организаций) в рамках договора о коллективной безопасности стран — членов СНГ. Можно утверждать, что учитывая технологическую развитость наших стран, совместные усилия гарантировали бы мощный удар по преступности.

Блокчейн — это технология, которая имеет шанс перевернуть сферу государственного регулирования, сферу государства в целом, а также все до одной сферы финансов. Области применения такой технологии множатся с каждым днем: находится все больше и больше сфер, в которых блокчейн может сыграть роль модернизирующего элемента. В их число входит и криминология, связи с которой блокчейну только предстоит образовать.

Блокчейн (от англ. blockchain) — это непрерывная последовательная цепочка блоков, содержащих информацию. Каждый блок имеет в своем заголовке метаданные (например, уникальная контрольная сумма, время создания), а также ссылку на предыдущий блок. Содержимое блока — это обычно список цифровых активов и команд вроде совершенных транзакций, их объемов и адресов участников сделок. Цепочка образует децентрализованную базу данных, которая является распределенным журналом для записи операций.

Информацию, содержащуюся в блоках цепочки, могут получить все пользователи сети, имеющие доступ к ней. Доступ открывает специальный закрытый ключ, созданный на основе криптографического алгоритма. Таким образом, хранение и передача данных в цепочке блокчейн являются защищенными и безопасными. На основе блокчейна разрабатывается программное обеспечение, способное выявлять и удалять, например, террористический контент до того, как он получит массовое распространение [3, с. 174].

База данных сохраняет всю историю транзакций, совершенных внутри цепочки. Информация о них доступна всем пользователям и может быть проверена в любой момент времени. При образовании нового блока данных реестр обновляется одновременно на всех компьютерах сети. После появления нового блока изменить его данные невозможно, а значит, невозможно подделать. Благодаря этим особенностям система является прозрачной и надежной.

Изначально предполагалось, что блокчейн-технология гарантирует полную свободу и независимость цепи, отсутствие единого администратора, то есть абсолютную децентрализацию внутренних процессов. Однако вследствие заинтересованности в новой технологии крупных компаний и финансовых институтов появились иные формы блокчейна, более централизованные и контролируемые. Они отличаются уровнем доступа к информации участников блокчейн-сети, а также их возможностью влиять на ее развитие.

Выделяют: публичный блокчейн; блокчейн, принадлежащий консорциуму; приватный (полностью частный) блокчейн.

В публичном блокчейне транзакции проходят в свободном порядке и никем не контролируются. Доступ к нему может получить любой человек. За протекающими в системе процессами смотрят все участники сети, от разработчиков до поставщиков услуг и простых пользователей. Каждый имеет возможность отправлять транзакции, принимать участие в процессе консенсуса и определять, какие блоки будут добавлены в сеть, а какие — отклонены.

Публичные блокчейны защищены принципами криптоэкономики, которая основывается на сочетании экономических стимулов и криптографических вычислений. В этом состоит основное отличие открытых блокчейнов от обычных экономических систем, которые строго регламентированы и управляются централизованно. В некоторых моментах даже создатели системы никак не могут повлиять на нее и вносить какие-либо поправки в код или данные. Система защищена от вмешательства разработчиков, а также от взлома. Поддержание безопасности не требует большого количества средств, однако ее ослабление может потребовать немалых вычислительных мощностей, что делает атаку невыгодной для злоумышленников.

Деятельность консорциумных блокчейнов контролируется заранее выбранным набором узлов. Так, некоторые блоки должны признавать другие действительными для добавления последних в цепь. По такому алгоритму работает, например, отслеживание транспортировки товаров. Блок-цепочка может быть как общедоступной, так и видимой исключительно для участников блокчейн-сети. Встречаются и «гибридные» системы, в которых корневые блоки являются общедоступными, но все члены блокчейна могут совершать лишь ограниченное число запросов и подтверждений транзакций некоторых частей блокчейна.

[4] Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (ред. от 02 .08. 2019) // Собрание законодательства РФ. 1996. № 25. Ст. 2954. Собрание законодательства РФ. 2019. № 31. Ст. 4463.

Приватный (полностью частный) блокчейн — это цепочка блоков, в которой добавление новых блоков осуществляется одной организацией. Доступ к информации блоков может быть открытым или ограниченным в той или иной степени. Такая система является полностью централизованной, поэтому она по уровню доступа близка к классическим сетям.

Преимуществами приватных блокчейнов считаются проверенные валидаторы, защищающие систему от атак, высокая скорость подтверждения транзакций, возможность контроля сети единым центром. Таким образом удается оперативно обновлять и улучшать функциональность системы, более точно прогнозировать дальнейшие действия и вносить необходимые изменения в блоки.

Изначально блокчейн стал использоваться на рынке криптовалют. Он рассматривался как альтернатива существующей банковской системе. Однако именно банки и другие финансовые институты впоследствии проявили большой интерес к технологии блокчейн, так как она обладает необходимыми для хранения и защиты информации свойствами. Благодаря ей исключается участие в транзакциях третьих лиц, закладываются основы экономики роботов.

На данный момент в технологии заинтересованы представители десятков различных сфер. Некоторые страны планируют вести земельный реестр с ее помощью, борясь с земельным мошенничеством. На основе блокчейна создаются системы цифровых удостоверений личности, системы подтверждения и сохранения права авторства и подлинности. Алмазная и энергетические индустрии работают над внедрением этой технологии для решения задач в области выработки и потребления ресурсов. Активно разрабатываются электронные платформы для анонимного онлайн-голосования на базе блокчейн. Блокчейн нашел свое применение также в сферах видеоигр, бизнеса, частного и государственного управления.

Возможности такого применения безграничны благодаря таким свойствам блокчейна, как общедоступность, надежность, высокая адаптивность и рентабельность. Таким образом можно бороться с кибертерроризмом, киберэкстремизмом и другими видами преступлений в Интернете. Однако важно отметить, что неграмотное распоряжение блокчейном с технической стороны может привести к риску роста криминальной активности и кибератак, так как благодаря развитию цифровых технологий кибертеррористы имеют больше возможностей для более изощренного планирования преступлений.

Технология блокчейн гарантированно защищает систему от подделок и мошенничества, это мешает террористам и экстремистам быстро и анонимно наносить атаки и доставать необходимую им информацию. Блокчейн может стать основой кибербезопасности, если данные пользователей будут храниться в его сети. Он защищает данные от взлома, кражи или уничтожения информации. При взломе традиционной системы хакер может получить доступ к тысячам объектов, но при взломе блокчейн-системы ему откроется доступ лишь к одному блоку информации. Это усложняет работу преступника, так как ему придется расшифровывать каждый фрагмент по отдельности, чтобы получить всю информацию. Антитеррористические группы некоторых стран уже применяют суперкомпьютеры с передовым программным обеспечением, в частности блокчейн-технологиями, для вычисления вероятности возникновения кибератак, сбора и анализа больших объемов данных из Интернета, выявления и распознавания расположения, перемещения и межличностных связей кибертеррористов, а также идентификации подозреваемых личностей и контроля над их преступной деятельностью.

В этой связи наблюдаются тенденции к развитию и совершенствованию законодательства в информационной сфере. Так, в начале 2018 года вступил в силу закон «О безопасности критической инфраструктуры». В данном документе дается разъяснение, какие госучреждения и компании должны считать себя критическими и какими способами можно защитить данные. Стоит отметить, что ответственные организации должны также отчитываться об инцидентах и проходить оценку безопасности. Вступил в силу также документ, позволяющий защищать финансовые средства граждан и организаций. В мае 2018 года Банк России внес изменения в положение «О требованиях к обеспечению защиты информации»[5]. В феврале 2019 г. в п. 1 Постановления Пленума Верховного Суда РФ «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем»[6] были внесены изменения, согласно которым предметом преступлений, предусмотренных статьями 174 и 174.1 Уголовного кодекса Российской Федерации, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления. Тем самым Верховный Суд РФ приравнивает криптовалюту к имуществу.

Еще в 2017 году Президент Российской Федерации В.В. Путин поручил Правительству РФ совместно с Центральным Банком РФ разработать нормативную базу, регулирующую операции с криптовалютами. В частности, внимание уделялось регистрации и налогообложению криптомайнеров, а также правовому регулированию первичного размещения криптовалют (ICO)[7]. Несмотря на эти поручения, до сих пор не принят законодательный акт, в котором были бы закреплены дефиниции терминов «криптовалюта», «биткоин», «майнинг», а

[5] URL: http://docs.cntd.ru/document/902352532 (дата обращения: 26.11.2019).

[6] Постановление Пленума Верховного Суда Российской Федерации от 26 февраля 2019 г. № 1 г. Москва «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». [Электронный ресурс]. URL: https://rg.ru/2019/03/07/postanovlenie-dok.html (дата обращения: 21.11.2019)

[7] «Биткоин в законе»: как в России отрегулируют криптовалюты и ICO. 2017. 24 окт. [Электронный ресурс]. URL: http://rbc.ru/money/24/10/2017/news242027 (дата обращения: 26.11.2019)

также был бы описан порядок проведения операций с использованием криптовалют в РФ.

Кроме того, в российском законодательстве не сформирован единый подход к пониманию терминов «кибертерорризм» и «киберэкстремизм», что приводит к несогласованности положений различных нормативных правовых актов, нечеткости определения компетенции правоохранительных органов в борьбе с этими негативными социальными явлениями.

Литература

1. Stepanenko R.F., Khazieva N.O., Khaziev A.K., Rybakov O.Y. Modern problems and hypotheses of general theory of law: succession and novation // Opcion. 2019. V. 35. Special Issue No. 22. Pp. 1097—1107.
2. Rybakov O.J., Rybakova O.S. Principles of information security of a child on the internet // Studies in Computational Intelligence. 2019. V. 826. Pp. 427-433.
3. Антонян Е.А., Аминов И.И. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6 (103). С. 167—177.
4. Антонян Е.А., Клещина Е.Н. О проблемах законодательного регулирования в сфере противодействия кибертерроризму и киберэкстремизму // Юридическое образование и наука. 2019. № 10. С. 28—31.
5. Валько Д.В. Киберпреступность в России и мире: сравнительный анализ. [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka (дата обращения: 10.10.2019).
6. Карцхия А.А. Цифровая трансформация права // Мониторинг правоприменения. 2019. № 1 (30). С. 25—29. DOI: 10.21681/2226-0692-2019-1-25-26.
7. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23. DOI: 10.21681/2311-3456-2019-3-18-23.
8. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2 (254). С. 5—17.
9. Рыбаков О.Ю. Приоритеты развития информационного общества в России: правовое обеспечение // Мониторинг правоприменения. 2017. № 3 (24). С. 71—76. DOI: 10.21681/2226-0692-2017-71-76.
10. Рыбаков О.Ю., Тихонова С.В. Информационные риски и эффективность правовой политики // Журнал российского права. 2016. № 3 (231). С. 88—95.

Рецензент: *Ефремова Ирина Алексеевна, доктор юридических наук, доцент, профессор кафедры уголовного права, ФГБОУ «Саратовская государственная юридическая академия», г. Саратов, Россия.*
E-mail: k_uip@ssla.ru