КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

Е. А. Антонян*,
И. И. Аминов**

Блокчейн-технологии в противодействии кибертерроризму[1]

Аннотация. *В статье современные технологии блокчейн названы революционным явлением, равным по значимости гениальному изобретению XX столетия — Интернету. Первоначально разработанные для цифровой валюты биткоина и запуска одноименной сети, технологии блокчейн создали платформу нового вида Интернета, повлияли на децентрализацию Сети по принципу распределенного реестра, стали использоваться во всевозможных разновидностях и сочетаниях для разнообразных целей, включая кибербезопасность.*

В статье утверждается, что применение технологии блокчейн для обеспечения кибербезопасности безгранично благодаря таким уникальным свойствам, как надежность, общедоступность, высокая адаптивность, экономическая эффективность, рентабельность. Использование блокчейн-технологий в целях борьбы с киберпреступностью, в том числе кибертерроризмом, может распространяться на контроль над финансовыми услугами, транспортной или любой другой отраслью. Однако рост криминальной активности с использованием технологий блокчейн будет также усиливаться, если правоохранительные органы не смогут технологически грамотно, с опережающими темпами обнаруживать эти развивающиеся центры, определять их действия и разрушать планы.

[1] Исследование выполнено при финансовой поддержки 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)
antonyaa@yandex.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** *Аминов Илья Исакович*, кандидат юридических наук, кандидат психологических наук, доцент, доцент кафедры криминологии и уголовно-исполнительного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
aminovii@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Ключевые слова: *цифровые трансформации, виртуальное пространство, технология, блокчейн, биткоин, децентрализация, анонимность, кибертерроризм, криптовалюта, киберугрозы, кибератаки, хеширование, шифровка информации.*

DOI: 10.17803/1994-1471.2019.103.6.167-177

Жизнь современного общества отмечена стремительным развитием компьютерных технологий, масштабным ростом числа пользователей Интернета, всеобщей киберинтеграцией. Цифровая трансформация охватила такие основополагающие сферы деятельности, как государственное управление, экономика, политика, законодательство, судопроизводство, бизнес, менеджмент, образование и наука. В виртуальное пространство переместились общение, обучение, банковские операции, покупки, хранение информации и многое другое. Одна из главных ролей в этих процессах принадлежит технологии блокчейн в различных ее разновидностях и сочетаниях.

Несомненно, блокчейн — революционное явление, по значимости сопоставимое с гениальным изобретением XX столетия — Интернетом. Первоначально (2008 г.) технология блокчейн (англ. blockchain, block chain — цепочка блоков) была разработана для цифровой валюты биткоин (от англ. bit — бит, т.е. единица измерения информации, и coin — монета), называемой «цифровом золотом», и запуска сети Биткоин[2]. Термин «блокчейн» означал полностью реплицированную распределенную базу (реестр) данных и относился к транзакциям в различных криптовалютах. Впоследствии технология цепочек блоков была распространена и на иные взаимосвязанные информационные блоки[3]. В настоящее время разрабатываются и реализуются новые варианты и виды применения блокчейна. Так, взрыв распространения цифровой информации привел к тому, что технология блокчейн создала платформу нового вида Интернета и способствовала появлению децентрализованных сервисов. В отличие от централизованного подхода, новые услуги основаны на децентрализованной распределенной сети, которая может использоваться для различных целей, включая кибербезопасность.

Технология блокчейн основывается на том, что у каждого пользователя базы данных, основанной на блокчейне, хранится ее полная копия (правило распределенного реестра). После любого внесения изменений в данную базу новая информация синхронизируется на компьютерах всех пользователей. Таким образом, отсутствует центральный депозитарий, который хранит базу данных, следит за ее актуальностью, надежно защищает от атак, поскольку потеря базы на одном и даже нескольких компьютерах никак не повлияет на сохранность информации: такие же копии хранятся у других пользователей. А если таких виртуальных хранилищ тысячи, миллионы или десятки миллионов, то такую базу данных можно считать относительно неуязвимой.

Посредством блокчейна информация через распределенные записи децентрализуется, последовательно хешируется (от англ. hashing — перемешивание, преобразование) и зашифровывается, что делает практически невозможным для злоумышленников ее выявление и осмысление[4]. Каждый раз, когда в распределенный реестр включаются новые данные, создается следующий блок, содержащий криптографически сформированный ключ, служащий для разблокировки произведенной записи.

Специфическим свойством технологии блокчейн является то, что внесение изменений

[2] *Галушкин А. А.* К вопросу о кибертерроризме и киберпреступности // Вестник Российского университета дружбы народов. Серия : Юридические науки. 2014. № 2. С. 44—49.

[3] *Генкин А. С.*, *Михеев А. А.* Блокчейн. Как это работает и что ждет нас завтра. М. : Альпина Паблишер, 2017. 592 с.

[4] *Luff C.* Cybersecurity and the future of blockchain technology // URL: http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm (дата обращения: 15.02.2019).

в базу данных (реестр) окончательно и необратимо: информация о транзакции запечатывается в виртуальный блок, который после регистрации действия синхронизируется со всеми копиями реестра. При этом блоки последовательно выстраиваются в цепочку. Таким образом, технология блокчейн гарантированно избавляет реестр от подделок и мошеннических действий в силу того, что внесение изменений возможно только в той части, которой владеет пользователь реестра, а также обеспечивает полную прозрачность операций в реестре и прослеживаемость всей цепочки блоков от момента создания. Срок хранения данных в реестре блокчейн неограничен, то есть информация может храниться фактически вечно[5].

На сегодняшний день блокчейн в наибольшей степени востребован в финансовом секторе (создание цифровых валют, совершение транзакций, обмен и хранение финансовой информации). Он получил прикладное использование и в других сферах, таких как смарт-контракты, регистрация публичных записей (регистрация права собственности на недвижимое имущество, лицензирование, создание и ликвидация организаций, записи актов гражданского состояния, выдача цифровых удостоверений личности, водительских прав, электронных медицинских карт и т.д.).

Вместе с тем блокчейн имеет и свои слабые места. В частности, при сосредоточении более чем 51 % узловых точек (вычислительных мощностей) в рамках одной замкнутой цепочки (пула) она приобретает абсолютный контроль над процессом регистрации сделок в блокчейне, сводя на нет основополагающее свойство блокчейна — децентрализацию реестров данных[6]. Кроме того, блокчейн не так уже анонимен, как это принято считать. Система блокчейнов служит виртуальной записью всех транзакций в сети, доступной для всех пользователей блокчейна. «Прозрачность» и общедоступность блокчейна означают, что любой пользователь, имеющий достаточный уровень компьютерной грамотности, способен отслеживать цифровые следы анонимных трейдеров. В связи с этим для повышения безопасности и анонимности блокчейн часто используется в даркнете — теневом Интернете (от англ. DarkNet — темная сеть) — с анонимным программным обеспечением The Onion Router (TOR), представляющим собой систему прокси-серверов, позволяющих тайно входить в Интернет, сохранять анонимность при посещении сайтов, обмене мгновенными сообщениями, работе с приложениями[7] и т.д.

Кроме предоставления очевидных преимуществ и нового качества жизни, тотальная цифровизация повлекла за собой не только масштабную зависимость общества от информационных технологий, но и возникновение киберпреступности, а также наиболее разрушительных ее форм — кибертерроризма и киберэкстремизма. Интернет реализовался в создании киберпространства, в котором террористы и экстремисты могут быстро и анонимно осуществлять обширный обмен информацией, беспрепятственно совершать коммуникации и наносить атаки на объекты, представляющие для них ценность.

Сегодня в Сети активно проводят работу такие террористические группы, как ХАМАС, Хезболла, египетская Аль-Гамаа аль-Исламия, Курдская рабочая партия, Аль-Каида, Исламское государство Ирака и Леванта (ИГИЛ), а также сотни других. Воинствующие радикальные организации рассматривают Интернет как идеальную арену для незаконной деятельности из-за крайне недостаточного законодательного регу-

[5] *Кумуков М. Ш.* Технология блокчейн: новые вызовы и возможности в системе мер по ПОД/ФТ (противодействие отмыванию денег и/или финансированию терроризма) // Ленинградский юридический журнал. 2018. № 2. С. 144—154.

[6] *Allen J.* How Blockchain Could Help Fight Cybercrime // URL: https://techacute.com/how-blockchain-could-help-fight-cybercrime/ (дата обращения: 15.02.2019).

[7] *Malik N*. How Criminals And Terrorists Use Cryptocurrency: And How To Stop It // URL: https://www.google.ru/search?ie=UTF-8&hl=ru&q=blockchain%20against%20cyberterrorism%20and%20cyber-extremism (дата обращения: 15.02.2019).

лирования отношений в киберсети, беспрепятственного распространения потока бесплатной информации, легкого доступа в онлайн-пространство практически из любой точки мира.

Сверхвозможности для кибертеррористов создали даркнет, а также неконтролируемые фискальной системой цифровые расчеты, виртуальную логистику, мгновенный обмен сообщениями, анонимность транзакций. Киберпреступники пользуются децентрализованной организацией теневого Интернета для проведения незаконных транзакций, для получения платежей от жертв вымогательств и для отмывания доходов. В целях осуществления преступных намерений террористические организации активно используют цифровые технологии — блокчейн, искусственный интеллект (англ. artificial intelligence, AI), большие данные (big data), дополненная и виртуальная реальность, роботизация, 3D-печать и др. Интернет используется ими для безопасной связи, сбора информации, распространения пропаганды, нанесения кибератак на базы данных и критические информационные инфраструктуры, ведения психологической и развязывания реальной войны, вербовки, рекрутинга бойцов и сочувствующих.

Излюбленной валютой для рынков даркнета стал биткоин. В теневом Интернете кибертеррористы за криптовалюту могут покупать все, что угодно, включая наркотики, лекарства, оружие, киллеров, анонимно участвовать в торговле людьми, травле, запугивании, провоцировании и осуществлении террористических и экстремистских актов. Недавнее исследование показало, что почти половина всех операций с биткоинами являются незаконными[8]. Рост криминальной активности с использованием криптовалют, вероятно, будет усиливаться, если правоохранительные органы не смогут технологически обнаруживать эти развивающиеся рынки, определять их действия и разрушать планы.

В данном контексте следует кратко, в самом общем виде, пояснить, что́ понимается под кибертерроризмом и в чем его отличительные черты. На этот счет существует много мнений, подходов, терминов, какого-то однозначного и общепринятого определения кибертерроризму пока не дано. Это, по нашему мнению, стало серьезным упущением, поскольку необходимо доподлинно знать и конкретно понимать все явления, с которыми приходится сталкиваться и бороться.

Под кибертерроризмом довольно часто понимают киберпреступность, однако явным отличием кибертерроризма является политический (и (или) идеологический, религиозно-этнический, социальный) мотив. Киберпреступность же нацелена исключительно на финансовую выгоду.

На основании анализа и обобщения российских и зарубежных источников[9] можно заключить, что *кибертерроризм* — это преднамеренная, идеологически и политически мотивированная преступная деятельность, осуществляемая в киберпространстве посредством цифровых технологий и направленная против информации, компьютерных систем, компьютерных программ и баз данных, а также объектов критической информационной инфраструктуры, которая создает угрозу жизни или здоровью людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения и органов власти, достижения преступных намерений, провокации военного конфликта. При этом террористические кибератаки могут быть направлены на объекты как виртуальной среды, так и реальной действительности.

Особо отметим, что Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[10] в ч. 4 ст. 2 определяет, что компьютерная атака — это целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты

[8] *Allman K*. The dark side of the Bitcoin // Law Society of NSW Journal. Iss. 42 (Mar 2018). URL: https:search.informit.com.au/documentSummary;dn=436097450333633;res=IELHSS (дата обращения:15.02.2019).

[9] *Галушкин А. А*. Указ. соч.

[10] СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

В свою очередь, Федеральным законом от 26.07.2017 № 194-ФЗ в Уголовный кодекс РФ[11] была введена ст. 274.1, определяющая наказания за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Отличительной особенностью кибертеррористических актов (атак) является то, что они, как правило, нацелены на критически важные системы инфраструктуры, чтобы отключить, например, водоочистную станцию, вызвать региональное отключение электроэнергии, нарушить работу трубопровода, нефтеперерабатывающего завода или объектов транспорта. По данным Комиссии по защите критической инфраструктуры США, возможные цели кибертерроризма включают банковскую индустрию, военные объекты, электростанции, центры управления воздушным движением и системы водоснабжения[12]. Подобные кибератаки могут разрушить крупные города, сорвать политические выборы в органы власти, обвалить финансовую систему страны, вызвать кризис общественного здравоохранения, вызвать перебои с поставками продовольствия, поставить под угрозу общественную и государственную безопасность, а также вызвать массовую панику и гибель людей.

Операции кибертеррора могут осуществляться с применением разнообразных кибертехнологий, среди которых:

— различные виды *вредоносного программного обеспечения (ПО)*, например X-Agent, X-Tunnel, PsExec и другие программы для удаленного выполнения команд, передачи файлов, шпионажа за нажатыми клавишами, уничтожения следов своего пребывания в Сети, периодического вычищения журналов событий и изменения атрибутов времени, изменения файлов;
— *расширенные длительные угрозы* (Advanced persistent threat, APT) — это сложные и концентрированные сетевые атаки, в результате которых террористы получают доступ в корпоративную сеть и остаются там незамеченными в течение длительного периода с целью кражи данных, не нанося ущерб непосредственно сети или организации. Как правило, APT атакует целевые организации в секторах с ценной информацией, таких как национальная оборона, производство и финансовая индустрия;
— *вредоносные вирусы, компьютерные «черви» и системы контроля* за программным обеспечением объектов критической инфраструктуры (водоснабжение, транспортные системы, электросети, военные системы, экологические комплексы и т.д.);
— *DoS-атаки* (от англ. Denial of Service — «отказ в обслуживании») и *DDoS-атаки* (от англ. Distributed Denial of Service — «распределенный отказ в обслуживании»), которые искусно наносятся террористами-хакерами для отключения корпоративных систем и сетей. Часто проводятся в рамках киберэкстракции (от англ. Cyber Extortion — «кибервымогательство, кибершантаж»);
— *взлом и кража особо важных данных* (Hacking and theft of critical data) государственных органов, учреждений и предприятий;
— *атака вымогателей* (Attak Ransomware), которые держат компьютерные системы в заложниках, пока жертвы не заплатят выкуп;
— *фишинговые атаки* (от англ. fishing — «рыбная ловля, выуживание») — самый распространенный тип кибератак, представляющих собой попытки киберпреступников собирать информацию от жертв по электронной почте,

[11] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

[12] *Nakamoto Satoshi*. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Pp. 2—3 ; *Rouse M.* Cyberterrorism // URL: https://searchsecurity.techtarget.com/definition/cyberterrorism (дата обращения: 15.02.2019).

которую они затем могут использовать для доступа к системам или для кражи личных данных жертв.

Для тайного общения в Интернете при планировании действий и координации атак террористическими организациями, например Аль-Каидой, все чаще применяются зашифрованные коммуникационные платформы Telegram или Signal. Джихадисты для распространения идеологической пропаганды предпочитают Twitter и Facebook. Для обмена сообщениями киберэкстремисты активно используют программы и приложения WhatsApp, Threema, Kik, Wickr и SureSpot[13].

Такие программы, как Google.Карты, способны предоставлять чрезвычайно важную для террористов информацию о расположении конкретных населенных пунктов или объектов, находить возможные точки входа в места, где планируются террористические атаки, а также рассматривать пути безопасного отхода и эвакуации. Потенциальные террористы в даркнете могут найти практически любой учебный материал: инструкции по созданию самодельных зажигательных и взрывных устройств, похищению людей и содержанию заложников, шантажу и запугиванию жертв. Есть даже руководства о том, как эффективно избежать онлайн-контроля со стороны антитеррористических групп.

Технологическая трансформация, запуск теневого Интернета и активное применение террористическими организациями цифровых технологий способствовали проявлению в современной онлайн-террористической деятельности новых опасных тенденций: 1) неуклонный и масштабный рост кибертерроризма; 2) целевое распространение идеологической и инструктивной информации на конкретную и наиболее восприимчивую аудиторию; 3) всемерная поддержка и поощрение приверженцев-одиночек[14].

В последнее десятилетие благодаря Интернету и применению цифровых технологий оперативное планирование террористов стало более децентрализованным, изощренным и технологичным. Киберпространство имеет трансграничный характер, поэтому в случае совершения кибертеррористического акта трудно установить место нахождения террористов. Расположение компьютера, с помощью которого совершается террористический акт, крайне редко совпадает с местом расположения объекта посягательства и последствий деяния. Кроме того, технологическую проблему составляет сохранность следов совершения преступления и, соответственно, процесс розыска его исполнителей, что существенно снижает шансы их обнаружить и обезвредить. Остаются неясными ответы на вопросы: переместятся ли террористические атаки в киберпространство и сократится ли число реальных террористических актов (взрывы, поджоги, расстрелы, захваты заложников, наезды транспортных средств на людей и т.п.) или же терроризм останется таким же насильственным и физически выраженным?

Транснациональный характер кибертерроризма обусловливает тесное взаимодействие правоохранительных органов и специалистов в области IT-технологий разных стран. В целях обеспечения обмена результатами финансовой разведки и информацией, касающейся преступного использования цифровых валют, в частности финансирования кибертерроризма, в 2016 г. Европол, Интерпол и Базельский институт управления создали совместное подразделение по борьбе с отмыванием денег, специализирующееся на цифровых валютах. В задачи группы входят сбор и анализ информации о преступном использовании криптовалют, расследование хранения доходов, полученных преступным путем, организация ежегодных семинаров и встреч представителей трех ведомств

[13] Is technology helping or hindering the fight against terrorism? // Dis-patch News & Politics, Science & Tech. December 15. 2017. URL: https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-the-fight-against-terrorism/ (дата обращения: 15.02.2019).

[14] Is technology helping or hindering the fight against terrorism?

и других учреждений, а также создание сети специалистов по биткоин-преступности[15]. При поддержке Европола в июле 2017 г. были закрыты два крупнейших даркнет-маркета AlphaBay и Hansa Market, что стало результатом крупной международной операции, в которой принимали участие США, Канада, Таиланд, Голландия, Великобритания, Франция, Литва, а также представители Европола, ФБР и Управления по борьбе с наркотиками США[16].

Очевидно, что для того, чтобы предотвратить террористические угрозы и радикализацию в киберпространстве, правоохранительные органы должны иметь возможность быть в технологическом отношении на шаг впереди киберкриминала. Изворотливость и профессионализм современных кибертеррористов, а также их фантастически возросшие технологические возможности требуют от правоохранительных органов всего мира разработки адекватных механизмов противодействия кибертерроризму, стратегия борьбы с которым должна быть направлена на предупреждение и минимизацию угроз и рисков, порождаемых глобальной цифровизацией. Конечная цель такого подхода должна состоять в исключении любых возможностей для действий террористов как в реальном мире, так и в киберпространстве.

Блокчейн открывает новые сверхэффективные способы противостояния кибератакам различными способами, одним из которых является надежная защита данных от взлома, кражи или уничтожения ценной информации. Если при взломе традиционной централизованной системы хакер за один вход может получить доступ ко всем тысячам объектов, то при взломе децентрализованной блокчейн-системы киберпреступники могут получить доступ только к одному фрагменту, что делает их действия более трудоемкими, так как придется многократно взламывать базу, чтобы получить полную информацию. В свою очередь, у служб безопасности и правоохранительных органов появляется дополнительное время для выявления источника опасности и устранения угрозы[17].

Возможность предотвращения кибератак заложена в самом принципе децентрализованной системы цепочки блоков, которая не только обеспечивает децентрализованную сеть для хранения информации, но и гарантирует ее безопасность за счет устойчивости к взлому хешированных и зашифрованных блоков. Сервер, основанный на блокчейне, может минимизировать атаки, создавая более разветвленную сеть и распределяя контроль между различными пользователями. Наличие автоматических распределенных регистров и неизменной истории транзакций позволяет предотвращать кибератаки. Последовательное хеширование и шифровка информации позволяют сохранять целостность данных[18].

Принцип безопасности распределенной сети может применяться и для защиты такой жизненно важной внешней инфраструктуры, как служба доменных имен (англ. domain name services, DNS) веб-сайтов компаний. В 2016 г. мощная кибератака на Twitter и Spotify продемонстрировала уязвимость текущей практики DNS, заключающейся в том, что ключ доступа хранится только на одном сервере, а его надежность строится на хешировании путем кодирования и криптографии. Сервер на основе распределенного блокчейн-реестра создает более широкую сеть ключей безопасности, что гарантированно минимизирует риск взлома или уничтожения системы[19].

---

[15] Europol and Interpol to fight cryptocurrency crime together // URL: http:www.coinfox.info/news/6404-europol-and-interpol-to-fight-cryptocurrency-crime-together (дата обращения: 15.02.2019).

[16] *Galbraith K*. The Emerging Threat of Cyberterrorism // Australian Outlook. 29 Jun 2018. URL: http://www.internationalaffairs.org.au/australianoutlook/the-emerging-threat-of-cyberterrorism/ (дата обращения: 15.02.2019).

[17] Blockchain Technology in the fight against Cybercrime / DISINI & DISINI // URL: https://privacy.com.ph/dndfeature/blockchain-technology-in-the-fight-against-cybercrime/ (дата обращения: 15.02.2019).

[18] *Allen J.* Op. cit.

[19] *Luff C.* Op. cit.

Помимо защиты самих данных, блокчейн способен защитить от кибератак и процесс обмена информацией. Например, такие инструменты обмена мгновенными сообщениями, как Facebook Messenger или WhatsApp, хотя и оснащены системами безопасности, все же имеют слабые места. WhatsApp, несмотря на сквозное шифрование для защиты содержимого сообщений, сохраняет метаданные (информацию о том, с кем общается пользователь), которые обычно хранятся в отдельных системах, и велика вероятность, что хакеры их взломают. Технология цепочки блоков может децентрализовать сеть, разделить метаданные и гарантировать их совокупную недоступность.

Системы защиты интернет-серверов и информационно-коммуникационных систем должны не просто успевать совершенствоваться вслед за все более совершенными способами и методами исполнения актов кибертерроризма, а значительно опережать их.

Антитеррористические группы ряда стран уже применяют суперкомпьютеры с передовым программным обеспечением, в частности технологиями блокчейн, для оценки рисков возникновения кибертеррористических актов, накопления и анализа огромных объемов данных из глобального интернет-облака, выявления и распознавания схемы дислокации, перемещений и межличностных связей кибертеррористов, идентификации личности подозреваемых, установления контроля над их террористической деятельностью и передвижениями.

В 2016 г. британская полицейская контртеррористическая группа по борьбе с терроризмом (CTIRU) вывела из Интернета более 3 500 наименований вредных и незаконных материалов, включая пропагандистские фильмы, учебные пособия по терроризму, а также видеоролики и публикации, пропагандирующие или поддерживающие терроризм и экстремизм. Компания Palantir из Кремниевой долины на основе технологии блокчейн и анализа больших данных создает и совершенствует программное обеспечение для отслеживания информации в целях борьбы с терроризмом для разведывательных, правоохранительных, частных детективных агентств, принося основателям компании доход в 1,5 млрд долл. США в год. Цифровая криминалистика также помогает следователям искать улики в цифровых отпечатках подозреваемых террористов, устанавливая их онлайн-активность, прослушивая разговоры и разыскивая покупки, чтобы найти доказательства преступных деяний. Специальное программное обеспечение, приобретенное у канадской компании Magnet Forensics, позволило ФБР США обнаружить улики на 30 электронных устройствах, принадлежащих террористам, ответственным за атаку во время Бостонского марафона (братья Царнаевы, 2013 г.).

Применение технологий блокчейн и продуктов на ее основе в противодействии кибертерроризму проводится, как правило, комплексно с другими супертехнологиями. Так, блокчейн в сочетании с искусственным интеллектом используется для фильтрации и идентификации важной информации, для поиска в огромных массивах данных.

На основе блокчейна разрабатывается программное обеспечение, способное выявлять и удалять террористический контент до того, как он получит массовое распространение. В 2018 г. Министерство внутренних дел Великобритании доложило о создании лондонской технологической компанией ASI Data Science комплексного инструмента искусственного интеллекта для обнаружения в 95 % террористического контента в онлайн-видео, с вероятностью выявления в 99,9 %[20].

Элементы технологии блокчейн присутствуют в программном обеспечении по выявлению и распознаванию лиц, в системах обнаружения взрывчатых веществ в транспортных средствах, роботах Packbots, способных проникать в чрезвычайно опасную для человека среду, и даже в высокотехнологичных лифтах, мгновенно до-

[20] Counter-terrorism strategy embraces tech, but warns of future extremist digital capabilities // URL: https://www.itpro.co.uk/cyber-terrorism/31247/quantum-computing-could-help-fight-terrorism-says-uk-gov (дата обращения: 15.02.2019).

ставляющих людей с верхних этажей небоскребов в вестибюль[21].

Область применения технологии блокчейн в кибербезопасности безгранична благодаря таким его уникальным свойствам, как надежность, общедоступность, высокая адаптивность, экономическая эффективность и рентабельность. Использование блокчейна для борьбы с киберпреступностью может быть распространено на финансовые услуги, законодательство, транспортную отрасль или любую другую отрасль, требующую проверки третьей стороной.

Разумеется, в основе всех этих разработок и механизмом их применения в правоохранительной деятельности должно быть соответствующее законодательство, своевременно реагирующее на новые риски и угрозы, а также легализующее применение цифровых технологий. Представляется необходимым ввести в правовое поле деятельность провайдеров обмена цифровых валют, а также совершение сделок по купле-продаже не только токенов, но и криптовалюты, что позволит решить ряд первостепенных задач, таких как противодействие финансированию террористической деятельности и отмыванию доходов. Следует отметить, что практическая реализация требований об идентификации трейдеров является сложной из-за отсутствия прямого контакта с пользователем и отсутствия опробованных механизмов идентификации применительно к криптовалютам.

Кроме того, законодательство должно регулярно совершенствовать уголовно-правовую оценку (квалификацию) киберпреступлений и киберправонарушений, вводить новые их виды, усиливать систему наказаний за кибертерроризм. Установить административные штрафы за такие правонарушения в виртуальной среде, как, например, неоднократный просмотр потокового террористического видеоконтента или пересылка файлов террористической и экстремистской направленности.

Таким образом, разработка высокотехнологичных цифровых механизмов противодействия кибертерроризму и объединение усилий государств всего мира является первоочередной задачей на современном этапе. Международному сообществу следует выработать единые для всех стран правила игры в сфере цифровых технологий, универсальный и общий для всех международный стандарт, который будет максимально учитывать интересы каждой страны. Должна быть улучшена трансграничная система обмена данными о киберугрозах. Вместе с тем меры безопасности не должны приниматься в ущерб технологическому прогрессу и инновациям. Свобода общения и коммуникаций, а также беспрепятственный обмен опытом и идеями в цифровую эпоху должны быть законодательно гарантированы.

БИБЛИОГРАФИЯ

1. *Галушкин А. А.* К вопросу о кибертерроризме и киберпреступности // Вестник Российского университета дружбы народов. Серия : Юридические науки. — 2014. — № 2. — С. 44—49.
2. *Генкин А. С.*, *Михеев А. А.* Блокчейн. Как это работает и что ждет нас завтра. — М. : Альпина Паблишер, 2017. — 592 с.
3. *Кумуков М. Ш.* Технология блокчейн: новые вызовы и возможности в системе мер по ПОД/ФТ (противодействие отмыванию денег и/или финансированию терроризма) // Ленинградский юридический журнал. — 2018. — № 2. — С. 144—154.
4. *Allen J.* How Blockchain Could Help Fight Cybercrime // URL: https://techacute.com/how-blockchain-could-help-fight-cybercrime/ (дата обращения: 15.02.2019).
5. *Allman K.* The dark side of the Bitcoin // Law Society of NSW Journal. — Iss. 42 (Mar 2018). — URL: https://search.informit.com.au/documentSummary;dn=436097450333633;res=IELHSS (дата обращения: 15.02.2019).

[21] Is technology helping or hindering the fight against terrorism?

6. Blockchain Technology in the fight against Cybercrime / DISINI & DISINI // URL: https://privacy.com.ph/dndfeature/blockchain-technology-in-the-fight-against-cybercrime/ (дата обращения: 15.02.2019).
7. Counter-terrorism strategy embraces tech, but warns of future extremist digital capabilities // URL: https://www.itpro.co.uk/cyber-terrorism/31247/quantum-computing-could-help-fight-terrorism-says-uk-gov (дата обращения: 15.02.2019).
8. Europol and Interpol to fight cryptocurrency crime together // URL: http://www.coinfox.info/news/6404-europol-and-interpol-to-fight-cryptocurrency-crime-together (дата обращения: 15.02.2019).
9. *Galbraith K.* The Emerging Threat of Cyberterrorism // Australian Outlook. — 29 Jun 2018. — URL: http://www.internationalaffairs.org.au/australianoutlook/the-emerging-threat-of-cyberterrorism/ (дата обращения: 15.02.2019).
10. Is technology helping or hindering the fight against terrorism? // Dispatch News & Politics, Science & Tech. — December 15. — 2017. — URL: https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-the-fight-against-terrorism/ (дата обращения: 15.02.2019).
11. *Luff C.* Cybersecurity and the future of blockchain technology // URL: http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm (дата обращения: 15.02.2019).
12. *Malik N.* How Criminals And Terrorists Use Cryptocurrency: And How To Stop It // URL: https://www.google.ru/search?ie=UTF-8&hl=ru&q=blockchain%20against%20cyberterrorism%20and%20cyber-extremism (дата обращения: 15.02.2019).
13. *Nakamoto Satoshi*. Bitcoin: A Peer-to-Peer Electronic Cash System. — 2008.
14. *Rouse M.* Cyberterrorism // URL: https://searchsecurity.techtarget.com/definition/cyberterrorism (дата обращения: 15.02.2019).

Материал поступил в редакцию 6 мая 2019 г.

BLOCKCHAIN TECHNOLOGY IN COUNTERING CYBER TERRORISM[22]

ANTONYAN Elena Aleksandrovna, Doctor of Law, Professor, Professor of the Department of Criminology and Penal Law of the Kutafin Moscow State Law University (MSAL)
antonyaa@yandex.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

AMINOV Ilya Isakovich, PhD in Law, PhD in Psychology, Docent, Associate Professor of the Department of Criminology and Penal Law of the Kutafin Moscow State University (MSAL)
aminovii@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *In the paper, modern blockchain technologies are called a revolutionary phenomenon, equal in importance to the ingenious invention of the 20th century — the Internet. Originally developed for Bitcoin digital currency and launching the network of the same name, the blockchain technology created a platform for the new type of the Internet, influenced the decentralization of the Network according to the distributed registry principle, and began to be used in various types and combinations for various purposes, including cybersecurity.*
The paper argues that the use of blockchain technology to ensure cybersecurity is infinite due to such unique properties as reliability, accessibility, high adaptability, economic efficiency, profitability. The use of blockchain

[22] The study is carried out with the financial support of the Russian Foundation for Basic Research, Research Project No. 18-29-16175 «Blockchain-technology for countering the risks of cyber-terrorism and cyber-extremism: criminological and legal research».

technologies to combat cybercrime, including cyberterrorism, may extend to control over financial services, transportation or any other industry. However, the growth of criminal activity using the blockchain technology will also be enhanced if the law enforcement agencies are not technologically competent, can detect these developing centers, determine their actions and destroy plans at a faster pace.

Keywords: *digital transformations, virtual space, technology, blockchain, bitcoin, decentralization, anonymity, cyber-terrorism, cryptocurrency, cyber threats, cyber attacks, hashing, encryption of information.*

REFERENCES (TRANSLITERATION)

1. Galushkin A. A. K voprosu o kiberterrorizme i kiberprestupnosti // Vestnik Rossijskogo universiteta druzhby narodov. Seriya : Yuridicheskie nauki. — 2014. — № 2. — S. 44—49.
2. Genkin A. S., Miheev A. A. Blokchejn. Kak eto rabotaet i chto zhdet nas zavtra. — M. : Al'pina Pablisher, 2017. — 592 s.
3. Kumukov M. Sh. Tekhnologiya blokchejn: novye vyzovy i vozmozhnosti v sisteme mer po POD/FT (protivodejstvie otmyvaniyu deneg i/ili finansirovaniyu terrorizma) // Leningradskij yuridicheskij zhurnal. — 2018. — № 2. — S. 144—154.