ISSN 2500-4255

УДК 343.9:004
DOI 10.17150/2500-4255.2019.13(4).555-563

БЛОКЧЕЙН В ЦИФРОВОЙ КРИМИНОЛОГИИ: ПОСТАНОВКА ПРОБЛЕМЫ

А.П. Суходолов[1], Е.А. Антонян[2, 3], М.В. Рукинов[4], М.Ю. Шамрин[2], М.Г. Спасенникова[5]
[1] Байкальский государственный университет, г. Иркутск, Российская Федерация
[2] Московский государственный юридический университет им. О.Е. Кутафина, г. Москва, Российская Федерация
[3] Российский государственный гуманитарный университет, г. Москва, Российская Федерация
[4] Санкт-Петербургский государственный университет, г. Санкт-Петербург, Российская Федерация
[5] Национальный научно-исследовательский институт общественного здоровья им. Н.А. Семашко, г. Москва, Российская Федерация

Информация о статье

Дата поступления
25 апреля 2019 г.

Дата принятия в печать
2 августа 2019 г.

Дата онлайн-размещения
23 августа 2019 г.

Ключевые слова
Криминология; цифровая криминология; преступность; киберсфера; киберпреступность; кибертерроризм; кибербезопасность; технология распределенных реестров/блокчейн; информация; новые технологии

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

Аннотация. Актуальность рассматриваемой в статье проблемы определяется тем, что прогнозируемый ущерб от киберпреступности в 2021 г. может составить 6 трлн дол. по сравнению с 3 трлн в 2015 г. Авторы выдвигают гипотезу о том, что блокчейн может стать именно той технологией, которая снизит масштабы ущерба от преступных посягательств в сфере цифровой экономики, облегчив контроль за противоправным движением финансов. Цель исследования заключается в анализе роли технологии распределенных реестров/блокчейн в цифровой криминологии, противодействии киберпреступности. При применении технологии блокчейн нет единой точки атаки на базу данных, а получить доступ к данным, зашифрованным при помощи ключа, невозможно без знания этого ключа. Ключи хранятся не централизованно, а у каждого пользователя-собственника. В статье изучается технология хранения данных в блокчейне или распределенном реестре (блокчейн является частным случаем распределенного реестра). При атаке на такой центр-сервер невозможно похитить сразу все данные, находящиеся на нем. Криминальной сфере будет нанесен ощутимый удар, так как сохраняется история операций, финансовые потоки будут видны в цепочке блоков и замаскировать их будет практически невозможно, что сведет на нет нелегальные транзакции, сильно усложнит финансирование террористических и экстремистских организаций. Поскольку база есть у всех пользователей-собственников, то хищение отобразится синхронно, скрыть его невозможно. Станет известно, чей секретный ключ использовался для доступа. Это будет прямо указывать на преступника, что само по себе способно его остановить. В статье содержится описание того, как именно распределенные реестры можно применять в борьбе с киберпреступностью. Авторы считают, что: 1) проблема распространения киберпреступности наиболее актуальна для развитых государств (с высоким показателем ВВП), поскольку чем более развито общество, тем более оно зависимо от цифровых технологий; 2) технология распределенных реестров/блокчейн поможет в противодействии кибератакам и, соответственно, защитит финансовые средства и конфиденциальную информацию от преступных посягательств.

BLOCKCHAIN IN DIGITAL CRIMINOLOGY: PROBLEM STATEMENT

Alexander P. Sukhodolov[1], Elena A. Antonyan[2, 3], Maxim V. Rukinov[4], Maxim Yu. Shamrin[2], Marina G. Spasennikova[5]
[1] Baikal State University, Irkutsk, the Russian Federation
[2] O.E. Kutafin Moscow State Law University, Moscow, the Russian Federation
[3] Russian State University for the Humanities, Moscow, the Russian Federation
[4] Saint Petersburg State University, Saint Petersburg, the Russian Federation
[5] N.A. Semashko National Research Institute of Public Health, Moscow, the Russian Federation

Article info

Received
2019 April 25

Accepted
2019 August 2

Available online
2019 August 23

Abstract. The problem under consideration is highly topical as damage from cybercrime is predicted to reach six trillion dollar in 2021, compared with 3 trillion in 2015. The authors put forth a hypothesis that blockchain could become the technology that will reduce the scale of damage from criminal infringements in the sphere of digital economy by simplifying control over illegal movement of capital. The goal of this research is to analyze the role that the technology of distributed registers/blockchain plays in digital criminology and counteracting cybercrime. In blockchain, there is no single point of attack on the database, and it is impossible to access data encrypted with a key without that key. There is not centralized storage for keys:

Keywords
Criminology; digital criminology; crime; cybersphere; cybercrime; cyberterrorism; cybersecurity; distributed registry/blockchain technology; information; new technologies

Acknowledgements
This research is financially supported by RFBR within project № 18-29-16175 «Blockchain technologies of counteracting cyber-terrorism and cyber-extremism: a criminology and legal study»

each user-owner stores them. The authors study the technology of storing data in blockchain or distributed register (blockchain being a special case of distributed register). If such a server center is attacked, it is impossible to steal all data that are stored on it at once. This will deliver a serious blow on the criminal transactions because the whole history of operations is saved, the financial flows are transparent in the chain of blocks and it will be virtually impossible to hide them, which will eliminate all illegal transactions and make the financing of terrorist and extremist organizations much more difficult. Because all users-owners have the database, the theft will be noticed immediately, and it cannot be hidden. It will get known whose secret key is used for access, and it will point directly at the perpetrator and could, in itself, stop them. The authors describe how distributed registers can be used to fight cybercrime. They believe that 1) the problem of cybercrime is most relevant for developed countries (with high GDP) because the more developed a society is, the more it depends on digital technologies; 2) the distributed registers/blockchain technology will help counteract cyberattacks and, consequently, will protect finances and confidential information against criminal infringements.

За последние десять лет уровень кибербезопасности, предупреждения киберпреступлений значительно изменился. Регистрируются все более изощренные киберпреступления в самых разных точках мира. Уровень и тип угрозы будут продолжать меняться по мере того, как новые технологии и возможности в информационной сфере будут открываться не только перед специалистами, но и перед представителями преступной среды, в том числе перед террористическими организациями. Все большее количество дипломированных IT-специалистов по различным мотивам начинают сотрудничество с криминальными группировками, террористическими организациями в различных преступных целях.

Ученые-криминологи из стран с романо-германской и англосаксонской правовыми системами используют различные термины для описания преступности в цифровой сфере. Одни коллеги разделяют киберпреступность и кибертерроризм, другие используют оба термина, описывая одно и то же деяние.

В странах с романо-германской правовой системой кибертерроризм чаще рассматривается как разновидность террористической деятельности. В российском праве под террористическим актом понимается совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями.

Термин «кибертерроризм» образован в результате слияния слов «кибер» («киберпространство») и «терроризм». Кибертерроризму свойственны черты обычного терроризма. Специфика заключается в способах и методах атак. Если обычный терроризм использует кинетические средства (например, взрывные устройства), то кибертерроризм подразумевает использование компьютерных технологий, сети Интернет и т.д. [1; 2]. Если раньше террористам нужно было захватить самолет и выдвинуть требования, то в настоящее время можно дистанционно захватить управление компьютерными системами аэропорта. При этом правоохранительные органы могут даже не знать, кто проводит эту атаку и из какой страны.

Впервые термин «кибертерроризм» был сформулирован еще в 1980-х гг. Барри Коллином. Он утверждал, что кибертерроризм формирует сближение двух миров — виртуального и физического [3], что предполагает отсутствие существенных различий между киберпреступностью и кибертерроризмом. Позже было сформулировано значительное количество иных определений киберпреступности и кибертерроризма [4].

Федеральное бюро расследований США трактует кибертерроризм как преднамеренную, политически мотивированную атаку на информацию (компьютерные системы, компьютерные программы и данные), которая приводит к насилию против некомбатантов, против субнациональных групп или подпольных агентов. Можно отметить размытость и неопределенность такого понимания кибертерроризма. Исходя из этого определения, к кибертерроризму можно причислить и ненасильственные онлайн-шалости, мошенничества или действия WikiLeaks, что видится крайне сомнительным. Можно согла-

ситься с тем, что подобное понимание кибертерроризма «обладает такой же степенью ясности, что и термин «кибербезопасность», то есть не обладает ею вообще» [5].

Одно из направлений предупреждения киберпреступности, кибертерроризма — исключение возможности получать дистанционное управление над системами сложных объектов (например, Центробанк, Пенсионный фонд, налоговые органы, предприятия атомной энергетики, железнодорожного транспорта, аэропорты и др.), совершать хищение данных или денежных средств этих организаций [6, с. 112; 7].

Определенная часть ученых упоминание кибертерроризма так или иначе связывают с криптовалютами. Данная позиция представляется не совсем верной. Криптовалюты появились позже, чем кибертерроризм, но они способствовали тому, что кибертеррористы стали чаще заявлять свои требования в криптовалютах, так как на какой-то момент времени они не были привязаны к конкретному государству и сложнее отслеживались. Однако если требования преступников выражены в наличных рублях, евро или долларах США, то это не является основанием запрещать оборот наличных рублей, евро или долларов США.

Не понимая, как проводить идентификацию клиентов криптовалютных бирж и контролировать обмен фиатных средств на криптовалюты, сотрудники правоохранительных органов ряда стран акцентируют внимание на потенциальном использовании криптовалют для легализации денежных средств, их незаконного вывода за рубеж и финансирования терроризма. На основании этого руководители некоторых государств устанавливают запретительное регулирование: не можешь контролировать — запрещай [8; 9].

Данная позиция укоренилась из-за наиболее резонансных случаев мошенничества и резкого снижения цены криптовалют в 2018 г. Однако если внимательно рассмотреть устройство технологии блокчейн и криптовалют как одного из случаев использования новой технологии, то можно убедиться, что криптовалюты менее анонимны, чем традиционные банковские переводы, а технология распределенных реестров или блокчейн как ее частный случай могут помочь в борьбе с киберпреступностью, кибертерроризмом.

Обозначенные проблемы являются крайне актуальными для цифровой экономики современного общества, что определяет интерес к ним со стороны ученых-криминологов [10, с. 76].

McAfee в своем отчете заявляет, что киберпреступность безжалостна, ее объемы не уменьшаются и она вряд ли остановится [11]. Данное мнение разделяет большинство организаций в сфере кибербезопасности, о чем свидетельствуют статистические показатели, представленные в их онлайн-отчетах [12][1].

Так, по данным организаций в сфере кибербезопасности, к 2021 г. ущерб от киберпреступности может достигнуть 6 трлн дол. по сравнению с 3 трлн в 2015 г.[2], что превысит прибыль от глобальной торговли наркотическими средствами всех видов. Данную информацию подтверждают ведущие эксперты и международные компании в области кибербезопасности (Oracle, McAfee), которые в своих прогнозах исходят из анализа статистических показателей прошлых лет, а также опираются на исследования в области организации кибератак, количество которых к 2021 г. также намного увеличится.

Последствия киберпреступности заключаются в многомиллионном ущербе, потере производительности, краже интеллектуальной собственности, финансовых данных, нарушении нормального режима работы объектов государственной власти и экономики, а также в нанесении вреда деловой репутации физических и юридических лиц, дискредитации государства и его правоохранительных органов.

По мнению Роберта Херджавека, основателя и генерального директора компании в области ИТ-безопасности Herjavec Group (поставщика услуг управляемой безопасности с офисами и центрами безопасности операций), рост стоимости ущерба от киберпреступности демонстрирует число организаций, не подготовленных к кибератакам[3].

Кибератаки являются наиболее быстро распространяющимся преступлением в США, постоянно увеличиваясь в размерах, сложности

[1] Internet Security Threat Report. 2019. Vol. 24. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf ; Norton Cyber Security Insights Report. 2017. Global Results. URL: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en ; Cybercrime Report 2018 // LexisNexis. Risk Solutions. URL: https://www.threatmetrix.com/digital-identity-insight/cybercrime-report/q1-2018.

[2] Terrifying Cybercrime and Cybersecurity Statistics and Trends [2018 Ed.]. URL: https://www.comparitech.com/vpn.

[3] The-2019 Official Annual Cybercrime Report / Herjavec group. URL: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report.

и стоимости наносимого ущерба. Так, взлом Yahoo (крупнейший за всю историю) затронул 3 млрд учетных записей пользователей, а атака на Equifax в 2017 г. — 145,5 млн клиентов, что превзошло крупнейшие взломы, о которых когда-либо сообщалось. Эти крупные кибератаки наряду с кибератаками WannaCry и NotPetya (кибератаки WannaCry и NotPetya представляли собой взлом серверов, приведший к нарушению функциональности целого ряда крупных корпораций более чем в 150 странах и, как результат, к перерыву в их работе и многим другим потерям, превысившим, по оценкам некоторых компаний, 300 млн дол. США [13]), которые произошли в 2017 г., не только масштабнее и сложнее, чем предыдущие, но и свидетельствуют о развитии криминальных кибертехнологий.

В последние годы зарегистрировано большое количество атак на весьма различные базы данных и краж персональных данных из них. Атака на «Сони Пикчерс» в ноябре 2014 г. демонстрирует масштаб проблемы, как и тот факт, что атаки подчас совершаются уже отдельными лицами или их небольшими группами. Последствием атаки стало опубликование сценариев будущих фильмов. Ущерб как для компании, так и для мировой кинематографической культуры в целом был колоссален [14].

В июне 2015 г. Управление кадровой службы США не сумело предупредить взлом систем, ставший одним из самых крупных взломов государственной базы данных с рекордным количеством пострадавших (21 млн чел.). Были украдены их данные, включая имена, даты рождения, адреса и даже отпечатки пальцев.

Для организации кибератак их исполнители используют вредоносные программы, выступающие в качестве кибероружия. Кроме причинения прямых убытков, рассматриваемые преступления ведут к такому косвенному негативному последствию, как международная напряженность. Например, в случаях с WannaCry и NotPetya некоторые государства выступили с обвинениями в адрес России как предполагаемого разработчика указанных программ. Нападение на Северную Корею, в результате которого веб-инфраструктура страны и сеть Интернет перестали функционировать на девять с половиной часов, многие рассматривали как атаку со стороны США.

В 2016 г. 15,4 млн граждан США стали жертвами кибератак, в результате которых были украдены их персональные данные конфиденциального характера, что на 16 % больше, чем в 2015 г. Убытки составили 16 млрд дол. — на 1 млрд больше, чем в 2015 г. [10, с. 79].

Конфиденциальные данные — это самый распространенный объект атаки киберпреступников. Для их похищения используют взлом баз данных, сопровождающийся кражей персональной финансовой информации. Процветает и продажа сканированных копий паспортов и других документов.

Таким образом, киберпреступность, кибертерроризм могут носить как локальный, так и трансграничный характер, приводя к ухудшению отношений между государствами, нарушению экономических и дипломатических связей, затруднению работы межгосударственных организаций, т.е. к безопасности мирового сообщества.

Эта криминологическая проблема наиболее актуальна для развитых государств (с высоким показателем ВВП), поскольку чем более развито общество, тем сильнее оно зависит от цифровых технологий. Однако правоохранительные органы даже самых высокоразвитых стран оказываются бессильны в борьбе с киберпреступлениями. К примеру, Япония переживает кризис в противодействии киберпреступности, при этом правительство страны не может изменить ситуацию кардинально. В Японии особенно остро встала проблема утечки данных. Общее число кибератак возросло с 12,8 млрд по состоянию на 2013 г. до 128,1 млрд по состоянию на 2016 г. Выходит, что в процентном соотношении активность киберпреступников за три года увеличилась на 900 % [15].

Основной способ предупреждения киберпреступности заключается во внедрении передовых технологий кибербезопасности в работу заинтересованных организаций. Общество и государство должны осознать, что многие современные системы безопасности, пароли и коды смогут спасти системы данных, важнейшие информационные банки. Например, одной из крупнейших жертв вируса WannaCry стала Национальная служба здравоохранения в Англии и Шотландии. Позже было установлено, что возможно было предотвратить атаку с помощью установки систем современной базовой информационной безопасности, что не было сделано своевременно.

Сегодня применяют меры для выявления зараженных систем, идентифицируют заражающие системы. Но такой подход во многом стал

терпеть неудачу, потому что количество кибератак значительно возросло. По этой причине надо искать новые пути защиты. Преступники, активно вторгающиеся в киберпространство, имеют хорошую технологическую подготовку и оснащенность, при этом, совершая преступления дистанционно, затрудняют возможность их идентификации благодаря технологиям сетей Интернет и Даркнет, что существенно снижает раскрываемость подобного рода деяний [16].

Преступность в Интернете растет, увеличивая как количество форм, так и свои размеры. В последние десять лет компании уже столкнулись с противоправным присвоением активов. В глобальном исследовании PwC говорится, что более трети всех респондентов стали жертвами кибератак, совершенных с помощью вредоносных программ и фишинга [12]. По данным McAfee, каждый день производится 80 млрд вредоносных объектов, 300 тыс. новых вредоносных программ, 780 тыс. записей (паролей) подвергается взлому. Эпидемия киберпреступности поразила США настолько сильно, что, по мнению специального агента Федерального бюро расследований, который расследует кибервторжения, каждый гражданин США должен ожидать, что все его данные (личная информация) будут украдены в ближайшем будущем[4].

Скорость интернет-соединения опережает нашу способность должным образом защитить себя. Всемирная паутина была изобретена в 1989 г. Первый в мире веб-сайт начал функционировать в 1991 г. Сейчас их насчитывается почти 1,9 млрд. Аналитическое агентство We Are Social и крупнейшая SMM-платформа Hootsuite совместно подготовили пакет отчетов о глобальном цифровом рынке. По представленным в отчетах данным, сегодня во всем мире Интернетом пользуется более 4 млрд чел. по сравнению с 2 млрд в 2015 г. [17].

Специалисты в сфере кибербезопасности прогнозируют, что к 2022 г. будет 6 млрд пользователей Интернета (75 % от прогнозируемого мирового населения в 8 млрд) и более 7,5 млрд пользователей — к 2030 г., т.е. 90 % от прогнозируемого мирового населения (8,5 млрд). «Степень сложности защиты бизнеса от кибератак возрастает пропорционально ряду факторов», — указывает Р. Херджавек. «Активисты возникающих угроз, известность взаимосвязанных устройств и… самое важное — объем данных, которые необходимо защитить, — все это усугубляет эту сложную задачу» — борьбы с кибератаками [18].

Microsoft полагает, что объемы онлайн-данных в 2020 г. будут в 50 раз больше, чем в 2016 г. Cisco подтвердила, что к 2021 г. трафик облачных центров обработки данных будет составлять 95 % от общего объема трафика центров обработки данных. По мнению экспертов по кибербезопасности, общий объем данных, хранящихся в облаке, включая общедоступные облака, управляемые поставщиками и компаниями, работающими в социальных сетях (например, AWS, Twitter, Facebook и т.д.), принадлежащие государству облака, доступные для граждан и предприятий, а также частные облака, принадлежащие корпорациям среднего и крупного размера, к 2021 г. будет в 100 раз больше, чем сегодня. Gartner прогнозирует, что в 2021 г. во всем мире будет продано более 0,5 млрд носимых устройств по сравнению с 310 млн в 2017 г. Носимые устройства включают умные часы, дисплеи, телекамеры, гарнитуры Bluetooth и фитнес-мониторы. Ожидается, что объем цифрового контента в мире увеличится с 4 млрд терабайт (4 зетабайта) в 2016 г. до 96 зетабайт к 2020 г. [там же]. Данные факторы будут способствовать масштабному росту киберпреступлений, для противодействия которым правоохранительным органам необходимо не отставать от преступников в использовании современных цифровых технологий.

Для хранения данных в цифровом виде используются их объемные хранилища, или базы данных, которые для киберпреступников являются аналогами банковских хранилищ или сейфов. Чем больше объем содержащейся в базе данных актуальной информации, тем больший интерес она представляет для киберпреступников. До 2008 г. альтернатив централизованному хранению данных (централизованное мы понимаем в том смысле, что администратором базы данных выступало одно доверенное лицо, которому доверяют хранение данных их фактические собственники) не существовало. У любой базы данных была одна центральная точка атаки (ранее — замок банковского сейфа), которую надо было вскрыть, чтобы получить доступ к хранящейся в базе информации.

В 2008 г. вышла «белая бумага» проекта «Биткоин», в которой представлен совершенно новый взгляд на хранение и защиту инфор-

[4] Norton Cyber Security Insights Report. 2017. Global Results. URL: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.

мации — технология блокчейн, основанная на объединении имевшихся и использовавшихся по отдельности технологий из сфер криптографии и хранения данных. По нашему мнению, эта новая технология имеет революционное значение в цифровой криминологии [19].

В блокчейне или распределенном реестре (блокчейн является частным случаем распределенного реестра) данные хранятся на компьютерах всех участников сети, центральный администратор сети отсутствует, а целостность данных и защита от противоправного доступа к ним третьих лиц гарантируются использованием криптографических примитивов (хэш-функция, асимметричное шифрование, использование публичного и секретного ключей, бинарные деревья).

Информация, хранимая в блокчейне, организована в виде цепочки блоков (отсюда и название), и каждый следующий блок связан с предыдущим таким образом, что внесение любых изменений в него автоматически изменяет все последующие блоки, а поскольку цепочка блоков хранится на компьютерах всех пользователей (собственников) этой базы данных, то внесение изменений не может быть незаметным. Помимо очевидного преимущества в виде неизменности данных, блокчейн также позволяет восстановить всю хронологию вносимых в них изменений (в централизованных базах данных хранится несколько резервных копий на конкретный момент времени, и полная хронология изменений недоступна).

Центральное звено, или единый администратор базы данных, отсутствует, и атака на такую базу по старым правилам становится неэффективной. Внесение изменений в содержащиеся в ней данные невозможно без знания секретного ключа собственника данных (в блокчейне нет общего хозяина данных, каждый из пользователей базы, внесших в нее записи или хранящий в ней информацию, сам и является ее собственником).

Базу данных, в которой хранится критически важная для функционирования государства информация (Центробанк России, Пенсионный фонд, налоговые органы и др.), ведет одна соответствующая организация (т.е. единый центральный посредник). Преступники видят единую цель, на которую следует нападать, получать контроль, совершать хищение данных. Если же хранение данных и их контроль распределить между несколькими организациями (сделать закрытый, частный блокчейн), то исчезает единая точка для атаки, а также появляются все преимущества неизменности данных и полная история всех операций.

Это поможет в борьбе с киберпреступлениями следующим образом:

– нет единой точки атаки на базу данных;

– получить доступ к данным, зашифрованным при помощи секретного ключа, невозможно без знания этого ключа, а ключи хранятся не централизованно, а у каждого пользователя, и атака на центр-сервер не даст возможность похитить сразу все данные;

– сохраняется история операций, поэтому видно, что и куда перевели или какие данные были считаны, а так как база есть у всех пользователей, то изменения отобразятся синхронно у всех и, более того, станет известно, чей секретный ключ использовался.

Ключевым является тот важный факт, что в блокчейне содержится информация обо всех данных, которые проходят через него. По мнению Т. Дрейпера, криминальной сфере будет нанесен ощутимый удар, так как все финансовые потоки будут видны в цепочке блоков и замаскировать их будет практически невозможно, что сведет на нет нелегальные транзакции, существенно усложнит финансирование террористических и экстремистских организаций [20]. Блокчейн может стать именно той технологией, которая значительно снизит масштабы криминальных процессов в теневой экономике, облегчив контроль за движением финансов. При этом можно предположить, что в будущем фиатные деньги станут основной валютой преступников и террористов, а не криптовалюты, работающие на прозрачном блокчейне.

Говоря о трекинге транзакций, следует упомянуть взлом криптовалютной биржи Cryptopia, который произошел в конце 2018 г. Хакеры перевели с торговой площадки крупную сумму денежных средств в криптовалюте (23 млн дол.) на свои кошельки, тем самым подорвав нормальную работу биржи. Полиция Новой Зеландии, используя современные цифровые технологии, в сотрудничестве с высококвалифицированными IT-специалистами добилась значительных успехов в выявлении организаторов данной атаки и возврате средств, так как украденная криптовалюта активно отслеживается через блокчейн. Обналичивание криптовалюты или же ее обмен на другие криптоактивы через сторонние крипто-

валютные биржи становится проблемой для преступников (торговые и обменные площадки могут замораживать подозрительные аккаунты и изымать с них средства, возвращая их обратно владельцам) [21]. Являясь распределенной базой данных, блокчейн хранит общую для всех информацию, которая сверяется на постоянной основе. Так как данные в блокчейне содержатся децентрализованным образом, преступники не могут повредить ключевой узел системы и организовать утечку или подмену информации. Такой формат хранения данных может использоваться не только для отслеживания транзакций, но и для создания универсальных закрытых регистров в абсолютно различных сферах деятельности [22].

Посредством использования технологии блокчейн можно вести борьбу с коррупционными схемами. Например, в Индии фальсификации в выборе подрядчиков достигают критических для государства и общества масштабов [23]. Блокчейн же обладает необходимыми качествами для создания распределенной системы учета голосов избирателей, тем самым исключая противоправные действия в выборном процессе. Специалисты уже работают над созданием такой модификации блокчейна, чтобы фальсификация выборов сводилась на нет [24].

Когда некоторые авторы на первый план выдвигают проблему криптовалюты (продукта блокчейна), с помощью которой финансируется терроризм, следует обратить внимание на следующее. ХАМАС собрала всего лишь 4 тыс. дол. в BTC-эквиваленте (биткоин) после анонса самого сбора в Telegram [25]. Это не та сумма, из-за которой криптовалюту можно именовать основным средством финансирования терроризма. Авторы считают, что криптовалюты не являются удобным средством для проведения финансовых операций в рамках террористических организаций. Это связано с тем, что их нужно переводить в фиатные деньги, что для террористов значительно усложняет весь процесс в целом. Использовать наличные деньги или банковские счета существенно проще.

Профессор Б.А. Спасенников пишет: «В современном цифровом мире борьба с киберпреступностью, к сожалению, отстает от технологических новаций криминала и террористических организаций, которые вербуют в свои ряды IT-специалистов, имеющих высокий IQ, ведущих внешне благопристойный образ жизни, предоставляя им интересную удаленную работу, соединенную с очень высоким доходом. Поэтому необходима технологическая революция и в полицейской деятельности, направленная на создание искусственного интеллекта в системах кибербезопасности, принципиально новых методов для борьбы с цифровой преступностью, которые бы опережали технологические возможности криминалитета и террористов; актуален поиск среди выпускников качественных IT-вузов будущих сотрудников полиции, органов безопасности, имеющих высокий уровень компетентности в сфере кибербезопасности, цифровой криминологии» [6, с. 86].

Итак, в современном цифровом мире регистрируется устойчивый рост киберпреступности, которая угрожает правопорядку, финансовой стабильности, государственным институтам ведущих мировых держав. Рост киберпреступности сопровождается серьезными кибертеррористическими угрозами, что требует поиска новых подходов к обеспечению кибербезопасности. По мнению авторов, технология распределенных реестров/блокчейн может обеспечить надлежащий уровень кибербезопасности, способна служить эффективным средством предупреждения киберпреступности, кибертерроризма в современном цифровом мире.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Спасенников Б.А. Актуальные проблемы уголовного права: обзор литературы / Б.А. Спасенников, Б.А. Швырев, А.М. Смирнов // Актуальные вопросы образования и науки. — 2015. — № 3–4 (49–50). — С. 35–41.

2. Спасенников Б.А. Актуальные проблемы уголовного права: обзор литературы / Б.А. Спасенников // Актуальные вопросы образования и науки. — 2015. — № 1–2 (47–48). — С. 36–38.

3. Colin B.C. The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge / B.C. Colin // 11th Annual International Symposium on Criminal Justice Issues. — URL: http://www.crime-research.org/library/Cyberter.htm.

4. Антонян Е.А. Блокчейн-технологии в противодействии кибертерроризму / Е.А. Антонян, И.И. Аминов // Актуальные проблемы российского права. — 2019. — № 6 (103). — С. 167–177.

5. Singer P.W. The Cyber Terror Bogeyman / P.W. Singer // Brookings. — 2012. — 1 Nov. — URL: https://www.brookings.edu/articles/the-cyber-terror-bogeyman.

6. Спасенников Б.А. Криминология: медико-социальный взгляд / Б.А. Спасенников. — Москва : Изд-во НИИ ФСИН России, 2018. — 184 с.

7. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / А.П. Суходолов, С.В. Иванцов, С.В. Борисов, Б.А. Спасенников. — DOI: 10.17150/2500-4255.2017.11(1).13-21 // Всероссийский криминологический журнал. — 2017. — Т. 11, № 1. — С. 13–21.

8. Смеркис В. Опыт развитых стран: почему ЕС запретил анонимную торговлю криптовалютами / В. Смеркис // Forbes. — 2018. — 24 Apr. — URL: https://www.forbes.ru/tehnologii/360519-opyt-razvityh-stran-pochemu-es-zapretil-anonimnuyu-torgovlyu-kriptovalyutami.

9. Баулин А. Криптовалюта попала под контроль: в Китае запретили ICO / А. Баулин // Forbes. — 2017. — 4 Sept. — URL: https://www.forbes.ru/tehnologii/349825-kriptovalyuta-popala-pod-kontrol-v-kitae-zapretili-ico.

10. Спасенников Б.А. Общая теория права / Б.А. Спасенников. — Москва : НИИ ФСИН России, 2018. — 214 с.

11. Cashen L. Cybercrime set to cost the world $6 trillion annually by 2021, could Blockchain be the answer? / L. Cashen. — URL: https://medium.com/natmin-pure-escrow/-656f334f7a09.

12. Lavion D. Global Economic Crime and Fraud Survey 2018 / D. Lavion. — URL: https://www.pwc.com/gx/en/forensics.

13. Metropoulos E. Global Cyber Terrorism Incidents on the Rise / E. Metropoulos, J.S. Platt // Marsh and McLennan Insights. — URL: https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.

14. Holden D. Is Cyber-Terrorism the New Normal? / D. Holden // Wired. — URL: https://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal.

15. Volodzko D. Japan's Cyberterrorism Crisis Threatens Us All / D. Volodzko // Forbes. — 2018. — 26 Nov. — URL: https://www.forbes.com/sites/davidvolodzko/2018/11/26/japans-cyberterrorism-crisis-threatens-us-all/#26561df06878.

16. Zerzri M. The Threat of Cyber Terrorism and Recommendations for Countermeasures / M. Zerzri. — URL: https://www.cap-lmu.de/download/2017.

17. Сергеева Ю. Интернет 2017–2018 в мире и в России: статистика и тренды / Ю. Сергеева // WebCanape. — URL: https://www.web-canape.ru/business/internet-2017-2018-v-mire-i-v-rossii-statistika-i-trendy.

18. Herjavec R. Official Annual Cybercrime Report / R. Herjavec // Cybersecurity Ventures. — URL: https://cybersecurityventures.com.

19. Накамото С. Биткойн: система цифровой пиринговой наличности / С. Накамото // Bitcoin. — URL: http://bitcoinwhitepapers.com/bitcoin_ru.pdf.

20. Partz H. Tim Draper Predicts Crypto Will Rule, Only Criminals Will Use Cash in Five Years / H. Partz // Cointelegraph. — URL: https://cointelegraph.com/news/tim-draper-predicts-crypto-will-rule-only-criminals-will-use-cash-in-five-years.

21. Henderson J. Police making ‘excellent progress’ in hunt for stolen Cryptopia funds / J. Henderson // ResellerNews. — 2019. — 11 Febr. — URL: https://www.reseller.co.nz/article/657565.

22. Bourque A. How Blockchain Can End Cannabis Looping and Smurfing Schemes / A. Bourque // Forbes. — 2019. — 28 Febr. — URL https://www.forbes.com/sites/andrebourque/2019/02/28/how-blockchain-can-end-cannabis-looping-and-smurfing-schemes/#522cf973605f.

23. Desai R.D. India Continues to Rank Among Most Corrupt Countries in the World / R.D. Desai // Forbes. — 2018. — 7 March. — URL: https://www.forbes.com/sites/ronakdesai/2018/03/07/india-continues-to-be-one-of-the-most-corrupt-countries-in-the-world/#128f927479c6.

24. Miller B. Blockchain Voting Startup Raises $2.2M / B. Miller // Government Technology. — 2018. — 8 Jan. — URL: https://www.govtech.com/biz/Blockchain-Voting-Startup-Raises-22M.html.

25. Cuen L. Blockchain Analysis Links Hamas Fundraising to Coinbase Bitcoin Account / L. Cuen // Coindesk. — 2019. — 7 Febr. — URL: https://www.coindesk.com/hamas-coinbase-bitcoin.

REFERENCES

1. Spasennikov B.A., Shvyrev B.A., Smirnov A.M. Topical Issues of Criminal Law: an Overview of Publications. *Aktual'nye voprosy obrazovaniya i nauki = Topical Issues of Education and Science*, 2015, no. 3–4 (49–50), pp. 35–41. (In Russian).

2. Spasennikov B.A. Topical Issues of Criminal Law: an Overview of Publications. *Aktual'nye voprosy obrazovaniya i nauki = Topical Issues of Education and Science*, 2015, no. 1–2 (47–48), pp. 36–38. (In Russian).

3. Colin B.C. The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. *11th Annual International Symposium on Criminal Justice Issues*. Available at: http://www.crime-research.org/library/Cyberter.htm.

4. Antonyan E.A., Aminov I.I. Blockchain Technology in Countering Cyber Terrorism. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law,* 2019, no. 6 (103), pp. 167–177. (In Russian).

5. Singer P.W. The Cyber Terror Bogeyman. *Brookings,* 2012, November 1. Available at: https://www.brookings.edu/articles/the-cyber-terror-bogeyman.

6. Spasennikov B.A. *Kriminologiya: mediko-sotsial'nyi vzglyad* [Criminology: medical and social outlook]. Moscow, Research Institute of the Federal Penitentiary Service of Russia Publ., 2018. 184 p.

7. Sukhodolov A.P., Ivantsov S.V., Borisov S.V., Spasennikov B.A. Topical issues of preventing economic crimes committed with the use of information and telecommunication networks. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2017, vol. 11, no. 1, pp. 13–21. DOI: 10.17150/2500-4255.2017.11(1).13-21. (In Russian).

8. Smerkis V. The experience of developed countries: why the EU banned anonymous trade in cryptocurrencies. *Forbes*, 2018, April 24. Available at: https://www.forbes.ru/tehnologii/360519-opyt-razvityh-stran-pochemu-es-zapretil-anonimnuyu-torgovlyu-kriptovalyutami. (In Russian).

9. Baulin A. Cryptocurrency gets under control: ICO is prohibited in China. *Forbes,* 2017, September 4. Available at: https://www.forbes.ru/tehnologii/349825-kriptovalyuta-popala-pod-kontrol-v-kitae-zapretili-ico. (In Russian).

10. Spasennikov B.A. *Obshchaya teoriya prava* [A General Theory of Law]. Moscow, Research Institute of the Federal Penitentiary Service of Russia Publ., 2018. 214 p.

11. Cashen L. *Cybercrime set to cost the world $6 trillion annually by 2021, could Blockchain be the answer?* Available at: https://medium.com/natmin-pure-escrow/-656f334f7a09.

12. Lavion D. *Global Economic Crime and Fraud Survey 2018.* Available at: https://www.pwc.com/gx/en/forensics.

13. Metropoulos E., Platt J.S. Global Cyber Terrorism Incidents on the Rise. *Marsh and McLennan Insights*. Available at: https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.

14. Holden D. Is Cyber-Terrorism the New Normal? *Wired*. Available at: https://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal.

15. Volodzko D. Japan's Cyberterrorism Crisis Threatens Us All. *Forbes*, 2018, November 26. Available at: https://www.forbes.com/sites/ davidvolodzko/2018/11/26/japans-cyberterrorism-crisis-threatens-us-all/#26561df06878.

16. Zerzri M. *The Threat of Cyber Terrorism and Recommendations for Countermeasures*. Available at: https://www.cap-lmu.de/download/2017.

17. Sergeeva Yu. The Internet in 2017-2018 in Russia and in the world: statistics and trends. *WebCanape*. Available at: https://www.web-canape.ru/business/internet-2017-2018-v-mire-i-v-rossii-statistika-i-trendy. (In Russian).

18. Herjavec R. Official Annual Cybercrime Report. *Cybersecurity Ventures*. Available at: https://cybersecurityventures.com.

19. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.* Available at: http://bitcoinwhitepapers.com. (In Russian).

20. Partz H. Tim Draper Predicts Crypto Will Rule, Only Criminals Will Use Cash in Five Years. *Cointelegraph*. Available at: https://cointelegraph.com/news/tim-draper-predicts-crypto-will-rule-only-criminals-will-use-cash-in-five-years.

21. Henderson J. Police making 'excellent progress' in hunt for stolen Cryptopia funds. *ResellerNews*, 2019, February 11. Available at: https://www.reseller.co.nz/article/657565.

22. Bourque A. How Blockchain Can End Cannabis Looping and Smurfing Schemes. *Forbes*, 2019, February 28. Available at: https://www.forbes.com/sites/andrebourque/2019/02/28/how-blockchain-can-end-cannabis-looping-and-smurfing-schemes/#522cf973605f.

23. Desai R.D. India Continues to Rank Among Most Corrupt Countries in the World. *Forbes*, 2018, March 7. Available at: https://www.forbes.com/sites/ronakdesai/2018/03/07/india-continues-to-be-one-of-the-most-corrupt-countries-in-the-world/#128f927479c6.

24. Miller B. Blockchain Voting Startup Raises $2.2M. *Government Technology,* 2018, January 8. Available at: https://www.govtech.com/biz/Blockchain-Voting-Startup-Raises-22M.html.

25. Cuen L. Blockchain Analysis Links Hamas Fundraising to Coinbase Bitcoin Account. *Coindesk*, 2019, February 7. Available at: https://www.coindesk.com/hamas-coinbase-bitcoin.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Суходолов Александр Петрович — проректор по науке Байкальского государственного университета, профессор, г. Иркутск, Российская Федерация; e-mail: science@bgu.ru.

Антонян Елена Александровна — профессор кафедры криминологии и уголовно-исполнительного права Московского государственного юридического университета им. О.Е. Кутафина, профессор кафедры уголовного права Российского государственного гуманитарного университета, доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: antonyaa@yandex.ru.

Рукинов Максим Владимирович — научный сотрудник Центра технологий распределенных реестров Санкт-Петербургского государственного университета, управляющий директор «Цифровая архитектура», г. Санкт-Петербург, Российская Федерация; e-mail: amfortiss@gmail.ru.

Шамрин Максим Юрьевич — старший преподаватель кафедры административного права Московского государственного юридического университета им. О.Е. Кутафина, кандидат юридических наук, г. Москва, Российская Федерация; e-mail: Akr177@protonmail.com.

Спасенникова Марина Геннадьевна — ведущий научный сотрудник Национального научно-исследовательского института общественного здоровья им. Н.А. Семашко, кандидат медицинских наук, доцент, г. Москва, Российская Федерация; e-mail: mspasennikova@gmail.com.

INFORMATION ABOUT THE AUTHORS

Sukhodolov, Alexander P. — Vice Rector for Research, Baikal State University, Professor, Irkutsk, the Russian Federation; e-mail: science@bgu.ru.

Antonyan, Elena A. — Professor, Chair of Criminology and Penal Law, O.E. Kutafin Moscow State Law University; Professor, Chair of Criminal Law, Russian State University for the Humanities, Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: antonyaa@yandex.ru.

Rukinov, Maxim V. — Researcher, Center of Distributed Registries Technology, Saint Petersburg State University, Managing Director of «Digital Architecture», Saint Petersburg, the Russian Federation; e-mail: amfortiss@gmail.ru.

Shamrin, Maxim Yu. — Senior Lecturer, Chair of Administrative Law, O.E. Kutafin Moscow State Law University, Ph.D. in Law, Moscow, the Russian Federation; e-mail: Akr177@protonmail.com.

Spasennikova, Marina G. — Leading Researcher, N.A. Semashko National Research Institute of Public Health, Ph.D. in Medicine, Ass. Professor, Moscow, the Russian Federation; e-mail: mspasennikova@gmail.com.

ДЛЯ ЦИТИРОВАНИЯ

Суходолов А.П. Блокчейн в цифровой криминологии: постановка проблемы / А.П. Суходолов, Е.А. Антонян, М.В. Рукинов, М.Ю. Шамрин, М.Г. Спасенникова // Всероссийский криминологический журнал. — 2019. — Т. 13, № 4. — С. 555–563. — DOI: 10.17150/2500-4255.2019.13(4).555-563.

FOR CITATION

Sukhodolov A.P., Antonyan E.A., Rukinov M.V., Shamrin M.Yu., Spasennikova M.G. Blockchain in digital criminology: problem statement. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 4, pp. 555–563. DOI: 10.17150/2500-4255.2019.13(4).555-563. (In Russian).