УДК 343.7:347.23:004
DOI 10.17150/2500-4255.2020.14(6).845-854

ПРЕСТУПЛЕНИЯ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫЕ В СФЕРЕ ФУНКЦИОНИРОВАНИЯ БЛОКЧЕЙНА: НОВЫЕ ПРЕСТУПНЫЕ СХЕМЫ И ИХ УГОЛОВНО-ПРАВОВАЯ ОЦЕНКА

С.М. Мкртчян
Волгоградский государственный университет, г. Волгоград, Российская Федерация

Информация о статье

Дата поступления
12 июня 2020 г.

Дата принятия в печать
21 декабря 2020 г.

Дата онлайн-размещения
30 декабря 2020 г.

Ключевые слова
Преступления против собственности; мошенничество; блокчейн; криптовалюты; биткоин; майнинг; ICO; вредоносные программы

Финансирование
Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00823

Аннотация. В современных условиях сферу функционирования блокчейна и оборота криптовалют следует признать одной из наиболее активно развивающихся отраслей хозяйствования, в том числе ввиду наличия таких уникальных особенностей, как децентрализованность сети, анонимность пользователей и их действий, невозможность отмены или возврата транзакций, а также высокая волатильность виртуальных валют. Указанные черты обусловили привлекательность технологии блокчейн не только для добросовестных хозяйствующих субъектов, но и для преступников. Длительное время большинством представителей отечественной и зарубежной юридической науки сфера функционирования блокчейна рассматривалась лишь как область распространения преступных посягательств, связанных с незаконным сбытом продукции, услуг либо материалов, оборот которых ограничен или запрещен (наркотические средства, оружие, порнографические материалы и т.п.), а также отмыванием полученных преступным путем доходов или финансированием терроризма. Современные общемировые тенденции в сфере борьбы с киберпреступностью не оставляют, однако, сомнений в том, что весьма утопичными являются представления о неуязвимости сети блокчейн для несанкционированного вмешательства путем модификации кодов, применения вредоносных программ и совершения хищений либо иных преступлений против собственности ее пользователей или третьих лиц. Названные тенденции, как показывает законодательная практика последних лет, пока не были восприняты на территории нашего государства. В рамках исследования, результаты которого отражены в настоящей статье, проведен анализ наиболее распространенных в общемировом виртуальном пространстве, включая его российский сегмент, схем совершения преступлений против собственности в сфере функционирования блокчейна. Описаны соответствующие действующему уголовному законодательству и принятые в отечественной судебной практике варианты квалификации подобных преступных деяний. Выявлены случаи несоответствия текстов некоторых статей УК РФ уровню общественной опасности и содержанию преступных деяний против собственности, совершаемых с использованием информационных технологий, в том числе в сфере функционирования блокчейна. Внесен ряд предложений по совершенствованию текстов ст. 158, 159.6, 165, 272 и 273 УК РФ.

PROPERTY CRIMES IN THE BLOCKCHAIN SPHERE: NEW CRIMINAL SCHEMES AND THEIR CRIMINAL LAW ASSESSMENT

Sona M. Mkrtchian
Volgograd State University, Volgograd, the Russian Federation

Article info

Received
2020 June 12

Accepted
2020 December 21

Abstract. The sphere of blockchain and circulation of cryptocurrency should be recognized as one of the most dynamically developing branches of economy, and this claim is further supported by its unique features, such as the de-centralized character of the net, the anonymity of users and their actions, the inability to recall or reverse the transaction, and a high volatility of virtual currencies. These characteristics made the blockchain technology attractive not only for law-abiding individuals, but also for

ISSN 2500-4255

Available online
2020 December 30

Keywords
Property crimes; fraud; blockchain; cryptocurrencies; bitcoin; mining; ICO; malicious software

Acknowledgements
This research was funded by the RFBR, Project number 20-011-00823

criminals. For a long time most legal scholars in Russia and abroad viewed the sphere of blockchain as the sphere of criminal actions connected with illegal trade in goods, services or materials, whose circulation is limited or forbidden (narcotic substances, arms, pornography, etc.), and with laundering of illegal gains or financing terrorism. Current global trends in combating cybercrime leave no doubt that the ideas of the invulnerability of the blockchain net to unsanctioned access through the modifications of codes, the use of malware, the invulnerability to thefts or other property crimes against users or the third party are rather utopian. The legislative practice of recent years shows that these trends have not yet been recognized in our country. The research presented in this article consisted in the analysis of property crimes in the sphere of blockchain that are most common in the global virtual space, including in its Russian segment. The author describes the options for the qualification of such criminal actions provided by the current legislation and used in Russian court practice. The author also identifies the cases when the texts of some Articles of the Criminal Code of the Russian Federation do not match the level of public danger and the essence of criminal infringements against property committed with the use of information technologies, including the sphere of blockchain. A number of suggestions on improving the texts of Art. 158, 159.6, 165, 272 and 273 of the CC of the RF are presented.

Осознание значимости сети блокчейн не только как виртуального пространства, предназначенного для обращения криптовалют, следует признать, пожалуй, наиболее яркой тенденцией в сфере виртуальных технологий в России за истекший 2019 год. Так, согласно распоряжению Правительства Российской Федерации «Об утверждении Стратегии развития экспорта услуг до 2025 года» от 14 августа 2019 г. № 1797-р, блокчейн, наряду с интернетом вещей, искусственным интеллектом и анализом больших данных, на государственном уровне назван развивающейся прорывной цифровой технологией, способной в том числе «повлиять на глобальную финансовую архитектуру»[1]. Впрочем, не менее устойчивой следует признать и общемировую тенденцию снижения уровня оптимизма, связанного с повсеместным внедрением и использованием технологии блокчейн. Однако, к сожалению, данная тенденция пока не находит отклика в законодательной практике Российской Федерации. Дело в том, что в соответствии с распоряжением Правительства Российской Федерации «Об утверждении Стратегии развития электронной промышленности Российской Федерации на период до 2030 года» от 17 января 2020 г. № 20-р в числе мероприятий и целевых индикаторов реализации данной Стратегии в части ключевого направления «Научно-техническое развитие» предусматривается разработка и промышленное освоение «технологии шифрования и криптозащиты», к последней из которых авторы соответствующего нормативного акта относят и «аппаратную реализацию технологий блокчейна»[2]. Несмотря на то что апробированные в практической деятельности и тщательно изученные компьютерные технологии уже давно используются для предупреждения и раскрытия правонарушений (облачные технологии, Big Data и т.п. [1]), применительно к блокчейн-технологии нелишним будет обратить внимание на очевидное: вряд ли можно признать эффективным средством защиты то, которое само нуждается в защите. Последнее подтверждается статистическими данными экспертов в сфере кибербезопасности и IT-технологий. Так, по данным агентства Reuters, убытки от преступности в сфере цифровых валют только за первые девять месяцев 2019 г. выросли до 4,4 млрд дол. США, т.е. более чем на 150 % по сравнению с показателями за весь 2018 г. в целом (1,7 млрд дол. США) [2]. Важное значение имеют и аналитические данные правоохранительных структур Российской Федерации. По словам начальника Главного управления экономической безопасности и противодействия коррупции МВД России А. Курносенко, размер материального ущерба, причиненного киберпреступлениями на территории нашей страны, к сентябрю 2019 г. превысил 10 млрд р., а за прошедшие три года динамика прироста преступлений в сфере ин-

[1] Об утверждении Стратегии развития экспорта услуг до 2025 года (вместе с «Планом мероприятий по реализации Стратегии развития экспорта услуг до 2025 года) [Электронный ресурс] : распоряжение Правительства РФ от 14 авг. 2019 г. № 1797-р // СПС «КонсультантПлюс».

[2] Об утверждении Стратегии развития электронной промышленности Российской Федерации на период до 2030 года [Электронный ресурс] : распоряжение Правительства РФ от 17 янв. 2020 г. № 20-р // СПС «КонсультантПлюс».

формационных технологий превысила 165 % (только за девять месяцев 2019 г. было зарегистрировано более 200 тыс. фактов совершения таких преступлений), причем отмечается устойчивый рост интереса злоумышленников к виртуальным активам [3]. Столь широкое распространение и значительное негативное влияние киберпреступности, в том числе в сфере функционирования блокчейна и оборота криптовалюты, кроме очевидных последствий в виде реального имущественного ущерба и упущенной выгоды, организационного вреда в форме банкротства и ликвидации виртуальных хозяйствующих субъектов, в долгосрочной перспективе может явиться причиной недоверия обычных пользователей к сети блокчейн и всем виртуальным продуктам, функционирующим на ее основе. Согласно современным криминологическим и криминалистическим исследованиям, состояние и динамика киберпреступности напрямую связаны со снижением активности в использовании онлайн-ресурсов, в частности интернет-банкинга, электронной коммерции и т.п., и способны оказывать непосредственное влияние на защищенность жизненно важных интересов в сфере защиты персональных данных и иных сведений, содержащих охраняемую законом тайну [4, с. 7; 5]. Очевидно, что в таком случае вряд ли можно будет говорить о создании благоприятных условий для развития интеллектуального, научного, изобретательского и творческого потенциала отдельных граждан и достойном уровне развития IT-технологий на территории страны.

С учетом последних изменений в ГК РФ, согласно которым криптовалюты, токены и иные виртуальные активы были отнесены к категории «цифровые права» как разновидности объектов гражданского оборота[3], уже нельзя вести речь о том, что сеть блокчейн может быть признана российской наукой, законодателем и правоприменителями лишь в качестве сферы распространения преступлений, связанных с незаконным оборотом запрещенных товаров, оплачиваемых виртуальными валютами (наркотики, оружие, порнографические материалы и прочие товары и услуги теневого рынка). Во-первых, следует учитывать постоянное повышение уровня изобретательности киберпреступников в современных условиях, которая простирается далеко за пределы использования лишь для коммуникации потенциала Теневой сети (DarkNet), программного обеспечения Tor, технологий VPN и подобных им и включает, например, широкое применение схем типа botnet (сеть подконтрольных компьютеров в целях использования мощностей) или ransomware («программы-вымогатели»: захват компьютера с требованием определенных действий) [6, с. 2] и многих других. Во-вторых, сообщения в авторитетных СМИ [7; 8] свидетельствуют о том, что сеть блокчейн становится уязвимой для преступников, совершающих в том числе преступления против собственности. Более того, рассматривать криптовалюту как предмет хищения (как имущество, а в некоторых случаях и как некий виртуальный эквивалент денежных средств) склонны и некоторые правоприменители. Так, еще в 2017 г. Ш. и О. были признаны виновными в совершении преступлений, предусмотренных ч. 3 ст. 272 и ч. 3 ст. 159 УК РФ. Они, получив незаконным путем доступ к личным данным пользователей сайта, от их имени размещали в сети Интернет ложную информацию о возможности вывода (обмена на фиатные деньги) биткоинов и таким образом ввели в заблуждение потерпевшего, который «в личном сообщении передал пользователю… (подставной пользователь, профиль которого контролировали Ш. и О. — *С. М.*) BTC-e код на 10 000 USD… рыночная стоимость которого… составляет 821 100 рублей...»[4]. Очевидно, что в данном случае этот самый BTC-e код (фактически это компьютерный код, содержащий информацию о наличии у данного лица криптовалюты на сумму 10 000 дол.) суд признал предметом одного из преступлений, ответственность за совершение которых регламентирована в гл. 21 УК РФ, т.е. приравнял его к имуществу, и в частности к денежным средствам.

С учетом приведенных выше рассуждений и статистических данных в рамках настоящего исследования было сформулировано несколько исследовательских задач: 1) выявление и изучение новых схем совершения преступлений против собственности в сфере функционирования блокчейна, получивших распространение в России и в мире, в целях определения будущих тен-

[3] О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации [Электронный ресурс] : федер. закон от 18 марта 2019 г. № 34-ФЗ // СПС «КонсультантПлюс».

[4] Приговор Сургутского городского суда (Ханты-Мансийский автономный округ — Югра) от 13 нояб. 2017 г. № 1-762/2017 по делу № 1-762/2017. URL: https://sudact.ru/regular/doc/SWC7elmLAaQR.

денций и направлений развития отечественной правоприменительной практики в процессе квалификации рассматриваемых преступлений; 2) анализ текста действующего Уголовного кодекса Российской Федерации с целью определения соответствия законодательной техники формулирования некоторых его положений изменяющимся общественным отношениям в сфере функционирования сети блокчейн и его эффективности в процессе борьбы с наиболее распространенными преступлениями против собственности, совершаемыми в названной сфере.

В настоящий момент эксперты выделяют несколько наиболее распространенных схем преступлений против собственности, совершаемых в сфере функционирования блокчейна. Первой из них, которая уже давно применяется киберпреступниками для получения информации с мобильных телефонов, является так называемый phone-porting, или получение конфиденциальной информации пользователя, в том числе кодов доступа к криптовалютным кошелькам в сети блокчейн, путем подмены идентификационного номера SIM-карты (в иностранной научной литературе такие киберпреступления, связанные с несанкционированным доступом, модификацией, уничтожением или взятием под контроль IT-систем, обычно относят к особой группе «киберзависимых» преступлений, т.е. таких деяний, которые не могут быть совершены без использования IT-систем и, следовательно, в значительной степени зависят от виртуального и анонимного контекста таких систем [9, с. 2]). В результате такой манипуляции преступники имеют возможность перевести даже с закрытого криптокошелька все виртуальные средства на принадлежащие им кошельки, а затем через другие онлайн-биржи вывести виртуальные средства, присвоив тем самым им статус добросовестного владения (как известно, вернуть транзакцию в блокчейне нельзя, поэтому фактически указанные виртуальные активы можно считать потерянными для их действительного владельца). Указанная схема была применена N.T., который таким образом похитил принадлежащие M.T. активы в криптовалютах на общую сумму 24 млн дол. США [10; 11]. Кроме того, в некоторых случаях злоумышленникам не приходится подбирать коды к криптокошелькам, так как они используют инсайдерскую информацию, полученную в процессе работы в соответствующих компаниях. Так, в конце января 2020 г. появилось сообщение о задержании в Токио двух мужчин, которые, по мнению правоохранительных органов, могли быть причастны к краже биткоинов на сумму 700 млн дол. США (78 млн иен), принадлежащих токийской криптографической фирме, в которой ранее работал один из соучастников, путем использования учетных данных этого бывшего сотрудника для получения доступа к биткоин-кошелькам компании и перевода криптовалюты на принадлежащие им счета [12]. Согласно действующему уголовному законодательству РФ и позиции Пленума Верховного Суда Российской Федерации, описанной в абзаце 1 п. 21 постановления от 30 ноября 2017 г. № 48, указанные выше преступные деяния должны быть квалифицированы по п. «г» ч. 3 ст. 158 УК РФ, так как виновные в этом случае используют учетные данные собственника без незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети[5]. Представляется, однако, что действующая редакция упомянутого уголовно-правового положения не может быть распространена на случаи хищений из виртуальных кошельков, так как термины, используемые при его формулировании, не допускают расширительного толкования. Чтобы избежать в будущем излишней казуистичности текста уголовного закона при появлении новых технологий хранения и оборота денежных средств в зашифрованном виде, а также учесть современные тенденции развития информационных процессов, целесообразно воспользоваться лексикой, уже используемой в тексте ч. 1 ст. 187 УК, п. 19 ст. 3 федерального закона от 27 июня 2011 г. № 161-ФЗ[6], а также в п. 1 ч. 1 ст. 2 федерального закона от 2 августа 2019 г. № 259-ФЗ[7], — «носитель информации» и «информационная система». Указанные понятия применимы и к электронным средствам платежа, и к площадкам хранения/оборота и электронных, и виртуальных денеж-

[5] Здесь и далее текст названного акта официального толкования приводится по: О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс] : постановление Пленума Верхов. Суда РФ от 30 нояб. 2017 г. № 48. URL: http://www.supcourt.ru/documents/own/26108.

[6] О национальной платежной системе [Электронный ресурс] : федер. закон от 27 июня 2011 г. № 161-ФЗ : (ред. от 27 дек. 2019 г.) // СПС «КонсультантПлюс».

[7] О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс] : федер. закон от 2 авг. 2019 г. № 259-ФЗ // Там же.

ных средств, а также к инвестиционным платформам, в рамках которых, согласно ч. 1 ст. 141.1 ГК РФ, только и могут быть реализованы правомочия по осуществлению и приобретению цифровых прав[8]. Представляется, что аналогичные изменения должны быть внесены и в п. «в» ч. 3 ст. 159.6 УК РФ.

На первый взгляд, по той же схеме простого использования личных кодов владельцев (без перекодирования) работает и один из традиционных методов киберпреступности — фишинг, т.е. получение доступа к конфиденциальным пользовательским данным (логины, пароли) посредством «массовой рассылки электронных писем от имени популярных брендов и личных сообщений в рамках различных сервисов со ссылками на поддельные страницы сайтов, которые практически неотличимы от реальных» [13, с. 117]. В рамках настоящего исследования интерес представляет следующая схема: злоумышленники допускают специальную ошибку в названии сайта, маскируя его под название известной и надежной онлайн-площадки по обмену криптовалютами, в результате чего невнимательный пользователь, пытаясь войти на фальшивый сайт, передает конфиденциальные данные, среди которых в том числе могут быть коды доступа к онлайн-кошелькам криптовалют (например, в Великобритании в июне 2019 г. была раскрыта деятельность преступной группы, похитившей таким образом 27 млн дол. США в криптовалюте [14]). Существуют также различные модификации фишинга. Например, в июне 2019 г. появились сообщения о том, что преступники путем применения символов Unicode для подделки названия сайта выдавали фишинговый сайт за официальный сайт первичного предложения (ICO) криптовалюты Facebook под названием Libra. На подставной странице невнимательным пользователям предлагалось обменять мифическую криптовалюту на совершенно реальные биткоин (Bitcoin) и эфириум (Ethereum) [15]. Согласно абзацу 2 п. 21 постановления Пленума Верховного Суда Российской Федерации, подобные деяния необходимо квалифицировать по ст. 159 УК РФ (происходит воздействие на сознание потерпевшего путем введения его в заблуждение относительно надежности передачи данных, идентичности соответствующего бренда, принадлежности сайта авторитетному, заслуживающему доверия хозяйствующему субъекту и т.п.). С учетом курса наиболее известных криптовалют современности (Bitcoin и Ethereum), весьма вероятно, некоторые подобные деяния необходимо будет квалифицировать по ч. 3 (или 4) названной статьи как мошенничество, совершенное в крупном (или особо крупном) размере (в зависимости от объемов хищения). Однако, как представляется, даже в этом случае не в полной мере будет учтен уровень общественной опасности личности виновного, который намеревается путем введения в заблуждение неограниченного круга лиц получить сверхприбыль, что свидетельствует о таких негативных, препятствующих его исправлению и предупреждению в дальнейшем совершения новых преступлений свойствах преступника, как алчность, стремление к легкой наживе и т.п., а также безразличие к судьбе и материальному положению множества людей. В таких условиях целесообразно включение в текст ч. 3 ст. 159 УК РФ в качестве квалифицирующего признака характеристики «в отношении неопределенного круга лиц» (иные аргументы к подобному предложению, но применительно к преступным ситуациям ICO-мошенничества были отражены также в другой работе автора настоящей статьи [16]).

Пожалуй, самой распространенной на сегодняшний день в мире преступной схемой, бросающей тень на «непогрешимость» блокчейна как максимально защищенной, не поддающейся взлому цепочки кодов, является совокупность разнообразных несанкционированных кибератак, предполагающих воздействие на коды «горячих» (открытых) электронных кошельков криптовалютных онлайн-бирж. Указанные субъекты виртуального пространства аккумулируют огромные объемы криптовалют других пользователей для их оборота (обмена на фиатные денежные средства, простого хранения, перевода между пользователями, отслеживания их курса и т.п.), поэтому они вынуждены держать хотя бы часть средств в открытых кошельках в целях обеспечения непрерывности виртуального взаимодействия, что и привлекает компьютерных мошенников. В зарубежной криминологической науке преступников, реализующих анализируемые здесь и далее преступные схемы (в отличие от описанных выше), обычно относят к типу high-security visions of crime, т.е. к технически подкованным преступникам, обладающим исключительным воображением, творческим подходом к совершению преступлений и инициативностью

[8] Гражданский кодекс Российской Федерации. Ч. 1 от 30 нояб. 1994 г. № 51-ФЗ [Электронный ресурс] : (ред. от 12 мая 2020 г.) // СПС «КонсультантПлюс».

в процессе поиска возможностей осуществления преступной деятельности, для противодействия деяниям которых требуются дополнительные приемы обеспечения безопасности данных [17, с. 869–870]. Указанное, очевидно, свидетельствует о повышенной общественной опасности личности таких преступников и совершаемых ими преступлений. К примеру, по сведениям агентства Reuters, онлайн-криптобиржа Mt. Gox прекратила свое существование после того, как преступники, создав ситуацию «распределенного отказа в обслуживании» путем отправки на биржу тысячи фантомных, созданных в результате модификации кода копий транзакций в целях замедления работы биржи и ее систем безопасности, вывели с подконтрольных этой бирже криптокошельков виртуальные активы на общую сумму 500 млн дол. США [18]. Иногда злоумышленники используют целую серию кибератак, реализуя их в составе преступной группы в отношении «горячих» кошельков, как это имело место, например, при взломе онлайн-биржи Binance. Преступникам удалось обойти систему безопасности и получить значительное количество пользовательских ключей API, кодов 2FA и иную информацию, содержащуюся в рамках кода всего одной транзакции, путем фишинга (подставные сайты), распространения вредоносных программ и других кибератак с независимых аккаунтов на всего лишь одну транзакцию в рамках «горячего» кошелька, в результате чего размер ущерба составил 40 млн дол. [19–21].

Чаще всего указанная выше схема перекодирования киберкошельков используется преступниками вследствие обнаружения ими бреши в системе безопасности, т.е. ошибки (уязвимости) в коде соответствующих кошельков. Наиболее известный случай применения подобной схемы был зафиксирован в результате хищения 55,4 млн дол. США в криптовалюте эфириум (Ethereum) путем использования ошибки в ключе кода децентрализованной автономной организации (DAO — площадка на базе эфириума для краудфандинга, т.е. для аккумулирования финансовых ресурсов на строго определенные нужды) в сочетании с функцией расщепления, т.е. злоумышленник бесконечно копировал («расщеплял») код, отвечающий за удостоверение наличия определенного объема криптовалюты («рекурсивный запрос к умному контракту») [22]. Кроме того, согласно результатам экспериментов некоторых специалистов в сфере кибербезопасности, проверяющих потенциал кодов сети блокчейн, в процессе генерации закрытых ключей доступа к киберкошелькам (78-значная строка чисел, которая защищает валюту, расположенную по определенному адресу) пользователю может быть присвоен ключ, общее математическое значение которого равно 1, 2, 3 или любому другому простому числу. Проблема заключается в том, что подобные коды чрезвычайно уязвимы для преступников, осуществляющих поиск кода путем подбора. Расшифровывая такой ключ, преступники перекодируют кошелек и получают доступ к средствам в криптовалюте [23]. Все описанные выше преступные деяния охватываются положениями ст. 159.6 УК РФ, так как представляют собой разновидности целенаправленного воздействия программных средств на информационно-телекоммуникационную сеть, нарушающего процессы обработки, хранения, передачи компьютерной информации, что позволяет виновным незаконно приобрести цифровой актив, т.е. право на соответствующие денежные средства, хранящиеся в криптовалюте. Согласно абзацу 2 п. 20 упомянутого ранее постановления Пленума Верховного Суда Российской Федерации, такие деяния, совершенные посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, необходимо квалифицировать дополнительно по ст. 272 или 273 УК РФ. Между тем, ввиду необходимости учета такой описанной выше разновидности модификации кода криптокошелька, как бесконечное копирование, необходимо привести в соответствие терминологию, используемую в текстах частей первых ст. 159.6, 272 и 273 УК РФ. Кроме того, в целях учета преступной активности некоторых пользователей вредоносного программного обеспечения представляется необходимым включить в объективную сторону преступления, признаки которого описаны в тексте ч. 1 ст. 273 УК РФ, такой альтернативный вид взаимодействия с вредоносными программами, как их изменение. Внесение изменений в код вредоносной программы, приобретенной виновным у других лиц, не всегда охватывается понятием «создание», что при условии буквального толкования положений ст. 273 УК РФ может способствовать уклонению недобросовестных лиц от уголовной ответственности. В целях учета разнообразных способов преступной модификации компьютерной информации

и постоянного совершенствования технической оснащенности преступников также необходимо в текст ст. 273 УК РФ включить указание на создание, использование и распространение определенного оборудования и его составных частей, которые могут быть использованы в процессе совершения данного преступления (после внесения изменений необходимо также обеспечить соответствие названия указанной статьи ее тексту). В зарубежной практике подобный законодательный опыт имеется, примером чему может служить содержание ст. 150bis УК Швейцарии[9].

Наиболее распространенной на территории Российской Федерации схемой совершения преступлений против собственности в сфере функционирования блокчейна следует признать несанкционированное использование энергетических и информационных мощностей для «производства» криптовалюты (этот процесс называется «майнинг»). Весьма часто злоумышленники подключаются без соответствующего уведомления энергетических компаний к подстанциям крупных промышленных предприятий (в частности, предметом разбирательства в суде явилось причинение ущерба Челябинской энергетической компании в размере 78 млн р. [24]), но появляются и более сложные IT-схемы. Обратимся к судебной практике. Б.С.А., уволенный из ГУП «ОИД», воспользовавшись созданным им еще в период работы в указанном учреждении никому не известным дополнительным способом регистрации нового пользователя в административной части сайта ГУП, путем создания новой учетной записи осуществил неправомерный доступ в административную часть указанного сайта, после чего произвел модификацию компьютерной информации путем введения имеющегося в его распоряжении кода скрипта с индивидуальным ключом для получения криптовалюты Monero в личное пользование, в результате чего в течение определенного времени преступник пользовался энерго- и интернет-трафиками ЭВМ неограниченного круга посетителей пользовательской части данного сайта. Используемый в преступных целях сайт относился к категории сайтов с большим числом ежедневных посещений, поэтому преступник и посчитал его достаточно эффективным для майнинга, требующего значительных энергетических и информационных ресурсов[10]. В рамках другого уголовного дела расследовались преступные деяния С.С.А., который использовал вредоносные программы для получения несанкционированного удаленного доступа путем подбора авторизационных данных (логина и пароля) к серверным ЭВМ других пользователей сети Интернет. При этом, согласно тексту судебного решения, следствием было установлено, что указанные вредоносные программы виновный применял именно в целях использования вычислительных мощностей компьютеров других пользователей при осуществлении майнинга, хотя злоумышленник и не достиг конечной цели по независящим от него обстоятельствам[11]. Аналогичное решение было вынесено в отношении А.В.В.[12] Во всех приведенных выше из практики российских судов примерах виновные были осуждены по статьям УК РФ, предусматривающим уголовную ответственность лишь за совершение преступлений в сфере компьютерной информации (Б.С.А. — по ч. 2 ст. 272 УК РФ, С.С.А. — по ч. 2 ст. 273 УК РФ, А.В.В. — по ч. 2 ст. 273 УК РФ), даже несмотря на то что в текстах указанных решений имелись утверждения правоприменителей о том, что виновные совершали соответствующие деяния в целях незаконного (и совершенно бесплатного) использования энергетических ресурсов и интернет-трафика. И если в последних двух случаях это можно объяснить тем, что, согласно ч. 2 ст. 30 УК РФ, уголовно-правовое значение имеет лишь приготовление к тяжким и особо тяжким преступлениям, то в первом случае неясно, почему следственные органы и суд не осуществили оценку размера ущерба, причиненного действиями Б.С.А., который осуществлял майнинг криптовалюты на протяжении целого месяца. Таким образом, за пределами правоприменительной оценки в подобных случаях могут остаться преступные намерения виновных причинить имущественный ущерб, с одной стороны, гражданам и предприятиям, которые вынуждены были платить

[9] Schweizerisches Strafgesetzbuch vom 21 Dez. 1937 : Stand. am 3 März 2020. URL: https://www.admin.ch/opc/de/classified-compilation/19370083/index.html.

[10] Приговор Советского районного суда г. Орла от 13 июня 2019 г. № 1-43/2019 по делу № 1-43/2019. URL: https://sudact.ru/regular/doc/u9BuZwWnfAd4.

[11] Приговор Собинского городского суда (Владимирская область) от 14 декабря 2017 г. № 1-1-276/2017 по делу № 1-1-276/2017. URL: https://sudact.ru/regular/doc/K742NqoD7LQn.

[12] Приговор Набережночелнинского городского суда (Республика Татарстан) от 21 февраля 2019 г. № 1-368/2019 по делу № 1-368/2019. URL: https://sudact.ru/regular/doc/c9L1n8QmqdmO.

за чрезмерное использование энергетических ресурсов и интернет-трафика, а с другой стороны, энергетическим и IT-компаниям, которые не получали соответствующего дохода за пользование названными ресурсами. Представляется, что обратить внимание правоприменителей на необходимость учета подобного преступного поведения могло бы дополнение абзаца 3 п. 22 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 описанием специального случая несанкционированного потребления электроэнергии и интернет-трафика путем получения несанкционированного доступа к компьютерной информации и (или) внедрения в автоматизированные компьютерные системы неопределенного круга пользователей специальных вредоносных программ (типа botnet) с указанием на необходимость квалификации подобных действий в совокупности по ст. 165 и 272 или 273 УК РФ. Впрочем, в обозримом будущем необходимо задуматься и об указании в тексте уголовного закона на возможность причинения имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ) посредством несанкционированного воздействия на информационно-телекоммуникационные сети в качестве квалифицирующего признака таких преступных деяний. Указанное, думается, послужило бы соблюдению баланса законодательного регулирования и, как следствие, соблюдению принципа справедливости (нормы о краже и компьютерном мошенничестве содержат специальное указание на названный выше признак, в сравнении с указанными нормами положения ст. 165 УК РФ описывают уникальный состав преступления — очевидно, что должны быть предусмотрены возможности для адекватной оценки действий лиц, совершающих и такие преступления посредством несанкционированного внедрения в информационно-телекоммуникационные сети), а также позволило бы учесть одно из типичных обстоятельств совершения соответствующих преступлений (в современных условиях весьма часто преступления против собственности, в том числе подлежащие квалификации по ст. 165 УК РФ, совершаются именно путем неправомерного воздействия на компьютерную информацию — можно даже утверждать, что это один из типичных способов совершения названных преступлений).

На основании изложенного представляется возможным сформулировать следующие предложения по совершенствованию текста УК РФ:

– об изменении редакций пунктов «г» ч. 3 ст. 158 и «в» ч. 3 ст. 159.6 УК РФ: «с банковского счета, а равно в отношении электронных денежных средств либо путем получения доступа к электронным или виртуальным носителям информации либо информационным системам, предназначенным для хранения и оборота денежных средств и (или) осуществления и приобретения цифровых прав»;

– о дополнении текста ч. 1 ст. 159.6 УК РФ словом «копирования» через запятую после слова «модификации»;

– об изменении названия ст. 273 УК РФ на «создание, использование и распространение вредоносного программного и аппаратного обеспечения» и редакции ч. 1 ст. 273 УК РФ: «создание, изменение, распространение или использование компьютерных программ, иной компьютерной информации, а также оборудования и его составных частей, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации»;

– о дополнении ч. 2 ст. 165 УК РФ пунктом «в» следующего содержания: «совершенное путем вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Williams M.L. Crime Sensing With Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns / M.L. Williams, P. Burnap, L. Sloan. — DOI: 10.1093/bjc/azw031 // The British Journal of Criminology. — 2017. — Vol. 57, iss. 2. — P. 320–340.

2. Chavez-Dreyfuss G. Cryptocurrency Crime Surges, Losses hit $4.4 Billion by End-September : CipherTrace Report / G. Chavez-Dreyfuss // Reuters. — 2019. — Nov. 27. — URL: https://www.reuters.com/article/us-crypto-currencies-crime/cryptocurrency-crime-surges-losses-hit-44-billion-by-end-september-ciphertrace-report-idUSKBN1Y11WH.

3. Фалалеев М. Воруют виртуально / М. Фалалеев // Российская газета. — 2019. — 12 дек. — URL: https://rg.ru/2019/12/10/mvd-ushcherb-ot-kiberprestuplenij-prevysil-10-milliardov-rublej.html.

4. Brands J. Connected and Fearful? Exploring Fear of Online Financial Crime, Internet Behaviour and Their Relationship / J. Brands, J. van Wilsem. — DOI: 10.1177/1477370819839619 // European Journal of Criminology. — 2018. — P. 1–22. — URL: https://doi.org/10.1177/1477370819839619.

5. Сачков Д.И. Оценка защищенности персональных данных в информационных системах / Д.И. Сачков, И.Г. Смирнова, В.Н. Быкова. — DOI: 10.17150/2072-0904.2015.6(3).21 // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2015. — Т. 6, № 3. — URL: http://brj-bguep.ru/reader/article.aspx?id=20134.

6. Van der Wagen W. The Hybrid Victim: Re-Conceptualizing High-Tech Cyber Victimization Through Actor-Network Theory / W. van der Wagen, W. Pieters. — DOI: 10.1177/1477370818812016 // European Journal of Criminology. — 2018. — P. 1–18. — URL: https://doi.org/10.1177/1477370818812016.

7. Пинкус М. В Челябинске впервые завели дела о хищении биткоинов / М. Пинкус // Российская газета. — 2018. — 26 янв. — URL: https://rg.ru/2018/01/26/reg-urfo/v-cheliabinske-vpervye-zaveli-dela-o-hishchenii-bitkoinov.html.

8. Скудаева А. Битва с биткоинами / А. Скудаева // Российская газета. — 2019. — 29 янв. — URL: https://rg.ru/2019/01/29/reg-cfo/v-cfo-poiavilsia-novyj-biznes-po-dobyche-deneg.html.

9. Kranenbarg M.W. Do Cyber-Birds Flock Together? Comparing Deviance Among Social Network Members of Cyber-Dependent Offenders and Traditional Offenders / M.W. Kranenbarg, S. Ruiter, J.-L. Van Gelder. — DOI: 10.1177/1477370819849677 // European Journal of Criminology. — 2019. — P. 1–21. — URL: https://doi.org/10.1177/1477370819849677.

10. Kaplan M. Hackers Are Stealing Millions in Bitcoin — and Living Like big Shots / M. Kaplan // The New York Post. — 2019. — Apr. 13. — URL: https://nypost.com/2019/04/13/hackers-are-stealing-millions-in-bitcoin-and-living-like-big-shots.

11. Petersson D. Thefts, Hacks and Surveillance: Whose Side Is Blockchain On? / D. Petersson // Forbes. — 2018. — Nov. 26. — URL: https://www.forbes.com/sites/davidpetersson/2018/11/26/thefts-hacks-and-surveillance-whose-side-is-blockchain-on/#720cff5933be.

12. Hill E. Tokyo Bitcoin Theft Duo Arrested by Police / E. Hill // Coin Rivet. — 2020. — Jan. 27. — URL: https://coinrivet.com/tokyo-bitcoin-theft-duo-arrested-by-police.

13. Sukhodolov A.P. Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects / A.P. Sukhodolov, A.V. Bychkov, A.M. Bychkova. — DOI: 10.17516/1997-1370-0542 // Journal of Siberian Federal University. Humanities & Social Sciences. — 2020. — № 13 (1). — P. 116–122.

14. Ilascu I. Fraudsters Spoof Blockchain.com to Steal $27M in Cryptocurrency / I. Ilascu // Bleeping Computer. — 2019. — June 27. — URL: https://www.bleepingcomputer.com/news/security/fraudsters-spoof-blockchaincom-to-steal-27m-in-cryptocurrency.

15. Beedham M. Watch out: Calìbra.com isn't the same as Facebook's Calibra.com / M. Beedham // The Next Web. — 2019. — June 24. — URL: https://thenextweb.com/hardfork/2019/06/24/calibra-fake-cryptocurrency-site-scam-ethereum.

16. Mkrtchian S.M. Criminal and Legal Protection of Relationships in the Area of Blockchains Functioning and Cryptocurrency Turnover: New Challenges / S.M. Mkrtchian. — DOI: 10.1007/978-3-030-13397-9_41 // Studies in Computational Intelligence. — 2019. — P. 355–361. — URL: https://doi.org/10.1007/978-3-030-13397-9_41.

17. Churchill D. Security and Visions of the Criminal: Technology, Professional Criminality and Social Change in Victorian and Edwardian Britain / D. Churchill. — DOI: 10.1093/bjc/azv092 // The British Journal of Criminology. — 2016. — Vol. 56, iss. 5. — P. 857–876.

18. Wolf B. Mt Gox: The Brief Reign of Bitcoin's Top Exchange / B. Wolf, E. Flitter // Reuters. — 2014. — Febr. 28. — URL: https://www.reuters.com/article/us-bitcoin-mtgox-insight-idUSBREA1 R06C20140228.

19. Whittaker Z. Binance Says More Than $40 Million in Bitcoin Stolen in 'Large Scale' Hack / Z. Whittaker, C. Shu // TechCrunch. — 2019. — May 8. — URL: https://techcrunch.com/2019/05/07/binance-breach.

20. Wilson T. Binance Hackers Shift Stolen Bitcoin, Identity Still Unclear: Researchers / T. Wilson // Reuters. — 2019. — May 9. — URL: https://www.reuters.com/article/us-crypto-currencies-binance/binance-hackers-shift-stolen-bitcoin-identity-still-unclear-researchers-idUSKCN1SF230.

21. Shaban H. Binance Says Hackers Stole $40 Million Worth of Bitcoin in one Transaction / H. Shaban // The Washington Post. — 2019. — May 8. — URL: https://www.washingtonpost.com/technology/2019/05/08/binance-says-hackers-stole-million-worth-bitcoin-one-transaction.

22. Dotson K. Ethereum DAO Attacked, over $55 Million of Ether Cryptocurrency Stolen / K. Dotson // SiliconANGLE. — 2016. — June 17. — URL: https://siliconangle.com/2016/06/17/ethereum-dao-attacked-over-55-million-of-ether-cryptocurrency-stolen.

23. Greenberg A. A 'Blockchain Bandit' Is Guessing Private Keys and Scoring Millions / A. Greenberg // WIRED. — 2019. — Apr. 23. — URL: https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys.

24. Зотикова В. Штраф за биткоин / В. Зотикова // Российская газета. — 2018. — 25 мая. — URL: https://rg.ru/2018/05/24/reg-pfo/v-orenburzhe-majnery-vozmestili-energetikam-ushcherb-v-78-mln-rublej.html.

REFERENCES

1. Williams M.L., Burnap P., Sloan L. Crime Sensing with Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns. *The British Journal of Criminology*, 2017, vol. 57, iss. 2, pp. 320–340. DOI: 10.1093/bjc/azw031.

2. Chavez-Dreyfuss G. Cryptocurrency Crime Surges, Losses hit $4.4 Billion by End-September: CipherTrace Report. *Reuters*, 2019, November 27. Available at: https://www.reuters.com/article/us-crypto-currencies-crime/cryptocurrency-crime-surges-losses-hit-44-billion-by-end-september-ciphertrace-report-idUSKBN1Y11WH.

3. Falaleev M. They steal virtually. *Rossiiskaya Gazeta*, 2019, December 12. Available at: https://rg.ru/2019/12/10/mvd-ushcherb-ot-kiberprestuplenij-prevysil-10-milliardov-rublej.html. (In Russian).

4. Brands J., Van Wilsem J. Connected and Fearful? Exploring Fear of Online Financial Crime, Internet Behaviour and Their Relationship. *European Journal of Criminology*, 2018, pp. 1–22. DOI: 10.1177/1477370819839619. Available at: https://doi.org/10.1177/1477370819839619.

5. Sachkov D.I., Smirnova I.G., Bykova V.N. Assessment of Personal Data Protectability in Information Systems. *Izvestiya Irkutskoi gosudarstvennoi ekonomicheskoi akademii (Baikalskii gosudarstvennyi universitet ekonomiki i prava) = Izvestiya of Irkutsk State Economics Academy (Baikal State University of Economics and Law)*, 2015, vol. 6, no. 3. DOI: 10.17150/2072-0904.2015.6(3).21. Available at: http://brj-bguep.ru/reader/article.aspx?id=20134. (In Russian).

6. Van der Wagen W., Pieters W. The Hybrid Victim: Re-Conceptualizing High-Tech Cyber Victimization through Actor-Network Theory. *European Journal of Criminology*, 2018, pp. 1–18. DOI: 10.1177/1477370818812016. Available at: https://doi.org/10.1177/1477370818812016.

7. Pinkus M. The first case on the theft of bitcoins was opened in Chelyabinsk. *Rossiiskaya Gazeta*, 2018, January 26. Available at: https://rg.ru/2018/01/26/reg-urfo/v-cheliabinske-vpervye-zaveli-dela-o-hishchenii-bitkoinov.html. (In Russian).

8. Skudaeva A. A fight with bitcoins. *Rossiiskaya Gazeta*, 2019, January 29. Available at: https://rg.ru/2019/01/29/reg-cfo/v-cfo-poiavilsia-novyj-biznes-po-dobyche-deneg.html. (In Russian).

9. Kranenbarg M.W., Ruiter S., Van Gelder J.-L. Do Cyber-Birds Flock Together? Comparing Deviance among Social Network Members of Cyber-Dependent Offenders and Traditional. *European Journal of Criminology*, 2019, pp. 1–21. DOI: 10.1177/1477370819849677. Available at: https://doi.org/10.1177/1477370819849677.

10. Kaplan M. Hackers Are Stealing Millions in Bitcoin — and Living Like big Shots. *The New York Post*, 2019, April 13. Available at: https://nypost.com/2019/04/13/hackers-are-stealing-millions-in-bitcoin-and-living-like-big-shots.

11. Petersson D. Thefts, Hacks and Surveillance: Whose Side Is Blockchain On? *Forbes*, 2018, November 26. Available at: https://www.forbes.com/sites/davidpetersson/2018/11/26/thefts-hacks-and-surveillance-whose-side-is-blockchain-on/#720cff5933be.

12. Hill E. Tokyo Bitcoin Theft Duo Arrested by Police. *Coin Rivet*, 2020, January 27. Available at: https://coinrivet.com/tokyo-bitcoin-theft-duo-arrested-by-police.

13. Sukhodolov A.P., Bychkov A.V., Bychkova A.M. Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects. *Journal of Siberian Federal University. Humanities & Social Sciences*, 2020, no. 13 (1), pp. 116–122. DOI: 10.17516/1997-1370-0542.

14. Ilascu I. Fraudsters Spoof Blockchain.com to Steal $27M in Cryptocurrency. *Bleeping Computer*, 2019, June 27. Available at: https://www.bleepingcomputer.com/news/security/fraudsters-spoof-blockchaincom-to-steal-27m-in-cryptocurrency.

15. Beedham M. Watch out: Calìbra.com isn't the same as Facebook's Calibra.com. *The Next Web*, 2019, June 24. Available at: https://thenextweb.com/hardfork/2019/06/24/calibra-fake-cryptocurrency-site-scam-ethereum.

16. Mkrtchian S.M. Criminal and Legal Protection of Relationships in the Area of Blockchain's Functioning and Cryptocurrency Turnover: New Challenges. *Studies in Computational Intelligence*, 2019, pp. 355–361. DOI: 10.1007/978-3-030-13397-9_41. Available at: https://doi.org/10.1007/978-3-030-13397-9_41.

17. Churchill D. Security and Visions of the Criminal: Technology, Professional Criminality and Social Change in Victorian and Edwardian Britain. *The British Journal of Criminology*, 2016, vol. 56, iss. 5, pp. 857–876. DOI: doi:10.1093/bjc/azv092.

18. Wolf B., Flitter E. Mt Gox: The Brief Reign of Bitcoin's Top Exchange. *Reuter*s, 2014, February 28. Available at: https://www.reuters.com/article/us-bitcoin-mtgox-insight-idUSBREA1R06C20140228.

19. Whittaker Z., Shu C. Binance Says More Than $40 Million in Bitcoin Stolen in 'Large Scale' Hack. *TechCrunch*, 2019, May 8. Available at: https://techcrunch.com/2019/05/07/binance-breach.

20. Wilson T. Binance Hackers Shift Stolen Bitcoin, Identity Still Unclear: Researchers. *Reuters*, 2019, May 9. Available at: https://www.reuters.com/article/us-crypto-currencies-binance/binance-hackers-shift-stolen-bitcoin-identity-still-unclear-researchers-idUSKCN1SF230.

21. Shaban H. Binance Says Hackers Stole $40 Million Worth of Bitcoin in one Transaction. *The Washington Post*, 2019, May 8. Available at: https://www.washingtonpost.com/technology/2019/05/08/binance-says-hackers-stole-million-worth-bitcoin-one-transaction.

22. Dotson K. Ethereum DAO Attacked, over $55 Million of Ether Cryptocurrency Stolen. *SiliconANGLE*, 2016, June 17. Available at: https://siliconangle.com/2016/06/17/ethereum-dao-attacked-over-55-million-of-ether-cryptocurrency-stolen.

23. Greenberg A. A 'Blockchain Bandit' Is Guessing Private Keys and Scoring Millions. *WIRED*, 2019, April 23. Available at: https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys.

24. Zotikova V. A fine for a bitcoin. *Rossiiskaya Gazeta*, 2018, May 25. Available at: https://rg.ru/2018/05/24/reg-pfo/v-orenburzhe-majnery-vozmestili-energetikam-ushcherb-v-78-mln-rublej.html. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Мкртчян Сона Мартиросовна — доцент кафедры уголовного права Волгоградского государственного университета, кандидат юридических наук, г. Волгоград, Российская Федерация; e-mail: s.mkrtchian1992@volsu.ru.

ДЛЯ ЦИТИРОВАНИЯ

Мкртчян С.М. Преступления против собственности, совершаемые в сфере функционирования блокчейна: новые преступные схемы и их уголовно-правовая оценка / С.М. Мкртчян. — DOI: 10.17150/2500-4255.2020.14(6).845-854 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 6. — С. 845–854.

INFORMATION ABOUT THE AUTHOR

Mkrtchian, Sona M. — Ass. Professor, Chair of Criminal Law, Volgograd State University, Ph.D. in Law, Volgograd, the Russian Federation; e-mail: s.mkrtchian1992@volsu.ru.

FOR CITATION

Mkrtchian S.M. Property crimes in the blockchain sphere: new criminal schemes and their criminal law assessment. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 6, pp. 845–854. DOI: 10.17150/2500-4255.2020.14(6).845-854. (In Russian).