УДК 343.3/.7
МРНТИ 10.77.51

М.С. Заркенов, Н.Ш. Жемпиисов
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Нур-Султан, Республика Казахстан

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ В ОБЛАСТИ НЕПРАВОМЕРНОЙ ДОБЫЧИ ЦИФРОВЫХ АКТИВОВ

Аннотация. В статье рассматриваются новые формы общественно опасных деяний, не нашедшие своего места в уголовном законодательстве и вопросы допустимости, целесообразности противодействия им и закрепления их в уголовном праве.

В настоящее время незаконное использование вычислительных мощностей всех видов компьютерных технологий для добычи цифровых активов становится все более актуальным видом преступлений среди общественно опасных деяний в сфере информационных технологий. Одним из главных преимуществ данного вида деяния является его прибыльность. В статье рассматриваются цифровые активы, признаки которых все чаще привлекают преступников для получения значительной прибыли. Анализируются различные способы неправомерной добычи цифровых активов, рассмотрены особенности исследуемого общественно опасного деяния.

В целях противодействия уголовным правонарушениям в сфере информационных технологий предложено установить в уголовном законодательстве общественно опасное деяние, направленное на неправомерное использование вычислительных ресурсов компьютерных технологий, а также нарушение работы вычислительной техники с целью добычи цифровых активов. Данная мера направлена на расширение возможностей противодействия информационной безопасности Республики Казахстан в целом.

Ключевые слова: криптовалюта; цифровой актив; криптоджекинг; крипто-майнер; криптоиндустрия; незаконный майнинг криптовалют; добыча цифровых активов; неправомерное использование вычислительных ресурсов; уголовное правонарушение в сфере информатизации и связи.

М.С. Заркенов, Н.Ш. Жемпиісов
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Нұр-Сұлтан қ., Қазақстан Республикасы

ЦИФРЛЫҚ АКТИВТЕРДІ ЗАҢСЫЗ ӨНДІРУ САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ЖАУАПКЕРШІЛІК

Аннотация. Мақалада қылмыстық заңнамада өз орнын таппаған қоғамдық қауіпті әрекеттердің жаңа нысандары және оларға қарсы іс-қимылдың жол берілуі, орындылығы және оларды қылмыстық құқықта бекіту мәселелері қарастырылады.

Қазіргі уақытта сандық активтерді өндіру үшін компьютерлік технологиялардың барлық түрлерінің есептеу қуатын заңсыз пайдалану ақпараттық технологиялар саласындағы әлеуметтік қауіпті әрекеттер арасында қылмыстың өзекті түріне айналуда. Әрекеттің бұл түрінің басты артықшылықтарының бірі-оның пайдалылығы. Мақалада сандық активтер қарастырылады, олардың белгілері қылмыскерлерді көбінесе айтарлықтай пайда табу үшін қызықтырады. Сандық активтерді заңсыз өндірудің әртүрлі әдістері талданды, зерттелетін әлеуметтік қауіпті әрекеттің ерекшеліктері қарастырылады.

Ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарға қарсы іс-қимыл мақсатында қылмыстық заңнамада компьютерлік технологиялардың есептеу ресурстарын заңсыз пайдалануға, сондай-ақ цифрлық активтерді өндіру мақсатында есептеу техникасының жұмысын бұзуға бағытталған қоғамдық қауіпті іс-әрекетті белгілеу ұсынылды. Бұл шара жалпы Қазақстан Республикасының ақпараттық қауіпсіздігіне қарсы іс-қимыл мүмкіндіктерін кеңейтуге бағытталған.

Түйінді сөздер: криптовалюта; цифрлық актив; криптоджекинг; крипто-майнер; криптоиндустрия; криптовалюталарды заңсыз өндіру; сандық активтерді өндіру; есептеу ресурстарын заңсыз пайдалану; ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар.

M.S. Zarkenov, N.Sh. Zhempiissov
The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Nur-Sultan c., the Republic of Kazakhstan

CRIMINAL LIABILITY IN THE FIELD OF ILLEGAL MINING OF DIGITAL ASSETS

Abstract. Currently, the illegal use of computing power of all types of computer technologies for the extraction of digital assets is becoming an increasingly relevant type of crime among socially dangerous acts in the field of information technology. One of the main advantages of this type of action is its profitability. In this regard, this article examines digital assets, the signs of which are increasingly attracting criminals to make significant profits. Various methods of illegal extraction of digital assets are analyzed. In addition, the features of the investigated socially dangerous act were investigated.

In order to counteract criminal offenses in the field of information technology, it is proposed to establish in the criminal legislation a socially dangerous act aimed at the illegal use of computer resources of computer technologies, as well as the violation of computer technology for the purpose of extracting digital assets.

Keywords: cryptocurrency; digital asset; cryptojacking; crypto-maner; crypto industry; illegal mining of cryptocurrencies; mining of digital assets; misuse of computing resources; criminal offenses in the field of information and communication.

DOI: 10.52425/25187252_2021_20_48

В настоящее время развитие компьютерных технологий и их быстрое внедрение в разные общественные отношения, а также распространение таких технологий, как мобильные устройства, появление сетей «Wi-Fi», доступность Интернета для широкого круга людей, создали условия для роста числа уголовных правонарушений в сфере информационных технологий. При этом, количество криминальных ухищрений и видов уголовных правонарушений в сфере информационных технологий неуклонно растет.

Так, одновременное развитие информатизации и экономики создало необычный для восприятия электронный финансовый инструмент – криптовалюту. Криптовалюта – это один из видов нефиатных электронных денег, выпуск и учет которых основан на криптографических методах, платежные единицы представлены в виде определенных электронных монет [1, 281 стр.]. Эта валюта не контролируется правительствами и национальными банками, то есть платежная система децентрализована [2, 34 стр.]. В связи с тем, что криптовалюта имеет электронную форму, она не имеет границ между странами для совершения каких-либо сделок (операций). В связи с чем, преступники видят в этом виде актива потенциал для анонимной отправки денег и отсутствие посредников.

Также преимуществами этой валюты являются анонимность ее пользователей, независимость от финансовых систем, невозможность ее контроля над транзакциями, невозможность подделки, простота генерации и т.д. Таким образом, эта валюта – альтернативная финансовая система будущего. Следовательно, в дальнейшем данный институт будет только совершенствоваться.

С бурным развитием электронной коммерции и популяризацией этих платежных инструментов количество уголовных правонарушений, относящихся к криптовалютам, в последнее время неуклонно растет и приобретает системный характер, создавая тем самым значительную угрозу национальным и международным интересам.

Рассматриваемое общественно опасное деяние связано с процессом генерации этих электронных денег. Еще одной особенностью исследуемой валюты является процесс ее добычи (майнинга) с использованием компьютерных технологий. Генерация таких денег аппаратным оборудованием, осуществляемая в ходе математического расчета хеш-функций для проведения операций на узлах криптовалютной сети, называется майнингом. Эту деятельность может осуществлять любое лицо, имеющее технические средства, используемые для добычи криптовалютных единиц [3, 106 стр.].

Согласно Закону Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республ-

лики Казахстан по вопросам регулирования цифровых технологий» от 25 июня 2020 года №347- VI, под цифровым майнингом понимается процесс выполнения вычислительных операций с применением вычислительных, энергетических ресурсов на основе указанных алгоритмов кодирования и обработки информации, обеспечивающий подтверждение полноты узлов данных в объектах информатизации с помощью блокчейн-технологии[1]. Сам по себе майнинг очень энергоемкий и часто может быть убыточным видом деятельности для тех, кто придерживается закона, в связи с чем, лица, занимающиеся майнингом, все чаще преступают нормы законодательства.

Одним из наиболее распространенных способов генерации криптовалют является использование вредоносных программ. Например, в сентябре 2020 года был запущен вирус «MrbMiner» нацеленный на добычу криптовалют, который распространился по интернету и атаковал системы «Microsoft SQL Server» [4]. Также, в июле 2018 года гражданин Японии Й. Шинкару был первым осужденным за незаконный майнинг криптовалют с использованием компьютерных систем пользователей без их разрешения [5].

Другой пример демонстрирует, как атаки на компьютерные технологии в Университете Святого Франциска Ксавьера (Канада) привели к тому, что организация закрыла доступ к своей сети на неделю, чтобы очистить компьютерные системы от вредоносных программ, предназначенных для тайного майнинга криптовалют[2].

Согласно отчету о кибербезопасности за 2020 год, крипто-майнеры лидируют в атаках вредоносных программ на организации по всему миру. Так, в 2019 году 38% компаний по всему миру пострадали от этих программ. Такая известность по добыче электронных валют обеспечивается низкими рисками и повышенным доходом[3]. В связи с этим, в основном вредоносные программы направлены на незаконное и скрытое использование ресурсов компьютерных технологий предприятий или отдельного пользователя. Такое скрытое использование (без согласия собственника) ресурсов чужих компьютеров в целях майнинга называется криптоджекингом. Это более скрытая угроза, чем программы-вымогатели. Пользователь с гораздо меньшей вероятностью узнает, что в системе установлен вредоносный майнер, если не считать случайных замедлений (задержек) в компьютере.

По оценкам некоторых ученых, средний «крипто-взломанный» компьютер может производить около 0,25 доллара Монеро в день, а если имеется около 2000 компьютеров, то это около 500 долларов в день или более 180 000 долларов в год [6].

И. Гройсман считает, что учитывая насколько легко настроить ботнет и отправлять фишинговые письма с вредоносным кодом, криптоджекинг будет использоваться гораздо чаще [7, 39 стр.]. Следовательно, в ближайшем будущем этот вид майнинга будет расти в еще большей степени.

Существуют также вредоносные программы, которые внедряются в код вебстраниц в виде скриптов для майнинга с помощью браузера. Когда пользователь посещает такой сайт, скрипт запускает систему для использования вычислительной мощности компьютерного оборудования последнего для майнинга криптовалют. Например, подобный инцидент произошел в государственных организациях Российской Федерации (далее - РФ) в результате внедрения вредоносных программ на их интернет-ресурсы с целью добычи криптомонет. Сам процесс майнинга происходил

---

[1] О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий: закон Республики Казахстан от 25 июня 2020 г. № 347-VI ЗРК [Электронный ресурс] - Режим доступа: http://adilet.zan.kz/rus/docs/Z2000000347 (дата обращения: 01.02.2021).

[2] Отключение сети из-за скрытой добычи биткоина // Tadviser. - 2020 [Электронный ресурс] - Режим доступа: https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%A3%D0%BD%D0%B8%D0%B2%D0%B5%D1%80%D1%81%D0%B8%D1%82%D0%B5%D1%82_%D1%81%D0%B2%D1%8F%D1%82%D0%BE%D0%B3%D0%BE_%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D0%B8%D1%81%D0%BA%D0%B0_%D0%9A%D1%81%D0%B0%D0%B2%D0%B5%D1%80%D0%B8%D1%8F_(St._Francis_Xavier_University) (дата обращения: 13.12.2020).

[3] 38% компаний стали жертвами криптомайнеров в 2019 году // Securitylab.ru - 2020 [Электронный ресурс] - Режим доступа: https://www.securitylab.ru/news/504282.php (дата обращения: 13.12.2020).

в тот момент, когда пользователи посещали интернет-ресурс[4].

Однако этот способ майнинга для немецких правоохранителей создает трудности в квалификации по той причине, что в большинстве случаев скрипты не нарушают целостность самой компьютерной системы, а лишь загружают ее значительно больше, пока пользователь не покинет сайт. В то же время, норма УК Федеративной Республики Германии (далее – УК ФРГ) предусматривает ответственность за незаконное удаление, преобразование, приведение в негодность и изменение пользовательских данных (ст. 303а УК ФРГ). Поэтому для того, чтобы квалифицировать данный случай в соответствии с этой нормой, необходимо воздействовать на информацию, содержащуюся в компьютерной технике [8, 94 стр.]. Такая ситуация свидетельствует о том, что одна из передовых развитых стран Европы сталкивается с трудностями в квалификации рассматриваемых деяний, а именно майнинга криптовалют при наличии действующего уголовного законодательства.

Между тем, отчет Федеральной службы уголовной полиции Германии за 2017 год уже содержал информацию о преступлениях, связанных с криптовалютами, и был направлен на динамичное совершенствование законодательства в сфере криптоиндустрии [8, 93 стр.].

За последние пять лет исследуемое деяние получило новый способ реализации этого правонарушения с использованием служебного положения. Например, в июне 2020 года было установлено, что государственные служащие Республики Татарстан использовали около десяти единиц компьютерной техники с целью добычи криптовалют. При этом аналогичное использование за шесть месяцев 2020 года было выявлено на 71 компьютерной технике, принадлежащей госучреждениям Татарстана [9]. Также, в середине 2020 года руководитель отделения почты России в течение 6 месяцев осуществлял цифровой майнинг криптовалют на своем рабочем месте. В течение этого времени оплата за интернет и электроэнергию осуществлялась именно этой организацией. В результате последний был привлечен к уголовной ответственности за злоупотребление должностными полномочиями[5].

Другой пример показывает, как сотрудник ядерного центра был осужден за попытку добыть цифровые активы на своем рабочем месте. Этот сотрудник был признан судом виновным по статье 272 УК РФ (несанкционированный доступ к информации с использованием служебного положения), статье 274 УК РФ (нарушение правил хранения компьютерной информации), статье 273 УК РФ (использование и распространение компьютерных вирусов)[6].

Кроме того, в некоторых аналогичных преступлениях РФ это деяние квалифицируется как злоупотребление должностными полномочиями (ч.1 ст.285 УК РФ). Правоохранители Украины квалифицируют данное деяние по части 2 статьи 188-1 (хищение воды, электрической или тепловой энергии путем ее несанкционированного использования) УК Украины.

Исследуемое деяние не обошло стороной и Казахстан. Так, в начале 2018 года был выявлен факт скрытого майнинга криптомонет на серверах информационных систем Департамента государственных доходов Карагандинской, Атырауской, Актюбинской и Северо-Казахстанской областей Комитета государственных доходов Министерства финансов РК и их территориальных подразделений, а также наиболее производительных рабочих компьютерах работников. Данный факт квалифицирован по статьям 207, 210 УК РК[7].

В этом случае интересна позиция И.Ш. Борчашвили о том, что нарушение

---

[4] Российские хакеры майнят криптовалюту на веб-страницах госорганизаций // Журнал ПЛАС. - 2019 [Электронный ресурс] - Режим доступа: https://plusworld.ru/daily/cat-kriptovalyuty/rossijskie-hakery-majnyat-kriptovalyutu-na-veb-stranitsah-gosorganizatsij/ (дата обращения: 11.02.2021).

[5] В Минеральных Водах СКР возбудил уголовное дело в отношении бывшего начальника Минераловодского почтампа, подозреваемого в злоупотреблении должностными полномочиями. // Следственное управление - 2020 [Электронный ресурс] - Режим доступа: https://stavropol.sledcom.ru/news/item/1467574/ (дата обращения: 11.02.2021).

[6] Сотрудник ядерного центра в Сарове получил условный срок за майнинг // РИА новости. – 2019 [Электронный ресурс] - Режим доступа: https://ria.ru/20191017/1559877712.html (дата обращения: 11.02.2021).

[7] Подпольные майнеры «окопались» в Министерстве финансов Казахстана // Казахстанская правда. - 2018 [Электронный ресурс] – Режим доступа: https://www.kazpravda.kz/news/obshchestvo/sotrudniki-minfina-rk-ispolzovali-gosserveri-dlya-maininga-kriptovalut---knb (дата обращения: 11.02.2021).

функционирования информационных систем или сетей телекоммуникаций выражается как во временном, так и в полном прекращении их функционирования, либо в их неправильном функционировании. При этом действия могут выражаться в удаленной модификации или уничтожении программного обеспечения, блокировании доступа к системе или сети, внедрении в их работу вредоносных программ, создании нештатной нагрузки [10, 386 стр.]. Таким образом, И.Ш. Борчашвили освещает такие схожие признаки незаконного майнинга криптовалют, как внедрение вредоносного программного обеспечения, создание нештатной нагрузки и другие ее возможные последствия. Тем самым, статья 207 УК РК охватывает некоторые признаки рассматриваемого деяния.

Более того, согласно диспозиции статьи 207 УК РК, указанные действия могут быть направлены только на информационную систему или сеть телекоммуникаций, то есть компьютерная техника непосредственно не учитывается.

Конечно, такая позиция законодателя, возможно, связана с тем, что информационные системы и сети телекоммуникаций являются более значимыми, чем компьютерная техника, а также в случае расширения путем включения компьютерной техники в диспозицию эта норма привела бы к применению данной нормы ко всем частным случаям в совокупности со статьями 205, 206, 210 и др. Тем не менее, для полноты и правильной квалификации рассматриваемого общественно опасного деяния необходимо охватить и компьютерные технологии, поскольку уголовно-правовые меры действующего законодательства ограничены только в отношении информационных систем и сетей телекоммуникаций, что позволяет злоумышленникам легально осуществлять рассматриваемое деяние в отношении компьютерных технологий любого гражданина и организации Республики Казахстан. Отсутствие таких сдерживающих мер может привести к колоссальному материальному и моральному ущербу, а также привести ко многим косвенным преступлениям (действия криптомайнеров могут открыть доступ другим киберпреступникам и привести к утечке информации и т.д.).

В связи с этим, в диспозиции статьи 207 УК РК следует дополнительно указать: «нарушение работы компьютерной техники с целью добычи цифровых активов» и изложить в следующей редакции:

«Статья 207. Нарушение работы компьютерной техники, информационной системы или сетей телекоммуникаций.

1. Умышленные действия (бездействие), направленные на нарушение работы компьютерной техники с целью добычи цифровых активов, информационной системы или сетей телекоммуникаций».

Такая позиция будет охватывать вычислительные ресурсы, как компьютерной техники, так и информационных систем и сетей телекоммуникаций.

По нашему мнению, в случаях, когда добыча криптовалют осуществляется на служебной компьютерной технике, не используемой в непосредственной деятельности, которая не может нарушить нормальную деятельность гражданина или организации, или когда сотрудник совершает данное деяние в служебном помещении на собственной компьютерной технике только с использованием электроэнергии и Интернета собственника организации, то деяние необходимо квалифицировать по статьям 195, 250, 361 УК РК.

Естественно, все эти решения не охватывают сути данного деяния, а именно незаконного добывания цифрового актива, поскольку существующие нормы предусматривают только способ совершения уголовного преступления в виде использования вредоносной программы (ст.210 УК РК) и последствия в виде нарушения нормальной работы информационной системы (ст.207 УК РК), причинения имущественного ущерба (ст.195 УК РК) и т.д. Так, действующее уголовное законодательство не предусматривает прямой меры сдерживания незаконной добычи самого цифрового актива, которая позволила бы адекватно и в полной мере противодействовать этому деянию.

Между тем, во всем мире предлагается ввести уголовную ответственность за незаконную добычу цифрового актива. Такого же мнения придерживаются около 54,6% проинтервьюированных респондентов, которые указывают на необходимость криминализации этого деяния.

Остановимся подробнее на признаках исследуемого деяния. Так, в настоящее время этот вид несет колоссальный скрытый ущерб. Вредными последствиями рассматриваемого деяния являются многократно увеличенное потребление электроэнергии, низкая производительность компьютерной техники, снижение работоспособности пользователя (замедляет работу, создает неудобства) и организаций, ущерб от возможных упущений организаций, сокращение срока службы компьютерных технологий и др.

Наибольший риск злоупотреблений со стороны сотрудников или внешних злоумышленников существует в организациях с большими вычислительными мощностями и низким уровнем контроля над ними. Наиболее уязвимыми являются бюджетные организации, а именно государственные и квазигосударственные организации, располагающие огромными датацентрами с тысячами серверов и компьютерным оборудованием. Чаще всего это может быть государственный сектор, крупные предприятия, в частности атомная электростанция, организации, где расположены суперкомпьютеры.

Можно заметить очевидные последствия незаконной добычи цифрового актива, что требует установления уголовно-правового запрета на это деяние. В связи с этим исследуемое общественно опасное деяние должно быть криминализировано.

Данное деяние представляет собой нарушение нормальной деятельности гражданина и организации. Так, объектом этого деяния являются права и законные интересы граждан и организаций по использованию вычислительной техники, информационных систем и сетей телекоммуникаций. Учитывая, что преступный умысел злоумышленника направлен на несанкционированное использование вычислительных ресурсов компьютерных технологий, информационных систем, сетей телекоммуникаций, предметом преступного посягательства являются любые компьютерные технологии (планшеты, смартфоны, «Интернет вещей» и др.), а также информация, информационные системы, сети телекоммуникаций.

По сути, исследуемое деяние осуществляется без согласия собственника, владельца и несет существенный вред законным интересам последнего. Обязательный признак общественно опасного деяния выражается в виде тайного неправомерного использования вычислительных ресурсов компьютерной техники, информационной системы или сети телекоммуникаций с целью извлечения имущественной выгоды в виде добычи цифровых активов для себя или других лиц или организаций. Мотивом деяния являются корыстные побуждения, направленные на получение условного вознаграждения (выгоды).

По конструкции объективная сторона деяния относится к формальному составу, то есть считается завершенной с момента совершения деяния, так как может привести к нарушениям в работе компьютерной техники, информационной системы или сети телекоммуникаций независимо от наступления этого результата. Субъективная сторона деяния характеризуется прямым умыслом. Мотивом деяния являются корыстные побуждения, направленные на получение условного вознаграждения (выгоды).

Кроме того, существует риск совершения данного деяния в отношении критически важных объектов информационно-коммуникационной инфраструктуры, а также с использованием служебного положения. В этой связи, целесообразно учитывать квалификационные составы для этих видов.

Проанализировав рассматриваемое деяние, предлагаем дополнить УК РК новым составом уголовного правонарушения, а именно:

«Статья 214. Неправомерное использование вычислительных ресурсов.

1. Тайное неправомерное использование вычислительных ресурсов компьютерной техники, информационной системы или сети телекоммуникаций с целью извлечения имущественных выгод в виде добычи цифровых активов для себя или других лиц или организаций.

2. Те же деяния, совершенные:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) с использованием своего служебного положения;

3) группой лиц по предварительному сговору.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия.».

Таким образом, в целях противодействия уголовным правонарушениям в сфере информатизации и связи предлагается установить в уголовном законодательстве общественно опасное деяние, направленное на неправомерное использование вычислительных ресурсов компьютерных технологий, а также на нарушение работы вычислительной техники с целью добычи цифровых активов. Данная мера позволит расширить возможности противодействия информационной безопасности Республики Казахстан в целом.

Список использованной литературы:

1. Ализаде, В.А. Судебная практика по делам о преступлениях преступных сообществ (преступных организаций) в сфере незаконного оборота наркотиков, совершенных с использованием информационно-телекоммуникационной сети Интернет и криптовалюты / В.А. Ализаде, А.Г. Волеводз // Библиотека криминалиста, 2017. - № 6(35). - С. 281-299.

2. Вепрев, С.Б. Криптовалюта как прорыв в области финансовых технологий XXI века / С.Б. Вепрев // Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола». – М.: Московская академия Следственного комитета Российской Федерации, 2019. - С. 33-38.

3. Свободный, Ф.К. Психологические факторы привлекательности криптовалют как средства финансовых расчетов / Ф.К. Свободный // Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола». – М.: Московская академия Следственного комитета Российской Федерации, 2019. - С. 104-108.

4. Cimpanu, C. New MrbMiner malware has infected thousands of MSSQL databases [Electronic resource] / C. Cimpanu // Zdnet. – 2020. - Access mode: https://www.zdnet.com/article/new-mrbminer-malware-has-infected-thousands-of-mssql-databases/ (Access data: 13.12.2020).

5. Osborne, Ch. Japan issues first-ever prison sentence in cryptojacking case [Electronic resource] / Ch. Osborne // Zdnet. – 2018. - Access mode: https://www.zdnet.com/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive/ (Access data: 13.12.2020).

6. Biasini, N. et al. Ransom where? Malicious cryptocurrency miners takeover, generating millions [Electronic resource] / N. Biasini // Talos Intelligence. – 2018. - Access mode: https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html (Access data: 03.04.2021).

7. Groysman, I. Revolution in crime: How cryptocurrencies have changed the criminal landscape / I. Groysman / CUNY Academic Works, 2018. - С. 53.

8. Печегин, Д.А. Проблемные аспекты квалификации криптопреступлений в Германии / Д.А. Печегин // Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола» – М.: Московская академия Следственного комитета Российской Федерации, 2019. - С. 92-96.

9. Хайруллин, А. На 71 компьютере в госорганах РТ был обнаружен майнинг криптовалюты [Электронный ресурс] / А. Хайруллин // Бизнесонлайн. – 2020. – Режим доступа: https://www.business-gazeta.ru/article/471853 (дата обращения: 13.12.2020).

10. Борчашвили, И.Ш. Комментарий к Уголовному кодексу Республики Казахстан: особенная часть (том 2) / И.Ш. Борчашвили // - Алматы: Жеті Жарғы, 2015. – 1120 с.

References:

1. Alizade, V.A. Sudebnaja praktika po delam o prestuplenijah prestupnyh soobshhestv (prestupnyh organizacij) v sfere nezakonnogo oborota narkotikov, sovershennyh s ispol'zovaniem informacionno-telekommunikacionnoj seti Internet i kriptovaljuty / V.A. Alizade, A.G. Volevodz // Biblioteka kriminalista, 2017. - № 6(35). - S. 281-299.

2. Veprev, S.B. Kriptovaljuta kak proryv v oblasti finansovyh tehnologij XXI veka / S.B. Veprev // Ispol'zovanie kriptovaljut v protivopravnyh celjah i metodika protivodejstvija: materialy Mezhdunarodnogo nauchno-prakticheskogo «kruglogo stola». – M.: Moskovskaja akademija Sledstvennogo komiteta Rossijskoj Federacii, 2019. - S. 33-38.

3. Svobodnyj, F.K. Psihologicheskie faktory privlekatel'nosti kriptovaljut kak sredstva finansovyh raschetov / F.K. Svobodnyj // Ispol'zovanie kriptovaljut v protivopravnyh celjah i metodika protivodejst-

vija: materialy Mezhdunarodnogo nauchno-prakticheskogo «kruglogo stola». – M.: Moskovskaja akademija Sledstvennogo komiteta Rossijskoj Federacii, 2019. - S. 104-108.

4. Cimpanu, C. New MrbMiner malware has infected thousands of MSSQL databases [Electronic resource] / C. Cimpanu // Zdnet. – 2020. - Access mode: https://www.zdnet.com/article/new-mrbminer-malware-has-infected-thousands-of-mssql-databases/ (Access data: 13.12.2020).

5. Osborne, Ch. Japan issues first-ever prison sentence in cryptojacking case [Electronic resource] / Ch. Osborne // Zdnet. – 2018. - Access mode: https://www.zdnet.com/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive/ (Access data: 13.12.2020).

6. Biasini, N. et al. Ransom where? Malicious cryptocurrency miners takeover, generating millions [Electronic resource] / N. Biasini // Talos Intelligence. – 2018. - Access mode: https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html (Access data: 03.04.2021).

7. Groysman, I. Revolution in crime: How cryptocurrencies have changed the criminal landscape / I. Groysman / CUNY Academic Works, 2018. - S. 53.

8. Pechegin, D.A. Problemnye aspekty kvalifikacii kriptoprestuplenij v Germanii / D.A. Pechegin // Ispol'zovanie kriptovaljut v protivopravnyh celjah i metodika protivodejstvija: materialy Mezhdunarodnogo nauchno-prakticheskogo «kruglogo stola» – M.: Moskovskaja akademija Sledstvennogo komiteta Rossijskoj Federacii, 2019. - S. 92-96.

9. Hajrullin, A. Na 71 komp'jutere v gosorganah RT byl obnaruzhen majning kriptovaljuty» [Jelektronnyj resurs] / A. Hajrullin // Biznesonlajn. – 2020. – Rezhim dostupa: https://www.business-gazeta.ru/article/471853 (data obrashhenija: 13.12.2020).

10. Borchashvili, I.Sh. Kommentarij k Ugolovnomu kodeksu Respubliki Kazahstan: osobennaja chast' (tom 2) / I.Sh. Borchashvili. - Almaty: Zheti Zharғy, 2015. – 1120 s.