помощи приложений, установленных в используемом девайсе, так и в браузере на сайте самого сервиса. Наиболее часто при совершении группового хулиганства преступники используют такие сервисы, как YouTubeLive и «ВКонтакте». Так, совершение в январе 2016 г. групповых хулиганских действий несовершеннолетними С., Н. и иными лицами, сопровождавшихся погромом в арендуемой на сутки квартире в г. Минске и повреждением чужого имущества, транслировалось онлайн на сервисе YouTubeLive.

Интернет активно применяют современные хулиганы для достижения целей по внесению в сознание других людей представления об их значимости, подтверждения причастности к определенной асоциальной группе, самовыражения, демонстрации процесса совершения хулиганских действий (независимо от форм их проявления) и получения ответной реакции в виде лайков или дизлайков. Соответственно, в виртуальном пространстве остаются следы таких действий, как в виде видеофайлов, так и текстовых файлов (электронная переписка в мессенджерах, на страницах социальных сетей или посты на выложенную в общий или приватный доступ видеозапись хулиганства). Например, хулиганские действия двух анархистов, выразившиеся в поджоге с использованием «коктейля Молотова» в июле 2017 г. в г. Ивацевичи билборда с изображением сотрудника милиции и надписью «Сила закона в его исполнении», были записаны на девайс пособника и выложены через социальную сеть и YouTube-канал для публичного просмотра.

Современные возможности интернета позволяют не только обеспечить дистанционную коммуникацию и создавать чаты, мессенджер-группы по интересам для обмена информацией в любой форме. Стремительно развивающиеся технологии являются удобным средством для размещения различного рода контента, в том числе видеофайлов с записью планирования или совершения хулиганских групповых действий. Такое использование технологий позволяет современным хулиганам существенно усилить эффект от их преступления, распространить информацию о нем, не ограничивая круг лиц. Наряду с мессенджерами и социальными сетями ими используется *видеохостинг*. При этом большинство подобных сервисов не предоставляют видео, следуя таким образом принципу «контент генерирует пользователь» (User-generated content). Наиболее популярными среди преступников являются YouTube (для загрузки видео нужно зарегистрироваться, а размер загруженных файлов не должен превышать 1Gb), видеопортал RuTube и сайт Vimeo.com.

Кроме того, ЭЦИ о хулиганстве может быть аккумулирована в виртуальном пространстве в виде видеофайлов, сохраняемых на серверах или ЦОДах камер видеонаблюдения, установленных в целях обеспечения общественной безопасности и охраны правопорядка. Например, с мая 2019 г. в Республике Беларусь функционирует республиканская система мониторинга общественной безопасности, разработанная в соответствии с Указом Президента Республики Беларусь от 25 мая 2017 г. № 187. В основу работы системы заложена технология KIPOD, которая позволяет вывести на новый уровень возможности белорусских правоохранителей по анализу Big Data и видеоконтента.

В контексте расследования хулиганства виртуальные следы представлены в виде ЭЦИ о событии хулиганства, находящейся в виртуальном пространстве, которая имеет доказательственное значение независимо от того, содержится ли она на определенном материальном (физическом) носителе и воспроизведена ли она в форме, доступной для визуального (аудиовизуального) восприятия.

Таким образом, к наиболее типичным местам обнаружения виртуальных следов по уголовным делам о хулиганстве относятся карты памяти и ПО девайса (в основном смартфонов), гаджеты, т. е. технические устройства, предназначенные для хранения ЭЦИ, в том числе флеш-накопители, ОЗУ ПК, винчестер ПК, создающий копию смартфона, ЦОДы и Дата-центры социальных сетей, мессенджеров, видеостриминговых сервисов.

УДК 342.9

М.В. Губич, кандидат юридических наук, временно исполняющий обязанности по должности заместителя начальника кафедры правовой информатики Академии МВД Республики Беларусь
gubichmv@yandex.by;
А.Ю. Богданкевич, курсант учебной группы 6112 4 «Б» курса факультета милиции Академии МВД Республики Беларусь
andreibogdankevitch@yandex.by

НАПРАВЛЕНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТ И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Цифровые технологии – неотъемлемая составляющая активности современного человека, организации, юридического лица. Их развитие происходит столь стремительно, что право не всегда успевает оперативно реагировать на появление новых технологических решений. По экспертным оценкам, по состоянию на середину октября 2019 г. капи-

тализация всех криптовалют составила более 220 млрд долл. США, что не могло не обусловить популярность цифровых активов как объекта научных исследований. Существует целый ряд технических качеств, с регулированием которых ранее не сталкивалась правовая наука: технологии распределенных реестров, безвозвратность проведенных операций (транзакций), отказ от централизованного хранения данных на серверах, возможность заключения и ведения смарт-контрактов непосредственно между сторонами при отсутствии посредников, возможность круглосуточного функционирования системы.

Указанные возможности не остались незамеченными криминалитетом. Так, по ряду экспертных оценок, в 2018 г. объем криминальных сделок, совершенных с использованием только лишь одной криптовалюты биткоин составил примерно 76 млрд долл., при этом основными направлениями криминального использования криптовалюты (в соответствии с отчетом Европола за 2018 г.) выступали:

незаконный оборот наркотических средств и психотропных веществ (применение теневых интернет-сервисов, продажа «химических конструкторов», позволяющих покупателю самостоятельно изготавливать наркотики);

отмывание преступных доходов (развитие нелегальных сервисов по конвертации криптовалюты и обналичивания фиатных средств, использование «программ-смесителей», которые позволяют запутать историю транзакций, отмывание через сайты азартных игр, использование криптовалюты при финансировании терроризма и т. д.);

корыстные преступления, где виртуальная валюта является предметом преступного посягательства (использование фейковых (поддельных) электронных кошельков, создание фишинговых сайтов (или сайтов-копий) популярных ресурсов, запуск краудинвестинговых проектов и инвестиционных фондов, собирающих средства в криптовалюте).

Необходимо акцентировать внимание на тенденции расширения спектра используемых в криминальных целях криптовалют. Если ранее в качестве абсолютного монополиста крипторынка выступал биткоин, то сейчас в криминальных сделках все чаще стали применяться валюты с высокой анонимностью (ZCash, Dash, Monero).

Популярность использования криптоалгоритмов в криминальной среде объясняется тем, что до настоящего времени не выработаны четкие правовые параметры криптовалюты и не установлены границы ее безопасного оборота.

С учетом международного и организованного характера компьютерной преступности в целом все обозначенные криминальные направления использования криптовалют характерны и для Республики Беларусь, в которой законодательное регулирование использования данных финансовых инструментов находится только на начальной стадии ста-

новления. В этой связи отечественному законодателю и правоохранительным органам необходимо выработать стандарты и методики противодействия указанным преступлениям, разработать такую модель правового регулирования оборота криптовалюты, в которой были бы решены задачи предупреждения совершения корыстных преступлений и поддержки инновационного развития экономики Беларуси.

Следует отметить, что с принятием Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» наша страна стала одним из лидеров в правовом регулировании порядка обращения криптовалюты, при этом определение Парка высоких технологий в качестве уполномоченного субъекта реализации норм данного документа имеет, несомненно, положительное значение в администрировании технологии реестра блоков транзакций, а также иных технологий, основанных на принципах распределенности, что позволяет национальным участникам отношений в рассматриваемой сфере совершать операции с использованием указанных технологий с большей степенью безопасности.

В настоящее время разрабатывается ряд проектов нормативных правовых актов в данной сфере, в том числе проект Декрета Президента Республики Беларусь, направленный на развитие действующего Декрета «О развитии цифровой экономики», что свидетельствует о реакции государства на развитие цифровой экономики и криптовалюты.

Однако, несмотря на предпринятые государством шаги, представляется необходимым выделить следующие перспективные направления правового регулирования рассматриваемых финансовых инструментов, что позволит как участникам операций и их использованием пребывать в большей безопасности, так и правоохранительным органам с большей результативностью противодействовать преступлениям, совершаемым с использованием криптовалют.

1. Определение единой международной правовой позиции относительно правовой сущности криптовалют, т. е. решение вопроса могут ли они быть включены в состав денежной массы или нет. В настоящее время существуют два основных мнения: виртуальные валюты не рассматриваются как формы денег, несмотря на наличие признаков, сходных с признаками денежных средств или электронных денег; криптовалюты должны быть приравнены к объектам гражданских прав с одновременным определением в специальных нормативных правовых актах пределов безопасности использования модели коллективного инвестирования (краудфандинга).

В рамках решения указанного вопроса необходима выработка и установление единого режима конвертации всех видов криптовалют в фиатные эквиваленты.

2. В целях противодействия рассматриваемым криминальным проявлениям необходимо установление обязательной идентификации владельцев криптовалюты и иных лиц, участвующих в ее обороте.

3. С учетом приведенных и иных примеров использования рассматриваемых финансовых инструментов в преступных целях полагаем необходимым введение ответственности за нарушение стандартов оборота криптоинструментов, а также создание открытой международной базы данных о лицах, допускающих такие нарушения.

Таким образом, криптовалюта является относительно новым и наиболее активно развивающимся элементом цифровой экономики, что объективно обусловило ряд проблемных вопросов, связанных с правовым регулированием ее оборота, в том числе организации эффективного противодействия криминальному использованию рассматриваемого финансового инструмента. При этом основными вопросами в правовом регулировании являются определение единой международной правовой позиции относительно правовой сущности криптовалюты, установление механизмов идентификации владельцев криптовалюты и иных лиц, участвующих в ее обороте, а также ответственности за нарушения стандартов оборота криптоинструментов.

УДК 342.9

М.В. Губич, кандидат юридических наук, временно исполняющий обязанности по должности заместителя начальника кафедры правовой информатики Академии МВД Республики Беларусь
gubichmv@yandex.by

СИСТЕМА СУБЪЕКТОВ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ И ИХ КОМПЕТЕНЦИЯ

Концепцией национальной безопасности Республики Беларусь и принятой в ее развитие Концепцией информационной безопасности определены основные функции системы обеспечения национальной безопасности, выполнение которых предполагает дальнейшее совершенствование имеющихся подсистем и механизмов, обеспечивающих надежность и устойчивость ее функционирования. Одним из направлений указанной деятельности является совершенствование деятельности субъектов противодействия компьютерным преступлениям.

Данные нормативные правовые акты закрепляют необходимость решения задач обеспечения национальной безопасности на основе системного подхода, в том числе посредством реализации комплекса

взаимосвязанных мер, направленных на выявление, предупреждение и нейтрализацию внутренних и внешних рисков, вызовов и угроз безопасности. Исключительно важную роль для обеспечения эффективности функционирования указанных субъектов играет их правильная, научно обоснованная организационная структура – система субъектов обеспечения информационной безопасности, а также противодействия преступления в сфере высоких технологий – как ее подсистема.

Следует указать, что субъекты, вовлеченные в рассматриваемую деятельность, многочисленны и разнообразны: граждане Республики Беларусь, иностранные граждане, общественные объединения, юридические лица; органы государственного управления, их структурные подразделения, должностные лица, которые наделены определенными полномочиями в данной сфере. Такая многосубъектность обусловлена комплексным характером противодействия преступлениям в сфере высоких технологий.

Защита жизни, здоровья, чести, достоинства, прав, свобод и законных интересов участников общественных отношений от преступных и иных противоправных посягательств относится к важнейшим функциям государства. Решение наиболее важных, основных вопросов в правоохранительной сфере входит в компетенцию органов государственного управления. Рассматривая деятельность Президента Республики Беларусь, Совета Безопасности Республики Беларусь, Национального собрания Республики Беларусь, Совета Министров Республики Беларусь в сфере противодействия компьютерным преступлениям, необходимо учитывать, что рассматриваемая система является подсистемой более высокого уровня – национальной безопасности. В этой связи решение вопросов противодействия преступлениям в сфере высоких технологий указанными субъектами осуществляется, как правило, в комплексе вопросов в сфере национальной безопасности.

Президент осуществляет общее руководство системой обеспечения национальной безопасности путем реализации своих полномочий в этой сфере через Совет Безопасности Республики Беларусь и его рабочий орган – Государственный секретариат Совета Безопасности Республики Беларусь, а также через Совет Министров Республики Беларусь. Президент Республики Беларусь определяет основные направления деятельности государства по защите жизненно важных интересов личности, общества и государства от внешних и внутренних угроз, осуществляет функцию координации деятельности по обеспечению национальной безопасности, в том числе противодействия преступлениям в сфере высоких технологий. Указанный элемент рассматриваемой системы является ее стратегическим центром, что позволяет ему эффективно выполнять возложенные на него задачи.