личными видами международных преступлений и преступлений международного характера под эгидой (в рамках) международных организаций, органов, конференций, совещаний.

В этой связи следует отметить актуальность международного сотрудничества правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий. Несмотря на ряд принятых универсальных международных соглашений в указанной сфере деятельности, определяющую роль, по нашему мнению, в противодействии совершению преступлений с использованием информационных технологий в нашей стране играет организационно-правовой механизм регионального сотрудничества в рамках Содружества Независимых Государств (СНГ).

В условиях устойчивого роста преступлений в этой сфере на территории государств – участников СНГ наблюдается активизация взаимодействия правоохранительных органов стран СНГ по ряду направлений. Так, одобрены и активно реализуются Межгосударственная программа сотрудничества государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий на 2016–2020 годы; Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности от 10 октября 2008 г.; Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, от 25 октября 2013 г.; Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г. и др.

Согласно вышеназванным документам противодействие преступлениям, совершаемым с использованием информационных технологий, обеспечивается:

путем обмена оперативной, статистической, научной, методической и другой информацией о состоянии преступности в сфере информационных технологий;

обмена информацией для пополнения единой базы данных о транснациональных преступных группах и преступных организациях, совершающих преступления с использованием информационных технологий;

проведения согласованных следственных действий, комплексных совместных или согласованных профилактических оперативно-розыскных мероприятий и специальных операций;

выполнения запросов от компетентных органов других государств – участников СНГ;

внедрения технологий, рекомендаций и согласованных мер, ограничивающих возможности совершения преступлений с использованием информационных технологий, и др.

В заключение следует отметить, что появление новых криминальных вызовов и угроз требует разработки повышенных требований к состоянию правопорядка и объективно обусловливает необходимость своевременной выработки превентивных мер, адекватных ее изменениям. Для Республики Беларусь особое значение приобретает взаимодействие нашего государства по предотвращению преступлений в сфере высоких технологий с другими государствами в рамках СНГ. Отсутствие специального международного соглашения, устанавливающего правовые основы противодействия преступности в сфере высоких технологий, и наличие ряда существенных различий не только в материальном и процессуальном уголовном законодательстве государств – участников СНГ, но и в критериях, связанных с определением значимости угрозы указанного вида преступлений, не позволяют говорить об эффективности существующих механизмов международного сотрудничества в борьбе с преступлениями в сфере высоких технологий.

Современная преступность приобретает транснациональный характер, расширяя сферы своего влияния. Негативные последствия данного явления препятствуют формированию благоприятных условий для социально-экономического развития нашего общества, а также подрывают механизмы обеспечения безопасности и укрепления правопорядка в белорусском государстве.

УДК 343.7

К.А. Мартинович, следователь постоянно действующей группы по расследованию преступлений в сфере высоких технологий, Дрибинский районный отдел Следственного комитета Республики Беларусь
starlp9@mail.ru

ПРОБЛЕМНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ХИЩЕНИЙ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК И ДЕНЕЖНЫХ СРЕДСТВ С НИХ

В последние годы кредитно-финансовые отношения как в Республике Беларусь, так и в других странах мира развиваются, являя нам все более новые и совершенные формы оплаты услуг, приобретения и покупки товаров, иных денежных операций. Одной из таких форм являются безналичные расчеты, осуществляемые с использованием банковских платежных карточек (БПК), активность обращения которых увеличивается каждый год. Общество постепенно переходит на ту ступень финансовых отношений, когда большая часть финансовых сбережений

хранится не в материальном виде, а именно на БПК. Издревле тяга к обогащению одолевала отдельными категориями граждан, не желающих самостоятельно зарабатывать на жизнь, ищущих легкие пути получения желаемого, и подталкивала к совершению хищений денежных средств, богатств, сокровищ и иных средств обогащения. С течением времени денежные средства и богатства в материальном виде стали замещаться банковскими платежными карточками. Соответственно, БПК все чаще стали являться непосредственным предметом преступления в уголовно-правовом значении.

В Республике Беларусь с ростом совершения преступлений, направленных на хищение БПК и с использованием БПК, правоприменительная практика пошла по пути квалификации таких хищений по ст. 212 Уголовного кодекса Республики Беларусь (УК). Эта норма уголовного законодательства предусматривает ответственность за хищение с использованием компьютерной техники.

За прошедшие годы написано немало научных трудов, рассматривающих вопросы квалификации хищений с использованием БПК. Некоторые авторы приводят доводы в поддержку сложившейся практики, другие ученые эти доводы оспаривают и считают данную правоприменительную практику в корне неверной. Однако, несмотря на все дискуссии в научном мире, обусловленные, как правило, различными подходами к трактовке как способов выражения объективной стороны состава преступления, предусмотренного ст. 212 УК, так и диспозиции этой статьи, исходя из анализа практики квалификации хищений денежных средств с использованием БПК, в подавляющем большинстве случаев рассматриваемые преступные деяния квалифицируются по ст. 212 УК. По нашему мнению, данный подход является абсолютно неверным, чему и будет дано дальнейшее обоснование.

Диспозиция ст. 212 УК содержит такие способы выражения объективной стороны, как изменение информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо введение в компьютерную систему ложной информации.

Для разбора диспозиции вышеуказанной статьи рассмотрим пример. К., воспользовавшись отсутствием внимания со стороны М., у которого он находился в гостях, с целью хищения денежных средств открыл кошелек М., откуда достал БПК, принадлежащую М., и листочек бумаги с записанным на нем ПИН-кодом, после чего, придя к ближайшему банкомату, вставил БПК в считывающее устройство для карточек, ввел ПИН-код, указанный на листочке бумаги, и обналичил денежную сумму в размере 300 р. Сопоставляя действия К. с объективной стороной ч. 1 ст. 212 УК, можно отметить следующее: К. никоим

образом своими действиями не изменяет информацию, обрабатываемую в компьютерной системе (банкомате), хранящуюся на машинных носителях (в данном случае машинным носителем выступает БПК) или передаваемую по сетям передачи данных, а также не вводит никакой ложной информации в компьютерную систему. Некоторые авторы считают, что ввод ПИН-кода от БПК, владельцем которой не является злоумышленник, и является вводом ложной информации, так как преступник выдает себя за владельца карточки, неправомерно пользуясь ею. Однако такой подход сложно назвать верным, так как К. вводит правильный ПИН-код, а иной информации, такой как, например, Ф.И.О. владельца карточки, кроме ПИН-кода, при снятии денежных средств с БПК не требуется. Возникает справедливый вопрос, для кого вводимая информация является ложной и в чем суть ее ложности?

В соответствии с абз. 1 п. 20 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищении имущества» хищение путем использования компьютерной техники возможно лишь посредством компьютерных манипуляций, которые заключаются в обмане потерпевшего или лица, которому имущество вверено или под охраной которого находится, с использованием системы обработки информации. Данное хищение может быть совершено как путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, так и путем введения в компьютерную систему ложной информации.

С тем, что изменения информации, а также ввода ложной информации в действиях К. не усматривается, мы уже разобрались. Но также в компьютерных манипуляциях, проводимых К. (снятие денег с БПК с использованием банкомата), отсутствует и обман потерпевшего или лица, которому имущество вверено или под охраной которого находится. Снятие денег с использованием банкомата является автоматизированным процессом, и никакое физическое лицо, которое должно одобрить данную операцию, за этим процессом не стоит. Банкомат как автоматизированная система не может определить, правомерно или нет были сняты денежные средства с той или иной БПК. Таким образом, К., похитив БПК М., совершил приготовление к хищению денежных средств с БПК, а дальнейшие действия К., выразившиеся в хищении денежных средств с БПК с использованием банкомата, необходимо квалифицировать по ч. 1 ст. 205 УК как кражу, а оснований для применения ст. 212 УК нет.

Анализируя вышеизложенное, целесообразно окончательно изменить подход к квалификации хищения БПК и последующего хищения с

текущего (расчетного) банковского счета, к которому привязана БПК, денежных средств, в пользу ст. 205 УК, и издание соответствующих нормативных правовых актов, закрепляющих в себе данный подход. Альтернативным вариантом решения данной правоприменительной проблемы может послужить внесение изменений в текст ч. 1 ст. 212 УК, в котором будет отражаться помимо имеющихся способов выражения объективной стороны такой способ, как хищение имущества путем использования банковской платежной карточки.

Таким образом, закрепление на практике вышеуказанного правоприменительного подхода, либо изменение формулировки диспозиции уголовно-правовой нормы будет способствовать более эффективной борьбе с преступностью в кредитно-финансовой сфере.

УДК 343.9.01

Л.Л. Мельник, следователь по особо важным делам главного следственного управления центрального аппарата Следственного комитета Республики Беларусь
l_melnik@sk.gov.by

О КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ КРИПТОВАЛЮТЫ КАК ПРЕДМЕТА И ПЛАТЕЖНОГО СРЕДСТВА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

В настоящее время правоохранительные органы, в том числе Республики Беларусь, столкнулись с новыми разновидностями преступных посягательств, предметами и платежными средствами совершения которых выступает криптовалюта. После правового урегулирования понятия криптовалюты в белорусском законодательстве в 2017 г., придания ей статуса объекта гражданских прав, который охраняется, в том числе и уголовным законом, наблюдается рост числа зарегистрированных преступлений с ее использованием. В течение 2018 г. возбуждено 6 уголовных дел, а за 10 месяцев 2019 г. – 13 уголовных дел, предметом преступления которых явилась криптовалюта, при этом из вышеуказанных 19 уголовных дел только по одному установлено лицо, совершившее хищение криптовалюты (ст. 212 Уголовного кодекса Республики Беларусь (УК)), остальные в настоящее время являются нераскрытыми. Наряду с вышеназванными уголовными делами в производстве следователей находятся уголовные дела, по которым криптовалюта выступает платежным средством совершения преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ, распространением порнографических материалов, в том числе с изображением несовершеннолетних. Можно полагать, что в последующие годы количество преступлений, в процессе совершения которых предметом и платежным средством выступит криптовалюта, будет увеличиваться.

В связи с цифровизацией жизнедеятельности общества, увеличением разнообразия способов хранения и накопления капиталов посредством криптовалют, в том числе представителями теневого рынка и преступной среды, назрела необходимость разработки методики расследования преступлений данной направленности. Ключевым блоком данной методики является криминалистическая характеристика преступления, в структуре которой характеризующая криминалистически значимая информация о криптовалютах выступает в качестве одного из основных элементов.

Криптовалюта как предмет преступного посягательства имеет присущие только ей отличительные признаки, которые обусловлены использованием технологии блокчейн при функционировании (на примере наиболее распространенной криптовалюты Bitcoin). Описание признаков криптовалюты имеет важное криминалистическое значение, так как предполагает специфический порядок обнаружения, фиксации и осмотра, а также последующего анализа имеющейся информации («электронных следов»), влияет на установление фактов, в том числе использования криптовалют конкретными пользователями и их деанонимизации.

По нашему мнению, к криминалистически значимым признакам криптовалюты можно отнести:

нематериальную природу криптовалюты. Данный признак означает, что криптовалюта – неовеществленный предмет и существует в электронном виде, при этом относится в соответствии с белорусским законодательством к иному имуществу;

отсутствие единого эмиссионного центра в виде банковской системы или правительства, которые осуществляли бы выпуск и регулирование криптовалют;

использование в международном обороте согласно Декрету Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» (далее – Декрет);

криптовалюта – универсальное средство обмена (согласно Декрету);

анонимность использования криптовалюты;

необратимость проведения транзакций;

прозрачность проведения транзакций в блокчейне.

Полагаем, при характеристике криптовалюты криминалистическое значение имеют также следующие сведения: