из большого массива данных постепенно исключаются лица, не удовлетворяющие поисковым признакам, как это сделано в вышеприведенном примере с розыском террориста. Как видно, основной целью негативного растрового поиска является исключение непричастных лиц.

Рассматриваемое мероприятие охватывает лишь автоматизированное сопоставление машинным способом; мероприятия по поиску, осуществляемые вручную, попадают под регламентацию иных норм. Например, не является растровым поиском обработка данных, которые ранее получены органом уголовного преследования в результате конфискации предметов, которые могут иметь значение доказательств; ознакомления с бумагами и электронными носителями информации и их изъятия; проведения полицией любого вида расследования (дознания) и принятия ею неотложных мер. Это позволяет разграничить растровый поиск и информационно-аналитическую деятельность.

Под термином «полицейское наблюдение» (polizeiliche Beobachtung) понимается планомерное, как правило, негласное наблюдение за лицом или объектом в целях установления его полного профиля перемещения. Полицейское наблюдение подразумевает ввод персональных данных обвиняемого или номерного знака (наружного обозначения) транспортного средства в контрольную систему, которая позволяет установить персональные данные, номерной знак или наружное обозначение. Если наблюдаемый объект проезжает мимо контрольного поста, то происходит регистрация данного события. При связывании полученных данных получают профиль перемещения, позволяющий отследить передвижение и действия лица. Рассматриваемое действие также служит установлению связей между наблюдаемым и иными лицами для выявления криминальных структур и борьбы с организованной преступностью.

В качестве объекта для осуществления полицейского наблюдения могут рассматриваться лицо, автомобиль, водное судно, летательный аппарат или контейнер и др. Для составления профиля перемещения могут использоваться различные данные, свидетельствующие о местоположении или действиях того или иного лица, например, о местоположении абонента сотового телефона или объекта, оснащенного системой глобального позиционирования, о местах совершения оплаты с использованием пластиковых магнитных карточек. В качестве контрольной системы используется, как правило, федеральная полицейская информационная система Inpol-neu.

Помимо установления личных данных могут фиксироваться такие сведения, как сопровождающее или контактирующее с фигурантом лицо, водитель, маршрут, транспортное средство и перевозимые предметы.

Проведенное рассмотрение позволяет выделить профиль лица (растр) и профиль его перемещения в качестве информационных моделей конкретного события, которые могут использоваться для розыска и установления лиц, представляющих интерес; ограничения круга лиц, подлежащих дальнейшей проверке; отслеживания передвижений и действий лица. При этом возможно выдвижение обоснованных версий о причастности фигуранта к ведению противоправной деятельности либо к определенному событию, установление его связей с иными лицами, получение другой значимой информации, выявление криминальных структур и решение иных частных задач негласного расследования.

С учетом принятия Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» представляется, что изложенные положения могут представлять интерес не только с точки зрения порядка осуществления действий, но и принципов правового регулирования общественных отношений, связанных с обработкой персональных данных лиц.

УДК 343.98

А.М. Хлус

ТЕНДЕНЦИИ РАЗВИТИЯ И ИННОВАЦИИ В МЕТОДИКЕ РАССЛЕДОВАНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Законом Республики Беларусь от 26 мая 2021 г. № 112-З «Об изменении кодексов по вопросам уголовной ответственности» внесен в Уголовный кодекс Республики Беларусь (УК) ряд изменений и дополнений. Существенные изменения коснулись уголовных статей, содержащихся в гл. 31, которая в настоящее время именуется «Преступления против компьютерной безопасности». Это обстоятельство определяет потребность совершенствования частных методик расследования преступлений данной группы. На примере преступления, предусмотренного ст. 349 «Несанкционированный доступ к компьютерной информации» УК, рассмотрим возможности совершенствования частной методики его расследования, что представляется аналогичным в связи с иными деяниями, посягающими на компьютерную безопасность.

Современные методики расследования, основываясь на полувековой традиции, формируются с учетом положений криминалистических характеристик определенного вида или группы преступлений. Не являются исключением в этом аспекте деяния, родовым объектом посягательства которых ранее рассматривалась информационная безопасность.

В качестве общих и наиболее значимых элементов криминалистической характеристики группы преступлений, посягающих на информационную безопасность, рассматривались: 1) личность преступника; 2) способы совершения преступления; 3) обстановка их совершения; 4) особенности образования следов.

Не анализируя все указанные элементы, обратим внимание, что характеристика личности преступника представлена с позиции ее криминологического понимания. Выделены три группы преступников. Одну составляют лица, совершающие деяние с целью самореализации и апробации своих навыков в сфере информационных технологий (хакеры, крэкеры, вирмейкеры). Вторая группа лиц характеризуется ярко выраженной корыстной направленностью совершаемых преступлений. К ним относятся упомянутые хакеры и крэкеры, а также компьютерные пираты. Третью группу составляют специалисты субъектов хозяйствования, государственных органов и организаций (программисты и т. п.), умышленно нарушающие правила эксплуатации компьютерной системы или сети.

Знание приведенной выше классификации преступников значимо для раскрытия и расследования преступных деяний, но в основу разработки криминалистической характеристики любого криминального деяния указанной выше группы должны быть положены сведения о материальных составляющих преступной структуры. Это дает возможность познать преступление в процессе его расследования, основываясь на следовой картине, отражаемой материальными элементами преступной системы.

Данная идея базируется на криминалистическом учении о материальной структуре преступления (А.Е. Гучок). В его основе представление о системе преступления, состоящей из ряда материальных элементов, вступающих во взаимосвязь в момент его совершения.

Учитывая положения упомянутого учения, рассмотрим материальные составляющие анализируемого преступления. В его материальной структуре можно выделить следующие материальные элементы: субъект, совершающий преступное деяние, объект и предмет преступного посягательства, средства совершения преступления.

Субъектом совершения данного преступления является человек, реализующий преступный замысел единолично либо в составе группы. Особенность субъекта рассматриваемого преступления в наличии у него специальных знаний в области компьютерной техники и информационных технологий. В преступной системе субъект вступает во взаимодействие с иными структурными элементами, оставляя на них следы преступных действий, информация о которых подлежит отражению в криминалистической характеристике. Эти следы могут быть обнаружены на средствах, которые использовались для несанкционированного доступа к компьютерной информации. Следует иметь в виду, что средства воздействия на объект отражают следы-действия (например, использование компьютерной программы для преодоления системы защиты) и материальные следы использования средства.

Субъекты неправомерного доступа к компьютерной информации подразделяются на две группы: внешние по отношению к объекту посягательства и внутренние, на которых возложены обязанности по соблюдению правил обслуживания объекта. Разновидностью последних являются близкие лица, пострадавшего от преступления (примечание к гл. 31 УК).

Объектом преступного посягательства с позиции учения о материальной структуре преступления следует считать материальную систему, на которую направлены преступные действия субъекта.

Криминалистический анализ ст. 349 УК позволяет в качестве объектов посягательства выделить компьютерные системы, сети и т. п. Данные «системы» и «сети» представляют собой непосредственный объект преступного посягательства. Но в широком понимании объектом для рассматриваемых преступлений являются организации, которым по неосторожности причиняется существенный вред или иные тяжкие последствия. Объектами выступают различные материальные системы, в отношении которых преступные действия виновного повлекли крушение, аварию, катастрофу (ч. 2 ст. 349 УК). Жертвами этих последствий могут быть люди, которых также надо рассматривать объектом посягательства.

На указанные «системы» и «сети» оказывается неправомерное воздействие, в результате которого формируется следовая картина. Криминалистическое исследование информации, содержащейся в следах, отраженных на объекте посягательства, обеспечивает познание иных, как правило, неизвестных на первоначальном этапе расследования элементов материальной структуры.

В тесной связи с объектом находится предмет преступного посягательства, в качестве которого нами понимается материальный элемент преступной системы, определяющий целевую направленность деяния. На основе анализа ч. 1 и 2 ст. 349 УК можно сделать вывод, что таким предметом выступает информация.

Неправомерный доступ к информации предполагает использование средств совершения преступления, в качестве которых используются материальные системы, обеспечивающие воздействие на объект и достижение цели доступа к компьютерной информации. Доступ к компьютерной информации путем нарушения системы защиты осуществляется посредством средств компьютерной техники с возможным использованием специальных компьютерных программ.

Выделение элементов материальной структуры рассматриваемого преступления не является самоцелью и не противопоставляется уче-

нию о криминалистической характеристике. Для формирования теоретической основы построения частной методики расследования необходимо, по нашему мнению, первоначально рассмотреть типичные элементы материальной структуры преступления, которые затем подлежат описанию (характеристике) в аспекте криминалистически значимой для расследования информации. Такое сочетание двух различных по своей сути криминалистических научных категорий можно представить в виде «криминалистической характеристики материальной структуры преступлений».

На основе вышерассмотренного для обсуждения предлагаются следующие выводы.

Во-первых, разработка криминалистических характеристик отдельных видов преступлений против компьютерной безопасности не дает о них полного представления и не может служить надежной основой для построения частных методик их расследования.

Во-вторых, в основу криминалистической характеристики отдельных видов преступлений против компьютерной безопасности должны быть положены сведения о типичных элементах материальной структуры данных видов преступлений.

УДК 343.98

А.В. Ходасевич

КРИПТОВАЛЮТА КАК ПРЕДМЕТ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА ПО ДЕЛАМ О ХИЩЕНИЯХ ИМУЩЕСТВА ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В настоящее время операции, совершаемые с использованием криптовалюты, получили широкое распространение. Базовые принципы функционирования криптовалютной индустрии, а именно: анонимность при проведении операций, отсутствие надлежащего контроля со стороны какого-либо государства в момент покупки и продажи такой валюты, трансграничность позволили представителям преступного сегмента использовать криптовалюту при совершении противоправных действий. Активное распространение манипуляций злоумышленников с операциями с использованием криптовалюты не позволяют законодателю в таком же темпе менять существующие правовые нормы под возникающие реалии цифрового общества.

Непосредственно суть каждой криптовалюты состоит в том, что она является своеобразным «денежным эквивалентом» и состоит из электронной записи (числовых единиц), которая используется участниками расчетов для проведения операций. При этом курс криптовалюты относительно той или иной валюты формируется спросом и предложением на рынке, функционирование же такой системы происходит децентрализованно в распределенной компьютерной сети, где платежная единица – это некая электронная монета. Поэтому, исходя из сути механизма, заложенного в процедурах покупки и продажи криптовалюты, возникает вопрос, можно ли криптовалюту отнести к предмету преступления по делам о хищениях имущества путем модификации компьютерной информации и какова в целом ее природа?

Поскольку предметом преступления по делам о хищениях имущества путем модификации компьютерной информации выступает имущество, что следует как из названия ст. 212 Уголовного кодекса Республики Беларусь (УК), так и из диспозиции данной статьи, то первоначально следует ответить на вопрос: «Какое именно содержание законодатель вкладывает в понятие «имущество?».

В комментарии к УК для определения понятия «имущество» как предмета посягательства против собственности принято выделять три признака имущества: физический признак (включает в себя такую характеристику предмета, как материальность, т. е. вещи, деньги, ценные бумаги и иные предметы материального мира, не лишенные своей вещной субстанции), экономический признак (вещь должна иметь стоимостный эквивалент), юридический признак (имущество должно быть чужое – принадлежать иному лицу, которое, соответственно, приобрело его и является собственником). В комментарии к гл. 24 УК к предмету хищений относится и право на имущество – полномочия собственника по владению, пользованию и распоряжению имуществом.

Однако криптовалюта не является ни видом денежных средств, в том числе электронных, ни видом ценных бумаг. В Декрете Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» под криптовалютой понимается биткоин, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена.

Данного определения недостаточно для отнесения криптовалюты к понятию «имущество», так как указание на суть криптовалюты как на средство обмена не позволяет в полной мере понять ее природу. При этом, как мы отмечали выше, криптовалюта имеет определенный денежный эквивалент. Приобретая некоторое количество криптовалюты, пользователь уплачивает определенную сумму денежных средств и