законом от 1 октября 2008 г. №164-ФЗ под компьютерной информацией понимается информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи.

А.Ф. Мицкевичем, А.В. Суслопаровым на основе отечественного и зарубежного опыта было проведено исследование понятия компьютерная информация. Они пришли к выводу, что под компьютерной информацией следует понимать сведения, передающиеся между субъектами посредством сигналов в форме электронного кода, пригодного для обработки сведений компьютерными средствами. Наличие кода, как и остальных характерных особенностей компьютерной информации, предполагает нахождение данных в компьютерной системе.

Под указанную трактовку компьютерной информации попадает, скорее, не конкретная информация, а ее форма представления, а именно доступная для восприятия электронно-вычислительной машиной (ЭВМ). В качестве ЭВМ может выступать технические устройства, начиная с персонального компьютера, сервера и иного промышленно-вычислительного оборудования и заканчивая смартфоном.

Содержание оперативно-розыскного мероприятия «получение компьютерной информации» выражается в способах реализации задач по поиску, регистрации и фиксации информации, которая представлена в конечном итоге в виде двоичного кода и не может восприниматься без использования специализированных устройств ввода-вывода данных непосредственно человеком.

Способы доступа к компьютерной информации в зависимости от формы контакта с ней можно разделить: на непосредственные; опосредованные, или удаленные; комплексные, или смешанные.

Одним из способов получения компьютерной информации является негласное получение дистанционного, или удаленного, доступа к устройствам, предназначенным для автоматизированной обработки оцифрованных данных (сетевые и персональные компьютеры, планшеты, смартфоны и др.) лицом, представляющим оперативный интерес, путем преодоления защиты доступа специальными техническими устройствами либо программами. Данный способ возможно использовать, лишь имея специальные технические познания либо привлекая специалистов.

Иной способ получения доступа к данным, находящимся на устройствах, предназначенных для автоматизированной обработки оцифрованных данных, – негласное получение непосредственного доступа к устройствам и носителям информации с последующими копированием или анализом данных, осуществляемым непосредственно с устройства.

Таким образом, получение компьютерной информации – поиск и получение доступа к сведениям (данным), хранящимся на электронных носителях информации и обрабатываемым устройствами обработки данных, путем использования устройств ввода-вывода и хранения данных с целью последующего приема, передачи, записи, регистрации, хранения либо непосредственного восприятия человеком.

Считаем целесообразным включение предлагаемой нами дефиниции в ведомственный нормативный правовой акт МВД России, а также последующую разработку организации и тактики проведения оперативно-розыскного мероприятия «получение компьютерной информации».

УДК 343.985

А.А. Дедковский

ОПЕРАТИВНО-РОЗЫСКНОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Анализ правоприменительной практики Республики Беларусь свидетельствует о том, что состояние преступности характеризуется не ростом киберпреступлений, а фактическим стиранием границ, разделявших их с иными традиционными для нашего общества преступлениями. Появление в Республике Беларусь новых способов совершения криминальных деяний с использованием криптовалют в настоящее время характерно не только для преступлений против собственности (ст. 209, 212 УК) и информационной безопасности (несанкционированный доступ к компьютерной информации (ст. 349 УК), компьютерный саботаж (ст. 351 УК), неправомерное завладение компьютерной информацией (ст. 352 УК), использование вредоносных программ (ст. 354 УК)), но и для таких связанных с легализацией (отмыванием) средств, полученных преступным путем, преступлений, как незаконный оборот наркотических средств (ст. 328 УК), изготовление и распространение порнографических материалов, в том числе с изображением несовершеннолетнего (ст. 343, 343^1 УК), организация незаконной миграции (ст. 371^1 УК), вымогательство (ст. 208 УК) и др. Несмотря на высокую латентность таких преступлений и отсутствие целенаправленного учета, в 2020 г. возбуждено более 100 уголовных дел, в которых фигурирует криптовалюта, если не как предмет преступного посягательства, то как средство достижения преступного результата.

Качественным отличием деяний, механизм которых предусматривает использование IT-технологий, от традиционных преступных посяга-

тельств является возможность совершения их удаленно, без физических контактов соучастников. Поэтому следовая картина таких преступлений обретает определенную специфичность и традиционных оперативно-розыскных и криминалистических средств и методов для собирания полноценной доказательственной базы уже недостаточно. Указанные особенности характерны и для преступлений, предметом или средством которых являются криптоактивы, в том числе криптовалюта, криптооблигации. Качество и полнота раскрытия данной категории преступлений во многом зависят от понимания оперативным сотрудником основополагающих принципов блокчейн-технологий, криповалютной экосистемы, технической и правовой природы криптовалют, точек соприкосновения криптоиндустрии с привычным фиатным финансовым миром.

К началу 2021 г. отмечены следующие особенности эволюционно развивающейся криптоиндустрии:

постоянный рост использования криптовалют в обществе. Согласно статистике сервиса Coin ATM Radar, количество криптоматов с 2016 г. по февраль 2020 г. увеличилось на 600 % (6 838 шт.), число стран, где они находятся, – до 73. Например, в Российской Федерации, несмотря на затяжное нахождение в правовом вакууме криптосообщества (с точки зрения скорости развития и внедрения IT-технологий), функционирует 49 криптоматов, позволяющих осуществлять криптообменные операции с фиатными (фидуциарными) валютами в 22 городах;

применение криптовалют в качестве платежного финансового инструмента. С мая 2019 г. мобильный оператор США AT&T начал принимать оплату через приложение BitPay в биткоинах (Bitcoin, BTC) и Bytecoin (BCN). Браузерное расширение Moon позволяет расплачиваться криптовалютой на одной из самых крупных торговых интернет-платформ Amazon.com. Отель в Швейцарии Dolder Grand с 1 мая 2019 г. начал принимать BTC для оплаты своих услуг, такой политики придерживаются и некоторые отели Испании (Casual Hoteles) и Канады (Sandman Hotel Group). Согласно вступившему с 1 сентября 2019 г. в силу руководству налогового департамента Новой Зеландии зарплата может выплачиваться в BTC и иной криптовалюте;

появление в криптоиндустрии крупных институциональных игроков (Morgan Stanley, Goldman Sachs);

разработка собственных стейблкоинов некоторыми центробанками, например Народным банком Китая – двухранговой системы цифровой валюты центрального банка, крупнейшим банком США JPMorgan – цифровой монеты JPM Coin;

начало торговли биткоин-фьючерсами на платформах Bakkt (с 23 сентября 2019 г.), BitMEX и CME Group;

обретением криптовалютой статуса официального платежного средства в ряде стран (Япония, Венесуэла, Исландия, Испания).

Если буквально год назад мы вели речь об использовании обществом криптовалюты в качестве альтернативного фиатным (фидуциарным) и электронным деньгам средства обмена, то уже сегодня банковское и бизнес-сообщество воспринимает нативную криптовалюту как новый финансовый инструмент, который нельзя больше игнорировать. Более того, ряд государств оценивают возможности использования стейблкоинов в своих финансовых моделях, а некоторые страны планируют их запуск уже в 2021 г.

Таким образом, существующие масштабы использования блокчейн-технологий (по состоянию на февраль 2021 г.), а также основанных на их принципах криптовалют, как и вовлеченность в эти процессы членов общества, указывают на невозможность их запрета не только в целях сохранения существующей финансовой системы, но и в целях противодействия современной преступности, стремительно распространяемой в киберпространстве.

Изложенное позволяет сделать следующие выводы.

Проблемы выявления и раскрытия преступлений, совершенных в виртуальном пространстве (киберпространстве), в том числе с использованием криптовалют, существуют практически в каждом государстве, и их решение возможно, как представляется, только на наднациональном уровне. Обмен научными и практическими знаниями о таком новом и достаточно специфическом сегменте человеческой активности, как криптоиндустрия, установление партнерских отношений правоохранительными органами разных стран являются ключевыми и обязательными компонентами в борьбе с новым вызовом преступности. Видится перспективным осуществление совместной международной многоуровневой партнерской работы, направленной:

на выявление и анализ новых способов совершения преступлений, механизм которых предусматривает использование криптовалют;

разработку эффективных средств и методов обнаружения следов в виртуальном пространстве, собирания доказательств, идентификации и задержания криптопреступников;

оказание международной технической помощи (поддержки) в оценке и криминалистическом анализе криптотранзакций в случаях использования биткоин-миксеров;

совместную модернизацию уголовно-процессуальных средств и полномочий для придания оперативно-розыскной значимой электронно-цифровой информации статуса доказательства.

Следовая картина преступлений, предметом или средством которых являются криптоактивы, в том числе криптовалюта, криптооблигации, весьма специфична, и традиционных оперативно-розыскных и криминалистических средств и методов для собирания полноценной доказательственной базы уже недостаточно. Модернизированные схемы достижения преступного результата свидетельствуют о необходимости постоянного системного совершенствования оперативно-розыскных и криминалистических средств и методов выявления, фиксации и сохранения следов преступления, формирования доказательственной базы в новых, виртуальных, условиях. Видится необходимой разработка методических рекомендаций, включающих в себя:

основополагающие принципы блокчейн-технологий, криповалютной экосистемы, технической и правовой природы криптовалют;

вопросы хранения изъятой или арестованной криптовалюты с учетом технических решений, предлагаемых криптоиндустрией (как представляется, наиболее безопасный вариант ее хранения – использование ведомственных аппаратных криптокошельков с мультиподписью);

анонимизацию поисково-следственной работы в dark Web (сервисы – https://www.producthunt.com/posts/this-person-does-not-exist или https://thispersondoesnotexist.com/; https://www.mightycall.com/virtual-phone-number/; https://www.virtualphone.com/);

возможное использование открытых ресурсов, например биткоин-платформ Blockchain.com, Blockchain.org;

листинг торговых онлайн-площадок в Dark Web (https://www.thedarkweblinks.com) и Darkfael. Для анализа криптотранзакций целесообразно использовать бесплатный софт WalletExplorer.com, который позволяет установить принадлежность кошелька к бирже, сервису или пулу, для анализа транзакций при наличии информации о биткоин-адресе преступника, мест нахождения криптовалютных банкоматов – Coin ATM Radar;

определение IP-адресов (https://www.ripe.net);

приобретение лицензий софтов и доступа к сервисам по анализу криптотранзакций, биткоин-адресов (например, средств анализа Chainalysis, Numisight, Elliptic, Crystal);

взаимодействие с IT-компаниями, финансовыми регуляторами (Национальный банк, Министерство финансов) по разработке механизмов обнаружения финансовых следов вывода криптовалют в фиат;

организационные и тактические особенности оперативной работы с лицами, оказывающими конфиденциальное содействие, с учетом специфики оперативного поиска.

Основное требование к разрабатываемым методическим рекомендациям – используемая терминология должна быть доступна для восприятия оперативным сотрудником, имеющим классическое юридическое образование и обладающим знаниями о традиционных оперативно-розыскных и криминалистических подходах к поиску и собиранию доказательств.

УДК 343

М.С. Десятов

УЧАСТИЕ ПРОКУРОРА В ОПЕРАТИВНО-РОЗЫСКНОМ ПРАВОПРИМЕНЕНИИ

Участие прокурора в современном оперативно-розыскном правоприменении имеет немаловажным значение. Так, в соответствии со ст. 21 Федерального закона «Об оперативно-розыскной деятельности» (далее – Закон об ОРД) Генеральный прокурор Российской Федерации и уполномоченные им прокуроры вправе требовать от руководителей органов, осуществляющих оперативно-розыскную деятельность, представление им оперативно-служебных документов, включающих в себя: дела оперативного учета, материалы о проведении оперативно-розыскных мероприятий с использованием оперативно-технических средств, учетно-регистрационную документацию, ведомственные нормативные правовые акты, регламентирующие порядок проведения оперативно-розыскных мероприятий.

Законодатель не только сконструировал исчерпывающий перечень документации, но и указал в части третьей ст. 21 Закона об ОРД ограничение на представление сведений о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, а также о лицах, оказывающих содействие этим органам на конфиденциальной основе, за исключением случаев, требующих их привлечения к уголовной ответственности.

Наряду с Законом об ОРД прокурорский надзор регламентирован ст. 29 Федерального закона «О прокуратуре Российской Федерации» (далее – Закон о прокуратуре), в которой конкретизирован предмет надзора. Предметом надзора являются: соблюдение прав и свобод человека и гражданина, соблюдение установленного порядка разрешения заявлений и сообщений о совершенных и готовящихся преступлениях; соблюдение установленного порядка выполнения оперативно-розыскных мероприятий; законность решений, принимаемых органами, осущест-