УДК 343.14+346.74

А. Б. Судницын

начальник кафедры уголовного процесса
Сибирского юридического института МВД России,
кандидат юридических наук

ОТДЕЛЬНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ В ДОКАЗЫВАНИИ СВЕДЕНИЙ ОБ ОПЕРАЦИЯХ С КРИПТОВАЛЮТОЙ ПРИ ПРОИЗВОДСТВЕ ПО УГОЛОВНЫМ ДЕЛАМ

К настоящему времени лица, совершающие преступления, не только широко используют технические и программные средства, информационно-телекоммуникационную сеть Интернет, но и осуществляют специфические формы расчетов криптовалютой. Высокая степень анонимности подобных расчетов, низкая проработанность возможностей использования в доказывании сведений об операциях с криптовалютой, потребность правоприменителей в соответствующих рекомендациях указывают на острую теоретическую и практическую актуальность указанных вопросов.

Отметим, что криптовалюта использует механизмы шифрования, дешифровать которые на настоящий момент невозможно. Однако, принимая во внимание открытость транзакции, связывающие использованные кошельки (открытость и публичность Блокчейна (Blockchain)), отметим, что у произведенных операций существуют элементы, которые могут быть выявлены, а сведения о них использованы в доказывании по уголовным делам. В качестве таковых сведений могут выступить данные об отдельных этапах перемещения криптовалюты (приобретение, продажа в различных формах).

Обоснованный вывод о предполагаемом месте нахождения компьютерной техники, которая используется в операциях с криптовалютой, позволит принять решение о проведении обыска (выемки), по результату которого — обнаружить и изъять соответствующие технические устройства.

Обратим внимание, что для покупки, обмена, продажи криптовалюты требуется наличие электронного кошелька (Wallet), управление которым происходит с помощью программы, клиента сети Биткоин (Bitcoin). Факт использования этого, а также и иного программного обеспечения, связанного с криптовалютой (при наличии

в нашем распоряжении изъятой компьютерной техники: компьютер, ноутбук, смартфон, планшет и пр.), может быть обнаружен путем производства осмотра предметов, а также в последующем при исследовании компьютерной информации. В связи с этим рекомендуется фиксировать посещенные веб-сайты и установленное программное обеспечение, причем не только путем указания в протоколе, но и с помощью скриншотов с экрана.

Сведения, полученные в ходе осмотра, могут быть подтверждены в результате исследования компьютерной информации, содержащейся на изъятых технических устройствах. Кроме того, путем производства экспертизы могут быть обнаружены дополнительные данные, а также сделаны выводы, недопустимые в ходе осмотра, подтверждающие операции с криптовалютой.

По результатам проведенных мероприятий в группе следственных действий «обыск — осмотр — экспертиза» должна четко прослеживаться связь сведений, подтверждающих операции с криптовалютой. Аналогичное содержание должно прослеживаться и в допросах лиц.

Круг вопросов, выясняемых в ходе допросов лиц, причастных к операциям с криптовалютой, определяется конкретной следственной ситуацией, сложившейся к этому моменту расследования. Обобщение результатов следственной и судебной практики демонстрирует, что в показаниях указанных лиц внимание акцентируется на деталях финансовых операций, связанных с переводом денежных средств в криптовалюту, а затем обратно. На эти же особенности обращается особое внимание и при приведении других доказательств в приговорах.

Обозначенные способы использования сведений об операциях с криптовалютой в доказывании по уголовным делам являются типичными. Их применение может иметь место как при расследовании преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, так и преступлений из иных сфер.

Другие формы установления сведений об операциях с криптовалютой и их дальнейшее использование в доказывании гипотетически возможно. Однако данная возможность в большинстве случаев упирается в непреодолимую на настоящий момент технологию шифрования данных, как заложенную в суть криптовалюты,

так и применяемую при обеспечении анонимного нахождения в сети Интернет. Вместе с тем представляются перспективными ряд возможностей использования сведений об операциях с криптовалютой в доказывании по уголовным делам.

Одной из главенствующих задач в рассматриваемых случаях является выявление лица, его идентификация в информационной среде (интернет-биржи, форумы, сайты и др.). В качестве средств достижения данной задачи могут выступить нижеприведенные предложения и примеры.

Автороведческий анализ (исследование, экспертиза) позволит установить автора текста, размещенного в информационной среде. При этом в силу огромного массива информации, хранящейся в интернет-среде, следует уделять первоочередное внимание автоматизации процесса распознания авторства текста в Интернете. Тем более подобные разработки имеются[1].

Кроме того, не следует забывать о современных возможностях технико-оперативно-аналитической работы. Так, примером подобной работы можно назвать установление, последующее задержание и осуждение Росса Уильяма Ульбрихта (Ross William Ulbricht) — владельца анонимной торговой площадки (подпольной биржи) SilkRoad, указавшего свой адрес электронной почты, позволивший выявить совпадения в его онлайн-деятельности[2].

Другой успешный пример: сотрудники управления по контролю за распространением наркотиков США (далее — DEA) выдали себя за продавца наркотических средств, получили в качестве оплаты биткоины, изобличили Эрика Дэниеля Хьюза (Eric Daniel Hughes). Указанному лицу вменили незаконную трату собственности, а именно — покупку незаконных веществ. Указанная операция была осуществлена на подпольной бирже SilkRoad, как пред-

[1]Деанонимизация во Всемирной сети — все ближе и ближе [Электронный ресурс] / habrahabr.ru. — Режим доступа: https://habrahabr.ru/post/165435. — Дата доступа: 01.11.2017 ; Software Helps Identify Anonymous Writers or Helps Them Stay That Way [Электронный ресурс] / The New York Times. — Режим доступа: https://bits.blogs.nytimes.com/2012/01/03/software-helps-identify-anonymous-writers-or-helps-them-stay-that-way. — Дата доступа: 01.11.2017.

[2]Silk Road fell due to a catalogue of errors by owner Ross Ulbricht [Электронный ресурс] / CoinDesk, Inc. — Режим доступа: https://www.coindesk.com/ross-ulbrichts-silk-road-head-smacking-rookie-errors. — Дата доступа: 01.11.2017.

полагается, путем создания сотрудниками DEA подставного аккаунта[1].

Подобные методы работы могут быть взяты на вооружение, благодаря чему возможно установление и последующее привлечение к ответственности лиц, совершающих преступления и использующих при этом расчеты посредством криптовалюты. Безусловно, при подобных операциях в действиях сотрудников правоохранительных органов не должно содержаться признаков провокации или иных преступлений.

Приведенные предложения подтверждают, что даже при наличии препятствий технического характера (некоторые из них непреодолимы на настоящий момент) сведения об операциях с криптовалютой могут быть получены при производстве по уголовным делам разнообразными способами (в т. ч. в обход технических препятствий), а полученные сведения могут быть использованы при доказывании по уголовным делам.

УДК 343.97

П. В. Тепляшин

доцент кафедры уголовного права и криминологии
Сибирского юридического института МВД России,
кандидат юридических наук, доцент

ИДЕОЛОГИЯ МОЛОДЕЖНОГО ТЕРРОРИЗМА В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ: ФАКТОРЫ И УСЛОВИЯ ФОРМИРОВАНИЯ, МЕРЫ ПРОТИВОДЕЙСТВИЯ

Среди значительного объема специальных криминологических и уголовно-правовых исследований идеологии молодежного терроризма до сих пор не уделено должного внимания особенностям идеологии молодежного терроризма в информационно-телекоммуникационных сетях. Как представляется, в настоящее

[1]Users Bitcoins Seized by DEA [Электронный ресурс] / The LTB Network. — Режим доступа: https://letstalkbitcoin.com/post/53700133097/users-bitcoins-seized-by-dea. — Дата доступа: 01.11.2017.