Во-вторых, ОРО осуществляется только уполномоченными субъектами. Субъектами данного обеспечения являются органы, уполномоченные осуществлять ОРД, и сотрудники их оперативных подразделений. В данном случае необходимо отметить, что имеется ряд проблем в разграничении и дублировании компетенции соответствующих субъектов. С одной стороны, на объектах, сферах или территориях, ОРО которых осуществляют назначенные оперативные сотрудники, могут выполнять оперативно-розыскную работу и сотрудники смежных или вышестоящих оперативных подразделений собственного ведомства. С другой – эти же объекты, сферы и территории находятся в ОРО взаимодействующих оперативно-розыскных органов, оперативные сотрудники которых также осуществляют на них ОРД.

В-третьих, содержание ОРО составляет комплекс оперативно-розыскных и иных мер. В состав оперативно-розыскных мер целесообразно включать ОРМ, а также мероприятия, осуществляемые в процессе использования содействия отдельных лиц. К иным мерам целесообразно относить мероприятия, которые оперативные сотрудники уполномоченных органов могут проводить в силу административно-правового статуса таких органов, например мероприятия в рамках административно-правовых режимов (разрешительная система, таможенные режимы, режимы государственной границы и в пунктах пропуска, режим защиты государственных секретов и др.) или контрольно-надзорной деятельности (экспортный контроль, административный надзор и др.).

В-четвертых, целью ОРО является охрана и защита соответствующих объектов, сфер или территорий. Как справедливо отмечает Л.А. Григорян, понятие «обеспечение» является родовым по отношению к понятиям «охрана» и «защита». Аналогичную точку зрения высказывают и другие исследователи. При этом Г.Б. Романовский констатирует, что охрана – деятельность, направленная на будущее, ее основная задача – недопущение правонарушения, устранение преград для реализации правомочия, профилактико-предупредительная деятельность. Защита – деятельность, возникающая в случае наличия конкретного правонарушения либо устранения такого состояния, которое реально приведет к наступлению негативных последствий, а также направленная на восстановление нарушенного права. Основываясь на данных подходах, в состав ОРО целесообразно включать: оперативно-розыскное прикрытие объектов, сфер или территорий, направленное на их охрану от преступных посягательств (для него присуща реализация таких видов ОРД, как предупреждение и выявление преступлений); оперативно-розыскное сопровождение досудебного и судебного производства, направленное на защиту указанных компонентов от преступных посягательств (здесь характерными являются такие виды ОРД, как пресечение и раскрытие преступлений, розыск).

Изложенное позволяет определить ОРО как комплекс оперативно-розыскных и иных мер, реализуемых органами, уполномоченными осуществлять ОРД, и сотрудниками их оперативных подразделений в целях охраны и защиты предприятий, организаций и иных объектов производственной или социальной сферы, отдельных сфер жизнедеятельности общества и государства или территорий от преступных посягательств.

Таким образом, ОРО является компонентом ОРД наравне с оперативно-проверочной работой, которую составляет комплекс ОРМ и других мероприятий, направленных на поддержку и принятие управленческих решений о допуске граждан к государственным секретам; работам, связанным с эксплуатацией объектов, представляющих повышенную опасность для жизни и здоровья граждан и окружающей среды; участию в ОРД; содействию на конфиденциальной основе органам, осуществляющим ОРД.

УДК 343.3/7

В.И. Пикта

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТ В ПРОТИВОПРАВНОЙ ДЕЯТЕЛЬНОСТИ

Анализ современного состояния преступности свидетельствует о росте использования цифровых валют в преступной деятельности, связанной с посягательством на правоотношения в сфере оборота наркотиков и информационной безопасности. Внедрение в экономику Республики Беларусь технологии реестра блоков транзакций (блокчейн), а также созданных на ее основе цифровых знаков (токенов) (далее – криптовалюта) хотя и позволило соответствовать современным тенденциям развития цифровых экономик, но физически лишило в силу технических особенностей контроля со стороны государства и правоохранительных органов за оборотом финансовых активов. Сложившаяся обстановка, при которой имеется реальная возможность анонимизации личности лица, осуществляющего финансовые транзакции с использованием криптовалюты, обусловливает совершение новых видов преступлений в виртуальном пространстве.

Для того чтобы лучше понять современные угрозы в этой сфере, целесообразно рассмотреть предпосылки использования криптовалют в противоправной деятельности, их содержание и основные тенденции.

Первоначально злоумышленники использовали криптовалюту как способ осуществления анонимных платежей. Именно криптовалюта в большинстве случаев является средством расчета при приобретении либо продаже наркотических средств, например криптовалюта Bitcoin.

Киберпреступность использует криптовалюту для получения оплаты за похищенную компьютерную информацию. Например, компьютерная атака, известная как WannaCry, заключалась в использовании вредоносного программного обеспечения, шифрующего все пользовательские данные на зараженных компьютерах. За расшифровку пользовательской информации злоумышленники предлагали услуги по дешифрованию в обмен на криптовалюту Bitcoin. В случае неуплаты возможность восстановления компьютерной информации в ее первоначальном виде утрачивалась навсегда. Так, в 2017 г. от данной компьютерной атаки по всему миру пострадало около 500 тыс. устройств, принадлежащих частным лицам, коммерческим организациям и государственным учреждениям.

Построенная на основе технологии блокчейн расчетная архитектура с использованием криптовалюты используется преступным контингентом вследствие имеющегося ряда преимуществ для указанной категории лиц:

правоохранительные органы – не имеют возможности заблокировать проведение операций с использованием криптовалюты, а тем более «заморозить» криптоактивы, как это представляется возможным сделать с обычными банковскими операциями и счетами;

физическое лицо – теоретически может хранить любое количество криптовалюты, зафиксировав приватный «ключ», который дает доступ к средствам, находящимся на криптокошельке, что делает криптовалюту сложной для конфискации и затрудняет принудительное взыскание средств;

злоумышленники – могут привлечь средства посредством принятия криптовалютных активов из любой точки мира и от любого лица, путем опубликования своих публичных адресов в криптовалюте на различных интернет-платформах.

Указанные обстоятельства свидетельствуют о достаточной распространенности криптовалюты среди преступного сообщества и объемы вовлеченности криптовалюты в противоправную деятельность продолжают расти.

Практика свидетельствует, что, несмотря на использование в противоправной деятельности широкого спектра криптовалют, наиболее предпочтительной из них является Bitcoin (более 76 % транзакций). Менее популярными, но вместе с тем постепенно набирающими оборот остаются такие криптовалюты, как Litecoin (7 % от всего объема транзакций) и анонимная Monero (4 %).

Вместе с тем сама по себе технология блокчейн при осуществлении криптовалютных транзакций не обладает абсолютной анонимностью. Форма приватности, которую предлагают криптовалюты, ограничивается псевдоанонимностью: с одной стороны, физическое лицо в блокчейне представлено псевдонимом; с другой – лица, проводящие транзакции с использованием криптовалюты, можно деанонимизировать, если они проходят под одним псевдонимом. В случае осуществления транзакций под разными псевдонимами, затрудняется процесс деанонимизации сторон в связи с отсутствием разработанных научно обоснованных практических рекомендаций по анализу криптовалютных транзакций.

Следует также отметить, что в последнее время наблюдается тенденция использования виртуальной валюты не только в качестве средства осуществления финансовых транзакций, но и как предмета преступного посягательства.

Развитие инструментария киберпреступников повлекло появление новых разновидностей преступлений, совершаемых с использованием криптовалюты:

хищение криптовалюты с использованием поддельных QR-кодов – генерирование специальными интернет-ресурсами QR-кодов, которые содержат адреса преступников, а не адреса, запрашиваемые пользователями, тем самым направляя все платежи с этого кода злоумышленникам;

распространение вредоносного программного обеспечения, предназначенного для изменения адресов криптокошельков при их вводе – подмена с помощью специально разработанного вредоносного программного обеспечения адресов электронных кошельков пользователей «зараженных» веб-браузеров, кроме того, вредоносный код имеет возможность компрометировать номера банковских платежных средств и информацию о пользователе, такую как пароли и файлы, и даже делать снимки экрана рабочего стола «жертвы»;

осуществление кибератак на частные и государственные организации – получение прибыли с систем, скомпрометированных в ходе кибератак, путем осуществления «майнинга» криптовалюты;

распространение конфиденциальных криптовалют и транзакций – в отличие от проведения транзакций с использованием Bitcoin, где все транзакции являются прозрачными, такие криптовалюты, как Monero и Zcash повышают анонимность пользователей за счет предоставления ложной публичной истории транзакций, отражающей недостоверную информацию о совершаемых операциях.

В заключение представляется возможным сделать следующие выводы:

современные тенденции киберпреступлений свидетельствуют о росте использования криптовалют для анонимизации финансовых операций, это связано с техническими особенностями технологии блокчейн, для которой характерны децентрализация эмиссии и оборота цифровых знаков (токенов), отсутствие внешних рычагов регулирования, определенная степень анонимности участников;

отсутствие разработанных научно обоснованных практических рекомендаций по анализу криптовалютных транзакций существенным образом снижает эффективность деятельности по противодействию незаконному обороту наркотиков и киберпреступности.

УДК 343.985.8

С.В. Пилюшин

ОБ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ

Эффективность выявления (раскрытия) преступлений безусловно зависит не только от полноты и своевременности поступления оперативно-розыскной информации, но и от ее качества и достоверности. Ценность она приобретает после проверки ее достоверности, значимости, полноты, возможности использования и т. д. Если информация не обладает перечисленными свойствами, то она является беспредметной, а следовательно, несущественной.

Под оперативно-розыскной информацией в теории ОРД принято понимать разновидность социальной информации, специфичной по цели получения (борьба с преступностью), методам получения и режиму использования, обеспечивающим