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

конспирацию, надежную зашифровку источников (в случае необходимости), возможность проверки сообщаемых сведений и их применение только специальными субъектами.

Следует обратить внимание, что специфика деятельности оперативных подразделений ОВД вносит свои коррективы в требования, предъявляемые к оперативно-розыскной информации. В большинстве случаев последняя становится средством познания для оперативных сотрудников широкого круга социальных явлений, в том числе связанных с криминогенными процессами. Многие из этих явлений довольно полно изучены юридическими науками. Тем не менее, рассматривая их через призму ОРД, особый интерес представляют явления, порождаемые преступлением, наличие либо обнаружение которых позволяет судить о вероятности его совершения.

Ценность оперативно-розыскной информации также может заключаться в возможности отражения объективных явлений, связанных с криминогенными процессами, происходящими на обслуживаемой территории (объектах); правовой оценки действий конкретных лиц; выбора соответствующей оперативно-розыскной тактики и т. п. Приоритетное значение придается информации, позволяющей сформировать представление о способах совершения преступлений, так как это позволяет выдвигать оперативно-розыскные версии и осуществлять соответствующие оперативно-розыскные мероприятия.

Вместе с тем не всякая поступающая информация представляет ценность. Например, информация, полученная в результате противодействия преступной среды, направленная на введение в заблуждение оперативных сотрудников; добываемая лицом с недостаточным уровнем профессионального опыта; несвоевременно полученная и т. д. Данные факторы влияют на выбор и осмысление такого рода явлений, способствуют выделению наиболее значимой информации. При невозможности своевременно оценить полученную оперативно-розыскную информацию, познать ее значимость может быть потеряна наиболее существенная ее часть, а оставшаяся будет являться «информационным шумом».

В теории ОРД информация, обладающая вышеперечисленными свойствами, определяется термином «оперативно значимая информация», возникновению которой предшествуют активные действия оперативных сотрудников по ее выявлению. В качестве элементов этих действий выделяют сбор первичной информации, ее предварительный анализ на предмет отнесения к оперативно-розыскной информации и уже в последующем анализ и проверку, позволяющие выделить оперативно значимую информацию, дающую основания для принятия оперативно-розыскных решений.

Таким образом, представляется возможным сделать вывод о том, что оперативно значимая информация является результатом трансформации оперативно-розыскной информации в процессе ее аналитической обработки и сопоставления с другими оперативными данными, поступающими из различных источников. Ее наличие позволяет оперативным сотрудникам устанавливать предметы, которые могут быть вещественными доказательствами (финансовые документы, товарно-материальные ценности, денежные средства и т. д.), места их хранения (сокрытия), способы вывода и легализации, что в целом отражает механизм реализации преступных замыслов, прямо или косвенно указывает на наличие состава противоправного деяния в действиях конкретных лиц.

УДК 342

***А.А. Подупейко***

## НЕКОТОРЫЕ ВОПРОСЫ ЦИФРОВИЗАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Современное развитие мирового сообщества требует постоянного совершенствования деятельности во всех сферах общественных отношений. Это обусловлено стремительным развитием информационно-цифровых технологий, которые стали основой функционирования различных субъектов в большинстве сфер деятельности. И государственные организации, и учреждения, и частные компании сегодня ставят цифровизацию в ряд своих основных и стратегических приоритетов для достижения устойчивого конкурентного преимущества в отрасли.

В Государственной программе развития цифровой экономики и информационного общества на 2016–2020 годы закреплено, что в Республике Беларусь процесс цифровой трансформации рассматривается как один из важнейших факторов обеспечения конкурентоспособности и инновационного развития как отдельных организаций, так и национальной экономики в целом.

Граждане также стали зависеть от информационных технологий. Они значительное количество времени проводят в социальных сетях. Смартфоны, планшеты, персональные компьютеры превратились в персональные центры управления каждого человека. При этом пользователи стремятся получить немедленно не только какие-либо сведения, но и товар или услуги.

При всех положительных и созидательных моментах информационно-цифровые технологии используются и для достижения негативных целей. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб как интересам отдельных учреждений и организаций, так и национальным интересам государства в целом.

Злоумышленники атакуют личные аккаунты граждан, сайты государственных органов, в том числе правоохранительных, преследуя при этом совершенно разные цели и интересы. Целью может быть похищение информации или демонстрация, насколько плохо защищен сайт органа, данные о служебной деятельности, конфиденциальные данные сотрудников, персональные данные граждан и др. Беспокойство вызывает также активное распространение в информационном пространстве фальсифицированной и недостоверной информации. Это создает предпосылки для преднамеренной дестабилизации устоявшихся общественных отношений.

Процессы глобализации, возникающие различные общественные вызовы и угрозы, цифровизация общества и, как результат, изменяющееся сознание и социальное поведение людей, а также цифровая трансформация учреждений, организаций, предприятий и компаний актуализируют необходимость корректировки деятельности и органов внутренних дел Республики Беларусь.