ции – криптокошелькам, личным кабинетам криптобирж и криптообменников. Мошенники, действуя анонимно в сети Интернет, создают поддельные страницы сайтов криптобирж и криптообменников для торговли или обмена криптовалюты, фальшивые версии официальных криптокошельков, размещая их в Google Play и Apple App Store, распространяют вредоносное программное обеспечение, которое шифрует файлы пользователя и требует выкуп в криптовалюте за их восстановление. Мошенники выдают себя за брокеров, обещая высокую доходность от торговли криптовалютой, забирают деньги своих клиентов. Все эти действия осуществляются анонимно с использованием специального программного обеспечения, позволяющего скрывать местонахождение мошенника. Однако преступные посягательства на цифровые активы могут осуществляться и открыто. Например, путем совершения грабежа, разбоя или вымогательства.

Преступления, в которых криптовалюта являлась средством совершения преступлений, как правило, связаны с торговлей запрещенными товарами, работами или услугами, взяточничеством, мошенничеством в сети Интернет. Прежде всего это преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ, порнографических материалов, оружия и боеприпасов. Через сеть Интернет в обмен на криптовалюту преступники оказывают услуги по изготовлению поддельных денежных знаков, документов (паспорта, водительские удостоверения), продают программное обеспечение для «взлома» устройств, имеющих доступ в сеть Интернет, персональные данные физических и юридических лиц, банковские платежные карточки и электронные кошельки, оформленные на подставных лиц – дропов. Такие сделки, как правило, осуществляются в криптовалюте с использованием тайников – закладок. В Республике Беларусь появились факты взяточничества, финансирования экстремизма и терроризма с использованием криптовалюты. Незаконные сделки в криптовалюте позволяют уклоняться от уплаты налогов, легализовывать денежные средства, полученные преступным путем.

Особого внимания заслуживают схемы мошенничества в сети Интернет через криптовалютное финансирование ICO (Initial Coin Offering). Мошенники рекламируют фальшивые проекты по выпуску и продаже новых токенов и в обмен на них анонимно собирают средства (фиатные или криптовалюту) от инвесторов, обещая в ближайшем будущем высокую доходность. Фальшивые проекты представляют собой информацию, размещенную на специально созданных сайтах, в мессенджерах и социальных сетях о возможности стать инвестором высокодоходного проекта, выпускающего новые токены, стоимость которых будет расти. По статистике, менее половины всех ICO продолжают существовать через четыре месяца после самого размещения монет. Распознать мошеннические проекты рядовому пользователю сети Интернет весьма проблематично. Южная Корея и Китай на законодательном уровне запретила ICO. В Республике Беларусь ICO разрешены для резидентов Парка высоких технологий.

Аналогичные «пирамиды» реализуются мошенниками через специально созданные сайты, предлагающие услуги облачного майнинга, участия в инвестиционных фондах, вымышленных аукционах и лотереях. Активно рекламируются боты для автоматической торговли криптовалютой, которые на самом деле похищают средства и (или) личную информацию пользователей.

Отдельного внимания заслуживают преступления, совершаемые в целях майнинга криптовалюты. В основном они связаны с распространением и скрытой установкой специальных программ, предназначенных для майнинга криптовалюты за счет аппаратных мощностей устройств пользователей сети Интернет. Ввиду того что майнинг является весьма энергозатратным, имеют место факты хищения электрической энергии майнерами.

Таким образом, преступность в сфере криптовалюты – сложная и многоаспектная проблема для большинства стран мира. По мере развития криптоиндустрии в Республике Беларусь эта проблема будет возрастать. Необходимо проводить дальнейшие исследования и разрабатывать новые методы борьбы с преступностью в этой сфере. Ключевым фактором успеха является сотрудничество и взаимодействие между правительствами, правоохранительными органами, банковскими финансовыми организациями внутри страны и за рубежом.

УДК 351.74 + 004

А.А. Шульченко

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ OSINT В СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ

Цифровизация становится неотъемлемым элементом деятельности любого человека. Повсеместно социальные и политические процессы, а также деятельность государственных органов перемещаются в цифровую среду и для того, чтобы успешно адаптироваться в обществе, люди создают различные цифровые профили на различных порталах, ведут страницы в социальных сетях, выкладывая при этом фотографии и иную информацию о себе. В современном информационном обществе, где совершение преступлений в виртуальном пространстве становится все более распространенным, органам внутренних дел (ОВД) необходимо активно использовать разные методы по установлению правонарушителей, в том числе эффективно могут применяться методы открытого исследования информации (OSINT).

Справочно: OSINT, или открытое исследование информации. Этот метод предоставляет возможность собирать и анализировать данные из различных открытых источников, таких как интернет, социальные сети, новостные статьи, форумы и другие общедоступные ресурсы.

Значительный рост киберпреступности подчеркивает важность эффективного мониторинга и анализа данных, доступных в сети Интернет. OSINT предоставляет сотрудникам возможность получать ценную информацию из открытых источников, таких как социальные медиа, форумы и другие онлайн-ресурсы. Это способствует не только выявлению и раскрытию преступлений, совершенных в сети Интернет, но и преступлений, совершенных по линии иных подразделений ОВД. Качественный OSINT также обеспечивает возможность оперативного реагирования на угрозы, связанные с виртуальной безопасностью.

Использование OSINT в современном мире становится неотъемлемым компонентом в борьбе с преступностью и обеспечением цифровой безопасности общества. OSINT позволяет также собирать информацию о потенциальных угрозах, стратегиях антигосударственных формирований и других аспектах, влияющих на национальную безопасность.

Непосредственно совокупность использования методов оперативно-розыскной деятельности (ОРД) значительно улучшит результативность OSINT. ОРД позволяет дополнить открытые источники информацией из закрытых и конфиденциальных источников, расширяя объем доступной информации. Кроме того, оперативные данные способны подтверждать или корректировать результаты OSINT, усиливая достоверность полученной информации. Применение методов ОРД в совокупности с OSINT дает возможность создания более полного и точного образа исследуемого объекта, что, в свою очередь, повышает эффективность аналитических процессов и оперативных действий в целом.

Часто сотрудники ОВД обладают лишь малой частью информации о личности преступника из-за чего затруднительно установить личность преступника. Как правило, имеется лишь фотография, «никнейм» или электронная почта, на которую был зарегистрирован аккаунт злоумышленника. Для решения данного вопроса можно воспользоваться одним из базовых и самых простых методов OSINT, который не требует специальных навыков, таким как «чат-боты» мессенджеров (Справочно: Чат-боты, или просто боты, представляют собой программы, которые автоматизированно взаимодействуют с пользователями через чатовые интерфейсы. Они могут выполнять различные задачи – от предоставления информации и ответов на вопросы до выполнения определенных команд и действий.). В качестве примера можно привести такие чат-боты мессенджера Telegram, как @telesint_bot, @ibhld_bot, @usersboxing_bot, которые используют информацию открытых источников и могут предоставить информацию о принадлежности владельца электронной почты, телеграмм-аккаунта, установить человека по фотографии, предоставить перечень групп, на которые подписано проверяемое лицо в мессенджерах и социальных сетях, установить, на каких сайтах и сервисах зарегистрирован пользователь. Исходя из собранной информации, сотрудники могут ограничить область поиска или даже получить данные, которые, с использованием ресурсов ОВД и оперативно-розыскных возможностей, позволят установить местонахождение разыскиваемого объекта.

Этот пример представляет собой простой сценарий, что может сказаться на качестве полученной информации, делая ее менее детализированной и точной.

Однако повсеместное внедрение в ОВД методов OSINT несет за собой ряд проблемных вопросов, основные из которых можно выделить. Так, ими являются:

1. Технические сложности. Обработка и анализ больших объемов данных из различных источников требует наличия высокопроизводительной компьютерной техники.

2. Обучение и подготовка персонала. Эффективное использование OSINT требует от сотрудников получения соответствующих знаний и навыков путем прохождения соответствующих курсов и программ. Обучение и подготовка сотрудников являются важной частью успешного внедрения.

3. Качество источников. Не всегда открытые источники обладают высоким качеством и достоверностью. Существует риск использования непроверенной или ошибочной информации, что может влиять на качество анализа и принятие решений.

Таким образом, совокупность сочетания методов OSINT и ОРД позволит повысить эффективность подразделений ОВД при выявлении и раскрытии преступлений, однако для полноценного и повсеместного внедрения OSINT необходимы значительные финансовые вложения в обучение персонала, приобретение необходимого программного обеспечения и технического оборудования, а также создание системы безопасности данных при использовании открытых источников.

УДК 343

А.В. Яскевич

ПРИВЛЕЧЕНИЕ СПЕЦИАЛИСТА В ПРОЦЕССЕ ВЫЯВЛЕНИЯ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ

Экономическую преступность можно рассматривать как особый вид экономических отношений рыночного характера, проявляющихся в криминальной сфере. Связь с рыночной системой экономических отношений заключается в том, что данный вид преступности связан с бизнесом, наличие которого является неотъемлемой частью рыночной системы хозяйствования.

Экономическая преступность наносит обществу значительные материальные и иные потери. Она способна дестабилизировать экономическую систему государства, нарушить действие рыночных экономических законов, может привести к дисфункции социальных институтов, социальных норм и связей.

Вместе с тем ведение борьбы с преступностью в сфере экономики невозможно без использования соответствующих знаний. В рыночной системе имеются свои специфические особенности, определяющие явный или скрытый смысл тех или иных событий, явлений объективной действительности, конкретного объекта либо отрасли экономики.

Эффективность выявления экономических преступлений во многом зависит от возможности получения оперативно-розыскной информации, т. е. наличия тех или иных фактов, отражающих сущность преступной деятельности, своевременности ее получения и анализа. Однако такая информация может оказаться бесполезной, если ее суть запутанна и непонятна для лица, ее получившего. Неопределенность чаще всего возникает из-за отсутствия полных, достоверных данных о той или иной хозяйственной операции, обоснованности и необходимости использования тех или иных технологических решений, применения каких-либо материалов и т. д.

Одним из путей восполнения недостающих элементов полученной информации являются собственные знания оперативного сотрудника. В силу профессиональной деятельности он может обладать определенным практическим опытом, позво-