

уничтожения либо маскировки следов противоправной деятельности – «цифровых следов».

Другой вид преступника, совершившего НДКИ, представлен злоумышленником, обладающим минимальными навыками обращения с компьютерной техникой. Как правило, он применяет одинаковые методы при совершении НДКИ различного уровня, приобретая преступную схему в теневой части сети Интернет, так называемом «Даркнете», либо используя методы социальной инженерии. Такие преступники редко обладают навыками противодействия раскрытию совершенного преступления, а потому оставляют «цифровые следы» своей противоправной деятельности. Злоумышленники реализуют свой преступный умысел исключительно с материальной составляющей, когда совершают НДКИ ради получения материальных благ.

Таким образом, оперативно розыскное противодействие несанкционированному доступу к компьютерной информации является одним из приоритетных направлений деятельности правоохранительных органов Республики Беларусь. Как показывает практика, несанкционированный доступ в настоящее время является не только самостоятельным видом преступной деятельности, но и стал инструментом в руках преступников для совершения других всевозможных преступлений. Особое значение при этом имеет знание элементов оперативно-розыскной характеристики данного вида преступлений, которое позволяет выступать информационной основой и эффективно проводить оперативно-розыскные и иные мероприятия, направленные на предупреждение, выявление и пресечение рассматриваемого преступления, а также выявление лиц, их подготавливающих, совершающих или совершивших.

УДК 343.98

А.М. Шинкевич

ПЕРСПЕКТИВЫ РАЗВИТИЯ И ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

Оперативно-розыскная деятельность (ОРД) является негласным государственно-правовым средством защиты общества и государства. В Республике Беларусь на законодательном уровне она совершенствуется с 1992 г. Каждый из органов, которым предоставлено право осуществлять ОРД, решает свои непосредственные задачи с использованием негласных методов. Преимущественно в органах внутренних дел ОРД направлена на борьбу с преступностью. Из всех уполномоченных

на ее осуществление органов наибольшее количество задач решается органами внутренних дел.

Несмотря на то, что на протяжении последних десяти лет общий уровень преступности ежегодно снижается, общественно опасные деяния в сети Интернет стремительно растут. В 2023 г. примерно четверть зарегистрированных в стране преступлений совершено с использованием сети Интернет, при этом процент раскрытия таких преступлений достаточно низкий.

В первую очередь, этому способствуют процесс широкомасштабной интеграции цифровых технологий в различные сферы деятельности человека и организаций, особенно в финансовые взаимоотношения между субъектами. Бесспорно, цифровизация белорусского общества является неизбежным процессом, благодаря которому у субъектов хозяйствования появляются широкие возможности оптимизации процессов, увеличения производительности, улучшения качества жизни и повышения эффективности работы во всех сферах жизнедеятельности человека. В связи с тем, что взаиморасчеты между физическими и юридическими лицами осуществляются удаленно с использованием интернет-банкинга, а большая часть общения и передача информации осуществляется через мессенджеры, социальные сети и почтовые сервисы, мошенники используют это в своих преступных целях, выдавая себя за добропорядочных членов общества.

Росту преступности в сети Интернет способствуют также и преимущества, которыми обладает глобальная сеть, а именно неограниченный доступ с возможностью подключения к ней в любой точке планеты, мгновенный обмен информацией, в том числе, зашифрованной, возможность анонимного взаимодействия между пользователями сети и использования специального программного обеспечения, позволяющего скрывать и подменять цифровые следы, оставленные преступниками. Указанные преимущества позволяют преступникам совершать преступления на территории Республики Беларусь, находясь при этом в любой точке планеты, где имеется возможность подключиться к сети Интернет.

Еще одним ключевым фактором, влияющим на рост преступности в сети Интернет, является возникновение, широкомасштабное распространение и использование в качестве платежного средства криптовалюты. По состоянию на апрель 2023 г. в мире существует более 5 000 криптовалют, но большая часть из них не имеет значительной рыночной капитализации. Хищения криптоактивов у владельцев, манипулирование ценой криптовалюты на биржевых рынках, создание

в сети Интернет фиктивных криптобирж, криптообменников, инвест-проектов, массовое вовлечение и обман пользователей сети Интернет, связанные с завладением и использованием криптовалюты, является распространенным в мире явлением. На сегодняшнее время наиболее популярной криптовалютой остается биткоин. Современные преступники, изучая состояние развития рынка цифровых технологий и оценивая риски разоблачения, начали активно использовать анонимные криптовалюты, которые, в отличие от биткоина, скрывают транзакции в своей цепочке блоков (Monero, Zcash, Dash и др.). Основное их преимущество заключается в повышенном уровне конфиденциальности и анонимности, который достигается за счет использования различных протоколов шифрования. Анонимные криптовалюты обеспечивают возможность незаконной торговли наркотиками и оружием, финансирование терроризма, распространение детской порнографии, киберпреступления, отмывание денег и др. Для хранения анонимных цифровых активов преступникам не нужны тайники, склады, банки, нужен всего только цифровой ключ (пароль, шифр, код) от электронного кошелька в виде символов. Управлять и распоряжаться цифровым активом может тот, кто знает цифровой ключ. Тайные необратимые переводы криптовалюты из одной точки планеты в другую с минимально возможными потерями осуществляются за считанные минуты. Правоохранители многих государств, в том числе и Республики Беларусь, не имея доступа к электронным кошелькам преступников, не в силах самостоятельно контролировать, приостановить такие переводы и идентифицировать пользователей.

Необходимо признать, что современные возможности ОРД, осуществляемой на территории Республики Беларусь, весьма ограничены, чтобы самостоятельно противостоять активно надвигающимся интернет-угрозам и организованной преступности в сети Интернет. Для борьбы с ней необходимо международное объединение усилий всех правоохранительных органов. В первую очередь международное сотрудничество и взаимодействие правоохранительных органов, своевременный обмен между ними оперативной информацией, методами и технологиями идентификации пользователей сети Интернет, владельцев цифровых активов, практическим опытом работы, технологиями, взаимопомощь и сотрудничество, позволят более эффективно противостоять современным рискам и угрозам развивающейся преступности.