ужесточить наказание за непредоставление в соответствии с действующим законодательством, а также за нарушение сроков предоставления сведений, интересующих правоохранительные органы в рамках проверочных мероприятий, а также в ходе расследования уголовных дел.

Исходя из вышеизложенного, можно сделать вывод о том, что при осуществлении вышеуказанных мер расследование преступлений в сфере экономики обретет более высокий темп, что повлияет на будущий результат его расследования и повысит вероятность изобличения виновного лица в совершении преступления в полной мере.

УДК 348.3

П.Л. Боровик

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ: АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ И РЕШАЕМЫЕ ЗАДАЧИ

Одним из ключевых этапов раскрытия преступлений является поиск информации, представляющей оперативный интерес, осуществляемый оперативными подразделениями органов внутренних дел. От объема, достоверности и качества оперативно-розыскной информации зависят точность оценки оперативной обстановки, полнота и правильность принимаемых решений, направленность планирования оперативно-розыскных мероприятий, четкость постановки задач перед исполнителями, эффективность контроля и достижение конечного результата.

Специфика решаемых задач в информационной среде накладывает отпечаток и на облик применяемых методов и средств. Так, основные актуальные и самостоятельные направления использования информационных технологий в оперативно-розыскной деятельности органов внутренних дел могут быть сформулированы в следующем виде:

проведение разведывательно-поисковых мероприятий в информационной среде, в том числе в закрытом и неиндексируемом сегменте сети Интернет (компьютерная разведка);

установление физического местонахождения криминальной компьютерной информации и ее автора (телекоммуникационная разведка);

накопление, систематизация и анализ полученной информации для использования ее в деятельности оперативных подразделений органов внутренних дел (аналитическая разведка);

объединение всех оперативно-розыскных учетов в единую автоматизированную информационно-поисковую систему;

использование экспертных систем, позволяющих обрабатывать значительные массивы информации, содержащиеся в средствах массовой информации и автоматизированных банках данных, выделяя из них сведения, представляющие оперативный интерес;

идентификация лиц и документирование их преступных действий с использованием аппаратно-программных средств оперативной информации, получаемой в ходе осуществления компьютерной разведки;

обеспечение комплексной информационной безопасности подразделений органов внутренних дел (осуществление мероприятий по защите информации ограниченного распространения, информационно-техническое противодействие криминальному проникновению в оперативно-служебную деятельность органов внутренних дел, защита оперативных подразделений от дезинформации и т. п.);

предупреждение и раскрытие преступлений, совершаемых с помощью информационных технологий;

использование возможностей геоинформационных и навигационных систем (регистрация пространственно-временной информации, ее накопление и сохранение в информационных системах в автоматизированном режиме;

контроль за перемещением подвижных объектов; взаимодействие подразделений и служб правоохранительных органов и др.).

Рассмотрим отдельные аспекты реализации некоторых вышеприведенных направлений использования информационных технологий в раскрытии преступлений.

Так, в рамках проведения компьютерной разведки целесообразно использовать так называемые сканеры сети – программные средства, разработанные для поиска хостов сети с открытыми портами. С помощью данных программ можно не только собрать сведения о компьютерах, подключенных к сети Интернет, но и проанализировать информацию об архитектуре внутренней локальной сети, используемом типе сетевого оборудования, открытых портах и др.

Состояние и динамика развития информационных технологий и сети Интернет, как принципиально нового и постоянно расширяющегося объекта оперативного поиска, выделяют из структуры компьютерной разведки ее отдельную разновидность – телекоммуникационную разведку, позволяющую не только определить физическое местонахождение криминальной компьютерной информации, но и установить лицо, совершающее противоправные деяния.

Особенностью аналитической разведки является ее интегративная функция, позволяющая из разрозненных фактографических данных синтезировать новые знания. В настоящее время существует целый ряд специализированных программных средств (как платных, так и бесплатных), позволяющих не только осуществлять сбор полезных для использования в раскрытии преступлений аналитических данных из открытых источников сети Интернет, но и выполнять сетевую аналитику в большом массиве данных: о конкретном лице и его социально-психологическом портрете (круг общения, психологические особенности, мотивационные и ценностно-нравственные качества); о нескольких страницах одного и того же лица в различных социальных сетях, в том числе зарегистрированных под вымышленными данными, для его идентификации в качестве их единого владельца; об IP-идентификаторе устройства, использовавшегося для выхода в сеть Интернет в конкретных случаях (например, для распространения детской порнографии, наркотических средств и др.); о некоторых действиях определенного

лица по его активности в сети Интернет (например, по использовавшемуся им номеру телефона – для регистрации в социальных сетях и электронных платежных системах, при размещении объявлений и т. п.).

К указанным средствам следует отнести программное обеспечение с возможностями контент-анализа (UFED, XRY, U2, «Мобильный криминалист», OSForensics и др.). Объектами контент-анализа в основном являются информационные ресурсы и тексты в местах сетевого общения (социальные сети, форумы, блоги и др.), а также сетевые ресурсы с высокой потенциальной возможностью размещения информации криминального характера (DarkNet и DeepWeb). Применение подобных технических возможностей позволяет обобщать и сопоставлять полученные материалы, благодаря которым становится доступным установление связей интересующих лиц, их контактных данных, выявление потенциальных возможных соучастников.

Не менее значимой на современном этапе остается проблема автоматизации учета существующих массивов оперативно значимой информации. Современное состояние информационного обеспечения оперативно-розыскной деятельности характеризуется множественностью локальных оперативно-справочных и розыскных учетов, что осложняет поиск и использование необходимой информации. Полагаем, что создание единого защищенного информационного пространства для обмена информацией оперативно-розыскного назначения, а также автоматизированных рабочих мест оперативных сотрудников позволит в конечном итоге повысить раскрываемость преступлений.

Таким образом, можно сформулировать следующие выводы: раскрытие преступлений должно осуществляться с применением всех возможных средств и методов, охватывающих информационные сферы (средства массовой информации, средства телекоммуникаций и связи, локальные и глобальные компьютерные сети); получение оперативно значимой информации из компьютерных систем и сетей, используемых в преступных целях, сегодня является актуальным и востребованным направлением деятельности оперативных подразделений органов внутренних дел; обнаружение информации, представляющей оперативный интерес, и ее использование дает дополнительные возможности по укреплению или расширению доказательственной базы по уголовным делам независимо от вида преступления.

УДК 341

А.И. Бородич

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В ЦИФРОВОЙ ЭКОНОМИКЕ

Нельзя не согласиться с тем, что в современных условиях на этапе развития науки и техники происходит переход мирового сообщества в единое информационное пространство, представляющее собой область деятельности по созданию, преобразованию, передаче, использованию, хранению информации, оказывающей воздействие на индивидуальное, общественное сознание и собственно информацию. В то же время на фоне позитивных проявлений в едином информационном пространстве имеются и проблемы, решение которых позволит существенно снизить воздействие преступности на цифровую сферу. Не анализируя весь спектр проблем, связанных с информатизацией мирового сообщества, укажем на некоторые из них:

на государственные органы, физических и юридических лиц оказывает отрицательное информационное воздействие деструктивная информация, умышленно включенная в информационный контент, неконтролируемое распространение данной информации служит инициирующим фактором для противоправных деяний;

информационная сфера как совокупность информации, информационной структуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, представляет собой систему регулирования общественных отношений, в том числе для реализации технологий манипулирования сознанием пользователей информацией (формирование положительных (отрицательных) качеств);

современное информационное пространство превратилось в арену противоборства государств, что требует создания международной информационной безопасности, исключающей нарушение мировой стабильности и создание угроз безопасности мирового сообщества в информационном пространстве;

создается основа для нарушения защищенности информационной системы, несущей угрозу жизни и здоровью людей, для всеобщего контроля за населением в масштабах как отдельно взятых государств, так и мирового сообщества в целом;

в информационном пространстве все больше совершается предусмотренных уголовным законодательством государств преступлений против информационной безопасности и иных преступлений, предметом или средством совершения которых являются информация, информационные системы и сети, что определяет тенденцию увеличения их удельного веса в объеме всей преступности.

Следующим этапом в развитии мирового сообщества стала цифровизация, имеющая тесную связь с информатизацией, следовательно, для нее характерны те же проблемы, на которые мы указали выше.

Цифровизацию ученые рассматривают в узком и широком смысле. В узком смысле цифровизация – преобразование аналоговой информации в цифровую форму. В широком смысле, как указывает В.Г. Халин, она представляет собой современный общемировой тренд развития экономики и общества, который основан на преобразовании информации в цифровую форму и приводит к повышению эффективности экономики государств, у которых она хорошо развита.

Вместе с тем на эффективность экономики государств наряду с другими экономическими преступлениями международного характера (деяния, наносящие ущерб экономическому, социальному и культурному развитию государств (фальшивомонетничество, легализация преступных доходов, коррупция и т. п.), например, влияет международная коррупция, способствующая достижению многих деструктивных целей (подкуп должностных лиц международных организаций и транснациональных корпораций, злоупотребление данными лицами своими полномочиями в личных или групповых интересах и др.).