

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 иницирующим 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.).

Говоря об экономических преступлениях, целесообразно выделять в самостоятельную категорию преступность в сфере цифровой экономики. Согласно статистическим данным среди преступлений экономической направленности число преступлений, совершаемых посредством использования злоумышленниками информационно-телекоммуникационных технологий, с 2013 по 2019 г. увеличилось в 25 раз и составило к концу 2019 г. более чем 14 % от общего числа преступлений, зарегистрированных за год. Ежегодный прирост числа таких преступлений за шесть лет составил 60–80 %. Никакая другая отрасль преступности за всю историю не росла столь стремительно, как инновационная.

Однако отметим, что эта цифра не характеризует в полном объеме размах исследуемого явления во многом вследствие его высокой латентности, проистекающей главным образом из правовой неграмотности или инертности пострадавших от преступлений. Кроме того, сложность состоит в том, что четко обозначить круг преступлений, так или иначе связанных с использованием электронной информации, автоматизированных средств ее обработки и хранения, практически невозможно, поскольку технические способы фиксации, обработки и хранения информации непрерывно эволюционируют, равно как способы совершения преступлений и объекты посягательств постоянно трансформируются. Несомненно, цифровые технологии в руках даже одного человека, не говоря уже об организованных преступных группах, могут превратиться в орудие совершения преступлений.

Из вышеизложенного следует, что, поскольку значительная часть экономических сделок сегодня совершается в сети Интернет, преступность в сфере цифровой экономики имеет трансграничный характер. Исходя из этого, нельзя обойти вниманием вопрос о международном сотрудничестве в сфере противодействия данному социально опасному явлению.

В целях противодействия преступности в сфере цифровой экономики предлагаем некоторые направления деятельности:

усиление правовой защиты физических и юридических лиц, пострадавших от преступности в сфере цифровизации, в виде усиления ответственности за использование при совершении преступлений информационно-коммуникационной среды и специальных инструментов цифровой экономики;

совершенствование виктимологической профилактики как специфической деятельности социальных институтов, концентрируемой на выявлении, устранении или нейтрализации факторов, обстоятельств, ситуаций, по причине которых происходит совершение преступлений в сфере цифровой экономики;

организационная, техническая и иная поддержка соответствующих подразделений правоохранительных органов, включая регулярное обновление программного обеспечения, криминалистической техники, подготовку специалистов и др.;

определение и закрепление субъектов противодействия преступности, правового регулирования их деятельности как на международном, так и национальном уровне, направлений и форм сотрудничества;

обобщение и учет зарубежного опыта стран с развитой цифровой экономикой в сфере противодействия преступности в данной сфере;

управление рисками цифровой безопасности в экономической сфере на уровне мировой интеграции, государства, отдельных отраслей народного хозяйства, предприятий.

УДК 343.985

*С.А. Войтихович*

## **ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ИНФОРМАЦИИ НА СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА ПРИ ВЫЯВЛЕНИИ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ**

Использование оперативно-розыскной информации на стадии возбуждения уголовного дела является одной из важных проблем теории и практики борьбы с преступностью, обусловленных имеющимися недостатками и упущениями в оперативной работе, которые проявляются в процессе трансформации оперативно-розыскной информации от получения до возможности ее использования в уголовном процессе, а также в процессе формирования доказательственной базы уже на стадии возбуждения уголовного дела.

Анализ следственной и оперативной работы показывает, что процесс возбуждения уголовного дела может развиваться в двух ситуациях.

В первой ситуации в орган внутренних дел поступает заявление гражданина или сообщение должностных лиц государственных органов, иных организаций о совершении противоправного деяния. В этом случае уполномоченным лицом принимается решение о проведении следственной проверки в порядке ст. 173 УПК Республики Беларусь. Оперативный сотрудник, которому поручено проведение такой проверки, принимает все меры, предусмотренные уголовно-процессуальным законом и иными нормативными правовыми актами, по установлению оснований для возбуждения уголовного дела.

Во второй ситуации имеют место случаи, когда возбуждению уголовного дела предшествует активная оперативная работа в рамках дела оперативного учета, в ходе которой осуществляется выявление, изучение, накопление и фиксация информации о противоправной деятельности лица в целях ее последующего использования в доказывании по уголовному делу.

Необходимо отметить, что установление обстоятельств, подлежащих доказыванию по экономическим преступлениям, возможно, как правило, только при проведении ОРМ. Например, доказать цель сбыта как конструктивного признака составов некоторых экономических преступлений, при которых преступник осуществляет указанные действия, посредством проведения следственных действий крайне затруднительно, а часто и просто невозможно. И поэтому в работе с информацией необходимо ее понимание и познание процесса ее использования в ОРД и на стадии возбуждения уголовного дела.

Ретроспективное познание – это приобретенное знание как особый вид информации и результат ее переработки. Информация и знание соприкасаются друг с другом лишь в пределах одного акта познания. В нем знание занимает место кон-