ждународное сотрудничество. Первым шагом на пути к реализации этой задачи может стать принятие комплексной международной стратегии кибербезопасности. Для ее реализации необходимы:

унификация терминологического аппарата;

гармонизация законодательной базы;

разработка конкретных планов действий, отчетливое указание их целей, а также спектра решаемых проблем;

тесное сотрудничество частного и государственного сектора, осуществляемого посредством обмена информацией, передовыми практиками (например, в сфере управления инцидентами, обучения специалистов и обычных пользователей ИКТ), а также путем проведения специальных учебных мероприятий (учений, тренингов) на государственном и международном уровнях.

УДК 343.985

В.Л. Венгловский

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫЯВЛЕНИИ НАРКОПРЕСТУПЛЕНИЙ

Используя интернет-технологии наркосбытчики получили возможность продавать наркотики бесконтактным способом и в определенной степени анонимно. Посредством сети Интернет создаются интернет-магазины, осуществляется реклама, привлечение и координация действий членов преступных групп в разных регионах страны, так и за ее пределами, что потребовало от правоохранителей в целях противодействия наркопреступлениям развивать и совершенствовать информационно-аналитическую деятельность.

Проделанный анализ научной и специальной литературы показал, что среди ученых и практиков отсутствует единое понимание сущности, задач и методов информационно-аналитической деятельности, что влечет существенные проблемы не только в области теоретической проработки рассматриваемого вопроса, но и в построении эффективной правоприменительной практики, организация которой осложнена наличием большого количества субъектов, в той или иной степени решающих задачи противодействия наркопреступности.

Одной из основных проблем при создании теоретической основы данной деятельности видится необходимость определения сущности и содержания информационно-аналитической деятельности при выявлении преступлений и как ее составной части – наркопреступлений, совершаемых в сети Интернет.

Ряд авторов в своих работах используют для обозначения рассматриваемой деятельности достаточно близкие по содержанию термины: «аналитическая разведка», «аналитическая работа», «аналитическая деятельность», «аналитический поиск».

Отдельные ученые относят информационно-аналитическую деятельность к числу методов познания и понимают под ним метод, заключающийся в комплексном применении сил, средств и методов оперативно-розыскной деятельности (ОРД) по сбору, обобщению и анализу конфиденциальной и легитимной информации, обеспечивающей приращение или получение новых знаний об объектах и субъектах криминальных проявлений, для упреждающего воздействия на преступность или определяют аналитический поиск как метод ОРД, предполагающий «проникновение» в документальные источники сведений и соответствующие массивы данных, содержащих знания об объектах, представляющих оперативный интерес, и их детальное изучение в целях получения оперативно значимой информации.

Вклад в развитие информационно-аналитической деятельности внес С.С. Овчинский, который в своей монографии «Оперативно-розыскная информация» предложил концептуальные основы информационного обеспечения оперативно-розыскной и профилактической деятельности органов внутренних дел.

В работе Е.Г. Белоглазова «Методология обеспечения аналитической разведки криминальных процессов и явлений» рассмотрены виды информационно-аналитической деятельности и источники информации, основанные на информационных технологиях, также определены основные направления этой деятельности применительно к различным оперативным подразделениям органов внутренних дел.

С.В. Пилюшин в своей работе «Аналитическая деятельность в принятии управленческих решений: сущность и значение» анализирует сущность информационно-аналитической деятельности на примере деятельности по выявлению экономических преступлений. При этом автор отмечает, что аналитическая деятельность вышеуказанных сотрудников осуществляется посредством применения конкретных методов познания, где для каждого характерна совокупность определенных принципов, правил, приемов и алгоритмов, сложившихся в четкую систему в процессе их применения.

В исследовании А.С. Щуровой «Незаконный оборот наркотиков в Интернете» делается акцент на том, что особенность незаконного оборота наркотиков, совершаемого посредством сети Интернет, заключается в использовании сетей телекоммуникаций и связи. При выявлении

данного вида преступлений объектом поиска выступает информация, отражающая направленность умысла на приобретение или сбыт наркотиков, как, например, непосредственно переписка приобретателя со сбытчиком, номера телефонов, паспортные и иные данные для совершения денежных переводов, иная информация, распространяемая через интернет, характеризующая преступную направленность. В свою очередь, объект и особенности информационно-аналитической деятельности автором раскрыты фрагментарно и не являются исчерпывающими, но при этом имеют прикладное значение при выявлении наркопреступлений.

Таким образом, в настоящее время отсутствует единый подход к пониманию понятия информационно-аналитической деятельности при выявлении преступлений, в том числе наркопреступлений, совершаемых в сети Интернет.

Ряд вопросов информационно-аналитической деятельности при выявлении наркопреступлений требуют научной проработки, наиболее актуальными для комплексного исследования являются аспекты, связанные с определением сущности, содержания, особенностей информационно-аналитической деятельности; получения информации и анализа ее источников, используемых при ее осуществлении; связанные с информационно-аналитическим и тактическим обеспечением данной деятельности.

УДК 343.98

О.П. Виноградова

ТАКТИКО-КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПРОВЕДЕНИЯ НЕВЕРБАЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Преступления в сфере информационно-телекоммуникационных технологий с каждым годом приобретают все большее распространение. Это связано с ростом уровня информатизации общества и внедрения интернет-технологий, что напрямую способствует увеличению таких преступлений, как кражи, совершенные с помощью интернет-технологий. В России на начало этого года насчитывалось 129,8 млн интернет-пользователей [1]. На рост пользователей сети Интернет, несомненно, повлияла пандемия коронавирусной инфекции COVID-19. Распространение коронавирусной инфекции повлияло на работу многих офлайн-площадок по продаже различных товаров и услуг и, следовательно, увеличилось количество интернет-магазинов. Все это, наряду с «цифровым невежеством» [2], обусловило значительное увеличение количества киберпреступлений.

В то же время, несмотря на понижение темпа роста рассматриваемых преступлений, нельзя не отметить, что кражи, совершенные с помощью интернет-технологий, и в целом все киберпреступления постоянно со временем видоизменяются и совершенствуются, что снижает эффективность по их выявлению, раскрытию и расследованию. Развитие преступной среды предопределяет возможность обезличивания злоумышленников, а также совершение таких преступлений дистанционно, что позволяет скрыть следы. В связи с этим растет уровень совершаемых рассматриваемых преступлений, поэтому деятельность правоохранительных органов в настоящее время направлена на выявление, раскрытие и расследование краж, совершенных с использованием интернет-технологий.

Лицам, проводящим осмотр, необходимо знать, что компьютерно-техническое устройство находится в выключенном состоянии, его необходимо оставить в этом состоянии, чтобы предотвратить потерю доказательственной информации, а если устройство было включено, то стоит обратить внимание на информацию, содержащуюся на экране, об уровне заряда устройства, об операционной системе, службе доступа к файлам и сети. В данной ситуации могут быть выявлены цифровые следы преступления. Как отмечают В.О. Давыдов и И.В. Тишутина, такие цифровые следы «имеют высокую скорость трансформации, легко уничтожаются и модифицируются, могут быть представлены бесконечным количеством копий, легко распространяются в компьютерных сетях и доступны в любой точке, где имеется подключение к сети Интернет, цифровой или электронный след может состоять из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких электронных носителях информации, подключенных как к одному, так и к нескольким компьютерам, объединенным в информационную систему или информационно-телекоммуникационную сеть» [3]. Стоит отметить также, что на устройстве, которое является объектом осмотра, может быть установлена защита, требующая ввода определенного защитного кода или другой специальной команды, и если не произвести вышеперечисленные действия, то информация на устройстве может быть уничтожена, и поэтому для получения доступа к осматриваемому устройству необходим пароль. В таком случае считается целесообразным получить указанные пароли добровольно. Если будут проведены все эти действия, то обнаружение и копирование значимой информации для расследования уголовного дела будет осуществлено в более короткий