В настоящее время такая деятельность регламентируется целой группой правовых норм, установленных открытыми актами законодательства, которые охватывают различные ее стороны. Вместе с тем объем правового регулирования данной сферы недостаточен. Нормативный материал носит фрагментарный характер, порождая локальные (изолированные) и разрозненные массивы правовых норм, касающиеся отдельных видов безопасности и относящиеся к разным отраслям права. Такая ситуация обусловлена тем, что обеспечение безопасности объектов, которые можно отнести к КВО, охватывается многими сферами общественных отношений и объективно может быть определено в любой из существующих правовых отраслей. Несмотря на то что в настоящее время в Республике Беларусь действует значительное число нормативных правовых актов различного уровня, регламентирующих тем или иным образом обеспечение безопасности КВО, существующие правовые предписания не охватывают в полной мере всей совокупности отношений, складывающихся в данной сфере. Нормативная регламентация обеспечения безопасности отдельных видов КВО осуществляется в основном на уровне подзаконных нормативных правовых актов. Необходимо отметить определенную неравномерность объема правового регулирования обеспечения безопасности различных видов КВО. В связи с этим видится целесообразным принятие законодательного акта, непосредственно регламентирующего обеспечение безопасности КВО, предметом регулирования которого являлись бы все аспекты деятельности уполномоченных субъектов по защите и охране соответствующих объектов.

Обеспечение безопасности КВО обладает собственным особым составом (содержанием): объект и предмет, субъекты и участники, мероприятия, средства и способы осуществления мероприятий, результаты.

Объект обеспечения безопасности КВО – общественные отношения, которые складываются в данной сфере и на защиту и охрану которых оно направлено. Предметом такого обеспечения является террористическая и иная противоправная деятельность, а также природные явления и технологические сбои, создающие угрозы безопасности КВО. Субъекты, к которым следует относить соответствующие государственные органы (органы внутренних дел, государственной безопасности и иные), их уполномоченных должностных лиц, а при реализации отдельных мер обеспечения безопасности КВО – сотрудников таких объектов. Участники – юридические и физические лица, оказывающие помощь в обеспечении безопасности КВО. Мероприятия по обеспечению безопасности КВО – совокупность действий должностных лиц уполномоченных государственных органов, сотрудников КВО, осуществляемых в процессе защиты и охраны соответствующих интересов. Такие мероприятия направлены на реализацию соответствующих мер обеспечения безопасности КВО (правовые, организационные, инженерно-технические, аппаратно-программные, специальные). Средства осуществления указанных мероприятий: технические – устройства, приборы, аппаратура и т. п.; информационные – базы и банки данных, документы и т. д.; материальные – финансовые активы, инженерно-технические сооружения и т. п. Способы осуществления таких мероприятий – оптимальные приемы их проведения уполномоченными субъектами с помощью имеющихся средств и при соблюдении определенных условий. Результат обеспечения безопасности КВО – итог совершения субъектами и участниками соответствующих мероприятий в процессе защиты и охраны соответствующих интересов с использованием имеющихся средств и посредством необходимых способов. В широком смысле результатом рассматриваемого обеспечения будет являться решение задач по обеспечению национальной безопасности.

В структуре обеспечения безопасности КВО могут быть выделены различные связи и отношения между ее элементами: организационные, правовые, психологические и т. д. Наиболее важными, по нашему мнению, являются связи между субъектами обеспечения безопасности КВО, которые реализуются в виде правоотношений, а также организационные связи, которые реализуются в рамках государственного управления рассматриваемой сферой.

Функции обеспечения безопасности КВО зависят от его основных системных свойств. Поэтому его основными функциями будут являться: режимная (предупреждение угроз безопасности КВО), поисковая (выявление угроз), правоохранительная (локализация угроз), компенсационная (возмещение причиненного вреда).

Функционирование обеспечения безопасности КВО будет проявляться в форме его реализации. Внешней формой обеспечения безопасности КВО целесообразно рассматривать нормативные правовые акты, в которых проявляются и закрепляются соответствующие мероприятия, проводимые в этой сфере, а также способы и средства их осуществления, вынесенные решения; внутренней формой – соответствующий процесс, который выражается в системе процедурных требований и элементов, связывающих в единое целое разные стороны деятельности по обеспечению безопасности КВО.

УДК 343.985.8

С.В. Пилюшин

ИНТЕРНЕТ КАК ПЛАТФОРМА ДЛЯ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

В связи со стремительным развитием информационных и телекоммуникационных технологий на современном этапе объем размещаемой в сети Интернет информации, представляющей оперативный интерес, постоянно возрастает. Сведения о лицах, событиях и обстоятельствах, способствующие решению задач, стоящих перед сотрудниками оперативных подразделений при осуществлении оперативно-розыскной деятельности, концентрируются в многочисленных информационных ресурсах сети. В этих условиях при осуществлении оперативно-розыскных мероприятий оперативные сотрудники должны приобретать навыки, позволяющие выявлять и документировать такие сведения, что позволит эффективно бороться с преступностью.

Речь идет о так называемой виртуальной разведке – разведке, ведущейся в информационных потоках, которые в гигантских количествах производятся всеми государственными и частными субъектами хозяйствования, а также отдельными гражданами. Исследователи данной тематики выделяют три основных направления: разведку в информационно-вычислительных компьютерных сетях; разведку в бумажных и электронных средствах массовой информации; разведку в непериодических изданиях, в том числе открытых и так называемых серых (т. е. не имеющих грифа секретности, но не предназначенных для массового распространения – отчетах о НИР, аналитических справках, деловой переписке, диссертациях и т. п.).

Виртуальная разведка представляет собой целый комплекс взаимосвязанных действий оперативного и технического характера. Важнейшим техническим компонентом виртуальной разведки является компьютерная разведка, а именно целенаправленная деятельность по добыванию с помощью средств вычислительной техники и программного обеспечения разведывательной информации, обрабатываемой в информационно-вычислительных сетях и (или) отдельных средствах вычислительной техники.

Еще в начале 90-х гг.аналитики спецслужб США обратили внимание на то, что большая часть необходимой информации без особого труда может быть получена через сеть Интернет. В развитых государствах на компьютерную разведку, осуществляемую спецслужбами, выделяются значительные денежные средства. У всех на слуху такие службы, как ЦРУ, ФБР, СИС, МОССАД, ФСБ. Цели компьютерной разведки выражаются в получении сведений о предмете, конечных либо прогнозируемых результатах, формах и способах деятельности субъектов, являющихся пользователями информационно-вычислительной сети, и используемом аппаратурном и программном обеспечении, протоколах управления и информационного взаимодействия и используемых средствах и методах защиты информации.

К сожалению, в силу многих складывающихся объективных факторов создание РУ-РО-ГОВД подразделений специализирующихся на выявлении преступлений в сфере высоких технологий, носит замедленный характер и в настоящее время в большинстве районных отделов таких специалистов нет. Данное обстоятельство негативно сказывается на эффективности работы криминальных подразделений в целом, своевременном получении оперативно-значимой информации о лицах и фактах, представляющих оперативный интерес. Большинство оперативных сотрудников не имеют навыков на достаточно высоком профессиональном уровне осуществлять оперативный поиск в сети Интернет. Усугубляет положение и материально-техническое обеспечение. В большинстве оперативных подразделений отсутствует возможность выхода в сеть с рабочих мест.

Необходимо учитывать и то, что технологическая сложность большинства сетевых процессов и значительный объем данных, выявляемых преимущественно в электронном виде, приводят к необходимости привлечения к проведению значительной части ОРМ специалиста, обладающего знаниями в области информационных технологий.

Разрешение данной проблемы лежит также в плоскости субъективных факторов, т. е. личном добросовестном отношении сотрудника к исполнению возложенных на него обязанностей, иными словами, в желании работать в данном направлении, самостоятельно повышать уровень профессионального мастерства.

Несмотря на проблемы, наблюдается тенденция к проявлению активности, что приводит пока еще к незначительным, но все-таки имеющим свои плюсы результатам в работе при осуществлении оперативного поиска в сети Интернет сотрудниками криминальных подразделений ОВД.

К основным направлениям осуществления оперативного поиска в сети Интернет можно отнести: поиск информации, которая может прямо или косвенно свидетельствовать о совершении противоправных действий; сбор материалов в отношении выделенного объекта оперативного поиска: физических и юридических лиц, предметов и событий в связи с их отношением к противоправной деятельности; анализ и использование полученных в компьютерной сети оперативных данных в качестве доказательств.

Использование сети Интернет не отражает в полной мере суть оперативного поиска в виртуальном пространстве. Многое зависит от поставленных целей, а также направления деятельности того или иного оперативного подразделения. Ведь для каждой оперативной службы специфика выявления признаков преступления при осуществлении оперативного поиска своеобразна. Так, например, для оперативных подразделений НиПТЛ достаточно обнаружение факта размещения в социальных сетях материалов порнографического содержания. После этого продолжаются мероприятия по установлению причастного к данному факту виновного лица. Иные подходы у оперативных сотрудников, осуществляющих борьбу с преступлениями экономической направленности. В данном случае поиск оперативной информации осуществляется вокруг конкретного лица, исследуются отдельные частные случаи, при этом оперативным сотрудником используется логический метод неполной индукции. И только после получения информации, ее детального анализа, сверки с иными информационными ресурсами, в том числе учетами ОВД, оперативный работник переходит к построению гипотезы, которая нуждается в доказывании, а именно должен сделать вывод об обнаружении признаков преступления, при их наличии он планирует дальнейшие оперативно-розыскные мероприятия.

В заключение отметим, что сотрудники оперативных подразделений должны быть в полном объеме обеспечены современными техническими средствами, позволяющими эффективно вести компьютерную разведку. На данном этапе должна быть организована подготовка соответствующих специалистов. Необходимо под другим углом взглянуть на теорию и практику оперативно-розыскной деятельности. Анализ публикаций в области осуществления оперативно-розыскной деятельности показывает, что эффективное оперативно-розыскное реагирование на преступные действия в пространстве, а именно в глобальной сети Интернет, требует корректировки методов ОРД.

УДК 343.985

С.С. Сипаков

УСТАНОВЛЕНИЕ ЛИЦ, ПРИЧАСТНЫХ К НЕЗАКОННОМУ ОБОРОТУ НАРКОТИКОВ, ПУТЕМ АНАЛИЗА ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИСПОЛЬЗУЕМЫХ ИМИ МОБИЛЬНЫХ ТЕЛЕФОНАХ И ПЛАНШЕТАХ

Для приобретения и реализации наркотиков активно используются средства мобильной связи, оснащенные современной системой навигации и поддержкой интернета.

Первоначально в мобильных телефонах были простейшие функции, в основном калькуляторы, органайзеры, и т. п. Постепенно с развитием технологий мобильные телефоны достигли очень высокого уровня функционирования операционной системы. Для подчеркивания возросшей функциональности и вычислительной мощности таких моделей используют термин «смартфон». Большую популярность в настоящее время приобрели планшеты – персональные электронно-вычислительные машины без отдельного системного блока и без клавиатуры и мыши с ограниченными функциями, которыми можно управлять прикосновениями пальцев.

Современные смартфоны и планшеты позволяют получить много информации об их владельцах, которые порой об этом даже не подозревают. При первом запуске устройства пользователь может не отключить включенную по умолчанию функцию геолокации, что позволит в дальнейшем отслеживать все его перемещения. Оперативная система Android позволяет просмотреть его маршруты в течение дня, а также фиксирует их на Google-картах в разделе Timeline. Аналогичными функциями пользуются большинство владельцев iPhone, iPad и аппаратов на Windows Phone. Также на современных смартфонах при первом запуске предлагается включить опцию поиска смартфона в случае его потери. Это поможет найти его или даже отследить передвижения вора в случае кражи. Стоит помнить, что гаджеты Apple также отслеживают информацию о часто посещаемых владельцем местах.