раскрытие особенностей правового регулирования отношений в рассматриваемой сфере (предмет, метод, способ и тип регулирования);

определение содержания и характеристик информационно-аналитического обеспечения правоохранительной деятельности;

формирование перечня правоохранительных органов (адресатов рекомендаций по правовому регулированию);

разработка системы нормативных правовых актов, регламентирующих как отдельные вопросы, так и информационно-аналитическую работу в целом.

Решение указанных задач позволит внедрить общие подходы к правовому регулированию информационно-аналитического обеспечения правоохранительной деятельности, унифицировать национальное законодательство государства, регулирующее правоотношения в указанной сфере, повысить эффективность правоприменительной деятельности субъектов обеспечения национальной безопасности.

Методологической основой разработки является диалектико-материалистический метод, а также комплекс методов:

общетеоретического уровня – системно-структурный, восхождение от абстрактного к конкретному;

эмпирического уровня – наблюдение, описание, сравнения (в том числе изучение и анализ нормативных правовых актов государства, регламентирующих деятельность уполномоченных субъектов в сфере обеспечения национальной безопасности, а также модельного законодательства Организации Договора о коллективной безопасности и Содружества Независимых Государств);

общелогических – анализ, синтез, обобщение;

конкретно-социологического уровня – интервьюирование специалистов в области правового регулирования отдельных сфер обеспечения национальной безопасности, проведение экспертных оценок;

специальных – формально-юридический, сравнительно-правовой, толкования правовых норм.

Таким образом, постановка указанных проблем предопределяет актуальность проводимого юридического анализа и разработки на основе полученных результатов рекомендаций и предложений по совершенствованию правового регулирования рассматриваемой сферы с учетом научно обоснованных положений юридической науки и с учетом базирующейся на обобщении и анализе практики правоохранительных органов.

УДК 343

С.А. Медведев

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-ПОИСКОВОЙ ДЕЯТЕЛЬНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Развитие информационных технологий в современном мире привело к тому, что объемы информации, циркулируемой в сети, постоянно растут. Сведения о гражданах, событиях и обстоятельствах, представляющих интерес для выполнения оперативно-розыскной деятельности (ОРД), концентрируются в многочисленных ресурсах сети. В этих условиях знания особенностей проведения оперативно-розыскных мероприятий (ОРМ) открывают перед оперативными подразделениями новые возможности в противодействии преступности.

В настоящее время обширно распространяются среди пользователей сети Интернет сервисы IP-телефонии, которые обеспечивают голосовую связь абонентов с дополнительными возможностями (визуальный контакт, конференц-связь). Очевидно, что оперативно-розыскной контроль подобных переговоров удовлетворяет признакам не только контроля в сетях электросвязи, но и такого оперативно-розыскного мероприятия, как слуховой контроль.

С развитием форм сетевого общения появляются новые методы проведения опроса. В киберпространстве имеются условия для получения сведений о криминальной активности лица при изучении сообщений в местах сетевого общения. В указанных местах может проводиться опрос лиц, которым известны сведения, представляющие оперативный интерес.

Особое содержание в сетевом пространстве приобретает ОРМ «оперативное отождествление». Как правило, такое мероприятие базируется на сравнении полученных из оперативных источников данных о личности фигуранта, который причастен к преступной деятельности, со сведениями о субъекте, сетевая активность которого изучается. К формам отождествления личности можно отнести опознание по фотографиям, которые размещают на персональных страницах социальных сетей, по указанным там же автобиографическим данным, по используемым псевдонимам, адресам электронной почты, номерам ICQ, IP-адресам.

Функционирование в сети Интернет мощных справочно-информационных систем создает условия для наведения справок путем прямого изучения размещенных в них документов, а также направления по электронной почте запросов в организации, у которых есть интересующие сведения.

Одним из наиболее сложных ОРМ при реализации в киберпространстве является оперативный эксперимент. Международной практике известны примеры осуществления оперативного эксперимента, которые связаны с созданием в сетевом пространстве негласно контролируемых объектов, представляющих интерес для преступников.

Ограниченное применение возможно и для контроля почтовых отправлений. Такие действия в конкретных ситуациях позволяют не только получать важные фактические данные, но и создавать препятствия обмену информацией между изучаемыми лицами.

Рост количества торговых операций, которые реализуются через сеть Интернет, заставляет расширять практику использования и ОРМ «проверочная закупка» и «контролируемая поставка» в целях выявления преступлений в сфере торговли и в сфере распространения запрещенных к обороту объектов. К примеру, в практике известно успешное применение проверочной закупки в ходе реализации контролируемых поставок наркотических средств.

Решение задач по поиску, отбору и систематизации оперативной информации предполагает применение информационных систем, позволяющих существенно расширить круг информации, необходимой для аналитической работы, и распространяется в нескольких направлениях.

Важной стороной информационного обеспечения деятельности оперативного сотрудника является организация содействия в анализировании имеющейся информации для формирования решений. Экспертные системы, применяющиеся в оперативной работе, занимают особое место среди информационного обеспечения.

Существует несколько видов экспертных систем раскрытия и расследования преступлений: выявления скрытых преступлений, прогнозирования преступлений, поиска и установления личности преступника.

В деятельности подразделений ОВД используется специализированное программное обеспечение, которое ориентировано на непосредственное применение при осуществлении ОРМ в направлении борьбы с информационной преступностью.

Следовательно, в информационном пространстве (при учете его социальной составляющей) на сегодняшний день может осуществляться практически любое из предусмотренных законом оперативно-розыскное мероприятие. В то же время при подготовке и проведении таких мероприятий оперативный сотрудник обязан учитывать специфику сетевого информационного пространства и сформировавшейся в нем криминогенной среды.

УДК 004.056

М.К. Новиков, Т.Ф. Старовойтова

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ЕДИНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТАМОЖЕННЫХ ОРГАНОВ РЕСПУБЛИКИ БЕЛАРУСЬ

В середине 2016 г. Государственным таможенным комитетом Республики Беларусь была введена единая автоматизированная информационная система таможенных органов (ЕАИС ТО) Республики Беларусь. Данная система включает в себя 40 информационных систем. Основные из них:

автоматизированная подсистема «Транзит Таможенного союза»;

Национальная автоматизированная система электронного декларирования;

автоматизированная информационная система автоматизации операций таможенного оформления и контроля, ведения базы данных таможенной информации на уровне пунктов таможенного оформления и таможни;

автоматизированная система управления рисками;

автоматизированная подсистема «Модуль автоматической рассылки сообщений».

Система защиты информации (СЗИ) ЕАИС ТО Республики Беларусь предназначена для обеспечения конфиденциальности, целостности и доступности информации ограниченного распространения и другой критичной информации, обрабатывающейся в ЕАИС ТО, а также для обеспечения защиты информации при взаимодействии ЕАИС ТО с внешними информационными системами.

СЗИ ЕАИС ТО включает в себя следующие подсистемы: управления пользователями и разграничения доступа, аудита событий, защиты каналов связи, криптографической защиты информации, антивирусной защиты, резервного копирования и восстановления работоспособности.

В конце 2016 г. система защиты информации ЕАИС ТО Республики Беларусь была аттестована. Это означает, что система защиты информации ЕАИС ТО Республики Беларусь класса Б2 (по СТБ 34.101.30-2007) соответствует всем требованиям законодательства Республики Беларусь в области защиты информации, а именно: Закону Республики Беларусь «Об информации, информатизации и защите информации», приказу Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации».

Но, несмотря на все принимаемые меры по защите информации, найти в огромном массиве данных конфиденциальную информацию и выявить факт записи ее на внешнее запоминающее устройство или передачи по сети, электронной почте очень сложно. DLP-система (систе-