УДК 343.98

И.А. Кузьмин

ОТДЕЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫЯВЛЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В статье рассмотрены вопросы организации информационного обеспечения оперативно-розыскной деятельности, порядок взаимодействия операторов связи с органами, уполномоченными на осуществление оперативно-розыскной деятельности.

Ключевые слова: информационное обеспечение, информационно-коммуникационные технологии, компьютерные преступления, ограничение конституционных прав и свобод граждан, системы оперативно-розыскных мероприятий.

I. A. Kuzmin

SEVERAL ISSUES OF INFORMATION SUPPORT FOR OPERATIVE-SEARCHED ACTIVITY AT DETECTION AND INVESTIGATON OF CRIMES CAUSED BY THE USE OF COMPUTER AND TELECOMMUNICATION TECHNOLOGIES

This article considers the issues of the organization of information support of operatively-investigative activity, the order of interaction of communication operators with the bodies authorized to carry out operational-search activity.

Keywords: Information support, information and communication technologies, computer crimes, restriction of constitutional rights and freedoms of citizens, system of operational-search activities.

По мнению видного ученого П.В. Сороколетова, мир сегодня стоит на пороге четвертой информационной революции [1]. Все более интенсивно протекают процессы глобализации, в том числе информатизации. Развиваются информационно-коммуникационные технологии (далее – ИКТ). Увеличивается как видовое разнообразие создаваемой, передаваемой, используемой и хранящейся информации, так и ее объем. Появляются новые способы передачи данных, процесс их передачи также ускоряется.

Возможность своевременного получения и фиксации информации становится одним из ключевых факторов успешности в самых разных сферах жизнедеятельности, в том числе и в деятельности правоохранительных органов. В современных условиях эффективная защита прав и интересов граждан, обеспечение законности «в превентивных целях» [2, с. 153] невозможны без должного информационного обеспечения (далее – ИО) органов внутренних дел, а также без использования ИКТ, отвечающих

современным требованиям. Анализ сложившейся практики показывает, что имеющиеся ресурсы не позволяют в полной мере решать задачи, которые ставятся перед ОВД в настоящее время.

Особое значение решение вопроса о своевременном и полном получении информации приобретает при осуществлении противодействия преступлениям, совершенным с использованием ИКТ. В этой связи Министерством внутренних дел реализован ряд мер по улучшению ИО. Так, приказом Министерства внутренних дел Российской Федерации от 8 июня 2006 г. № 420 была утверждена программа «Создание единой информационно-коммуникационной системы органов внутренних дел» (далее – Программа), целью которой стало создание единой информационно-телекоммуникационной системы ОВД путем совершенствования ИО ОВД, посредством реконструкции и оборудования объектов ОВД новыми и перспективными телекоммуникационными и программно-техническими комплексами с использованием современных телекоммуникационных, информационных и биометрических технологий.

Позднее, 20 мая 2008 г. приказом Министерства внутренних дел Российской Федерации № 435 утверждена новая редакция Программы, в период реализации которой подразделения ОВД получили возможность оперативно пользоваться различной информацией посредством приобретенного и установленного оборудования с помощью специально разработанного программного обеспечения.

Спектр получаемой в оперативном режиме информации чрезвычайно широк: персональные данные граждан, сведения о регистрации, имеющихся транспортных средствах, оружии, действующих и утраченных паспортах, сведения о привлечении к уголовной и административной ответственности, похищенных номерных вещах, выписки из единых государственных реестров юридических лиц и индивидуальных предпринимателей и многое другое.

В настоящее время информационные ресурсы, используемые правоохранительными органами, формируются не только из учетов, ведущихся непосредственно ОВД, но также из информации, предоставляемой ОВД различными государственными, муниципальными, частными учреждениями, организациями и предприятиями.

Оперативный доступ к такой информации существенно ускоряет и облегчает многие вопросы, возникающие в процессе осуществления оперативно-служебной деятельности. В то же время одним из негативных аспектов быстрого доступа к информации становится потенциальная опасность «утечки» информации третьим лицам и использования ее в незаконных целях. Для пресечения или минимизации такой опасности разработаны различные инструкции по работе со справочно-информационными сервисами, согласно которым доступ к информационно-телекоммуникационным ресурсам ОВД предоставляется строго ограниченному кругу лиц по заявкам установленного образца, утвержденных уполномоченными руководителями. За незаконное использование информации действующим законодательством предусмотрена уголовная,

административная и гражданская ответственность, а также дисциплинарная ответственность в соответствии с ведомственными нормативными правовыми актами.

Таким образом, реализован комплекс мер по предоставлению заинтересованным сотрудникам ОВД оперативного доступа к различным данным, используемым в процессе осуществления ежедневной оперативно-служебной деятельности, при этом документально регламентирован порядок доступа и установлена ответственность за нарушения, допущенные в ходе ее неправомерного использования.

Анализ практики показывает, что несмотря на существенное улучшение ИО, реализацию дополнительных мер по развитию ИКТ в системе МВД России, говорить о достаточности имеющегося ИО не приходится. Имеется ряд нерешенных вопросов, из числа которых одним наиболее важным представляется организация ИО противодействия преступлениям, совершенным с использованием современных ИКТ.

Актуальность вопроса подчеркивает изучение статистических сведений о преступности. Так, за 9 месяцев 2017 г. на территории Российской Федерации зарегистрировано 62 496 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, что составило 4 % от общего числа зарегистрированных преступлений. Число преступлений в сфере ИКТ и компьютерных технологий более чем в два раза превышает число выявленных преступлений коррупционной направленности (24 856), в два раза превышает суммарное число убийств, покушений на убийство, умышленных причинений тяжкого вреда здоровью, изнасилований и покушений на изнасилование (26 464), значительно превышает суммарное количество грабежей и разбойных нападений (50 346) [3].

Для противодействия преступлениям в сфере ИКТ и компьютерных технологий правоохранительные органы должны обладать знанием способов совершения таких преступлений, тактики и методики выявления, раскрытия и расследования преступлений данной категории; стремиться к превосходству над злоумышленниками в уровне технической оснащенности и скорости получения информации. Особенно актуален данный вопрос при осуществлении противодействия мошенничествам и кражам, совершенным с использованием ИКТ. Однако многие сотрудники ОВД, осуществляющие противодействие преступлениям, совершенным с использованием современных информационно-коммуникационных технологий, сталкиваются с рядом существенных трудностей при получении необходимой информации, что негативно сказывается на итогах оперативно-служебной деятельности. Опросы сотрудников территориальных ОВД показывают, что основными проблемами организации ИО в борьбе с преступлениями, совершенными с использованием ИКТ, являются следующие:

1. Несвоевременность получения информации о соединениях между абонентами и (или) абонентскими устройствами, особенно в случаях, когда информация необходима от оператора связи, не имеющего представительств в регионе местонахождения инициатора запроса.

2. Длительность получения информации от интернет-провайдеров, а также от владельцев и администраторов различных интернет-ресурсов.

3. Сложность идентификации и обнаружения фактических собственников, а также администраторов и пользователей некоторых интернет-ресурсов.

Очевидно, эти проблемы требуют решения. Ортодоксальным способом решения представляется внесение изменений в нормативные правовые акты, регламентирующие порядок взаимодействия ОВД с операторами связи, интернет-провайдерами, владельцами и администраторами различных интернет-ресурсов с учетом развития ИКТ, а также ряда иных факторов. В Российской Федерации с 1992 г. принято более 30 таких нормативных правовых актов. При этом законотворческая инициатива в данном направлении постоянно находит свое отражение как в законопроектах, так и принятых законах. Так, к числу наиболее значимых законов из числа принятых в 2016–2017 гг., без сомнения, относится так называемый «закон Яровой» [4,5], установивший расширение полномочий правоохранительных органов, новые требования к операторам связи и операторам почтовой связи.

Не подвергая сомнениям важность и актуальность вопроса систематизации законодательства в сфере связи, полагаем, что не менее важным в противодействии преступлениям, совершенным с использованием ИКТ, является изменение самого порядка взаимодействия ОВД с операторами связи.

В настоящее время все операторы связи, в том числе интернет-провайдеры обязаны установить и обеспечивать функционирование систем оперативно-розыскных мероприятий [6] (далее – СОРМ), первые из которых начали внедряться с 80-х гг. Данные СОРМ посредством программно-аппаратных комплексов, администрируемых подразделения-ми Федеральной службы безопасности, обеспечивают доступ к информации о телефонных переговорах, а также интернет-трафику пользователей. Факт существенной востребованности успешного функционирования СОРМ подчеркивает то, что в 2016 г. судами общей юрисдикции было выдано 893,1 тыс. разрешений на проведение оперативно-розыскных мероприятий (далее – ОРМ), ограничивающих конституционные права и свободы граждан, в том числе на прослушивание телефонных переговоров, снятие информации с технических каналов связи, контроль почтовых, телеграфных и иных сообщений [7]. Также необходимо отметить, что по состоянию на 20 ноября 2017 г. в реестре лицензий в области связи, ведущемся Роскомнадзором, содержатся данные о 35 044 лицензиях [8]. Такое большое количество лицензиатов на оказание услуг связи, значительное количество ОРМ, связанных с получением информации, передаваемой посредством сетей электросвязи, предполагает детальное регламентирование взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими ОРД.

В соответствии с правилами взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими ОРД, органы федеральной службы безопасности осуществляют взаимодействие с

операторами связи при проведении в рамках ОРД ОРМ, связанных с использованием технических средств, в том числе в интересах других уполномоченных органов. Информационные системы, содержащие базы данных, а также технические средства подключаются оператором связи к пункту управления органа федеральной службы безопасности через точки подключения. Точки подключения в субъекте Российской Федерации определяются органом федеральной службы безопасности [9, 10].

Изложенная формулировка означает, что «другие уполномоченные органы», в том числе ОВД, при осуществлении ОРД используют точки подключения, предоставленные федеральной службой безопасности. Алгоритм взаимодействия федеральной службы безопасности с другими уполномоченными органами не предложен. На практике вопросы определения точек подключения для нужд других уполномоченных подразделений решаются, как правило, отдельными соглашениями с федеральной службой безопасности на уровне субъектов Российской Федерации по усмотрению руководителей уполномоченных подразделений. Такой правовой пробел во взаимодействии между уполномоченными государственными органами, осуществляющими ОРД, и операторами связи приводит к тому, что вопрос оперативного доступа к информации, имеющей ключевое значение для раскрытия десятков тысяч преступлений, совершенных с использованием ИКТ, выносится в плоскость дополнительных соглашений между федеральной службой безопасности и другими уполномоченными органами. При этом никак не регламентированы порядок и сроки заключения таких соглашений, не установлен порядок контроля и надзора за их исполнением.

Полагаем, что данная ситуация может служить почвой для нарушения прав и свобод как граждан, в отношении которых проводятся ОРМ, ограничивающие конституционные права и свободы, так и граждан, пострадавших от преступлений, совершенных с использованием ИКТ.

Решение данной проблемы представляется во внесении изменений в Правила в части установления порядка и сроков заключения соглашений между уполномоченными подразделениями федеральной службы безопасности и уполномоченными государственными органами, осуществляющими ОРД на региональном уровне. В этой связи предлагаем п. 13 Правил дополнить словами: «Орган федеральной службы безопасности по письменному запросу руководителя органа, осуществляющего в соответствии с Федеральным законом “Об ОРД” оперативно-разыскную деятельность, в течение 3 месяцев с момента получения запроса предоставляет органу, осуществляющему ОРД, точку подключения с учетом оперативно-технических возможностей данного органа».

Полагаем, что такая мера позволит повысить эффективность противодействия преступлениям в сфере ИКТ, обеспечить защиту законных прав и интересов граждан.

Список использованной литературы

1. Сороколетов П.В. Мир на пороге четвертой информационной революции. URL: http://dissers.ru/books/2/755-1.php (дата обращения 30.11.2017).

2. Грибунов О.П. Технико-криминалистическое обеспечение раскрытия и расследования преступлений: отдельные аспекты современного состояния // Криминалистические чтения на Байкале–2015: материалы междунар. науч.-прак. конф. / ФГБОУВО "Российский государственный университет правосудия" Восточно-Сибирский филиал. Иркутск, 2015. С. 150–154.

2. Состояние преступности в России за январь-сентябрь 2017 г. Отчет ФКУ «Главный информационно-аналитический центр» МВД Российской Федерации. URL: https://mvd.ru/?utm_medium=source&utm_source=rnews/sb_1709.pdf (дата обращения 25.11.2017).

3. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон РФ от 06 июля 2016 г. № 374-ФЗ // Рос. газ. 2016. 11 июля.

4. О внесении изменений в Уголовный кодекс Российской Федерации и уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон РФ от 06 июля 2016 г. № 375-ФЗ // Там же. 2016. 11 июля.

5. Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть I: Общие требования: приказ Мин-ва информ. технологий и связи РФ от 16 янв. 2008 г. № 6 // Гарант.

6. Сводные статистические сведения о деятельности федеральных судов общей юрисдикции и мировых судей за 2016 год: судебный департамент при Верховном суде Рос. Федерации. // URL: http://www.cdep.ru/index.php?id=79&item=3832 (дата обращения 25.11.2017).

7. Реестр лицензий в области связи: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://rkn.gov.ru/communication/register/license/ (дата обращения 30.11.2017).

8. Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность: постановление Правительства Российской Федерации от 27 авг. 2005 г. № 538 // Гарант.

9. Об информации, информационных технологиях и о защите информации: федер. закон РФ от 27 июля 2006 г. № 149-ФЗ // Рос. газ. 2006. 29 июля.