УДК 343.985

Д. Л. Харевич,
кандидат юридических наук, доцент,
доцент кафедры оперативно-розыскной
деятельности факультета милиции
УО «Академия Министерства
внутренних дел Республики Беларусь»

О ПЕРСПЕКТИВАХ СОВЕРШЕНСТВОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ, НАПРАВЛЕННОЙ НА БОРЬБУ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ В СЕТИ ИНТЕРНЕТ

В настоящее время наблюдаются качественные изменения в способах совершения преступлений террористического и экстремистского характера, характеризуемые все более частым использованием возможностей сети Интернет и созданных на ее базе сетей более высокого уровня, хранением информации и следов преступлений на различных средствах компьютерной техники (СКТ), в том числе смартфонах, планшетах и др. Органы, осуществляющие оперативно-розыскную деятельность (ОРД), постоянно адаптируют используемый ими тактический инструментарий с целью более эффективного противодействия такой преступности. Однако к настоящему времени процесс адаптации существующих оперативно-розыскных мероприятий (ОРМ) к новым потребностям противодействия высокотехнологичной преступности во многом исчерпал свои возможности. Необходимо качественное обогащение тактического потенциала ОРД новыми ОРМ, построенными с учетом вышеуказанных современных особенностей ведения преступной деятельности.

Анализ существующих высокотехнологичных способов совершения преступлений экстремистского и террористического характера показывает, что при использовании преступниками определенных приемов уклонения от привлечения к уголовной ответственности традиционные способы выявления и раскрытия таких преступлений оказываются малоэффективными в связи с невозможностью

установления личности преступника. К указанным приемам относятся: использование теневого сегмента сети Интернет; применение средств анонимизации интернет-пользователей, криптостойких программных продуктов, виртуальных телефонных номеров; привлечение к совершению преступлений посредников, не осведомленных о факте своей причастности к совершению преступлений и поддерживающих контакты с организатором лишь по переписке; использование криптовалют, эмиссия которых не контролируется государственными органами.

В ряде случаев следы преступления в виде компьютерных файлов зафиксировать и изъять для целей правоохранительной деятельности с использованием существующих средств затруднительно или крайне сложно. Часто это связано с использованием алгоритмов стойкого шифрования данных, реализованных во многих программных продуктах. Оно может применяться как при хранении данных, так и их передаче. В первом случае изъятие носителя, данные на котором сохранены указанным способом, или доступ к удаленному ресурсу, на котором осуществляется хранение таких данных, чаще всего не позволяет ознакомиться с ними без пароля для дешифрования. Характеризуя использование шифрования при передаче данных, отметим, что интернет-пользователями часто используются сервисы по шифрованной передаче сообщений, удаляемых автоматически после прочтения. Многие мессенджеры (например, *Telegram*) имеют режимы настройки, исключающие использование серверов для централизованного хранения пересылаемых сообщений, последние хранятся в шифрованном виде лишь на устройствах отправителя и получателя. Это исключает возможность изъятия указанных сообщений по запросу правоохранительного органа через компанию, осуществляющую администрирование соответствующего ресурса. Восстановить содержание таких зашифрованных сообщений на устройствах отправителя и получателя при соблюдении ими стандартных мер безопасности чаще всего также не представляется возможным. Доступ к данным, сохраненным на внешних серверах или хранящимся в зашифрованном виде, возможен лишь при знании паролей или кодов доступа, получить которые традиционными способами не всегда возможно.

Предусмотренные в настоящее время Законом «Об оперативно-розыскной деятельности» ОРМ не позволяют эффективно преодолевать перечисленные способы уклонения от привлечения к уголовной

ответственности и сокрытия следов, в связи с чем представляется актуальной необходимость приведения тактических возможностей ОРД в соответствие с уровнем ведения преступной деятельности. Решением вышеуказанных проблем во многих случаях может являться проведение негласных ОРМ, связанных с удаленным контролем передаваемых сообщений или иной хранимой локально информации непосредственно на том устройстве, в котором они созданы (хранятся) в период времени, пока они не будут зашифрованы или стерты.

Во многих странах данная проблема решается путем расширения перечня ОРМ или прав правоохранительных органов использовать специализированное программное обеспечение для решения указанной задачи. Так, Федеральным законом России от 6 июля 2016 г. № 374-ФЗ «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» нормативно определено новое ОРМ «получение компьютерной информации». В ФРГ законом «О повышении эффективности и практикоориентированности осуществления уголовного судопроизводства» от 17 августа 2017 г. перечень негласных следственных действий дополнен онлайновым обыском (*Online Durchsuchung*), предусматривающим возможность негласного проникновения в персональный компьютер и подобные ему устройства затрагиваемого лица с целью ознакомления с содержанием находящихся на нем файлов, а также предусмотрена возможность осуществления контроля телекоммуникаций путем такого проникновения [1]. Данная мера в целях борьбы с терроризмом впервые была законодательно урегулирована в ФРГ в 2008 году, но на практике использовалась с 2005 года [2, с. 127]. Предложение о дополнении УПК аналогичным по названию мероприятием со сходным содержанием рассматривается законодательным органом Швейцарии [3]. С 2007 года в Австрии ведется дискуссия о возможности внесения в законодательство нового мероприятия под названием онлайновый розыск (*Online Fahndung*), предусматривающего негласную установку правоохранительными органами программного обеспечения на компьютерные системы с целью контроля сообщений, передаваемых с их помощью [4]. Согласно французскому закону «О направлениях и совершенствовании внутренней безопасности» от 08.02.2011 г. правоохранительные органы получили право проведения негласных мероприятий с

использованием специализированного программного обеспечения. По состоянию на 2009 год МВД Великобритании на основании законов «О неправомерном использовании компьютера» (*Computer Misuse Act*) и «О регулировании следственных действий» (*Regulation of Investigatory Powers Act*) проводило удаленные обыски (*Remote Searches*) и планировало внедрить их проведение в масштабах ЕС [5].

Под онлайновым обыском в ст. 100b УПК ФРГ понимается осуществляемое с использованием технических средств без ведома затрагиваемого лица проникновение в используемую им информационно-техническую систему и сбор в ней данных [1]. Исследователи указывают на удаленный способ проводимого при этом обследования [2, с. 124–125]. В определении, приводимом в швейцарском законопроекте, подчеркивается, что проникновение осуществляется с целью внедрения в обследуемую систему одной или нескольких компьютерных программ, позволяющих осуществить перехват и считывание данных в нешифрованном виде [3, с. 42]. На использование шифрования как основания, дающего возможность применять рассматриваемое негласное действие, обращается внимание в австрийском законопроекте [4, с. 2].

В связи с вышеизложенным представляется необходимым нормативно регламентировать право органов, осуществляющих ОРД, разрабатывать и использовать программное обеспечение, предназначенное для удаленного негласного сбора информации на СКТ. С соблюдением гарантий охраны конституционных прав граждан требуется также предусмотреть в нормативных правовых актах возможность проведения ОРМ, позволяющих осуществлять вышеуказанным способом получение: 1) компьютерной информации, хранящейся в виде документов, файлов и т. д. в памяти СКТ, на подключенных к нему съемных носителях и удаленных ресурсах; 2) технической и служебной информации, циркулирующей между целевым СКТ и сетью передачи данных (IP и MAC адреса, характеристики передаваемых сетевых пакетов, аппаратного и программного обеспечения СКТ); 3) перехват информации, передаваемой через СКТ в ходе переговоров с использованием интернет-телефонии или при передаче сообщений; 4) фиксацию акустической и видеоинформации в жилище путем удаленной активации микрофонов и видеокамер, находящихся на СКТ лица, представляющего оперативный интерес.

Список цитированных источников

1. Zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens : Gesetz, 17 Aug. 2017, № 3202 // Bundesgesetzblatt, Teil I [Elektronisches Ressource]. 2017. № 58. Aufrufsmodus: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_ BGBl&start=//*[@attr_id=%27bgbl117s3202.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s3202.pdf%27%5D__1506068549994. Aufrufsdatum: 22.09.2017.

2. Харевич Д. Л. Негласное расследование в Германии [Электронный ресурс] : монография / Д. Л. Харевич // М-во внутр. дел Респ. Беларусь, Акад. МВД. Минск : Акад. МВД, 2010. 287 с. Режим доступа: https://elibrary.ru/item.asp?id= 29395139. Дата доступа: 22.09.2017.

3. Erläuternder Bericht zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) : Vernehmlassungsvorlage des Bundesrates [Elektronisches Ressource]. Aufrufsmodus: https://www.admin.ch/ch/d/gg/ pc/documents/1719/Bericht.pdf. Aufrufsdatum 22.09.2017.

4. Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden : Entwurf, № 192/ME [Elektronisches Ressource]. Aufrufsmodus: https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/fname_521691.pdf. Aufrufsdatum 22.09.2017.

5. Gardham, D. Government plans to extend powers to spy on personal computers / D. Gardham // The Telegraf [Electronic resource]. 2009. 4 Jan. Access mode: http://www.telegraph.co.uk/news/uknews/law-and-order/4109031/Government-plans-to-extend-powers-to-spy-on-personal-computers.html. Access date: 22.09.2017.