УДК 343.985

Д.Л. Харевич

ЮРИДИЧЕСКОЕ СОДЕРЖАНИЕ УДАЛЕННОГО ОСМОТРА КОМПЬЮТЕРНЫХ СИСТЕМ ИЛИ СЕТЕЙ

В настоящее время наблюдаются качественные изменения в преступности, характеризуемые все более частым использованием возможностей сетей передачи данных (Интернет и др.), высокотехнологичных средств и орудий совершения преступлений (средств компьютерной техники (СКТ) и др.) [1]. Законодателем осуществляется адаптация правовой регламентации тактических возможностей органов, осуществляющих оперативно-розыскную деятельность, с целью эффективного противодействия такой преступности. Например, ряд мер был предусмотрен в новой редакции Закона Республики Беларусь «Об оперативно-розыскной деятельности» (далее – Закон об ОРД).

Вместе с тем принятие вышеуказанных изменений лишь частично решило имеющиеся проблемы противодействия преступлениям, совершаемым с использованием сети Интернет, что часто обусловлено использованием преступниками алгоритмов стойкого шифрования дан-

ных. Изучение зарубежного опыта показывает, что решением вышеуказанных проблем во многих случаях может являться проведение негласных мероприятий, связанных с удаленным контролем того устройства, в котором создана или хранится представляющая оперативный интерес информация, в период времени, пока она не будет зашифрована или стерта. В последние годы соответствующие меры были предусмотрены в законодательстве Великобритании, России, Франции, ФРГ и предложены для рассмотрения в качестве законопроектов в Австрии, Швейцарии [2; 3, с. 127].

Обзор определений таких негласных мероприятий в зарубежном законодательстве позволяет выделить их следующие характерные черты:

негласный характер проведения, обусловленный необходимостью преодоления мер противодействия раскрытию (расследованию) преступления, состоящих в применении криптостойкого шифрования или приемов анонимизации пользователя;

способ осуществления – удаленное проникновение и осмотр (копирование), при которых инициатор не находится в месте расположения обследуемого СКТ;

средства получения информации – специальные программы, разработанные и используемые инициатором проведения мероприятия;

информация, представляющая оперативный интерес, – файлы или данные, хранящиеся на обследуемом СКТ, подключенных к нему носителях информации или удаленных ресурсах, к которым имеется доступ с указанного СКТ.

Какова же юридическая сущность действий, производимых при проведении вышеназванных высокотехнологичных мероприятий (действий)? Как видно из вышеприведенного перечня характерных признаков, совокупность производимых действий образует тактический комплекс, имеющий определенное сходство с такими предусмотренными в Законе об ОРД оперативно-розыскными мероприятиями, как «контроль в сетях электросвязи», «оперативный осмотр», «сбор образцов». С ОРМ «контроль в сетях электросвязи» их объединяет направленность на получение хранящихся в цифровом виде данных, которые могут передаваться или передаются с использованием сетей передачи данных и иных сетей электросвязи; с ОРМ «оперативный осмотр» – содержание производимых действий, по аналогии с осмотром состоящих в обследовании и последующем изъятии объектов, представляющих оперативный интерес; последняя из названных операций указывает на сходство с ОРМ «сбор образцов».

Обратимся к различиям между указанными мероприятиями. Отметим, что в ходе обсуждения данной проблематики многие исследователи

высказывали точку зрения о том, что исследуемые высокотехнологичные мероприятия (действия) являются разновидностью ОРМ «контроль в сетях электросвязи». При доказывании тождественности указанных высокотехнологичных мероприятий (действий) и контроля в сетях электросвязи делалась ссылка на то, что в ходе таких мероприятий получение информации осуществляется с использованием сетей электросвязи и в отношении информации, хранящейся в таких сетях (ч. 1 ст. 31 Закона об ОРД). Однако если следовать этому аргументу, то к ОРМ «контроль в сетях электросвязи» следует также отнести разновидности оперативного опроса с использованием указанных сетей, а также слухового контроля, при которых информация передается по указанным сетям (в обоих случаях общим является как способ передачи информации, так и ее характер), что однозначно не соответствует подходу, отраженному в действующем оперативно-розыскном законодательстве (ч. 2 ст. 21 и ч. 2 ст. 30 Закона об ОРД). Полагаем, что причисление исследуемых высокотехнологичных мероприятий (действий) к контролю в сетях электросвязи будет идти вразрез тенденции к дифференциации отдельных понятий и институтов оперативно-розыскного права, ставшей лейтмотивом при разработке нового оперативно-розыскного законодательства Беларуси.

Как следует из определения ОРМ «контроль в сетях электросвязи», приведенного в ч. 1 ст. 31 Закона об ОРД, оно осуществляется в связи с передачей данных и сообщений по сетям электросвязи или ее хранением в инфраструктуре указанных сетей. Согласно ст. 1 Закона Республики Беларусь «Об электросвязи» к указанным данным и сообщениям относятся телефонные вызовы, телеграфные сообщения, служебные и информационные сообщения, сетевые пакеты сетей передачи данных. И хотя этот перечень является открытым, исходя из логики отнесения к нему отдельных элементов, можно утверждать, что хранящиеся на компьютере файлы не могут быть причислены к данным и сообщениям. Безусловно, многие из таких файлов могут предназначаться для последующей передачи по сетям электросвязи, однако подобный подход делает неправомерным сбор других данных (файлов и т. д.), не имеющих отношения или какой-либо взаимосвязи с сетью электросвязи или созданных на компьютере, не имеющем подключения к сети электросвязи. Например, если сеанс доступа к услугам электросвязи не осуществляется либо информация хранится локально на СКТ, не передается по сетям электросвязи и не предназначается для такой передачи, то обосновать возможность получения указанной информации путем проведения ОРМ «контроль в сетях электросвязи» проблематично.

Рассматривая особенности исследуемых высокотехнологичных мероприятий (действий), следует подчеркнуть, что существующие спосо-

бы проведения ОРМ «контроль в сетях электросвязи» не подразумевают установление контроля над самим СКТ, которым пользуется лицо, представляющее оперативный интерес; осуществляется лишь перехват информации, находящейся в сети операторов электросвязи в то время, когда она передается через указанные сети или хранится в них (например, ч. 4 ст. 31 Закона об ОРД). Установление непосредственного контроля над СКТ правоохранительным органом зарубежного государства, в законодательстве которого регламентирована возможность проведения исследуемых высокотехнологичных мероприятий (действий), значительно расширяет тактические возможности при их осуществлении данным зарубежным правоохранительным органом в сравнении с предусмотренными ОРМ «контроль в сетях электросвязи», поскольку позволяет такому правоохранительному органу проводить удаленное обследование аппаратной и программной конфигурации целевого СКТ и подключенных к нему устройств, перехват паролей шифрования и т. д. [3, с. 130–135]. Таким образом, определенная часть производимых действий связана с проведением обследования СКТ, что сложно рассматривать как составную часть ОРМ «контроль в сетях электросвязи».

Точку зрения о различии между данными мероприятиями разделяют и немецкие правоведы, обоснованно разделившие в собственном законодательстве аналоги данных ОРМ, допускающих использование программных продуктов для получения информации в интересах негласного расследования, на два самостоятельных действия: контроль телекоммуникации (в форме «онлайнового наблюдения», Online-Überwachung) и онлайновый обыск (Online-Durchsuchung) [4, s. 827].

В теории ОРД имеются теоретические основания для разграничения ОРМ «контроль в сетях электросвязи» от исследуемых высокотехнологичных мероприятий (действий). Нетрудно заметить, что в оперативно-розыскном законодательстве Республики Беларусь одним из оснований деления ОРМ на виды выступает такой признак, как метод познания окружающей действительности, лежащий в основе соответствующего ОРМ. Если в основе ОРМ «контроль в сетях электросвязи» лежит метод, содержание познавательных действий которого составляет негласное восприятие, слежение, контроль за представляющими оперативный интерес лицами, их поведением, а также объектами и обстановкой на них [5, с. 37; 6, с. 24], то содержание познавательных операций, имеющих место при проведении второго из сравниваемых тактических комплексов, в большей степени отражает обследование материальных объектов с целью отыскания и фиксации следов преступной деятельности [6, с. 32]. Следует отметить, что в ранних трудах исследователей теории ОРД (Д.В. Гребельский, А.Ф. Возный, В.Г. Самойлов) приведенные познавательные действия рас-

сматривались как единое целое, однако в последующем А.Е. Чечетиным обоснована точка зрения относительно их самостоятельности. Аргументами в пользу этого являлись различия в целях (установление происходящих событий, изучение поведения лиц в первом случае; поиск и фиксация следов преступной деятельности во втором); пассивный познавательный характер, подразумевающий отсутствие непосредственного контакта с наблюдаемым объектом в первом случае в противовес активному, инициативному характеру действий во втором; более широкий пространственный охват в первом случае и ограниченная локализация поиска во втором [4, с. 38]. С учетом приведенных рассуждений представляется, что отделение ОРМ «контроль в сетях электросвязи» от исследуемых высокотехнологичных мероприятий (действий) имеет под собой не только логическое, правовое, но и научное обоснование.

Указанные доводы позволяют сделать вывод о некоторой степени родства познавательных методов, лежащих в основе как изучаемых высокотехнологичных мероприятий (действий), так и оперативного осмотра. Вместе с тем следует отметить и очевидные различия: удаленный характер обследования в первом случае и непосредственный – во втором. Согласно ст. 26 Закона об ОРД оперативный осмотр может осуществляться в отношении ограниченного перечня объектов (жилища и иного законного владения гражданина, помещений, зданий, сооружений, транспортных средств, иных объектов и территории организации, участка местности), к которым при ограничительном толковании не относятся ресурсы сети Интернет, память СКТ или машинные носители компьютерной информации. Осмотр указанных ресурсов, памяти и носителей допускается лишь в случае, если они расположены в перечисленных осматриваемых объектах, например, СКТ находится в помещении, которое подвергается осмотру. Однако при проведении удаленного обследования данное условие не выполняется, поэтому ОРМ «оперативный осмотр» в отношении удаленных СКТ и сетевого ресурса проводиться не может.

Разграничение между ОРМ «сбор образцов» и рассматриваемыми высокотехнологичными мероприятиями (действиями) можно провести по признаку того, в какой степени инициатор ОРМ обладает информацией о местонахождении объектов, представляющих для него оперативный интерес. Нельзя произвести сбор образцов, если неизвестно их местонахождение. В этой связи в оперативно-розыскной практике сбору образцов предшествует проведение ОРМ «оперативный осмотр», направленное на решение названной задачи. Аналогичный подход использован в уголовном процессе и криминалистике для отграничения обыска от выемки. Таким образом, действия, составляющие ОРМ «сбор образцов», можно представить как содержание последующего этапа проведения изучаемых

высокотехнологичных мероприятий (действий). Заметим, что аналогичный подход отражен законодателем в формулировке ч. 2 ст. 26 Закона об ОРД, допускающей копирование и изъятие предметов и документов в ходе оперативного осмотра.

При проведении ОРМ «оперативный осмотр» и «сбор образцов» Закон об ОРД допускает копирование и изъятие программных продуктов, выступающих в качестве разновидности «предметов и документов». Следует отметить, что под программным продуктом понимается набор машинных программ, процедур и связанных с ним документации и данных. Могут ли все данные, хранящиеся на СКТ, рассматриваться в качестве разновидности программного продукта? Полагаем, что положительный ответ на данный вопрос поставит знак равенства между средством обработки данных, в качестве которого выступают программные продукты, и результатом этой деятельности. Законодатель также разделяет данные понятия, используя в формулировке ст. 351 УК Республики Беларусь словосочетание «компьютерная информация или программа»; аналогичный подход отмечается в ст. 354 УК Республики Беларусь. Данные, хранящиеся на СКТ, подключенных к нему носителях и удаленных ресурсах в общем случае не входят в содержание понятия «программный продукт» и выступают самостоятельными объектами, частично охватываемыми понятием «компьютерная информация». В связи с этим можно сделать заключение о том, что существующие нормы Закона об ОРД не предусматривают проведение ОРМ «оперативный осмотр» и «сбор образцов» в отношении компьютерной информации как самостоятельного предмета.

Проведенное рассмотрение позволяет сделать обоснованный вывод о том, что в настоящее время в законодательстве отсутствуют нормы, явно регламентирующие проведение вышеназванных высокотехнологичных мероприятий (действий). В этой связи наиболее последовательным решением задачи приведения тактических возможностей органов, осуществляющих ОРД, в соответствие с потребностями в эффективном раскрытии преступлений, совершаемых в сети Интернет, является дополнение оперативно-розыскного законодательства новым ОРМ, охватывающим описанные выше тактические приемы.

Это позволит решить такие потенциальные проблемы ведения ОРД в сети Интернет, выявленные в ходе интервьюирования практических сотрудников, как признание действий оперативных сотрудников незаконными и невозможность использования собранных таким образом материалов ОРД в уголовном процессе.

Выскажем ряд соображений относительно его наименования. С учетом проведенного выше рассмотрения относительно содержания и ха-

рактера познавательного процесса при проведении исследуемых высокотехнологичных мероприятий (действий) полагаем, что термин «осмотр» наиболее точно отражает суть производимых действий. В этой связи для обозначения нового ОРМ предлагаем использовать название «удаленный осмотр компьютерных систем или сетей» (сокращенно «удаленный осмотр»). Очевидно, что с учетом специфики рассматриваемого ОРМ практический смысл имеет лишь негласная форма его проведения.

По аналогии с ОРМ «оперативный осмотр», определение которого приведено в ч. 1 ст. 26 Закона об ОРД, соответствующее понятие можно определить как «негласное обследование компьютерной системы или сети и сбор хранящихся в них данных, при которых исполнитель не находится в месте расположения указанных системы или сети, проводимые с использованием специализированного программного обеспечения в целях получения сведений, необходимых для выполнения задач оперативно-розыскной деятельности».

Таким образом, повышение эффективности решения задач ОРД в противодействии преступлениям, совершаемым с использованием СКТ, современных средств телекоммуникации и компьютерных сетей, возможно путем дополнения перечня ОРМ, предусмотренных Законом об ОРД, новым мероприятием «удаленный осмотр компьютерных систем или сетей» («удаленный осмотр»). Содержание данного мероприятия можно определить как «негласное обследование компьютерной системы или сети и сбор хранящихся в них данных, при которых исполнитель не находится в месте расположения указанной системы или сети, проводимые с использованием специализированного программного обеспечения в целях получения сведений, необходимых для выполнения задач ОРД».

1. Харевич Д.Л. О перспективах совершенствования правового обеспечения борьбы со сбытом наркотиков в сети Интернет // Теоретические и прикладные вопросы борьбы с преступлениями, совершаемыми с использованием информационных технологий : сб. материалов Междунар. заоч. науч.-практ. конф., Могилев, 30 нояб. 2017 г. / Могилев. ин-т М-ва внутр. дел Респ. Беларусь ; редкол.: Ю.А. Матвейчев (отв. ред.) [и др.]. Могилев, 2017.

2. Харевич Д.Л. О перспективах совершенствования правового регулирования оперативно-розыскной деятельности, направленной на борьбу с терроризмом и экстремизмом в сети Интернет // Проблемы обеспечения национальной и региональной безопасности: правовые и информационные аспекты : материалы Междунар. науч.-практ. конф., Минск, 2 нояб. 2017 г. : в 2 т. / Ин-т нац. безопасности Респ. Беларусь ; редкол.: А.Л. Лычагин (гл. ред.) [и др.]. Минск, 2018. Т. 2.

3. Харевич Д.Л. Негласное расследование в Германии [Электронный ресурс] / М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». Минск, 2010. URL: https://elibrary.ru/item.asp?id=29395139 (дата обращения: 22.09.2017).

4. Fox D. Realisierung, Grenzen und Risiken der „Online-Durchsuchung“ // Datenschutz und Datensicherheit. 2007. № 11.

5. Чечетин А.Е. Актуальные проблемы теории оперативно-розыскных мероприятий. М., 2006.

6. Басецкий И.И., Гайдельцов В.С. Терминологический словарь к Закону Республики Беларусь «Об оперативно-розыскной деятельности». Минск, 2009.