УДК 343.98.068
DOI: 10.17277/voprosy.2015.02.pp.096-100

СНЯТИЕ ИНФОРМАЦИИ С ТЕХНИЧЕСКИХ КАНАЛОВ СВЯЗИ: УСЛОВИЯ ГАРАНТИРОВАНИЯ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА

А. И. Анапольская, В. Н. Влазнев

Тамбовский филиал ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», г. Тамбов

Рецензент канд. юрид. наук, профессор В. В. Назаров

Ключевые слова: компьютерная информация; оперативно-розыскное мероприятие; права и свободы человека и гражданина; снятие информации с каналов связи; электронная почта.

Аннотация: Исследованы сущность и содержание понятия снятия информации с технических каналов связи. Определены основания для проведения данного оперативно-розыскного мероприятия и связанные с такой деятельностью проблемные вопросы соблюдения прав и свобод человека и гражданина.

Прогресс в области электроники способствовал массовой компьютеризации практически всех сфер жизни, в том числе и тех, которые связаны с общением граждан. В частности, деловая и личная переписка все чаще осуществляется с использованием услуг электронной почты (e-mail – *англ.* electron mail). Сообщения, отправляемые по электронной почте, доходят до адресата в считанные секунды, даже если он находится на другом конце планеты.

В последние годы, помимо правомерного использования, электронная почта все чаще становится средством реализации преступных намерений: координации преступной деятельности, мошенничества, шантажа, угроз, рассылки вредоносных программ и т.д. Своевременное и надлежащим образом организованное выявление данных сведений имеет существенное значение для предупреждения, раскрытия и расследования преступлений.

Анапольская Алина Игоревна – кандидат юридических наук, доцент кафедры «Публичное право», e-mail: alinaanapolskya@mail.ru; Влазнев Владимир Николаевич – кандидат юридических наук, доцент кафедры «Публичное право», Тамбовский филиал ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», г. Тамбов.

Достижению указанной цели во многом способствует проведение такого оперативно-розыскного мероприятия, как снятие информации с технических каналов связи.

В криминалистической литературе тактические особенности проведения снятия информации с каналов связи так или иначе рассматривались в работах Б. В. Андреева, Р. С. Белкина, В. П. Бахина, В. Б. Вехова, Ю. В. Гаврилина, В. А. Губанова, В. В. Кириченко, Е. Ф. Коноваловой, В. К. Лисиченко, М. В. Салтевского и других ученых. Однако тактика проведения снятия информации с каналов связи остается еще недостаточно разработанной и требует учета определенных особенностей, характеризующих порядок его организации и проведения, а также условий гарантирования прав и свобод человека.

Согласно ст. 23 Конституции РФ, каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [1]. В федеральном законе «Об оперативно-розыскной деятельности» в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств, среди прочих оперативно-розыскных мероприятий, предусмотрена норма, которая предоставляет оперативным подразделениям государственных органов возможность вмешиваться в сферу личного общения между людьми путем снятия информации с технических каналов связи (к которым, среди прочего, следует отнести и Интернет) [2, ст. 6].

Ограничение этого права возможно только на основании решения суда, в котором должны быть четко определены организации, предоставляющие услуги доступа к информационным сетям, используемым лицом, в отношении которого осуществляется оперативно-розыскное мероприятие. Указанным организациям предлагается заблокировать доступ определенного субъекта к его электронному почтовому ящику и обеспечить хранение адресованной ему корреспонденции, сохраняя при этом режим конфиденциальности и целостности [3, с. 97]. При этом оперативно-розыскное мероприятие может быть нацелено лишь на получение информации, поступающей с определенных серверов или от определенного лица.

К проведению снятия информации с технических каналов связи следует привлекать специалиста высокого класса (поскольку некоторые программы могут быть настроены на самоуничтожение в случае несанкционированного доступа). Преодолеть действующую систему защиты самостоятельно оперативный работник, как правило, не в состоянии [4].

Для того чтобы установить, где и как искать корреспонденцию электронной почты необходимо осознавать принципы ее работы. Например, при передаче электронной почты через Интернет используется следующая цепочка: отправитель электронного письма; почтовый сервер-отправитель; сеть (Интернет); почтовый сервер получателя; получатель электронного письма.

Сообщения электронной почты формируются на экране монитора, сохраняясь при этом во временной (оперативной) памяти компьютера. Только после отправки сообщения с персонального компьютера на почтовый сервер организации или через модем к провайдеру, сообщение может

быть сохранено на определенном носителе в компьютере отправителя. Такое сохранение не является обязательным, например, оно отсутствует в режиме отправки письма через почтовый веб-сайт в Интернет или абонент может сразу же удалить письмо.

Именно поэтому, наиболее значимыми признаками снятия информации с технических каналов связи, передающих электронную почту, выступают:

– адрес в сети передачи данных с коммутацией пакетов, в том числе IP-адрес для сети Интернет в формате xxx.xxx.xxx.xxx (например, 010.011.012.130);

– адрес электронной почты в формате «имя почтового ящика@домен. домен верхнего уровня» (например, info@ssu.gov.ua);

– аппаратный адрес устройства, присоединенного к сетевой среде.

Отметим, что при проведении выемки электронной корреспонденции определенного лица или организации, осуществляемой у оператора связи, порядок действия меняется. В договорах о предоставлении услуг коммутируемого доступа к сети Интернет, как правило, есть пункт, согласно которому провайдер обязуется принимать общепринятые в Интернете технические и организационные меры для обеспечения конфиденциальности информации, получаемой или отправляемой абонентом. Указанный пункт договора поддерживается ст. 53 закона РФ «О связи», согласно которому сведения об абонентах и оказываемых им услугах связи являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством РФ. Такая информация, согласно ст. 64, может быть предоставлена операторами связи уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности РФ для выполнения возложенных на эти органы задач в случаях, установленных федеральными законами [5]. Таким образом, законом защищены не только сообщения (их содержание), которые передаются по техническим каналам связи, но и информация (сведения) о них.

Для осуществления указанных действий необходимо выяснить, услугами какого провайдера пользуется лицо, электронная корреспонденция которого подлежит изъятию и фиксации. Это можно сделать, определив номер провайдера, с которым связывается абонент. Однако для доступа к серверу провайдера абонент может использовать не только свое, но и чужое техническое средство.

Другим способом является направление запросов провайдерам, действующим в данной местности, в целях выяснения информации о наличии на их сервере электронного почтового ящика конкретного лица. Если таковой имеется, выясняются данные о прошлом общении в сети (время, размер сообщения, стороны и т.д.). Такая информация регистрируется в файлах протоколов работы аппаратуры, однако хранится довольно непродолжительное время. Законодательство РФ, позволяя сотрудникам оперативных подразделений осуществлять снятие информации с технических каналов связи, не определило в своих нормах порядок соотношения (идентификации) конечного оборудования с абонентом, ведь пользоваться таковым может не только сам фигурант, но и члены его семьи. Исходя

из этого, фактически проведение указанного оперативно-розыскного мероприятия соотносится не столько с абонентом, сколько с конечным оборудованием, отодвигая на второй план личность, в отношении которой оно проводится. В результате создается юридическая коллизия, обусловленная тем, что совершение действий, ограничивающих право на личную неприкосновенность, свидетельствует, с одной стороны, о неправомерном вмешательстве в частную жизнь лица, что фактически приводит к нивелированию конституционных принципов [6, с. 76]. С другой стороны, производство снятия информации с технических каналов связи при отсутствии идентификации абонента свидетельствует об отсутствии оснований полагать, что в его частную жизнь вмешивались представители правоохранительных органов.

Таким образом, деятельность следователя и сотрудника оперативного подразделения невозможно представить без систематического и планомерного получения информации об объектах уголовного преследования. Для этого могут применяться различные средства и методы, которые предусмотрены уголовным процессуальным законодательством. Важное место в системе принадлежит такому оперативно-розыскному мероприятию, как снятие информации с технических каналов связи. Однако в тактике проведения указанного действия существует много пробелов, устранение которых могло бы способствовать формированию действенных механизмов обеспечения прав и свобод человека и гражданина.

Список литературы

1. Конституция Российской Федерации с внесенными поправками от 21 июля 2014 г. // Собр. законодательства РФ. – 2014. – № 31. – Ст. 4398.

2. Об оперативно-розыскной деятельности [Электронный ресурс] : федер. закон от 12.08.1995 № 144-ФЗ (в ред. от 21.12.2013) // КонсультантПлюс : офиц. сайт. – Режим доступа : www.consultant.ru (дата обращения: 15.04.2015).

3. Анапольская, А. И. Использование оперативно-технических средств подразделениями уголовного розыска в процессе раскрытия хищений денежных средств в сфере электронных расчетов / А. И. Анапольская // Междунар. науч. ин-т «Educatio». – 2014. – № 5, ч. 1. – С. 96 – 100.

4. Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств : указ Президента РФ от 1 сент. 1995 г. № 891 // Собр. законодательства РФ. – 1999. – № 24. – Ст. 2954.

5. О связи [Электронный ресурс] : федер. закон от 7.07.2003 № 126-ФЗ (в ред. от 21.07.2014) // КонсультантПлюс : офиц. сайт. – Режим доступа : www.consultant.ru (дата обращения: 15.04.2015).

6. Краснослободцева, Н. К. Соотношение понятий «свобода» и «права» человека / Н. К. Краснослободцева // Ленингр. юрид. журн. – 2014 . – №4 (38). – С. 75 – 83.

References

1. *Sobranie zakonodatel'stva RF* (Corpus of Legislative Acts of the Russian Federation), 2014, no. 31, art. 4398.

2. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156039 (accessed 15 April 2015).

3. Anapol'skaya A.I. *International Scientific Institute "Educatio"*, 2014, no. 5, part. 1, pp. 96-100.
4. *Sobranie zakonodatel'stva RF* (Corpus of Legislative Acts of the Russian Federation), 1999., no. 24, art. 2954
5. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=168320 (accessed 15 April 2015).
6. Krasnoslobodtseva N.K. *Leningrad Law Journal*, 2014, no. 4 (38), pp. 75-83.

Information Retrieval from Technical Communication Channels: Conditions Safeguarding the Rights and Freedoms of Man and Citizen

A. I. Anapolskaya, V. N. Vlaznev

Tambov Branch of the Russian Presidential Academy of National Economy and Public Administration, Tambov

Keywords: computer information; e-mail; information retrieval from communication channels; operational search activities; rights and freedoms of man and citizen.

Abstract: The paper examines the nature and content of the concept of information retrieval from technical communication channels. The authors identified the reasons for carrying out this investigative activity and related activities, the issues of safeguarding the rights and freedoms of man and citizen.