ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПОНЯТИЕ, СОДЕРЖАНИЕ И ОСОБЕННОСТИ ПРОИЗВОДСТВА ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ

К.М. Гердт, Вит.В. Поляков
Алтайский государственный университет, г. Барнаул

Исчерпывающий перечень оперативно-розыскных мероприятий (ОРМ) определен в ст. 6 Федерального закона "Об оперативно-розыскной деятельности", Федеральный закон от 06.07.2016 № 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 дополнил этот перечень новым мероприятием, названным "получение компьютерной информации". Тактические особенности производства ОРМ "получение компьютерной информации" направлены на сбор уголовно-релевантной ориентирующей й информации в компьютерных средствах и системах. Однако на сегодняшний день научные разработки, позволяющие сформулировать конкретные практические рекомендации по проведению данного ОРМ, явно недостаточны. В связи с этим актуальной задачей является исследование содержания, вкладываемого Законодателем в ОРМ "получение компьютерной информации".

Прежде чем приступить к анализу самого ОРМ "получение компьютерной информации", нужно определить исходное понятие "компьютерная информация". Это понятие на уровне законодательства закреплено в гл. 28 УК РФ, где в примечании 1 к ст. 272 обозначено, что под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В редакции ст. 272 УК РФ законодатель дал определение компьютерной информации через форму ее представления, а не через перечисление средств ее хранения, обработки и передачи. Это позволяет выделить некоторые оперативно и криминалистически значимые особенности компьютерной информации, в частности, такие как:

- возможность преобразования информации из одной формы в другую и копирование на различные виды машинных носителей;
- возможность передачи по информационно-коммуникационным сетям связи;
- возможность доступа к ней различных лиц, причем одновременного и с разных устройств;
- возможности ее уничтожения.

Таким образом, под компьютерной информацией следует понимать не какой-то особый вид информации, а специфическую форму ее представления, приспособленную для обработки в компьютерных устройствах, передачи по каналам связи и хранения на специализированных носителях. Уточним, что правильнее здесь было бы говорить даже не об информации, а о данных, которые становятся информацией только при их осмыслении, помещении в определенный контекст [1].

Теперь отметим, что понятие "получение компьютерной информации" Законодателем не закреплено. В криминалистической литературе предлагаются множество вариантов его интерпретации. Так, Е.С. Дубоносов под получением компьютерной информации понимает оперативно-техническое мероприятие, направленное на сбор сведений, циркулирующих в компьютере или сети компьютеров, а также содержащихся на различных носителях машинной информации, и последующую их фиксацию (или без нее) для решения оперативно-розыскных задач [2]. В.Ф. Васюков полагает, что данное мероприятие проводится уполномоченным лицом, осуществляющим оперативно-розыскную деятельность, в

целях получения содержания текстовых сообщений пользователей услугами связи (сети Интернет) в виде голосовой информации, изображений, звуков, видео-, электронных сообщений, а также сведений о фактах их передачи, доставки и (или) обработки [3]. С.В. Баженов полагает, что рассматриваемое мероприятие заключается в получении информации, содержащейся на жестком диске компьютера или иных электронных носителях, связанных с компьютером каналом связи на основе технологии удаленного доступа по информационно-телекоммуникационным сетям, в том числе с применением заблаговременно внедренных закладных устройств и (или) программного обеспечения [4]. По мнению А.Ю. Шумилова, в рамках получения компьютерной информации подлежат контролю и фиксации характеристики магнитных полей, возникающих при обороте компьютерной информации в сети электрической связи (компьютерной сети) [5].

Наиболее удачным нам представляется определение сущности исследуемого понятия, предложенное Ю.В. Волгиным. Он определяет данное ОРМ как комплекс действий с использованием специально разработанных технических и программных средств, направленных на поиск и извлечение компьютерной информации, а также приведение ее к форме, позволяющей проанализировать и оценить ее содержание, проводимых оперативно-техническими подразделениями федеральной службы безопасности и органов внутренних дел [6].

Анализ приведенных точек зрения позволяет сделать вывод о том, что под получением компьютерной информации следует понимать оперативно-розыскное мероприятие, проводимое уполномоченным лицом, осуществляющим оперативно-розыскную деятельность, с использованием специальных технических и программных средств, направленное на поиск, извлечение и сбор данных текстовых сообщений, голосовой информации, изображений, звуков, видео и иных электронных сообщений пользователей связи и сети Интернет, а так же данных, содержащихся на различных носителях машинной информации. Сущность данного мероприятия - это контроль и слежение за криминальной сферой путем производства аналитических и исследовательских действий с использованием специального программно-технического обеспечения. Его цель - копирование данных с компьютерных устройств всех типов, которыми пользуются юридические и физические лица, для последующих обработки и анализа.

Основу ОРМ составляют достаточно сложные в техническом плане и требующие специальной подготовки действия, направленные на добывание хранящейся в компьютерных системах или передаваемой по техническим каналам связи информации о лицах и событиях, которые вызывают оперативный интерес. В большинстве случаев их правильное осуществление невозможно без участия специалиста. Это закреплено в части 4 ст. 6 ФЗ "Об оперативно-розыскной деятельности". Именно, ОРМ, связанные с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов федеральной службы безопасности и органов внутренних дел.

Можно выделить четыре группы источников оперативно значимых компьютерных данных, причем для получения каждого из них присутствует своя специфика:

1. К техническим источникам такого рода могут быть отнесены:

а) сведения из средств вычислительной техники, включая средства сотовой связи и мобильные устройства, обеспечивающие доступ к сетевым ресурсам;

б) данные на носителях компьютерной информации;

в) устройства, фиксирующие компьютерные данные, поступающие от различных датчиков (радиочастотных идентификаторов, GPS-трекеров, нательных датчиков, передающих физиологические показатели и сведения о местоположении, и

т.п.), стационарных и мобильных измерительных устройств, систем геопозиционирования, видеонаблюдения и видеофиксации;

г) сетевое оборудование, через которое осуществляются коммуникационные акты разрабатываемых лиц. Сюда можно отнести данные с навигационных систем автотранспорта, системы "умного дома", бытовые приборы, информационные датчики в местах общественного пользования и т.п.

2. К информационным источникам сети Интернет можно отнести:

а) информационные ресурсы, содержащие сведения о совершении преступлений и лицах, их совершающих (сайты криминальных структур и т.п.);

б) места сетевого общения (закрытые сетевые форумы и чаты, сообщества криминальной направленности в социальных сетях и др.) криминально настроенных лиц и их персональные страницы в социальных сетях.

3. Как источник получения оперативно-значимой компьютерной информации могут быть выделены сетевые каналы коммуникации, задействованные преступниками для координации действий. К ним относится использованием электронной почты, средств обмена сообщениями, приложений VoIP (интернет-телефонии), мессенджеров (ICQ, Skype, WhatsApp, Viber, Telegram и др.), и т.п., причем многие из них предоставляют услуги шифрования передаваемых данных.

4. Источником оперативно значимой информации могут являться выборки, генерируемые по заданным условиям при анализе сведений из различных баз данных, формируемых в информационных системах государственных органов и коммерческих структур, в том числе банков и операторов связи.

Рассмотрим закрепленные законом условия проведения анализируемого ОРМ. Согласно части второй ст. 8 ФЗ "Об оперативно-розыскной деятельности" оно отнесено к числу ОРМ, ограничивающих конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища. Его проведение допускается на основании судебного решения и при наличии следующей информации:

1) о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно;

2) о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно;

3) о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

Той же статьей допускается возможность осуществлять получение компьютерной информации без судебного решения по основаниям, предусмотренным п. 5 части второй ст. 7 ФЗ "Об оперативно-розыскной деятельности" (связанным с необходимостью на длительной основе организовывать и проводить работу по обеспечению безопасности органов, осуществляющих оперативно-розыскную деятельность) при наличии согласия гражданина в письменной форме.

Содержание ОРМ «получение компьютерной информации» связано с применением определенных способов доступа к информационным источникам, содержащихся в компьютерных системах. К таким способам можно отнести следующие:

- Негласное применение специального программного обеспечения и оборудования для скрытного съема данных с компьютерных устройств, в том числе тайный дистанционный доступ к компьютерам, имеющим сетевое подключение.

- Оперативно-розыскной мониторинг представляющих оперативный интерес сетевых информационных ресурсов.
- Негласная установка в компьютерные устройства разрабатываемых лиц специального программного обеспечения, позволяющего фиксировать содержание осуществляемых с этих компьютеров сеансов связи.
- Применение аналитического программного обеспечения для выявления оперативно значимой информации в базах данных различного назначения.
- Негласный или гласный осмотр компьютеров, мобильных телефонов, планшетов и других устройств, хранение сопровождается копированием компьютерной информации.

Отдельно укажем на необходимость разграничения таких оперативно-розыскных мероприятий как "получение компьютерной информации" и "снятие информации с технических каналов связи". До появления анализируемого нами ОРМ второе мероприятие было основным, посредством его осуществлялось получение информации, хранящейся в сети Интернет. С помощью снятия информации с технических каналов связи осуществлялся контроль и фиксация сообщений пользователей интернета с использованием двух методов: пассивного контроля и активного перехвата [7]. Когда оперативно-розыскными органами осуществляется только отслеживание и копирование данных, которые хранятся в компьютерах пользователей серверов системных администраторов, без вмешательства в их поток, то в этом случае применяется метод пассивного контроля. Если же должностные лица органов, осуществляющих ОРД, в момент передачи информации, передаваемой пользователями сети Интернет, предпринимают действия по немедленному ее перехвату, а также осуществляют изменение содержания передаваемого сообщения либо его уничтожение, в результате чего оно не доходит до адресата, то такой метод является активным. С появлением специализированного ОРМ активный метод перехвата информации используется для снятия информации с технических каналов связи, а извлечение информации из компьютерных хранилищ, помещенной туда после ее передачи применяется для получения компьютерной информации.

Разграничение между данными ОРМ происходит по способу проведения. В рамках получения компьютерной информации, наряду с перехватом с помощью специальных технических средств информации, передаваемой по каналам технической связи (сеть Интернет, мессенджер "Whatsapp" и др.), производится осмотр различных компьютерных устройств, в том числе и мобильных, жестких дисков и иных устройств, предназначенных для хранения информации, на предмет наличия интересующей следствие информации, что не входит в снятия информации с технических каналов связи [8[. Результаты проведения ОРМ «получение компьютерной информации» фиксируются, помимо протокола проведения ОРМ, в изъятых документах, содержащих нужные сведения. Результаты проведения ОРМ «снятие информации с технических каналов связи» указываются в материалах, на которых зафиксирована перехваченная информация.

При получении компьютерной информации сотрудники оперативно-розыскных органов могут столкнуться с определенными трудностями, такими как:

- нехватка специалистов, которые профессионально владеют информационными технологиями;
- отсутствие системы специальной подготовки и повышения квалификации оперативных сотрудников по использованию информационных систем;
- сложности в систематизации компьютерной информации о лицах и криминальных проявлениях;

- недостаточная регламентация в действующем законодательстве и ведомственных подзаконных нормативных правовых актах процедуры изъятия компьютерной информации.

Выводы. Получение компьютерной информации является относительно новым видом оперативно-розыскных мероприятий, в связи с чем ему присущи проанализированные в настоящей работе недостатки в законодательном закреплении понятийного аппарата и в разработке методических рекомендаций по осуществлению ОРМ. Кроме того, получение компьютерной информации обладает рядом специфических особенностей, рассмотренные в настоящей работе, которые должны учитываться в практике правоохранительных органов.

Библиографический список

1. Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. - 2010. - № 2. - С. 206-209.
2. Дубоносов Е.С. Оперативно-розыскное мероприятие "получение компьютерной информации": содержание и проблемы проведения // Известия Тульского государственного университета. Экономические и юридические науки. - 2017. - № 2.2. - мерово. - 2017. - С. 121.
3. Васюков В.Ф. К вопросу о содержании нового термина "получение компьютерной информации" в теории оперативно-розыскной деятельности // Материалы международной научно-практической конференции "V Балтийский юридический форум "Закон и правопорядок в третьем тысячелетии". - 2017 - С.146-146.
4. Баженов С.В. Оперативно-розыскное мероприятие "получение компьютерной информации" // Научный вестник Омской академии МВД России. - 2017. - № 2. - С. 33.
5. Шумилов А.Ю. Получение компьютерной информации как новое оперативно-розыскное мероприятие: первые шаги научного познания // Оперативник (сыщик). - 2016. - № 4. - С. 35.
6. Волгин Ю.В. К вопросу о понятии "получения компьютерной информации" как вида оперативно-розыскных мероприятий // Защита субъективных прав и охраняемых законом интересов : сб. трудов II Междунар. науч.-практич. конф. (24 марта 2017 г.). - Кемерово, 2017. - С.24-30.
7. Нагорняк Р.В. Получение компьютерной информации: содержание и разграничение с другими оперативно-розыскными мероприятиями // Сборник материалов Всероссийской научно-практической конференции молодых учёных. Современность в творчестве начинающего исследователя. - Восточно-Сибирский институт МВД России. - 2017. - С.161-164.
8. Осипенко А.Л. Новое оперативно-розыскное мероприятие "Получение компьютерной информации": содержание и основы осуществления // Вестник Воронежского института МВД России. - 2016. - № 3. - С. 83-90.