Будкевич А. А.

К ВОПРОСУ О ДОСТУПЕ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Белорусский государственный университет,
пр. Независимости, 4, 220030 Минск, Беларусь, *lawcrim@bsu.by*

Постоянное обеспечение безопасности граждан и государства от преступных посягательств невозможно без систематического проведения оперативно-розыскных и иных мероприятий правоохранительными органами с целью добывания сведений, представляющих оперативный интерес.

В настоящее время значительные объемы информации сосредотачиваются в информационных ресурсах и разных технических устройствах в цифровой форме на различных электронных устройствах и системах. В связи с этим перед подразделениями, осуществляющими оперативно-розыскную деятельность (далее – ОРД), возникает задача осуществлять эффективный поиск, фиксацию и накопление компьютерной информации.

Компьютерная информация с технической точки зрения может быть получена:

– при копировании данных с внешних устройств хранения информации;

– дистанционно или непосредственно, получив доступ к устройствам памяти, установленным в компьютере через компьютерную сеть;

– через технические каналы связи и входящие в них промежуточные обслуживающие устройства.

Получаемая информация может быть в виде текстов, фотографий, схем, видеофильмов, документов и т. п. [1].

В различных структурах, представляющих интерес для правоохранительных органов, имеются компьютеры, не включенные в компьютерную сеть и не подключенные к каналам связи, где хранится так называемая с их точки зрения «конфиденциальная информация», доступ к которой имеет ограниченное число лиц и которая в значительной мере представляет оперативный интерес для правоохранительных органов.

Следует отметить, что в Законе Республики Беларусь от 15.07.2015 «Об оперативно-розыскной деятельности» (далее – Закон об ОРД) не совсем полно регламентирован доступ к компьютерным данным в целях сбора оперативно-значимой информации, проводимой подразделениями, осуществляющими ОРД. Следует отметить, в ст. 31 «Контроль в сетях электросвязи» Закона об ОРД дано исчерпывающее понятие указанного оперативно-розыскного мероприятия (далее – ОРМ) – получение, преобразование и фиксация с помощью технических средств данных и сообщений, принимаемых, передаваемых, обрабатываемых, хранящихся в сетях электросвязи. Как видно из приведенного содержания статьи, регламентации снятия информации, хранящейся в компьютерах, не подключенных к сетям электросвязи, не указано.

Как отмечал профессор А. Л. Осипенко [3], законодательно такой вариант закрепления соответствующих мер был предложен в модельном законе «Об оперативно-розыскной деятельности (новая редакция) (принят на XXVII пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (постановление от 16 ноября 2006 г. № 27-6), где указанное мероприятие было названо «мониторинг информационно-телекоммуникационных сетей и систем» и определено как получение сведений, необходимых для решения конкретных задач оперативно-розыскной деятельности, и их фиксация путем наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и ее передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам.

По мнению профессора А. Л. Осипенко, такое определение, излишне перегруженное техническими деталями, содержит технические неточности, не дает достаточно четкого представления о содержании предлагаемого мероприятия. Следует согласиться с мнением А. Л. Осипенко и в том плане, что термин «мониторинг» связывается со сбором, анализом и оценкой информации в определенной сфере, деятельностью по наблюдению за соответствующими явлениями, и его использование вряд ли можно признать удачным для обозначения всех тех действий, направленных на получение компьютерной информации [2].

Как общеизвестно, основной способ собирания оперативно-розыскной информации – это проведение ОРМ, перечень которых определен в ст. 18 Закона об ОРД. Казалось бы, что в указанном Законе отражен исчерпывающий перечень ОРМ, однако получение компьютерной информации в качестве самостоятельного ОРМ законодатель почему-то не определил, скорее всего, посчитав, что ОРМ – «Контроль в сетях электросвязи» – дает исчерпывающее понятие доступа к компьютерной информации в целях сбора оперативно-розыскной информации для борьбы с преступными проявлениями.

Следует отметить определение, приведенное в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступностью в сфере компьютерной информации, где компьютерная информация обозначена как «информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи».

Как следует из приведенного тезиса, законодатели Содружества Независимых Государств предвидели, что компьютерная информация, представляющая интерес, может находиться на компьютере, который не имеет доступа к внешним сетям электросвязи. На таких носителях зачастую содержится информация, позволяющая правоохранительным органам своевременно предотвращать и пресекать преступные проявления лиц,

представляющих опасность для общества и государства. Как показывает практика работы правоохранительных органов, преступники зачастую хранят представляющую оперативный интерес информацию на компьютерных устройствах, не подключенных к сетям электросвязи (речь идет о запрещенных террористических организациях, на компьютерах лидеров и членов которых сосредотачивалась информация о способах изготовления взрывчатых веществ, о тактике террористической деятельности и т. п.). Получить такую информацию без проведения ОРМ практически невозможно. Часто лица, вовлеченные в преступную деятельность, устанавливают на компьютеры, не подключенные к внешней среде, программы, которые предусматривают уничтожение содержимого информационных носителей при несанкционированном входе в базу данных компьютера, применяют различные программы, затрудняющие получение информации и т. п. Получить такую информацию на законных основаниях в рамках действующего законодательства – одна из первостепенных задач правоохранительных органов.

Необходимо отметить, что получение (снятие) информации, находящейся в памяти такого компьютера, проведением ОРМ – не регламентировано. На наш взгляд, следует снятие информации, находящейся в памяти компьютера, не имеющего доступ к каналам электросвязи, или получение информации, хранящейся в накопителях компьютера, не подключенного к сетям компьютерной связи, определить как самостоятельное ОРМ – «Получение компьютерной информации».

Следует отметить, что расширение практики осуществления рассматриваемого ОРМ потребует решения целого комплекса организационных и правовых проблем, совершенствования нормативной регламентации вопросов обеспечения прав граждан. В соответствующих нормативных правовых актах должны быть уточнены полномочия органов, осуществляющих ОРД.

На наш взгляд, новое ОРМ должно будет отнесено к мероприятиям, которые требуют санкционирования прокурором. Указанное ОРМ должно проводиться только в рамках обоснованно заведенного дела оперативного учета. Тактика проведения указанного ОРМ будет регламентирована ведомственными нормативными документами соответствующих министерств и ведомств, наделенных полномочиями осуществления ОРД.

В рамках тезисов рассматриваемой темы нельзя не затронуть вопрос о применении проверяемыми лицами так называемых мер по шифрованию информации, содержащейся в их компьютерах. Следует согласиться с профессором А. Л. Осипенко, что решение этой проблемы необходимо искать не столько в правовом поле, сколько в адекватном наращивании и технологическом совершенствовании арсенала специальных средств, применяемых оперативными сотрудниками.

Библиографический список

1. Ефремова, М. А. К вопросу о понятии компьютерной информации / М. А. Ефремова // Российская юстиция. – 2012. – № 7. – С. 51.

2. Осипенко, А. Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления / А. Л. Осипенко // Научный вестник Омской академии МВД России. – 2017. – № 2. – С. 38–48.

3. Осипенко, А. Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения / А. Л. Осипенко // Вестник Воронежского института МВД России. – 2015. – № 2. – С. 13–19.

Вишневская В. П.

АКТУАЛЬНЫЕ ВОПРОСЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ, ВКЛЮЧЕННЫХ В ПРОЦЕСС РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

ГУО «Институт пограничной службы Республики Беларусь»,
ул. Славинского, 4, 220103 Минск, Беларусь, *ips@gpk.gov.by*

Одним из значимых аспектов подготовки специалистов, включенных в процесс расследования преступлений, является наличие у них теоретических знаний и практических навыков использования антиманипулятивных технологий профессионального общения и психологической защиты от деструктивного воздействия.

В научной литературе в зависимости от области знаний, направлений научных (отечественных и зарубежных) школ, в которых изучаются различные аспекты психологической защиты личности, представлено множество точек зрения и предложений относительно путей решения обозначенной проблемы (от психоаналитических технологий до специфических особенностей профессионального общения в следственной практике и др.).

Вопросам психологической защиты личности посвящены многочисленные публикации. В рамках рассматриваемой проблемы целесообразно обратить внимание на исследования Р. В. Вольнова, Г. В. Грачева, Е. Л. Доценко, Н. С. Ефимовой, И. К. Мельника и др., в которых представлены некоторые виды и механизмы психологической защиты, манипулятивные технологии.

Психологическая защита – «употребление субъектом психологических средств устранения или ослабления ущерба, грозящего ему со стороны другого субъекта» [3, с. 70].

Психологическая безопасность «является ведущей характеристикой, определяющей развитие социально и психологически здоровой личности. Одним из основных психологических условий ее развития является формирование самосознания, включающего самопознание (опасный-безопасный тип личности), самоотношение (адекватная самооценка), саморегулирующую (уравновешенность, способность регулировать