Научная статья
УДК 343.98

ОСОБЕННОСТИ И ПРАВОВЫЕ АСПЕКТЫ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ «СНЯТИЕ ИНФОРМАЦИИ С ТЕХНИЧЕСКИХ КАНАЛОВ СВЯЗИ» И «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Владимир Викторович Петров
Академия права и управления ФСИН России,
Рязань, Россия, v.v.petrov@ro.ru

Аннотация. В данной статье автором рассматриваются особенности и некоторые правовые аспекты оперативно-розыскных мероприятий «снятие информации с технических каналов связи» и «получение компьютерной информации» с использованием сетей документальной электросвязи [1, с 184–189]. Описывается процесс внедрения комплекса технических средств для обеспечения оперативно-розыскных мероприятий на сетях документальной электросвязи, в том числе некоторые сопутствующие законодательные инициативы. Проводится анализ двух видов оперативно-розыскных мероприятий, их сущности, особенностей и правовых аспектов проведения.

В данной работе анализируются некоторые этапы внедрения информационных систем, направленных на повышение эффективности оперативно-розыскных мероприятий на сетях документальной электросвязи с конца XX века по наши дни. Кроме того, изучается период становления и сопутствующие социальные феномены, характерные для развития современных технологий как в оперативно-розыскной деятельности, так и в целом. Акцентируется особое внимание на актуальности и перспективности таких мероприятий в оперативно-розыскной деятельности, совершенствовании законодательных норм, регламентирующих их применение [2, с. 21]. На основании анализа действующего законодательства автором рассматриваются некоторые проблемные вопросы, приводятся мнения ученых, изучающих данное направление, а также предлагается толкование некоторых правовых аспектов.

Ключевые слова: система оперативно-розыскных мероприятий, документальная электросвязь, оперативно-розыскная деятельность, снятие информации с технических каналов связи, получение компьютерной информации, понятийная характеристика мероприятий, каналы связи.

Для цитирования: Петров В. В. Особенности и правовые аспекты проведения оперативно-розыскных мероприятий «снятие информации с технических каналов связи» и «получение компьютерной информации» // Вестник Уфимского юридического института МВД России. 2025. № 1 (107). С. 132–145.

Original article

FEATURES AND LEGAL ASPECTS OF CONDUCTING OPERATIONAL-SEARCH MEASURES “REMOVING INFORMATION FROM TECHNICAL COMMUNICATION CHANNELS” AND “OBTAINING COMPUTER INFORMATION”

Vladimir V. Petrov
Academy of Law and Management of the Federal Penitentiary Service of Russia,
Ryazan, Russia, v.v.petrov@ro.ru

Abstract. The article examines the features and some legal aspects of the operational-search activities “removing information from technical communication channels” and “obtaining computer information” using documentary telecommunication networks [1, p. 184–189]. It describes the process of implementing a set of

technical means to ensure operational-search activities on documentary telecommunication networks, including some related legislative initiatives. An analysis of two types of operational-search activities, their essence, features and legal aspects of implementation is carried out.

This paper analyzes some stages of the implementation of information systems aimed at increasing the efficiency of operational-search activities on documentary telecommunication networks from the end of the 20th century to the present day. In addition, the period of formation and related social phenomena characteristic of the development of modern technologies both in operational-search activities and in general are studied. Particular attention is focused on the relevance and prospects of such measures in operational-search activities, and to the improvement of legislative norms regulating their application [2, p. 21]. Based on the analysis of current legislation, the author examines some problematic issues, provides the opinions of scientists studying this area, and also offers an interpretation of some legal aspects.

Keywords: system of operational-search measures, documentary telecommunication, operational-search activities, removal of information from technical communication channels, obtaining computer information, conceptual characteristic of measures, communication channels.

For citation: Petrov V. V. Features and legal aspects of conducting operational-search measures "removing information from technical communication channels" and "obtaining computer information" // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2025. No. 1 (107). P. 132–145. (In Russ.)

Введение

Актуальность темы настоящей работы обусловлена прежде всего развитием новых информационных и коммуникационных технологий, вследствие чего научно-технический прогресс рассматривается как единый процесс, являющийся важнейшим фактором, определяющим развитие общества, в котором закономерным является тот факт, что в повседневной деятельности большинства людей все чаще применяют современные технические средства [3, с. 24]. Исключением не стала и та часть общества, которая занимается противоправной деятельностью, контроль за такой деятельностью со стороны правоохранителей всегда являлся приоритетной задачей для государства. Актуальность создания и разработки систем для получения информации от лиц, представляющих оперативный интерес, а также компьютерной информации для оперативно-розыскной деятельности невозможно переоценить. В соответствии со статьей 2 Федерального закона «Об оперативно-розыскной деятельности»[1] (далее – ФЗ об ОРД) основные задачи в оперативно-розыскной деятельности включают в себя выявление, предупреждение, пресечение и раскрытие преступлений, розыск лиц, уклоняющихся от уголовного наказания, а также добывание информации о событиях или действиях, представляющих угрозу безопасности Российской Федерации. Реализация этих задач невозможна без использования современных технических средств и методов получения и обработки информации, что требует от субъектов оперативно-розыскной деятельности постоянного осмысления и сопоставления используемых методов и практик, применяемых в борьбе с различными преступными посягательствами.

Для рассмотрения мероприятий, указанных в названии настоящей статьи, обратимся к проблеме целесообразности их проведения. Она обусловлена применением все новых современных технологий, предполагающих их использование не только с учетом уголовно-правовых дефиниций, но и с возможностями применения специальных знаний как в области информационно-телекоммуникационных систем, так и в области используемого программного обеспечения. Без изучения основных терминов и принципов построения таких систем, по нашему мнению, невозможно объяснить их сущность и базовые понятия.

В контексте оперативно-розыскной деятельности (далее – ОРД) для решения ее

[1] Об оперативно-розыскной деятельности : федеральный закон от 12 августа 1995 г. № 144-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

основных целей и задач иногда необходимо углубленное понимание некоторых специфических терминов, используемых в данной сфере. Это обусловлено тем, что ОРД является многоаспектной деятельностью, включающей в себя широкий спектр задач, решаемых посредством проведения оперативно-розыскных мероприятий. Например, для сбора и анализа информации нередко необходимо изучение принципов функционирования тех или иных информационных систем, углубленное изучение терминов, консультации с техническими специалистами. В связи с этим вопросы погружения в терминологию ОРД являются чрезвычайно обширными и требуют от сотрудников правоохранительных органов постоянного обновления и расширения своих знаний и навыков. Прежде всего, это обусловлено ее комплексностью, что подразумевает множество факторов, относящихся к сложной модели для восприятия неподготовленному человеку. Однако стоит отметить, что интерпретация и толкование некоторых понятий со стороны ученых, специализирующихся на изучении данного направления, способны помочь осмыслить и понять некоторые аспекты для последующего правильного применения.

Некоторые основные понятия, которые приводят исследователи, изучающие принципы применения таких мероприятий, не всегда удается определить, насколько они соответствуют законодательным нормам, что является основной проблемой в формировании и осмыслении нормативных основ, используемых для подготовки и проведения оперативно-розыскных мероприятий, применяемых с использованием информационно-телекоммуникационных технологий. Частой проблемой при изучении возможностей данных оперативно-розыскных мероприятий является тот факт, при котором законодательные аспекты рассматриваются отдельно, при этом они не включают в себя согласованное с законодательством техническое толкование каких-либо процессов, что не всегда позволяет изучить все стороны описываемого процесса.

При анализе и обобщении некоторых материалов данной работы нельзя не отметить и тот факт, что контроль телекоммуникационных систем, используемых для передачи различных сигналов в процессе осуществления оперативно-розыскной деятельности, всегда был очень актуальной темой для исследования учеными, по-разному описывающими процесс получения информации при проведении оперативно-розыскных мероприятий по снятию информации с технических каналов связи и получению компьютерной информации».

Методы

В качестве объекта исследования рассматриваются уголовно-правовые правоотношения, возникающие между участниками уголовного судопроизводства в процессе осуществления оперативно-розыскной деятельности, и теоретические предложения по толкованию оперативно-розыскных мероприятий по снятию информации с технических каналов связи и получению компьютерной информации. В процессе исследования данной темы автор применял общенаучные методы и подходы, которые использовались для сбора эмпирических данных и их последующего анализа.

Основу методологии исследования составил диалектический метод научного познания, который обеспечил комплексный анализ вопросов, касающихся оперативно-розыскной деятельности и применяемых в сетях документальной электросвязи оперативно-розыскных мероприятий. Из числа частно-научных методов были выбраны сравнительно-правовой, формально-юридический и кибернетический. Эти методы в конечном итоге использовались для разработки рекомендаций по толкованию оперативно-розыскных мероприятий, рассматриваемых в данной работе.

Результаты

Пристальное внимание к проблематике взаимодействия государства и Интернета впервые было уделено на встрече тогда еще премьер-министра Российской Федерации В. В. Путина с «интернет-общественностью» 28 декабря 1999 г. В результате этой

встречи в широких кругах начато формирование неоднозначного мнения. Одна сторона участников дискуссии, преимущественно представляющих государственные органы, была привержена позиции, что введение таких систем государством является своевременным и необходимым, а другая сторона выражала диаметрально-противоположное мнение. Противоположное мнение исходило от «общественности» и представителей различных коммерческих телекоммуникационных структур. Они считали, что внедрение специализированных систем по контролю сети Интернет может быть преждевременно и нецелесообразно. В то время широко обсуждалось мнение доктора физико-математических наук А. А. Солдатова, одного из пионеров сети Интернет в России, выступающего против введения специального государственного регулирования сети Интернет и предлагающего следовать опыту западных стран, которые воздерживаются от специального контроля над ней[1].

Обращаясь к истокам формирования сегодняшней модели построения информационно-телекоммуникационных систем, используемых оперативно-розыскными органами, отметим, что государство в очередной раз столкнулось с проблемой своевременного реагирования на те или иные задачи, продиктованные сложившейся оперативной обстановкой, борьбой с преступностью, а также различными террористическими формированиями, составляющими большую угрозу целостности конституционного строя государства. Все эти вновь возникшие тенденции о свободе слова, свободе интернета и другие либеральные взгляды, развивавшиеся на фоне резкого скачка информационного прогресса, только осложняли запланированные шаги в построении единой системы обеспечения оперативно-розыскной деятельности со стороны государства. Это время в современной России, как и во всем мире, было ознаменовано появлением мобильных устройств, укоренением культуры их использования и, как следствие, применением различных телекоммуникационных систем лицами при осуществлении своих преступных посягательств.

В работе О. В. Джиган приводится мнение одного из ведущих социологов современности, специализировавшегося на изучении теории информационного (постиндустриального) общества М. Кастельса о том, что в современном обществе происходит трансформация социальности, а в силу возникновения новых возможностей коммуникации общество приобретает сетевой индивидуализм. Такое видение ситуации свидетельствовало о зарождении информационального общества при генерировании, обработке и передаче информации, которое стало фундаментальными источником производительности и власти [4, с. 110]. Высказанное М. Кастельсом мнение говорило о крайней необходимости и востребованности мер, обеспечивающих контроль за всплесками противоправных и деструктивных явлений, создающих угрозу государственности.

В процессе изучения социокультурного явления отдельно хотелось бы отметить самые ранние попытки государства внедрить такие системы, которые смогли бы применяться для контроля использования технических средств на сетях электросвязи. Одно из первых упоминаний таких нормативных документов приходится на 1992 год, тогда в свет вышли требования к использованию средств связи для обеспечения оперативно-розыскных мероприятий Министерства безопасности Российской Федерации[2], предписывающие Министерству связи Российской Федерации оказывать всяческое

[1] Открытое письмо А. А. Солдатова Интернет-общественности // Московский либертатум. URL: https://libertarium.ru/s-openletter.html (дата обращения: 19.01.2025).

[2] Об использовании средств связи для обеспечения оперативно-розыскных мероприятий Министерства безопасности Российской Федерации : приказ Минсвязи РСФСР от 24 июня 1992 г. № 226 (с изменениями и дополнениями). Доступ из справ.-правовой системы «КонсультантПлюс».

содействие Министерству безопасности Российской Федерации, в том числе предоставляя помещения и оборудование для проведения оперативно-розыскных мероприятий по снятию информации с технических каналов связи. После этого в свет с завидным постоянством выходили новые приказы и другие нормативные документы, которые дополняли или заменяли отдельные пункты предыдущих документов, которые и ввели понятие таких систем, как «системы оперативно-розыскных мероприятий (далее – СОРМ)»[1].

В результате ретроспективного анализа причин создания таких систем можно сделать вывод о том, что государственные органы, несмотря на «мнение общественности», были готовы к развитию информационно-телекоммуникационных технологий и все чаще сталкивались с тем, что при оперативной необходимости обоснованным является использование систем, которые позволяли бы быстро, качественно и, что не мало важно, негласно решать поставленные в процессе осуществления оперативно-служебной деятельности задачи. Такие системы успешно внедрялись с начала XXI века, они получили наименование «СОРМ», что определяло их как технические средства для обеспечения оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и радиосвязи [5, с. 72]. Одними из первых понятий таких систем, закрепленных на законодательном уровне, было предложено Министерством Российской Федерации по связи и информатизации 25 июля 2000 г.[2]

Безусловно, неоспоримым считается и тот факт, что одним из основных методов, используемых в наше время в оперативно-розыскной деятельности для получения информации с различных устройств, является проведение оперативно-розыскных мероприятий «снятие информации с технических каналов связи» и «получение компьютерной информации». Основные задачи при проведении таких мероприятий соответствуют целям и задачам оперативно-розыскной деятельности и направлены на выявление, пресечение, предупреждение и раскрытие преступлений, осуществление розыска лиц, скрывающихся от следствия, суда, органов дознания, установление уклоняющихся от уголовного наказания, а также розыска без вести пропавших.

Оперативно-розыскные мероприятия «снятие информации с технических каналов связи» и «получение компьютерной информации» входят в перечень мероприятий общих для всех субъектов оперативно-розыскной деятельности, а также дополняют виды оперативно-розыскных мероприятий, указанных в статье 6 ФЗ об ОРД. Право на проведение рассматриваемых оперативно-розыскных мероприятий субъектам оперативно-розыскной деятельности предоставляется в рамках специальных полномочий, которые определенны системой законодательства Российской Федерации, межведомственными соглашениями, а также ведомственными нормативными правовыми актами. В настоящее время к таким субъектам относятся: МВД России, ФСИН России, ФСБ России, ФСО России, ФТС России, СВР России.

Перейдем к изложению сущности и принципов таких оперативно-розыскных мероприятий, как «снятие информации с технических каналов связи» и «получение компьютерной информации». Одним из ос-

[1] Методические рекомендации по порядку действий по обеспечению выполнения обязательных требований в части организации на сетях электросвязи системы оперативно-разыскных мероприятий (СОРМ) // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://rkn.gov.ru/docs/Metodicheskie_rekomendacii_po_vypolneniju_objazatel6nykh_trebovanija_v_chasti_SORM.docx (дата обращения: 20.01.2025).

[2] О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования: Приказ Минсвязи Российской Федерации от 25 июля 2000 г. № 130 (с изменениями и дополнениями). Доступ из справ.-правовой системы «КонсультантПлюс».

новных и наиболее существенных отличий мероприятий этого вида от других является то, что при их выполнении привлекаются специальные сотрудники, наделенные на то особыми полномочиями, а их проведение возможно только в порядке согласованного межведомственного взаимодействия с использованием ресурсов Федеральной службы безопасности Российской Федерации и органов внутренних дел Российской Федерации[1].

В ходе выполнения данных мероприятий ограничиваются охраняемые Конституцией Российской Федерации права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а для ограничения таких прав в ходе выполнения указанных мероприятий субъектам оперативно-розыскной деятельности необходимо судебное решение.

Правовыми нормами определен ряд требований, без выполнения которых затрагиваемые в данной работе оперативно-розыскные мероприятия не могут проводиться. К этим требованиям можно отнести имеющуюся у субъекта оперативно-розыскной деятельности информацию о причастности лица к различным противоправным деяниям, по которым обязательно должно проводиться предварительное следствие, а также при наличии информации о государственной, военной, экономической и экологической угрозе Российской Федерации.

В связи с тем, что стремительный технический прогресс способствовал развитию информационных технологий и различных информационных сервисов, а практически каждый житель страны стал использовать мобильный телефон, в том числе и для осуществления доступа к различным информационным ресурсам и системам, в настоящее время проведение высокотехнологичных оперативно-розыскных мероприятий наиболее востребовано. Например, применение рассматриваемых в данной работе мероприятий может помочь оперативным подразделениям, осуществляющим оперативно-розыскную деятельность, в быстром поиске без вести пропавших лиц, а также при документировании противоправной деятельности с использованием современных устройств связи. В случаях, не терпящих отлагательств, данные мероприятия могут выполняться, исходя из мотивированного постановления руководителя органа, осуществляющего оперативно-розыскную деятельность, а для определения местоположения без вести пропавшего недееспособного лица либо несовершеннолетнего – с письменного разрешения законного представителя, что, в свою очередь, значительно уменьшает сроки, затраченные на установление в процессе обработки информации о соединениях, осуществляемых мобильными устройствами связи, с фиксацией их местоположения. При выполнении таких мероприятий существенно сокращается время поиска без вести пропавших лиц, однако оперативным подразделениям необходимо обязательно уведомить в течение 24 часов судебный орган, а в течение 48 часов должно быть получено решение суда, иначе такие мероприятия должны быть прекращены[2].

Рассматривая принципы применения мероприятия «снятие информации с технических каналов связи», можно сделать вывод о том, что главной его задачей в процессе применения оперативными подразделениями будет являться получение и фиксация при помощи специальных технических средств как графической, текстовой, так и иной информации, обрабатываемой в технических каналах связи [6, с. 70]. При выполнении данных мероприятий исследуются технические каналы, производится копирование информации, а также иные действия с после-

[1] Об оперативно-розыскной деятельности : федеральный закон от 12 августа 1995 г. № 144-ФЗ (в последней ред.). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Там же.

дующей ее фиксацией на носителях[1]. Стоит отметить, что такие оперативно-розыскные мероприятия должны соответствовать принципам законности, конфиденциальности, своевременности, обоснованности, а также полученные результаты должны быть защищены от посторонних лиц.

При упоминании в данной работе технических каналов связи стоит понимать, что сети электросвязи используются при приеме и передаче сигналов, звуков, изображений, письменного текста и других знаков, при помощи технических средств по радио, проводным и другим электромагнитным системам[2]. Для проведения данных мероприятий, как отмечалось ранее, и были спроектированы и введены в эксплуатацию специальные системы технических средств по применению на них СОРМ, обеспечивающих все требования при выполнении своих функций[3].

Основной целью создания таких систем было техническое обеспечение оперативно-розыскной деятельности посредством контроля за передачей данных на сетях документальной электросвязи[4]. А их внедрение помогло фиксировать и контролировать процесс передачи данных в сетях документальной электросвязи[5]. В процессе проектирования этих систем учитывались требования приказа Гостелекома Российской Федерации от 21 июля 1999 г., в котором устанавливались требования к субъектам оперативно-розыскной деятельности для получения необходимой информации. Для операторов связи приказом Мининформсвязи России от 16 января 2008 г. № 6 были установлены определенные нормы для сетей электросвязи при осуществлении функций оперативно-розыскной деятельности[6].

В России нередко случается так, что начинания остаются незавершенными. Например, когда закон обозначает определенные оперативно-розыскные мероприятия, он должен содержать хотя бы их общие описания и понятия. Существует достаточное число противоречий среди ученых, занимающихся изучением новых технических подходов в оперативно-розыскной деятельности. Они связаны с толкованием оперативно-розыскного мероприятия «получение компьютерной информации» в части трактования и сопоставления с техническими процессами [7, с. 76].

Рассматривая сущность и принципы применения другого, нового вида мероприятия, появившегося с введением 6 июля 2016 г. Федерального закона № 374-ФЗ[7],

---

[1] Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» // под ред. В. С. Овчинского, М., 2022. С. 127–128.

[2] О связи : федеральный закон от 7 июля 2003 г. № 126-ФЗ (в последней ред.). Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Об утверждении Порядка предоставления доступа к сети Интернет : Приказ Госкомсвязи России от 27 марта 1999 г. № 47. М.: Госкомсвязь России, 1999.

[4] Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» / под ред. В. С. Овчинского, М., 2022. С. 488.

[5] Об утверждении Положения о порядке, общих условиях и принципах использования на территории Российской Федерации систем глобальной подвижной персональной спутниковой связи и требованиях по обеспечению информационной безопасности для российских сегментов указанных систем : приказ Государственного комитета Российской Федерации по телекоммуникациям от 21 июля 1999 г. № 22 // Бюллетень нормативных актов федеральных органов исполнительной власти. 1999. № 47. Ст. 1.1–1.9.

[6] Об утверждении Требований к сетям электросвязи для проведения оперативно-разыскных мероприятий. Часть I. Общие требования : Приказ Министерства информационных технологий и связи Российской Федерации от 16 января 2008 г. № 6. Доступ из прав.-правовой системы «КонсультантПлюс».

[7] 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 : федеральный закон от 6 июля 2016 г. № 374-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

видим, что их проведение осуществляется посредством все тех же упомянутых ранее СОРМ, которые обеспечивают и получение компьютерной информации. С появлением таких мероприятий стали рассматриваться иные формы компьютерной информации, а также применение специальных методов ее получения и весьма обширные свойства ее хранения и предоставления[1].

В нормах законодательства понятие «компьютерная информация» применяется в примечании к статье 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации». Под понятием «компьютерная информация» в Уголовном кодексе Российской Федерации понимаются те сведения, которые представляются в форме электрических сигналов независимо от средств их хранения, обработки и передачи[2]. В статье 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ под понятием «информация» так же, как и в других нормах, понимается, что это те данные, которые не зависят от формы их передачи[3].

Определение понятия «компьютерная информация», закрепленное в «Соглашении о сотрудничестве государств-участников Содружества Независимых Государств (далее – Соглашение о сотрудничестве) в борьбе с преступлениями в сфере компьютерной информации», где под термином «компьютерная информация» понимается та информация, которая содержится в памяти компьютерных систем, на физических носителях информации, в форме, доступной чтению и определению этими системами, а также предполагающая передачу по каналам связи[4].

Переход между компьютерной информацией и компьютерной системой является важным аспектом современных информационных технологий. Компьютерная информация представляет собой данные, структурированные для достижения определенных целей, в то время как компьютерная система является совокупностью аппаратных и программных средств, предназначенных для обработки и хранения такой информации. Переход между ними осуществляется посредством программного обеспечения, которое выполняет интерпретацию и преобразование данных в формат, понятный компьютерной системе, что позволяет осуществлять обработку и хранение информации в режиме реального времени. В том же Соглашении о сотрудничестве, определяющем понятие «компьютерная система», коротко упоминается о наличии программно-аппаратных средств, осуществляющих ее обработку, передачу, сбор, а также хранение в автоматическом режиме[5], что позволяет сделать вывод о правильном интерпретировании организации рассматриваемой темы.

Получение компьютерной информации в качестве оперативно-розыскного мероприятия выступает одним из ключевых инструментов противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей и систем. Оно направлено на выявление, предупреждение, пресечение и раскрытие таких преступлений, а также на выявление лиц, их совершивших. При проведении данного оперативно-розыскного мероприятия правоохранительным органам предоставля-

---

[1] Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» / под ред. В. С. Овчинского. Москва, 2022. С. 99–100.

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.12.2024). Ст. 272 // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

[3] Об информации, информационных технологиях и о защите информации (с изм. и доп., вступ. в силу с 01.03.2023) : федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 29.12.2022). Доступ из справ.-правовой системы «КонсультантПлюс».

[4] О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» : федеральный закон от 1 июля 2021 г. № 237-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

[5] Там же.

ется право получать доступ к компьютерной информации, хранящейся на электронных носителях, в том числе и к информации, содержащейся в базах данных. В то же время данное ОРМ должно осуществляться в строгом соответствии с законодательством, с соблюдением прав и свобод граждан, а также с учетом ограничений, установленных законодательством, в частности, в отношении информации, составляющей государственную, служебную, коммерческую или личную тайну.

При правовом регулировании оперативно-розыскного мероприятия по получению компьютерной информации необходимо учитывать требования, предъявляемые к лицензируемому виду деятельности по предоставлению услуг передачи данных. Эти требования распространяются на все действующие сети документальной электросвязи и связаны с выполнением единых норм к сетям документальной электросвязи (далее – СДЭС). Анализ правового регулирования рассматриваемых мероприятий показывает, что снятие информации с технических каналов связи и получение компьютерной информации схожи по принципу применения, так как их выполнение осуществляется на одной технической базе с использованием СОРМ на сетях СДЭС. Кроме того, оба мероприятия характеризуются негласным способом получения информации, заключающимся в контроле за передачей и приемом информации конкретными пользователями в процессе предоставления услуг связи на СДЭС.

В результате анализа истории развития СОРМ можно сказать, что применяемая модель для выполнения рассматриваемых мероприятий связана с проектированием таких систем и учетом требования ФЗ об ОРД и ФЗ о связи, основной целью которых выступало техническое обеспечение негласно проводимых мероприятий в сетях операторов связи, выполняющих передачу данных, в том числе в сети Интернет и на сетях СДЭС[1] [8, с. 54].

С положительной стороны стоит отметить и то, что существенное увеличение возможностей получения оперативной информации в рассматриваемых в данной работе мероприятиях связанно с вступлением в силу 1 июля 2018 г. постановления Правительства Российской Федерации от 12 апреля 2018 г. № 445[2]. Настоящими правилами установлены сроки, а также порядок хранения сообщений пользователей, технические требования к применяемому оборудованию, соответствующие правила и нормы для хранения данных. Принятие таких нормативных правовых актов позволило дополнительно защитить граждан от терроризма и противодействовать любым формам вовлечения их в преступную деятельность, а принятые поправки в различные законодательные нормы, прежде всего, направлены на противодействие терроризму, экстремистской деятельности и усилению общественной безопасности. Для реализации этих целей за операторами, предоставляющими услуги связи, закреплена обязанность хранения текстовых и голосовых пользовательских сообщений в сетях передачи данных [9, с. 187].

Такие нормы установлены за теми организациями, которые осуществляют передачу голосовой и текстовой информации, а также иные услуги связи, в том числе и передачу данных, и обеспечивают функционирование сетей документальной электросвязи.

При передаче голосовой информации операторы связи обязаны хранить ее копии на территории Российской Федерации в неизменном виде в течение 6 месяцев с даты окончания ее приема, доставки, передачи либо обработки в принадлежащих им техни-

[1] Об утверждении Порядка предоставления доступа к сети Интернет : приказ Госкомсвязи России от 27 марта 1999 г. № 47. М.: Госкомсвязь России, 1999.

[2] Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи : постановление Правительства Российской Федерации от 12 апреля 2018 г. № 445. Доступ из справ.-правовой системы «КонсультантПлюс».

ческих средствах накопления данных. Стоит отметить, что согласно правилам, введенным 1 октября 2018 г., при передаче голосовой информации операторы связи должны хранить информацию, отправленную и полученную пользователями, в течение 6 месяцев. Под такой информацией понимаются изображения, звуки, видео, сообщения, а также голосовая информация, переданная пользователями в сетях документальной связи. Другим важным аспектом при обработке данных операторами связи является то, что массивы информации хранятся с 1 октября 2018 г. в полном объеме, в неизменном при приеме и передаче состоянии в течение 30 суток. К такой информации можно отнести сведения о переписке в социальных сетях, различных информационных ресурсах, вложенные файлы и другие данные, передаваемые по сетям связи[1].

С учетом достижений технического прогресса во всех сферах жизнедеятельности человека, в том числе и при решении вопросов оперативно-розыскной деятельности законодательно предъявляются высокие требования для эффективного функционирования оперативных подразделений.

А. Л. Осипенко, анализируя некоторые положения ФЗ об ОРД, указывает, что законодательно данный вид мероприятий не нужно соотносить с формами подключения субъектами оперативно-розыскной деятельности к информационным системам оператора связи либо к устройствам хранения компьютерной информации в открытом доступе. Основой таких мероприятий выступают достаточно сложные в техническом плане действия, которые связаны с использованием определенных знаний по получению содержащейся в компьютерных системах или передаваемой по техническим каналам связи данных о лицах, представляющих оперативный интерес [10]. В связи с этим в части 4 статьи 6 ФЗ об ОРД указано, что рассматриваемые мероприятия выполняются с помощью согласованного взаимодействия с использованием ресурсов Федеральной службы безопасности Российской Федерации и органов внутренних дел Российской Федерации[2]. Не можем не согласиться с этой точкой зрения, ведь данная норма обусловлена необходимостью разграничения и упорядочивания таких работ.

В процессе идентификации личности в информационной среде также возможно получение некоторой служебной информации (учетные данные, абонентские идентификаторы, IP-адреса и т. п.), которая может образовываться и в процессе оперативно-розыскной деятельности, хоть и не требует судебного решения. Данный факт вызывает споры среди ученых и общественности, так как затрагивает баланс между интересами государства в борьбе с преступностью и правами граждан на неприкосновенность частной жизни и личную тайну. С одной стороны, оперативно-розыскная деятельность является важным инструментом в борьбе с преступностью, и для ее эффективного проведения необходима гибкость в получении информации. С другой стороны, отсутствие судебного контроля за получением служебной информации может приводить к злоупотреблениям и нарушениям прав граждан. В связи с этим данный вопрос требует тщательного рассмотрения и поиска баланса между этими противоположными интересами. По мнению С. С. Епифанова, в процессе выполнения мероприятий, рассматриваемых в данной научной работе, при возникновении оперативной необходимости для получения служебной информации, судебное решение не требуется, однако нельзя гарантировать, что со служебной информацией не будет передаваться и личная информация, а для

[1] Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи : постановление Правительства Российской Федерации от 12 апреля 2018 г. № 445. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Там же.

этого основанием все же должно являться судебное решение[1].

Анализируя мнения ученых, занимающихся исследованием в части описания процессов, рассматриваемых в настоящей научной работе, нельзя вновь не прибегнуть к мнению и не согласиться с А. Л. Осипенко о том, что одним из способов получения компьютерной информации в техническом плане все же является получение такой информации с использованием технических каналов связи и входящих в их состав промежуточных устройств [10, с. 85].

Однако стоит отметить и негативно влияющий на процесс получения информации фактор в области рассматриваемой темы. К такому фактору относится то, что информация, передаваемая в сетях документальной электросвязи, хранится в неизменном при приеме и передаче виде, а объектами, представляющими оперативный интерес, при использовании различных информационных систем и средств, могут применяться средства криптографической защиты и различные методы шифрования данных (VPN-сервисы, анонимайзеры, tor-маршрутизации и т. п.) [11, с. 56].

Несмотря на использование субъектами ОРД современных тактических подходов и технических средств, все чаще отмечается тенденция к применению новых и изощренных способов сокрытия противоправной деятельности со стороны лиц, представляющих оперативный интерес. Такое «противодействие» с использованием современных технических средств и методов неблагоприятно влияет на достижение целей в оперативно-розыскной деятельности, что, в свою очередь, усложняет и задачу получения (снятия) необходимой информации и раскрытия преступлений [12, с. 106].

Дискуссии о формах проведения оперативно-розыскных мероприятий «снятие информации с технических каналов связи» и «получение компьютерной информации» ведутся достаточно долгое время. Способы сопоставления законодательных норм и технические аспекты проведения таких мероприятий рассмотрены в исследовании П. А. Рязанова, который считает, что мероприятия должны проводиться исключительно на технических каналах связи СДЭС и не должны взаимодействовать непосредственно с источником и получателями сигналов, минуя систему оперативно-розыскных мероприятий [13, с. 50].

Заключение

Тема проведения оперативно-розыскных мероприятий, связанных с получением компьютерной информации, является актуальной и требует тщательного изучения в контексте уголовно-правовых и технических аспектов [14, с. 152]. Несмотря на это, научно-технический прогресс оказывает существенное влияние на развитие уголовно-правовых наук, что требует выработки единого мнения и определения единого толкования таких мероприятий [15, с. 142]. Однако ввиду специфики темы и невозможности охватить все ее аспекты целесообразно сосредоточиться на изучении правовых норм, социокультурных явлений, истории и хронологии изменений законодательства, сущности и алгоритмов рассматриваемых мероприятий.

Таким образом, на данном этапе исследования на основании изложенного в заключение можно предложить следующие обоснованные выводы:

1. Рассматриваемые технические средства для обеспечения оперативно-розыскных мероприятий применяются на сетях телефонной, подвижной и беспроводной связи и радиосвязи, а основной целью внедрения таких систем является техническое обеспечение оперативно-розыскных мероприятий при передаче данных на сетях документальной электросвязи.

2. Мероприятия по снятию информации с технических каналов связи проводят-

[1] Научно-практический комментарий к Федеральному закону «Об оперативно-розыскной деятельности» (постатейный) / К. К. Горяинов, С. С. Епифанов, А. Н. Журавлев и др. Москва : Проспект, 2021. С. 47.

ся с использованием сетей документальной электросвязи с применением комплекса технических средств для обеспечения оперативно-розыскных мероприятий.

3. Мероприятия по получению компьютерной информации проводятся с использованием тех же сетей документальной связи и комплекса технических средств для обеспечения оперативно-розыскных мероприятий.

4. Вместе с тем требуется правовое закрепление толкования организации и порядка проведения оперативно-розыскных мероприятий по снятию информации с технических каналов связи и получению компьютерной информации.

5. Применение систем оперативно-розыскных мероприятий на сетях документальной электросвязи позволяет осуществлять не только снятие информации с технических каналов связи, но и получение компьютерной информации. При этом для проведения таких мероприятий правоохранительным органам необходимо законное основание, такое как судебное решение или согласие владельца информации.

6. Важным аспектом является также обеспечение конфиденциальности полученной в процессе оперативно-розыскной деятельности информации и ее защита от несанкционированного доступа.

СПИСОК ИСТОЧНИКОВ

1. Петров В. В. Проведение оперативно-разыскных мероприятий по снятию информации с технических каналов связи в отношении лиц, осужденных за преступление экстремистской направленности и террористического характера // Вестник Воронежского института ФСИН России. 2024. № 1. С. 184–189.

2. Захарцев С. И., Игнащенков Ю. Ю., Сальников В. П. Оперативно-розыскные мероприятия в XXI веке: монография. Санкт-Петербургский университет МВД России, Академия права, экономики и безопасности жизнедеятельности. СПб.: Фонд «Университет», 2006. 427 с.

3. Бронников И. А. Современные тенденции и перспективы информационного общества // Вестник Московского университета. Серия 12: Политические науки. 2017. № 6. С. 7–26.

4. Джиган О. В. Философские аспекты использования сетевых технологий // Экономические и социально-гуманитарные исследования. 2015. № 1 (5). С. 110–115.

5. Крюков Ю. С., Ярыгин А. Г. СОРМ в сетях Интернет-провайдеров // Защита информации. Инсайд. 2006. № 3 (9). С. 70–73.

6. Омелин В. Н., Квитко А. В. Информационные технологии в оперативно-розыскной деятельности органов внутренних дел // Научный портал МВД России. 2011. № 4 (16). С. 68–73.

7. Лагуточкин А. В. Получение компьютерной информации: вопросы теории и практики // Вестник Академии Следственного комитета Российской Федерации. 2023. № 1 (35). С. 75–81.

8. Котухов М. П. Перевод результатов оперативно-розыскной деятельности в доказательства: дис. … канд. юрид. наук. Казань, 2001. 231 с.

9. Корнаухова Н. Г., Катков С. В. Получение компьютерной информации: проблемы теории и практики // Вестник Восточно-Сибирского института МВД России. 2020. № 1 (92). С. 182–191.

10. Осипенко А. Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. 2016. № 3. С. 83–90.

11. Криптографические методы защиты информации и VPN в IP сетях / П. М. Мовсарова, Х. Р. Визирова, М. А. Бийсултанова и др. // Тенденции развития науки и образования. 2019. № 56-2. С. 55–58.

12. Батоев В. Б. Преступления, совершаемые с использованием или применением информационно-телекоммуникационных технологий: способы их совершения и количественные характеристики // Правопорядок: история, теория, практика. 2023. № 3 (38). С. 101–112.

13. Рязанов П. А. Техническая разведка побочных электромагнитных излучений и наводок средств вычислительной техники как вид оперативно-розыскного мероприятия // Научный дайджест Восточно-Сибирского института МВД России. 2023. № 1 (19). С. 47–52.

14. Епифанов С. С. Интеграция научных знаний как фактор развития оперативно-розыскной деятельности и средств ее обеспечения // Уголовно-исполнительная система Российской Федерации: вопросы исполнения уголовных наказаний, реализации мер пробации, взаимодействия с публичной властью и институтами гражданского общества: сборник тезисов выступлений и докладов участников Международной научно-практической конференции, приуроченной к 90-летию со дня образования Академии ФСИН России. Рязань: Академия права и управления Федеральной службы исполнения наказаний, 2024. С. 149–154.

15. Иванов И. В. Научно-технический прогресс и уголовное законодательство России // Аграрное и земельное право. 2022. № 8 (212). С. 142–143.

REFERENCES

1. Petrov V. V. Conducting operational search measures to remove information from technical communication channels in relation to persons convicted of extremist and terrorist crimes // Bulletin of Voronezh Institute of the Federal Penitentiary Service of Russia. 2024. No. 1. P. 184–189. (In Russ.)

2. Zakhartsev S. I., Ignashchenkov Yu. Yu., Salnikov V. P. Operational-search measures in the 21st century: monograph. St. Petersburg University of the Ministry of Internal Affairs of Russia, Academy of Law, Economics and Life Safety. St. Petersburg: University Foundation, 2006. 427 p. (In Russ.)

3. Bronnikov I. A. Modern trends and prospects of the information society // Bulletin of Moscow University. Series 12: Political Sciences. 2017. No. 6. P. 7–26. (In Russ.)

4. Dzhigan O. V. Philosophical aspects of using network technologies // Economic and social-humanitarian studies. 2015. No. 1 (5). P. 110–115. (In Russ.)

5. Kryukov Yu. S., Yarygin A. G. SORM in the networks of Internet providers // Information protection. Inside. 2006. No. 3 (9). P. 70–73. (In Russ.)

6. Omelin V. N., Kvitko A. V. Information technologies in operational-search activities of internal affairs bodies // Scientific portal of the Ministry of Internal Affairs of Russia. 2011. No. 4 (16). P. 68–73. (In Russ.)

7. Lagutochkin A. V. Obtaining computer information: issues of theory and practice // Bulletin of the Academy of the Investigative Committee of the Russian Federation. 2023. No. 1 (35). P. 75–81. (In Russ.)

8. Kotukhov M. P. Conversion of the results of operational-search activities into evidence: dis. ... Cand. of Law. Kazan, 2001. 231 p. (In Russ.)

9. Kornaukhova N. G., Katkov S. V. Obtaining computer information: problems of theory and practice // Bulletin of East Siberian Institute of the Ministry of Internal Affairs of Russia. 2020. No. 1 (92). P. 182–191. (In Russ.)

10. Osipenko A. L. New operational-search measure “Obtaining computer information”: content and principles of implementation // Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia. 2016. No. 3. P. 83–90. (In Russ.)

11. Cryptographic methods of information protection and VPN in IP networks / P. M. Movsarova, H. R. Vizirova, M. A. Biysultanova et al. // Trends in the development of science and education. 2019. No. 56-2. P. 55–58. (In Russ.)

12. Batoev V. B. Crimes committed with the use or application of information and telecommunication technologies: methods of their commission and quantitative characteristics // Law and order: history, theory, practice. 2023. No. 3 (38). P. 101–112. (In Russ.)

13. Ryazanov P. A. Technical reconnaissance of side electromagnetic radiation and interference from computing equipment as a type of operational-search activity // Scientific digest of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2023. No. 1 (19). P. 47–52. (In Russ.)

14. Epifanov S. S. Integration of scientific knowledge as a factor in the development of operational-search activities and the means of ensuring it // The criminal-executive system of the Russian Federation: issues of execution of criminal penalties, implementation of probation measures, interaction with public authorities and civil society institutions: a collection of abstracts of speeches and reports of participants in the International scientific and practical conference dedicated to the 90th anniversary of the foundation of the Academy of the Federal Penitentiary Service of Russia. Ryazan: Academy of Law and Management of the Federal Penitentiary Service, 2024. P. 149–154. (In Russ.)

15. Ivanov I. V. Scientific and technological progress and criminal legislation of Russia // Agrarian and land law. 2022. No. 8 (212). P. 142–143. (In Russ.)

Информация об авторе:
В. В. Петров, адъюнкт.

Information about the author:
V. V. Petrov, adjunct.

Статья поступила в редакцию 21.01.2025; одобрена после рецензирования 13.02.2025; принята к публикации 21.03.2025.

The article was submitted 21.01.2025; approved after reviewing 13.02.2025; accepted for publication 21.03.2025.