УДК/UDC 343.98

Характерные особенности оперативно-розыскных мероприятий «снятие информации с технических каналов связи» и «получение компьютерной информации»

Фролкин Николай Павлович
кандидат юридических наук, доцент
ведущий научный сотрудник
Центр исследования проблем российского права «Эквитас»
г. Москва, Россия
e-mail:marinafrolkina@mail.ru

Яковец Евгений Николаевич
доктор юридических наук, профессор, заслуженный юрист Российской Федерации
ведущий научный сотрудник
Центр исследования проблем российского права «Эквитас»
г. Москва, Россия
e-mail: koshka997@mail.ru
SPIN-код: 8190-5220
AuthorID: 524115

Аннотация

В статье рассматриваются сущность и содержание оперативно-розыскных мероприятий «снятие информации с технических каналов связи» и «получение компьютерной информации, требующих получения судебного решения. Приводятся дефиниции этих мероприятий, определяется нормативно-правовая основа их проведения, а также называются объекты, предметы, субъекты и другие элементы рассматриваемых понятий. Анализируются подходы к оценке некоторых (несекретных) аспектов организации и тактики проведения указанных мероприятий. Уточняется порядок использования их результатов в уголовном судопроизводстве. Снятие информации с технических каналов связи дифференцируется по отношению к использованию в исправительных учреждениях системы ФСИН России аудиовизуальных, электронных и иных технических средств надзора и контроля для предупреждения побегов и других преступлений, а также нарушений установленного порядка отбывания на-

казания осуждёнными. Рассматриваются процессуальные действия, которые также следует отличать от указанных оперативно-розыскных мероприятий. Обращается особое внимание на недопустимость нарушения норм действующего законодательства и соблюдение тайны связи при снятии информации с технических каналов связи и получении компьютерной информации.

Ключевые слова: оперативно-розыскная деятельность, оперативно-технические мероприятия, судебное решение, снятие информации с технических каналов связи, получение компьютерной информации, операторы связи, каналы связи, носители информации.

Characteristic features of operational search activities "removal of information from technical communication channels"and "obtaining computer information"

Frolkin Nikolay Pavlovich
Candidate of Law, Associate Professor
Leading Researcher
Center for the Study of Problems of Russian Law "Equitas"
Moscow, Russia
e-mail:marinafrolkina@mail.ru

Yakovets Evgeny Nikolaevich
Doctor of Law, Professor, Honored Lawyer of the Russian Federation
Leading Researcher
Center for the Study of Problems of Russian Law "Equitas"
Moscow, Russia
e-mail: koshka997@mail.ru
SPIN-код: 8190-5220
AuthorID: 524115

Abstract

The article discusses the essence and content of operational investigative measures "removing information from technical communication channels"and "obtaining computer information requiring a court decision. Definitions of these events are given, the regulatory

framework for their implementation is determined, and objects, objects, subjects and other elements of the concepts under consideration are also named. The approaches to the assessment of some (unclassified) aspects of the organization and tactics of these events are analyzed. The procedure for using their results in criminal proceedings is being clarified. The removal of information from technical communication channels is differentiated in relation to the use of audiovisual, electronic and other technical means of supervision and control in correctional institutions of the Federal Penitentiary Service of Russia to prevent escapes and other crimes, as well as violations of the established procedure for serving sentences by convicts. The procedural actions are considered, which should also be distinguished from the specified operational investigative measures. Special attention is paid to the inadmissibility of violating the norms of current legislation and observing the secrecy of communication when removing information from technical communication channels and receiving computer information.

Key words: operational-investigative activity, operational-technical measures, court decision; removal of information from technical communication channels, acquisition of computer information, communication operators, communication channels, information carriers.

Общая характеристика и правовая основа снятия информации с технических каналов связи. Снятие информации с технических каналов связи (СИТКС) – это оперативно-розыскное мероприятие (ОРМ), связанное с получением, преобразованием и фиксацией путём съёма характеристик электронных и других физических полей с помощью специальных технических средств различных видов сигналов, передаваемых по техническим каналам связи (исключая телефонные, телеграфные и компьютерные каналы связи), для решения задач оперативно-розыскной деятельности (ОРД).

Каналы связи представляют собой связующее звено в любой современной системе передачи данных и могут создаваться различными способами в зависимости от своей схемы и особенностей объекта коммуникации. Они могут представлять собой физические проводные каналы, которые основываются на использовании специализированных кабелей, а также могут быть волновыми. Волновые каналы связи формируются для организации в определённой среде всевозможных видов радиосвязи

с использованием антенн, а также выделенной полосы частот. Проводные каналы связи как оптические, так и электрические, в свою очередь, подразделяются на два основных типа – проводные и беспроводные. В связи с этим оптический и электрический сигналы могут передаваться через провода, эфир, а также другими способами [1].

С учётом того, что телефонные, телеграфные и компьютерные каналы связи являются непременными атрибутами осуществления иных ОРМ (контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; получение компьютерной информации) можно предположить, что к числу контролируемых технических каналов связи в ходе осуществления СИТКС относятся только *телексные, факсимильные, селекторные, радиорелейные* каналы передачи данных. Осуществляется рассматриваемое ОРМ и на сетях глобальной подвижной персональной спутниковой связи [2].

СИТКС предусмотрено п. 11 ч. 1 ст. 6 Федерального закона «Об оперативно-розыскной деятельности» [3]. Отдельные моменты, связанные с его осуществлением, нашли отражение и в других нормах ФЗ об ОРД: ст.ст. 5–8, п. 1 ч. 1 ст. 15, ч. 1 ст. 17, а также в ст.ст. 53, 63, 64 Федерального закона «О связи» [4]; ч. 5 ст. 15 Федерального закона «О федеральной службе безопасности» [5] и в следующих подзаконных, ведомственных и межведомственных нормативных правовых актах: Указе Президента РФ от 1 сентября 1995 г. № 891 *«Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» [6]; Правилах взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность,* утверждённых постановлением Правительства РФ от 27 августа 2005 г. № 538 (с изм. и доп.) [7]; *Типовых требованиях к плану мероприятий по внедрению технических средств для проведения оперативно-разыскных мероприятий,* утверждённых приказом Минкомсвязи России и ФСБ России от 1 августа 2017 г. № 391/437 [8]; *Требованиях к сетям электросвязи для проведения оперативно-разыскных мероприятий.* Часть I. Общие тре-

бования. Утверждены приказом Мининформсвязи России от 16 января 2008 г. № 6 [9]; Требованиях к сетям электросвязи для проведения оперативно-разыскных мероприятий. Часть II. Требования к сетям передачи данных. Утверждены приказом Минкомсвязи России от 27 мая 2010 г. № 73 [10]; *Правилах применения оборудования систем коммутации, включая программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий.* Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий. Утверждены приказом Минкомсвязи России от 16 апреля 2014 г. № 83 [11]; и др. Кроме того, для реализации результатов СИТКС в уголовном процессе применяют *Инструкцию о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд:* утв. приказом МВД России, МО России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68[12].

СИТКС относится к классу оперативно-технических мероприятий (ОТМ). Для технического обеспечения подобных ОРМ на сетях (службах) документальной электросвязи, используемых для предоставления услуг передачи данных телематических служб [13][1], создана Система технических средств по обеспечению оперативно-розыскных мероприятий (СОРМ). Требования, предъявляемые к Системе технических средств, регламентированы приказом Государственного комитета РФ по связи и информации от 27 марта 1999 г. № 47 [14]. *Порядок внедрения Системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования* утверждён приказом Минсвязи России от 25 июля 2000 г. № 130 (ред. от 25.10.2000) [15].

[1]Телематические службы – службы электросвязи, за исключением телефонной, телеграфной служб и службы передачи данных, предназначенные для передачи информации через сети электросвязи.

Общая характеристика и правовая основа получения компьютерной информации. Получение компьютерной информации (ПКИ) занимает особое место среди оперативно-розыскных мероприятий. В современном мире виртуальные (электронные, цифровые) данные сопровождают человека буквально на каждом шагу. Они концентрируются в информационных системах, циркулируют в сети Интернет, других информационно-телекоммуникационных сетях (ИТКС). В связи с этим в оперативно-розыскной науке и на практике ведётся активный поиск оптимальных форм и методов сбора компьютерной информации, представляющей оперативный интерес. При этом, как правило, отмечается недостаточная правовая регламентация получения доступа к компьютерным данным в интересах ОРД. До недавнего времени вариант законодательного закрепления соответствующих действий был предложен лишь в Модельном законе «Об оперативно-розыскной деятельности (новая редакция)», принятом на XXVII пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (постановление от 16 ноября 2006 г. № 27-6), где данное мероприятие именуется *«мониторинг информационно-телекоммуникационных сетей и систем» и определяется как «получение сведений, необходимых для решения конкретных задач ОРД, и их фиксация путём наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и её передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам».*

В принципе данное определение верно по своей сути и его можно принять за основу в ходе дальнейших рассуждений.

ПКИ наряду с СИТКС и ПТП также относится к классу ОТМ. Для технического обеспечения его проведения используется СОРМ, о которой говорилось выше.

Действия оперативных сотрудников, осуществляющих ПКИ, нацелены на проникновение в аппаратные компьютерные средства (персо-

нальные компьютеры, периферийные устройства, ИТКС, носители информации), принадлежащие подозреваемым в совершении преступлений лицам, с помощью определённых способов, которые предполагают использование специальных технических или программных средств, с целью копирования компьютерной информации, представляющей оперативный интерес. К таким способам, в частности, могут быть отнесены:

- негласное применение специального программного обеспечения и оборудования для скрытного съёма данных на закрытых сетевых ресурсах, которые могут представлять потенциальный оперативный интерес;

- оперативно-розыскной мониторинг сетевых информационных ресурсов, представляющих оперативный интерес, который реализуется через автоматизированный поиск данных, содержащих запрещённую к распространению информацию;

- изучение материалов, связанных с деятельностью организованных преступных сообществ;

- контроль закрытых для общего доступа мест сетевого общения представителей криминальной среды;

- негласная установка в компьютерные устройства, принадлежащие проверяемым лицам, специального программного обеспечения, позволяющего фиксировать содержание осуществляемых с них сеансов связи [16].

Свойства компьютерной информации, имеющие криминалистическое и оперативно-розыскное значение, заключаются в следующем:

1) она достаточно просто и быстро *преобразуется* из одной объектной формы в другую, *копируется* (размножается) на различные виды машинных носителей и *пересылается на любые расстояния*, ограниченные только радиусом действия современных средств электросвязи;
2) при изъятии компьютерной информации, в отличие от изъятия материального предмета (вещи), она *сохраняется в первоисточнике;*

3) в случае необходимости доступ к ней могут иметь одновременно *несколько пользователей сети ЭВМ.*

Выделяются *два основных вида* компьютерной информации – *общего пользования* (общедоступная) и *охраняемая законом* (ограниченного доступа).

К сведениям ограниченного доступа относится та компьютерная информация, которая удовлетворяет двум обязательным условиям:

- она должна быть документированной – зафиксированной на материальном носителе, с реквизитами, позволяющими её идентифицировать;

- доступ к такой информации должен ограничиваться в соответствии с законодательством Российской Федерации [17].

Компьютерная информация обладает также особым свойством, которое активно используется злоумышленниками при совершении противоправных деяний. Это – обезличенный характер последней (отсутствие признаков, прямо указывающих на связь с подозреваемым), а также возможность её быстрого и полного уничтожения.

Понятие компьютерной информации на уровне отечественного законодательства закреплено лишь в гл. 28 УК РФ, где в примечании 1 к ст. 272 (Неправомерный доступ к компьютерной информации) отмечается, что под этим термином следует понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Таким образом, под компьютерной информацией подразумевается не какой-то особый вид информации, а лишь специфическая *форма* её представления, приспособленная для обработки с помощью средств компьютерной техники.

Средства компьютерной техники, как известно, по своему функциональному назначению подразделяются на две основные группы: 1) аппаратные средства (Hard Ware); 2) программные средства (Soft Ware).

Под *аппаратными средствами* понимаются механические, электрические и электронные технические устройства, используемые для со-

здания, систематизации, обработки, хранения, приёма и передачи данных. К ним относятся:

1) персональный компьютер (ПК) – комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач (персональные и сетевые компьютеры, серверы, ноутбуки, сотовые телефоны, смартфоны, планшеты, банкоматы и др.). ПК является *оконечным оборудованием обработки данных,* которое предназначено для преобразования пользовательской информации в данные для передачи по линиям связи (кодирование) и осуществления обратного преобразования (декодирование). Таким образом, ПК может являться средством передачи информации, её получателем или тем и другим одновременно. Компьютерная информация может на некоторое время «задерживаться» в микросхемах памяти ПК.

   Передача и (или) приём компьютерной информации посредством использования ПК предполагает наличие линий связи и каналов связи [18]. В качестве таковых рассматриваются ИТКС. При обработке на промежуточных сетевых устройствах (серверах, маршрутизаторах, концентраторах, модемах и др.) компьютерная информация может оставлять *цифровые следы;*
2) периферийное оборудование – аппаратные средства, имеющие в информационной системе подчинённый кибернетический статус (принтеры, сканеры, факсы и др.). В их микросхемах также может временно накапливаться компьютерная информация;
3) физические носители компьютерной информации, перечень которых достаточно широк (встроенные и внешние накопители на жёстких магнитных дисках, флэш-карты, CD-диски, DVD-диски и др.). На этих носителях такая информация сохраняется длительное время и может перемещаться, копироваться с одного ПК на другой.

Под *программными средствами* компьютерной техники в соответствии с положениями ст. 1261 ГК РФ понимается представляемая в объективной форме совокупность данных и команд, предназначенная для функционирования ЭВМ и других компьютерных устройств в целях получения определённого результата, включая подготовительные материалы, получаемые в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Практически все ОРМ, фигурирующие в ч. 1 ст. 6 ФЗ об ОРД, нацелены на получение оперативной информации в той или иной форме (в устной или текстовой, графической, в форме видео- или аудиозаписи, фотоизображения и т.д.). Некоторые из них допускают получение результатов ОРМ и в виде компьютерных файлов (снятие информации с технических каналов связи, наведение справок, сбор образцов для сравнительного исследования, обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.). В связи с этим ПКИ как оперативно-розыскное мероприятие *отражает* способ получения оперативной информации, представленной в компьютерной (виртуальной) форме.

Следует подчеркнуть, что до издания Федерального закона от 6 июля 2016 г. № 374-ФЗ (так называемый Закон Яровой) [19] ПКИ охватывалось содержанием таких ОРМ, как «Снятие информации с технических каналов связи» и «Контроль почтовых отправлений, телеграфных и иных сообщений» (в последнем случае – в качестве средства слежения за электронной почтовой перепиской), с которыми оно имеет много общего. Вполне очевидно, что решение о закреплении ПКИ в качестве самостоятельного ОРМ связано с *широчайшей распространенностью* компьютерной формы представления оперативно значимой информации и специфическими свойствами последней, обусловливающими особые способы её получения, а также *исключительной важностью* в плане противодействия киберпреступности и кибертерроризму [20].

Как показывает практика, в своей профессиональной деятельности оперативно-розыскные органы (ОРО) могут сталкиваться со следующими киберпреступлениями:

- сбыт наркотических средств, психотропных веществ или их аналогов, совершаемый с использованием ИТКС, включая сеть Интернет, квалифицируемый по признакам ст. 228.1, ч. 2, п. «б» (Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества);

- мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

- распространение или оборот с помощью сети Интернет порнографических материалов, подпадающее под признаки п. «б» ч. 3 ст. 242 (Незаконные изготовление и оборот порнографических материалов или предметов), п. «г» ч. 2 ст. 242.1 УК РФ (Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних), а также п. «г» ч. 2 ст. 242.2 УК РФ (Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов);

- распространение через Интернет материалов экстремистского характера, подпадающее под признаки ст. 282.1 УК РФ (Организация экстремистского сообщества) и ст. 282.2 УК РФ (Организация деятельности экстремистской организации), которые тесным образом связаны с терроризмом.

Известны и другие виды киберпреступлений, представляющих высокую общественную опасность, включая организацию через Интернет заказных убийств [21] и различных видов вымогательства[22], склонение к самоубийству, незаконное приобретение и продажу особо ценных диких животных и водных биологических ресурсов [23], и др.

Общеизвестно, например, насколько активно действует в киберпространстве запрещённая в России террористическая организация ИГИЛ, решая задачи распространения своей идеологии, вербовки новых членов, демонстрации своей беспрецедентной жестокости [24].

Нормативная регламентация рассматриваемого ОРМ определена п. 15 ч. 1 ст. 6 ФЗ об ОРД. Отдельные моменты, связанные с его осуществлением, нашли отражение и в других нормах ФЗ об ОРД: ч. 4 ст. 6 и ч. 2 ст. 8, а также ст.ст. 53, 63, 64 Федерального закона «О связи», ч. 5 ст. 15 ФЗ о ФСБ, пп. 3.1, 4, 6 ст. 10.1; подпункте 2 п. 2; п. 3 ст. 15.8 Федерального закона «Об информации, информационных технологиях и о защите информации» [25]. Кроме того, к регламентации ПКИ имеют отношение следующие нормативные правовые акты:

- *Конвенция о преступности* в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23 ноября 2001 г. (Российская Федерация к данной Конвенции не присоединилась[2]) [26];

- *Доктрина информационной безопасности* Российской Федерации, утверждённая Указом Президента РФ от 5 декабря 2016 г. № 646 [27];

- *Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы,* утверждённая Указом Президента РФ от 9 мая 2017 г. № 203 [28];

- *Перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации,* утверждённый постановлением Правительства РФ от 1 июля 1996 г. № 770 (с изм. и доп.) [29];

- *Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-*

[2]Нашей стране не удалось договориться о приемлемых для себя условиях трансграничного доступа к компьютерным системам. В марте 2008 г. по инициативе Президента РФ было признано утратившим силу ранее принятое распоряжение «О подписании Конвенции о киберпреступности» от 15 ноября 2005 г. № 557-рп, в соответствии с которым Россия оставляла за собой право определиться с участием в Конвенции при условии пересмотра положений п. «b» ст. 32. Тем не менее, большинство положений данной Конвенции являются ориентиром для российских государственных органов в ходе международного сотрудничества в данной области.

розыскную деятельность, утверждённые постановлением Правительства РФ от 27 августа 2005 г. № 538 (с изм. и доп.);

- *Правила хранения организаторами распространения информации в информационно-телекоммуникационной сети Интернет информации о фактах приёма, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети Интернет и информации об этих пользователях, предоставления её уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации,* утверждённые постановлением Правительства РФ от 31 июля 2014 г. № 759 [30]; и др.

Использование результатов ОРД в уголовном судопроизводстве основывается на нормах уголовно-процессуального законодательства (ст. 89 УПК РФ), оперативно-розыскного закона (ст. 11 ФЗ об ОРД). Механизм использования результатов ОРД детально регламентирован Инструкцией О порядке предоставления результатов оперативно-розыскной деятельности дознавателю, органу дознания, следователю, прокурору или в суд.

Сходство и основные различия между СИТКС и ПКП. Правила осуществления СИТКС во многом аналогичны тем, которые регламентируют ПКИ. Поэтому и *юридические условия* проведения этих двух ОРМ являются сходными. Это две группы условий – общеобязательные, а также характерные для экстренных ситуаций.

Как известно, СИТКС и ПКИ, затрагивающие право граждан на тайну частной жизни, проводятся на основании соответствующих судебных решений. В этой связи *общеобязательными условиями* являются:

1) наличие оперативной информации, предусмотренной ч. 2 с. 8 ФЗ об ОРД;
2) получение судебного решения для начала проведения данного ОРМ (ч. 2 ст. 8 ФЗ об ОРД) и, в случае необходимости, – продление срока его осуществления (ч. 6 ст. 9 ФЗ об ОРД);

3) наличие документально оформленного задания оперативного подразделения (в форме мотивированного постановления, утверждённого соответствующим руководителем) для специализированного подразделения;
4) проведение указанных ОРМ с использованием оперативно-технических сил и средств исключительно органов федеральной службы безопасности или органов внутренних дел (ч. 4 ст. 6 ФЗ об ОРД);
5) запрет на проведение СИТКС и ПКИ по основаниям, предусмотренным пп. 1–4 и 6 ч. 2 ст. 7 ФЗ об ОРД, в целях осуществления оперативно-проверочной работы. Исключением является возможность их осуществления для обеспечения безопасности органов, осуществляющих ОРД (см.: п. 5 ч. 2 ст. 7 ФЗ об ОРД).

Условия, характерные для экстренного проведения указанных ОРМ (согласно чч. 3 и 7 ст. 8 ФЗ об ОРД), подразделяются на следующие категории.

Первая *категория* условий (свойственна как для СИТКС, так и для ПКИ) реализуется в следующих случаях:

а) наличие обстоятельств, которые не терпят отлагательства и могут привести к совершению тяжкого или особо тяжкого преступления;

б) получение данных о событиях и действиях (бездействии), создающих угрозу безопасности Российской Федерации.

В этих ситуациях предусмотрено:

1) оформление мотивированного постановления руководителя органа, осуществляющего ОРД;
2) наличие документально оформленного задания для осуществления указанного мероприятия специализированными подразделениями;
3) уведомление в течение 24 час. о начале проведения данного мероприятия суда (судьи);

4) при необходимости продолжения СИТКС или ПКИ – получение инициатором указанного ОРМ в течение 48 час. с момента его начала соответствующего судебного решения.

Вторая категория условий (относится только к проведению СИТКС) реализуется в случае получения сообщения о без вести пропавшем лице, в связи с чем допускается получение информации о соединениях абонентского устройства, находящегося у без вести пропавшего лица, с иными абонентами и (или) их абонентскими устройствами, иным оборудованием. В этой ситуации предусмотрено:

1) получение письменного согласия законного представителя без вести пропавшего лица в том случае, если последнее является несовершеннолетним либо лицом, признанным в установленном порядке недееспособным или ограниченно дееспособным;
2) оформление мотивированного постановления руководителя органа, осуществляющего ОРД, вынесенного в течение 24 час. с момента поступления сообщения о без вести пропавшем лице;
3) подготовка документально оформленного задания для осуществления указанного мероприятия специализированными подразделениями;
4) уведомление в течение 24 час. о начале проведения данного мероприятия суда (судьи);
5) при необходимости продолжения данного мероприятия – получение инициатором СИТКС в течение 48 час. с момента его начала соответствующего судебного решения.

А.В. Чуркин отмечает частный случай проведения ПКИ, когда искомая компьютерная информация может быть получена и без судебного решения либо без вынесения об этом компетентным руководителем оперативно-розыскного органа мотивированного постановления. Например, в ситуации, когда подозреваемый непосредственно задержан с поличным на месте совершения преступления в общественном или ином месте, и оперативный сотрудник осматривает его личное техническое сред-

ство (компьютер, смартфон, планшет или другое аналогичное устройство) [31].

Следует подчеркнуть, что сбор компьютерной информации из открытых источников (получение общедоступной информации) также не требует судебного решения, но он и не относится к ПКИ, а представляет собой наведение справок или его автоматизированную разновидность – «информационный поиск».

Формы проведения СИТКС и ПКИ могут быть различными. Профессор А.Ю. Шумилов отмечал допустимость как гласной, так и негласной форм их осуществления, причём, приоритет отдавал негласному проведению указанных ОРМ [32]. В.Н. Медведев называет исключительно негласную форму проведения данных ОРМ [33].

С учётом сказанного представляется предпочтительней точка зрения авторов курса лекций «Правовые основы оперативно-розыскной деятельности», которые предлагают рассматривать три формы проведения указанных ОРМ: 1) гласную (реализуется непосредственно самим инициатором – оперативным сотрудником); 2) зашифрованную (осуществляется с участием представителей предприятий, учреждений и организаций); 3) негласную (проводится самостоятельно оперативно-техническими подразделениями федеральной службы безопасности и органов внутренних дел) [34].

В связи с этим в качестве субъектов СИТКС и ПКИ рассматриваются:

- сотрудники оперативных подразделений, обладающие специальными познаниями и навыками в области информационных технологий;

- конфиденты, выполняющие задания оперативных сотрудников во время пребывания на объектах внедрения;

- сотрудники ОТП федеральной службы безопасности и органов внутренних дел, которые осуществляют соответствующие ОРМ по заданиям оперативных подразделений как самостоятельно, а также путём конспиративного подключения к станционной аппаратуре предприятий связи, других организаций и учреждений, располагающих необходимы-

ми техническими каналами и средствами связи для снятия соответствующей информации;

- операторы связи, которые по требованию органов федеральной службы безопасности обязаны включать в состав аппаратных средств дополнительные оборудование и программные средства и создавать другие условия, необходимые для проведения ОТМ [35], а также работники иных предприятий, организаций и учреждений, участвующие в проведении данного мероприятия.

Профессор А.Ю. Шумилов наряду с перечисленными в качестве дополнительных субъектов рассматривал также руководителя оперативно-розыскного органа, утверждающего задание на проведение СИТКС или ПКИ, судью, который санкционирует их проведение, а применительно к проведению ПКИ – также специалиста по компьютерной информации, оказывающего помощь при проведении данного ОРМ [36].

Объекты СИТКС и ПКИ являются сходными, к ним относятся:

1) лица, подготавливающие, совершающие или совершившие преступное деяние, по которому производство предварительного следствия обязательно;
2) случайные лица, не относящиеся к криминальной среде, контактирующие с проверяемыми объектами СИТКС и ПКИ по техническим каналам связи.

А вот *предметы* рассматриваемых ОРМ различаются между собой.

Предметом СИТКС является: 1) информация, передаваемая по контролируемым техническим каналам связи (кроме телефонной, телеграфной и компьютерной); 2) данные о местоположении соответствующего абонентского устройства, получаемые путём снятия информации с технических каналов связи.

Особый интерес представляют возможности СИТКС, связанные с *геолокацией,* применение которой позволяет сотрудникам ОРО идентифицировать или определять реальное географическое местоположение таких объектов, как радарные источники, мобильные телефоны, базо-

вые станции или любые девайсы, подключённые к Интернету. Наряду с этим появляются дополнительные возможности, связанные с противодействием средствам технической разведки организованных преступных группировок.

Предметом ПКИ является компьютерная информация, передаваемая по контролируемым техническим каналам связи.

Профессор А.Л. Осипенко справедливо отмечает, что получение оперативно значимой компьютерной информации предполагает в частности обследование информационных объектов сети Интернет, среди которых следует выделить:

а) закрытые информационные ресурсы, содержащие сведения о совершении преступлений и лицах, их совершающих (сайты криминальных структур, через которые распространяется социально опасная информация, реализуются предметы, запрещённые к обороту, ведётся пропаганда криминального образа жизни, вовлекаются в противоправную деятельность новые участники 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. Оперативно значимая информация на указанных объектах может концентрироваться в виде следов противоправной деятельности, ссылок на материалы, запрещённые к распространению, сообщений лиц, осведомлённых об обстоятельствах подготовки и совершения преступлений.

Среди источников получения оперативно значимой компьютерной информации, по мнению указанного автора, особое место занимают сетевые каналы коммуникации, задействованные злоумышленниками для координации действий с использованием электронной почты, средств обмена сообщениями, приложений VoIP (интернет-телефонии), мессенджеров и т.п. Обнаружение и контроль таких каналов оперативными подразделениями обеспечивает им существенные преимущества. При этом важно учитывать, что количество сетевых сервисов, устанавливающих текстовую, голосовую и видеосвязь между компьютерами через Интер-

нет, постоянно увеличивается (ICQ, Skype, WhatsApp, Viber, Telegram и др.), причём многие из них предоставляют услуги шифрования передаваемых данных [37].

Следует учитывать, что спектр технических источников оперативно значимой компьютерной информации в ближайшее время будет расширяться и за счёт новых видов так называемых «умных вещей», оснащённых микропроцессорами и способных осуществлять обмен данными с ИТКС (навигационные системы автотранспорта, системы «умного дома», «умные» бытовые приборы, информационные датчики в местах общественного пользования и т.п.). Смена в современном обществе концепции «Интернета вещей» на «Интернет всего» предполагает подключение к сети практически всех объектов и инфраструктур, обслуживающих интересы как отдельных граждан, так и общества в целом [38]. Вполне очевидно, что в потоках данных, формируемых в соответствующих системах, объективно присутствуют значительные объёмы информации, представляющей интерес и для оперативно-розыскных органов [39].

Место проведения СИТКС и ПКИ Закон не определяет. Можно предположить, что в качестве такового следует рассматривать помещения предприятий мобильной связи, иных организаций и учреждений, а также помещения специализированных подразделений органов федеральной службы безопасности и органов внутренних дел.

Рассматриваемые ОРМ, как правило, являются продолжаемыми, длительными по времени мероприятиями. *Срок их проведения* может составлять до 180 суток со дня получения судебного решения, если иное не указано в самом постановлении. При необходимости продления срока действия постановления судья выносит судебное решение на основании вновь представленных материалов. Однако, располагая информацией о конкретных сроках поступления интересующей его информации, инициатор вправе провести в этот период ОРМ *разового* характера. При этом течение срока вынесенного решения не прерывается.

Контроль за циркулирующей в контролируемых сетях информацией, которая содержит сведения, составляющие *государственную тайну*, допускается только при условии соблюдения режима секретности.

Полученные в ходе СИТКС и ПКИ данные оформляются:

– при их проведении лично сотрудником оперативного подразделения – справкой или рапортом;

– сообщением лица, оказывающего содействие оперативно-розыскному органу, если последнее задействовано при их осуществлении;

– при проведении зашифрованного или негласного осуществления рассматриваемых ОРМ специализированным подразделением самостоятельно или с участием других лиц и специалистов – актом, а также объяснениями (заявлениями) лиц, участвовавших в проведении данного мероприятия.

К оперативно-служебным документам приобщается звукозапись в тех случаях, если она осуществлялась (в ходе проведения СИТКС) или полученная компьютерная информация в виде файлов, представляющих собой последовательный набор данных, хранящийся на определённом физическом носителе и имеющий собственные имя и расширение (при осуществлении ПКИ).

Полученные результаты ОРД вводятся в уголовный процесс путём допроса сотрудников оперативных подразделений (за исключением сотрудников ОТП) и иных лиц, осуществлявших данное мероприятие (кроме лиц, оказывающих содействие оперативно-розыскному органу), осмотра и прослушивания представленных звукозаписей и носителей компьютерной информации, их приобщения к уголовному делу в качестве вещественных доказательств.

СИТКС, кроме всего прочего, следует отличать от использования в исправительных учреждениях (ИУ) системы ФСИН России аудиовизуальных, электронных и иных *технических средств надзора и контроля* для предупреждения побегов и других преступлений, нарушений установленного порядка отбывания наказания и в целях получения необходимой информации о поведении осуждённых, которое осуществляется без

соответствующего судебного решения, поскольку последние заранее предупреждаются об их применении [40]. Вместе с тем, как отмечает профессор С.С. Епифанов, некоторые виды специальных технических средств, предназначенных для получения оперативной информации в условиях ИУ, могут использоваться сотрудниками иных оперативно-розыскных органов для решения стоящих перед ними задач [41], в том числе – по осуществлению СИТКС.

Процессуальным аналогом СИТКС является следственное действие «Получение информации о соединениях между абонентами и (или) абонентскими устройствами», предусмотренное ст. 186.1 Уголовно-процессуального кодекса РФ [42]. Его содержание заключается в получении следователем (дознавателем) от оператора связи сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также данных о номерах и месте расположения приёмо-передающих базовых станций (п. 24.1 ст. 5 УПК РФ). Оно также проводится по постановлению следователя (дознавателя) на основании полученного судебного решения.

Данное следственное действие необходимо отличать от контроля и записи переговоров (ст. 186 УПК РФ), а также выемки носителей информации о соединениях между абонентами (ст. 183 УПК РФ). Получение информации о соединениях не предусматривает установления содержания самих контролируемых переговоров. Выемка предполагает принудительное изъятие носителей информации о соединениях, состоявшихся в прошлом. Контроль и запись переговоров предусматривает производство выборки необходимых сведений, осуществляемой операторами связи, и их представление следователю (дознавателю), являясь процессуальным аналогом ОРМ «прослушивание телефонных переговоров».

Что касается ОРМ «получение компьютерной информации», то привести подробное описание всех особенностей его применения в настоящее время не представляется возможным, поскольку, как уже под-

чёркивалось, пока отсутствует чёткое нормативное толкование содержания данного мероприятия, и в достаточной мере не наработана практика его применения. Между тем, потенциал применения ПКИ в сочетании с СИТКС и другими ОТМ при решении задач ОРД, несомненно, высок, особенно если речь заходит об использовании при этом искусственного интеллекта (ИИ). Самые серьёзные перспективы ИИ открывает в ходе обработки так называемых Больших Данных (Big Data), содержащих разрозненную и неявную компьютерную информацию об объектах, представляющих оперативный интерес. В ходе подобного анализа появляется возможность формирования «электронного досье» на потенциальных преступников, обнаружения и визуализации их латентных связей с иными представителями криминалитета, выявления организованных преступных группировок и установления их специализации, а также степени организованности, распределения ролей, причастности фигурантов к тем или иным криминальным событиям. Более того, результаты анализа Больших Данных создают реальную основу для применения оперативно-розыскных мер в ходе прогнозирования событий, угрожающих безопасности государства за счёт обнаружения «цифровых следов» с заданными свойствами, указывающими на высокую вероятность подготовки либо совершения определённых криминальных деяний.

Таким образом, для оптимизации ПКИ и других, тесно связанных с ним ОТМ, для поиска и исследования компьютерной и иной информации необходимо использование автоматизированных логико-аналитических систем, основанных на применении ИИ. Судя по последним материалам, поступающим, например, из МВД России [43, 44], в целесообразности подобных мер никто из должностных лиц, определяющих стратегию информатизации органов внутренних дел, сегодня нисколько не сомневается. Данное обстоятельство можно расценивать как отрадный факт и значительный шаг вперёд в противодействии преступности, поскольку ещё каких-то 20–25 лет назад эта идея у многих руководителей указанного ведомства вызывала определённое недопонимание.

Список литературы:

1. Андреевич Е. Каналы связи: виды, характеристики // URL: SYL.ru: https://www.syl.ru/article/201507/new_kanalyi-svyazi-vidyi-harakteristiki (дата обращения: 23.06.2021).

2. Положение о порядке, общих условиях и принципах использования на территории Российской Федерации систем глобальной подвижной персональной спутниковой связи (ГППСС) и требованиях по обеспечению информационной безопасности для российских сегментов указанных систем: утв. приказом Гостелекома РФ от 21 июля 1999 г. № 22. Пп. 1.5; 2.2.6: 3.12; 3.14; 4.47 // Российская газета. 1999. 14 декабря.

3. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-Ф // Российская газета. 1995. 18 августа. Далее – ФЗ об ОРД.

4. О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ (с изм. и доп.) Ст.ст. 12–16 // Российская газета. 2003. 10 июля. Далее – Федеральный закон «О связи».

5. О федеральной службе безопасности: Федеральный закон от 03.04.1995 № 40-ФЗ // Российская газета. 1995. 12 апреля. Далее – ФЗ о ФСБ.

6. Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств: Указ Президента РФ от 1 сентября 1995 г. № 891 // Собрание законодательства Российской Федерации. 1999. № 24. Ст. 2954.

7. Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность: утв. постановлением Правительства РФ от 27 августа 2005 г. № 538 // Российская газета. 2005. 2 сентября.

8. Типовые требования к плану мероприятий по внедрению технических средств для проведения оперативно-разыскных мероприятий: утв. приказом Минкомсвязи России и ФСБ России от 1 августа 2017 г. № 391/437 // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 31 августа 2017 г.

9. Требования к сетям электросвязи для проведения оперативно-разыскных мероприятий. Часть I. Общие требования: утв. приказом Мининформсвязи России от 16 января 2008 г. № 6 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2008. № 9. Ст. 11057.

10. Требования к сетям электросвязи для проведения оперативно-разыскных мероприятий. Часть II. Требования к сетям передачи данных: утв. приказом Минкомсвязи России от 27 мая 2010 г. № 73 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2010. № 30. Ст. 17748.

11. Правила применения оборудования систем коммутации, включая программное обеспечение, обеспечивающее выполнение установленных действий при

проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий: утв. приказом Минкомсвязи России от 16 апреля 2014 г. № 83 // Российская газета. 2014. 18 июля.

12. Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: утв. приказом МВД России, МО России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 // Российская газета. 2013. 13 декабря.

13. Об утверждении руководящего документа отрасли «Телематические службы»: приказ Минсвязи РФ от 23 июля 2001 г. № 175.

14. Общие технические требования к системе технических средств по обеспечению функций оперативно-розыскных мероприятий на сетях (службах) документальной электросвязи: утв. приказом Государственного комитета РФ по связи и информации от 27 марта 1999 г. № 47 // СвязьИнформ. 1999. № 7.

15. Порядок внедрения Системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования: утв. приказом Минсвязи России от 25 июля 2000 г. № 130 // Российская газета. 2000. 29 августа.

16. Теория оперативно-розыскной деятельности: учебник / под ред. К.К. Горяинова, В.С. Овчинского. – 4-е изд., перераб. и доп. – М.: ИНФРА-М, 2018. С. 354.

17. Вехов В.Б. Криминалистическая характеристика преступлений в сфере компьютерной информации // URL: http://www.cyberpol.ru/public/metodica_vehov-p1.doc (дата обращения: 09.06.2021).

18. Основы телекоммуникаций // URL: http://www.vicgain.ru/modems/1.htm (дата обращения: 01.06.2021).

19. 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. Ст. 3 // Российская газета. 2016. 8 июля.

20. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. – М.: Норма, 2017. – 528 с.

21. Ищенко Е. П. Новые информационные технологии обеспечения раскрытия и расследования преступлений // URL: http://kkrimlguvd.org.ua/conferences/article/3 (дата обращения: 07.02.2021).

22. Степанова Ю. Мошенники научились ботать. Информацию из Telegram начали использовать для шантажа // Коммерсант. 2021. 2 марта // URL: https://www.kommersant.ru/doc/4711513 (дата обращения: 02.03.2021).

23. Уголовно-процессуальный кодекс РФ от 18 декабря 2001 г. № 174-ФЗ // Российская газета.2001. 22 декабря. Ст. 258.1, ч. 1.1.

24. Осипенко А. Л. Оперативно-розыскная деятельность в период Четвёртой промышленной революции // Актуальные проблемы теории оперативно-розыскной деятельности: сборник научных трудов / под общ. ред. К. К. Горяинова, В. С. Овчинского. – М.: ИНФРА-М, 2017. – С. 356.

25. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Российская газета. 2006. 29 июля.

26. Конвенция о преступности в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23 ноября 2001 г. // URL: https://base.garant.ru/4089723/ (дата обращения: 23.08.2021).

27. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

28. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы: утв. Указом Президента РФ от 9 мая 2017 г. № 203 // Президент Российской Федерации // URL: http://kremlin.ru/acts/bank/41919 (дата обращения: 24.06.2021).

29. Перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, утверждённый постановлением Правительства РФ от 1 июля 1996 г. № 770 // Собр. законодательства Рос. Федерации. – 1996. – № 28, ст. 3382.

30. Правила хранения организаторами распространения информации в информационно-телекоммуникационной сети Интернет информации о фактах приёма, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети Интернет и информации об этих пользователях, предоставления её уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, утверждённые постановлением Правительства РФ от 31 июля 2014 г. № 759 // Российская газета. 2014. 6 августа.

31. Чуркин А. В. Некоторые правовые аспекты проведения оперативно-разыскного мероприятия «Получение компьютерной информации» // Оперативник (Сыщик). 2018. № 2(55). Апрель. М.: Издательский дом Шумиловой И.И., 2018. С. 28–34.

32. Основы оперативно-разыскной деятельности: учебник в 2 т. Т. 1: Общая часть / [С.П. Жданов, О.Г. Карпович, Е.С. Недосекова и др.]: предисл.: В.Б. Мантусова; под ред.: Шумилова А. Ю. – Люберцы: РИО Российской таможенной академии, 2020. – С. 251.

33. Медведев В. Н. Правовое регулирование снятия информации с технических каналов связи в оперативно-розыскной деятельности: автореф. дис. ... канд. юрид. наук. – СПб.: Санкт-Петербургский университет МВД России, 2003. – С. 10.

34. Правовые основы оперативно-розыскной деятельности: курс лекций. – Тюмень: Тюменский институт повышения квалификации сотрудников МВД России, 2012. – С. 98.

35. О федеральной службе безопасности: Федеральный закон от 03.04.1995 № 40-ФЗ (с изм. и доп.) // Российская газета. 1995. 12 апреля. Ст. 15, ч. 5.

36. Основы оперативно-разыскной деятельности: учебник в 2 т. Т. 1: Общая часть / [С. П. Жданов, О. Г. Карпович, Е.С. Недосекова и др.]: предисл.: В.Б. Мантусова; под ред.: Шумилова А. Ю. – Люберцы: РИО Российской таможенной академии, 2020. – С. 255.

37. Теория оперативно-розыскной деятельности: учебник / под ред. К. К. Горяинова, В. С. Овчинского. – 4-е изд., перераб. и доп. – М.: ИНФРА-М, 2018. – С. 353.

38. Ваннах М. Через Интернет вещей – к Интернету всего // URL: https://www.computerra.ru/183215/cherez-internet-veshhey-k-internetu-vsego/ (дата обращения: 26.06.2021).

39. Теория оперативно-розыскной деятельности: учебник / под ред. К. К. Горяинова, В. С. Овчинского. – 4-е изд., перераб. и доп. –М.: ИНФРА-М, 2018. – С. 316.

40. Уголовно-исправительный кодекс РФ от 8 января 1997 г. № 1-ФЗ (с изм. и доп.) Ст. 92, ч. 5 // Российская газета. 1997. 16 января. Ст. 83.

41. Епифанов С. С. Научно-техническое обеспечение правоохранительной деятельности в уголовно-исполнительной системе (междисциплинарное исследование правовых, организационных и методологических аспектов): монография. – Рязань: Издательство «Концепция», 2018. – С. 163.

42. Уголовно-исправительный кодекс Российской Федерации от 8 января 1997 г. № 1-ФЗ (с изм. и доп.) Ст. 92, ч. 5 // Российская газета. 1997. 16 января. Далее – УПК РФ.

43. В МВД России подведены итоги первого в истории ведомства хакатона «Искусственный интеллект на службе полиции» // Официальный сайт МВД России. 2021. 27 мая // URL: https://мвд.рф/news/item/24328582/ (дата обращения: 29.05.2021);

44. В МВД России обсудили вопросы внедрения искусственного интеллекта в работу полиции // Официальный сайт МВД России. 2021. 27 мая // URL: https://мвд.рф/news/item/24411920/ (дата обращения: 29.05.2021).

References:

1. Andreevich E. Communication channels: types, characteristics // URL: SYL.ru: https://www.syl.ru/article/201507/new_kanalyi-svyazi-vidyi-harakteristiki (access date: June 23, 2021).

2. Regulations on the procedure, general conditions and principles for the use of global mobile personal satellite communications systems (GPPSS) on the territory of the Russian Federation and requirements for ensuring information security for the Russian segments of these systems: approved. by order of the State Telecom of the Russian Federation dated July 21, 1999 No. 22. Pp. 1.5; 2.2.6: 3.12; 3.14; 4.47 // Russian newspaper. 1999. December 14.

3. On operational-search activity: Federal Law of August 12, 1995 No. 144-FZ // Rossiyskaya Gazeta. 1995. August 18. Next - the Federal Law on OSA.

4. On Communications: Federal Law No. 126-FZ of July 7, 2003 Art. 12-16 // Russian newspaper. 2003. 10 July. Further - the Federal Law "On Communications".

5. On the Federal Security Service: Federal Law No. 40-FZ of April 3, 1995 // Rossiyskaya Gazeta. 1995. April 12. Next - the Federal Law on the FSB.

6. On streamlining the organization and conduct of operational-search activities using technical means: Decree of the President of the Russian Federation of September 1, 1995 No. 891 // Collection of the legislation of the Russian Federation. 1999. No. 24. Art. 2954.

7. Rules for the interaction of telecom operators with authorized state bodies carrying out operational-search activities: approved. Decree of the Government of the Russian Federation of August 27, 2005 No. 538 // Rossiyskaya Gazeta. 2005. September 2.

8. Typical requirements for the action plan for the introduction of technical means for conducting operational-search activities: approved. Order of the Ministry of Telecom and Mass Communications of Russia and the Federal Security Service of Russia dated August 1, 2017 No. 391/437 // Official Internet portal of legal information (www.pravo.gov.ru) August 31, 2017

9. Requirements for telecommunication networks for carrying out operational search activities. Part I. General requirements: approved. by order of the Ministry of Information and Communications of Russia dated January 16, 2008 No. 6 // Bulletin of Norms. federal acts. authorities of the isp. authorities. 2008. No. 9. Art. 11057.

10. Requirements for telecommunication networks for carrying out operational search activities. Part II. Requirements for data transmission networks: approved. Order of the Ministry of Telecom and Mass Communications of Russia dated May 27, 2010 No. 73 // Bulletin of Norms. federal acts. authorities of the isp. authorities. - 2010. No. 30. Art. 17748.

11. Rules for the use of switching systems equipment, including software that ensures the implementation of established actions during operational-search activities. Part III. Rules for the use of equipment for switching and routing information packets of data transmission networks, including software that ensures the implementation of established actions during operational-search activities: approved. Order of the Ministry of Telecom and Mass Communications of Russia dated April 16, 2014 No. 83 // Rossiyskaya Gazeta. 2014. July 18.

12. Instructions on the procedure for presenting the results of operational-search activities to the body of inquiry, investigator or court: approved. by order of the Ministry of Internal Affairs of Russia, the Ministry of Defense of Russia, the FSB of Russia, the FSO of Russia, the Federal Customs Service of Russia, the SVR of Russia, the Federal Penitentiary Service of Russia, the Federal Drug Control Service of Russia, the Investigative Committee of the Russian Federation dated September 27, 2013 No. 776/703/509/507/1820/42/535/398 / 68 // Russian newspaper. 2013. December 13.

13. Approval of the guiding document of the industry "Telematic services": order of the Ministry of Communications of the Russian Federation dated July 23, 2001 No. 175.

14. General technical requirements for the system of technical means to ensure the functions of operational-search activities on networks (services) of documentary telecommunications: approved. Order of the State Committee of the Russian Federation for Communications and Information dated March 27, 1999 No. 47 // SvyazInform. 1999. No. 7.

15. The procedure for implementing the System of technical means to ensure operational-search activities on telephone, mobile and wireless networks and public personal radio call: approved. by order of the Ministry of Communications of Russia dated July 25, 2000 No. 130 // Rossiyskaya Gazeta. 2000. August 29.

16. Theory of operational-search activity: textbook / ed. K. K. Goryainova, V. S. Ovchinsky. – 4th ed., revised. and additional – M.: INFRA-M, 2018. P. 354.

17. Vekhov V. B. Forensic characteristics of crimes in the field of computer information // URL: http://www.cyberpol.ru/public/methodica_vehov-p1.doc (date of access: 06/09/2021).

18. Fundamentals of telecommunications // URL: http://www.vicgain.ru/modems/1.htm (access date: June 01, 2021).

19. On Amendments to the Federal Law "On Combating Terrorism" and certain legislative acts of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure public safety: Federal Law No. 374-FZ of July 6, 2016. Art. 3 // Russian newspaper. 2016. July 8.

20. Fundamentals of combating cybercrime and cyberterrorism: a reader / comp. V. S. Ovchinsky. – M.: Norma, 2017. 528 p.

21. Ishchenko E. P. New information technologies for ensuring the disclosure and investigation of crimes // URL: http://kkrimlguvd.org.ua/conferences/article/3 (access date: July 02, 2021).

22. Stepanova Yu. Fraudsters have learned to bot. Information from Telegram began to be used for blackmail // Kommersant. 2021. March 2 // URL: https://www.kommersant.ru/doc/4711513 (access date: February 03, 2021).

23. Code of Criminal Procedure of the Russian Federation of December 18, 2001 No. 174-FZ // Rossiyskaya gazeta.2001. Dec 22. Art. 258.1, part 1.1.

24. Osipenko A. L. Operative-investigative activity during the Fourth Industrial Revolution // Actual problems of the theory of operational-investigative activity: collection of scientific papers / ed. ed. K. K. Goryainova, V. S. Ovchinsky. – M.: INFRA-M, 2017. – P. 356.

25. On information, information technologies and information protection: Federal Law of July 27, 2006 No. 149-FZ // Rossiyskaya Gazeta. 2006. July 29.

26. Computer Crime Convention (ETS No. 185). Concluded in Budapest on November 23, 2001 // URL: https://base.garant.ru/4089723/ (access date: August 23, 2021).

27. Doctrine of information security of the Russian Federation: approved. Decree of the President of the Russian Federation of December 5, 2016 No. 646 // Collection of the legislation of the Russian Federation. 2016 No. 50. Art. 7074.

28. Strategy for the development of the information society in the Russian Federation for 2017–2030: approved. Decree of the President of the Russian Federation of May 9, 2017 No. 203 // President of the Russian Federation // URL: http://kremlin.ru/acts/bank/41919 (access date: June 24, 2021).

29. The list of types of special technical means intended (designed, adapted, programmed) for secretly obtaining information, approved by Decree of the Government of the Russian Federation of July 1, 1996 No. 770 // Collection of the legislation Russian Federation. 1996. No. 28. Art. 3382.

30. Rules for the storage by the organizers of the dissemination of information in the Internet information and telecommunications network of information about the facts of reception, transmission, delivery and (or) processing of voice information, written text, images, sounds or other electronic messages of users of the Internet information and

telecommunications network and information about these users , providing it to authorized state bodies carrying out operational-investigative activities or ensuring the security of the Russian Federation, approved by Decree of the Government of the Russian Federation of July 31, 2014 No. 759 // Rossiyskaya Gazeta. 2014. 6 August.

31. Churkin A. V. Some legal aspects of the operational-search activity "Obtaining computer information"// Operative (Detective). 2018. No. 2(55). April. M.: Shumilova I. I. Publishing House, 2018. Pp. 28–34.

32. Fundamentals of operational-investigative activities: a textbook in 2 volumes. T. 1: General part / [S. P. Zhdanov, O. G. Karpovich, E. S. Nedosekova and others]: foreword: V. B. Mantusov; under the editorship of: Shumilova A. Yu. - Lyubertsy: RIO of the Russian Customs Academy, 2020. P. 251.

33. Medvedev V. N. Legal regulation of the removal of information from technical communication channels in operational-search activities: author. dis. ... cand. legal Sciences. - St. Petersburg: St. Petersburg University of the Ministry of Internal Affairs of Russia, 2003. P. 10.

34. Legal foundations of operational-search activity: a course of lectures. - Tyumen: Tyumen Institute for Advanced Training of Employees of the Ministry of Internal Affairs of Russia, 2012. P. 98.

35. On the Federal Security Service: Federal Law No. 40-FZ of April 3, 1995 (as amended and supplemented) // Rossiyskaya Gazeta. 1995. April 12. Art. 15, part 5.

36. Fundamentals of operational-investigative activities: a textbook in 2 volumes. T. 1: General part / [S. P. Zhdanov, O. G. Karpovich, E. S. Nedosekova and others]: foreword: V. B. Mantusov; under the editorship of: Shumilova A. Yu. - Lyubertsy: RIO of the Russian Customs Academy, 2020. P. 255.

37. Theory of operational-search activity: textbook / ed. K.K. Goryainova, V.S. Ovchinsky. – 4th ed., revised. and additional – M.: INFRA-M, 2018. P. 353.

38. Vannakh M. Through the Internet of things - to the Internet of everything // URL: https://www.computerra.ru/183215/cherez-internet-veshhey-k-internetu-vsego/ (access date: June 26, 2021).

39. Theory of operational-search activity: textbook / ed. K. K. Goryainova, V. S. Ovchinsky. – 4th ed., revised. and additional -M.: INFRA-M, 2018. P. 316.

40. Criminal Correctional Code of the Russian Federation of January 8, 1997 No. 1-FZ Art. 92, part 5 // Russian newspaper. 1997. January 16. Art. 83.

41. Epifanov S. S. Scientific and technical support of law enforcement in the penitentiary system (an interdisciplinary study of legal, organizational and methodological aspects): monograph. - Ryazan: Publishing house "Concept 2018. P. 163.

42. Criminal Correctional Code of the Russian Federation of January 8, 1997 No. 1-FZ (as amended and supplemented) Art. 92, part 5 // Russian newspaper. 1997. January 16. Further - Code of Criminal Procedure of the Russian Federation.

43. The Ministry of Internal Affairs of Russia summed up the results of the first hackathon in the history of the department "Artificial intelligence in the service of the police"// Official website of the Ministry of Internal Affairs of Russia. 2021. May 27 // URL: https://mvd.rf/news/item/24328582/ (access date: May 29, 2021).

44. The Ministry of Internal Affairs of Russia discussed the implementation of artificial intelligence in the work of the police // Official website of the Ministry of Internal Affairs of Russia. 2021. May 27 // URL: https://mvd.rf/news/item/24411920/ (access date: May 29, 2021).