УДК 343.985.2

Е.С. Поликарпов, М.А. Ледовская, С.Г. Клюев, А.Г. Александров

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОТДЕЛЬНЫХ ВИДОВ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ, ПРОВОДИМЫХ В СЕТИ ИНТЕРНЕТ

Краснодарский университет Министерства внутренних дел Российской Федерации, Краснодар, Россия

В статье проведен сравнительный анализ отдельных видов оперативно-розыскных мероприятий, связанных с получением информации из средств ее обработки и хранения. Проанализированы следующие виды оперативно-розыскных мероприятий, проводимых в информационно-телекоммуникационной сети Интернет: «наблюдение», «снятие информации с технических каналов связи» и «получение компьютерной информации». Рассмотрены изменения законодательства в этой области и правовая основа оперативно-розыскного мероприятия «получение компьютерной информации». Реализация первых двух видов оперативно-розыскных мероприятий частично или полностью может быть заменена новым видом ОРМ. Проанализирована нормативно-правовая база отдельных оперативно-розыскных мероприятий. Рассмотрены основные понятия и термины в области построения каналов передачи данных: провайдер хостинга, обладатель информации, владелец сайта в сети «Интернет», канал связи, узел вторичной сети, информация, компьютерная информация, вычислительная машина (компьютер), понятие ЭВМ. Также рассмотрена базовая эталонная модель взаимодействия открытых систем, состоящая из семи уровней взаимодействия: прикладного уровня, уровня представления, сеансового уровня, транспортного уровня, сетевого уровня, канального и физического уровней. Представлены технические средства, соответствующие каждому из уровней. Рассмотрены виды информации, получаемой на каждом из уровней. Предложены две группы средств для получения компьютерной информации: средства дистанционного доступа к компьютерной системе и средства физического доступа к компьютерной системе или электронному носителю информации. Предложена общая характеристика содержательной части оперативно-розыскного мероприятия «получение компьютерной информации».

Ключевые слова: получение компьютерной информации, оперативно-розыскное мероприятие, интернет, технический канал связи, оператор связи, провайдер хостинга.

Введение.

В последнее время количество информации, циркулирующей в сети Интернет, непрерывно увеличивается. В качестве обыденных средств ежедневной коммуникации и получения информации можно отметить сервисы электронной почты, чаты, социальные сети, информационные службы, файл-обменные ресурсы, использование IP-телефонии и т.д.

Согласно недавно опубликованных данных аналитического агентства We Are Social и одной из крупнейших SMM-платформ Hootsuite,

по состоянию на январь 2018 года активных пользователей сети Интернет 4.021 млрд., а это больше половины населения земли.

Внимание к сети Интернет, как средству коммуникации, кроме добропорядочных граждан также проявили и криминальные элементы. Современные информационные технологии вызывают интерес у преступников и террористов. Формы совершения преступлений в сети Интернет могут быть самыми разнообразными: от простого общения между преступными группами до продажи запрещенных веществ и предметов, например, наркотиков, оружия, а также планирования и совершения террористических актов.

Ежегодная публикация центра жалоб на интернет-преступность (IC3) «Отчет о преступности в Интернете в 2017 году» показывает, что в прошлом году поступило около 300 000 жалоб с сообщенными о краже более 1,4 млрд. долларов. Кроме того, отчет отразил наиболее распространенные виды преступлений, о которых сообщали жертвы, в тройку вошли: мошенничество с продажей товаров, кража личных данных и мошенничество с использованием социальной инженерии.

Выявление, предупреждение, пресечение и раскрытие преступлений – одна из задач оперативно-розыскной деятельности. Свое отражение данная задача также нашла в сети Интернет. Развитие информационных технологий сформировало сложную иерархию посредников услуг и сервисов в сети. При осуществлении сбора доказательств и документировании преступной деятельности важно различать оператора-связи (интернет провайдера) и провайдера хостинга, которые, как правило, являются разными юридическими лицами.

Основные понятия в области информационных технологий и информационного пространства сформулированы в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Так, провайдер хостинга – лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет [1]. Важно выделить еще одного участника, обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [1]. И, наконец, владелец сайта в сети «Интернет» – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте [1].

Обладатель информации или владелец сайта на договорных условиях с провайдером хостинга предоставляет доменное имя и

возможность доступа к информации через сеть Интернет. По сути хостинг провайдер владелец удаленного сервера, на котором пользователь размещает или хранит свою информацию в электронном виде (электронные документы, контент). В результате возникает необходимость описания содержательной части отдельных видов ОРМ.

Основная цель данной статьи в проведении сравнительного анализа отдельных видов оперативно-розыскных мероприятий, связанных с получением информации из средств ее обработки и хранения.

Основная часть.

Для сравнительного анализа выберем следующие виды оперативно-розыскных мероприятий: наблюдение, снятие информации с технических каналов связи и получение компьютерной информации. Для успешной реализации указанных оперативно-розыскных мероприятий необходимо взаимодействие с оператором связи и (или) провайдером хостинга. Реализация первых двух видов ОРМ имеет сформировавшиеся цели, объекты и содержательную часть.

Наиболее распространенным и простым в реализации в сети Интернет можно выделить ОРМ «наблюдение». Реализация данного вида ОРМ может быть осуществлена посредством интернет-мониторинга. Для проведения используются сервисы поисковых систем и социальные медиа-ресурсы. Сейчас также активно применяются специализированные сервисы по поиску и контролю информации в киберпространстве, которые включают в себя следующие стандартные наборы функций:

– формирование полнотекстовых поисковых запросов на предоставление информации из сети Интернет (социальные сети, форумы, блоги и т.д.);

– возможность сбора и обработки информации при помощи лингвистических словарей терминов, по видам контента (посты, репосты, комментарии, графические изображения, видеозаписи).

Кроме того, имеются функции уточненного поиска и возможности использования логических элементов, мониторинг контента при помощи лингвистических словарей терминов в различных временных разрезах (ежесуточно, ежечасно и т.д.), мониторинг контента по количеству упоминаний указанного термина или словосочетания.

Проведение интернет-мониторинга возможно так же осуществлять в рамках других оперативно-розыскных мероприятий. Фиксация выявленной незаконно размещённой информации, высказываний на почве межнациональной розни, распространения наркотиков и т.д. производится путем получения соответствующего контента. Эти действия можно осуществить путем копирования (получения) соответствующего файла

(файлов) расположенного на удаленном сервере. Данные действия могут проводиться при взаимодействии с владельцем хостинга (хостинг-провайдера).

На практике для использования в качестве доказательства применяются следующие способы получения интернет-контента: печать содержимого веб-страниц используя браузер; печать с приложением рапорта сотрудника; осмотр информационного ресурса с привлечением понятых; такой же осмотр, но с участием специалиста; взаимодействие с оператором связи; экспертиза; нотариальное заверение содержимого сайта [2].

Также в сети достаточно активно применяется перехват трафика. Перехват трафика можно осуществлять в рамках оперативно-розыскного мероприятия «снятие информации с технических каналов связи» (СИТКС).

Оперативно-розыскное мероприятие «СИТКС» проводится при помощи систем технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ) во взаимодействии с оператором связи. В соответствии с статьей 64 «Обязанности операторов связи и ограничение прав пользователей услугами связи при проведении оперативно-розыскных мероприятий, мероприятий по обеспечению безопасности Российской Федерации и осуществлении следственных действий» Федерального закона от 07.07.2003 № 126-ФЗ «О связи» и постановлением правительства от 27.08.2005 № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» оператор связи обязан взаимодействовать с органами осуществляющими оперативно-розыскную деятельность

Для понимания содержательной части и характера получаемой информации при проведении данного оперативно-розыскного мероприятия рассмотрим основные понятия и термины технических каналов связи.

Канал связи – это путь прохождения сигналов электросвязи, образованный последовательно соединенными каналами и линиями вторичной сети ЕАСС (Единая автоматизированная сеть связи) при помощи станций и узлов вторичной сети ЕАСС, обеспечивающий при подключении оконечных устройств вторичной сети передачу сообщения от его источника к получателю. Каналу электросвязи присваивают названия в зависимости от вида электросвязи, например: телефонный канал связи, телеграфный канал связи, канал передачи данных [3].

Узел вторичной сети – комплекс технических средств, обеспечивающий соединение станций вторичной сети ЕАСС. В

зависимости от объекта коммутации различают узел коммутации каналов и узел коммутации сообщений (пакетов) [3].

Таким образом, к техническим каналам связи можно отнести линии (непосредственно провода, оптоволокно или радиоканал) и сетевые узлы (концентраторы, повторители, маршрутизаторы, прокси-серверы и т.д.). Основной способ реализации данного ОРМ это перехват пакетов сетевого трафика или получение информации (содержательной, статистической) с коммутационных узлов (коммутатор, маршрутизатор) (Рисунок 1), соответственно получение информации в рамках ОРМ из перечисленных устройств можно отнести к СИТКС.

Для понимания характера получаемой информации рассмотрим базовою эталонную модель взаимодействия открытых систем. Для облегчения взаимодействия оборудования пакетной сети от разных производителей выбрана базовая эталонная модель взаимодействия открытых систем (ЭМВОС). Модель состоит из семи уровней взаимодействия. Каждому из уровней соответствует свое техническое средство: прикладной, представлений, сеансовый и транспортный уровни основаны на таких устройствах как, компьютеры, шлюзы, сервера, системы хранения данных; сетевому уровню соответствуют маршрутизаторы (роутеры); канальный уровень образован за счет коммутаторов и концентраторов; физический уровень — это ретрансляторы, повторители, соединительные провода, волоконно-оптические линии связи и радиоканал.

Рисунок – 1 Общее представление канала передачи данных

Эталонная модель взаимодействия открытых систем показывает, какой тип информации можно получить на каждом из уровней: уровни приложений и представлений подразумевают прямое получение информации или получение информации из перехваченного контента (E-mail, web, чаты и т.д.); сеансовый уровень позволяет получить статистическую информацию абонентов о времени начала и завершении соединения; транспортный уровень содержит сведения о порте отправителя и получателя, а также об их состоянии (закрыт или открыт); сетевой уровень содержит идентификаторы (IP-адрес) отправителя и получателя; канальный уровень позволяет идентифицировать идентификаторы оборудования (MAC-адрес) отправителя и получателя; на физическом уровне информация представлена в виде битового потока (Рисунок 2, Рисунок 3).

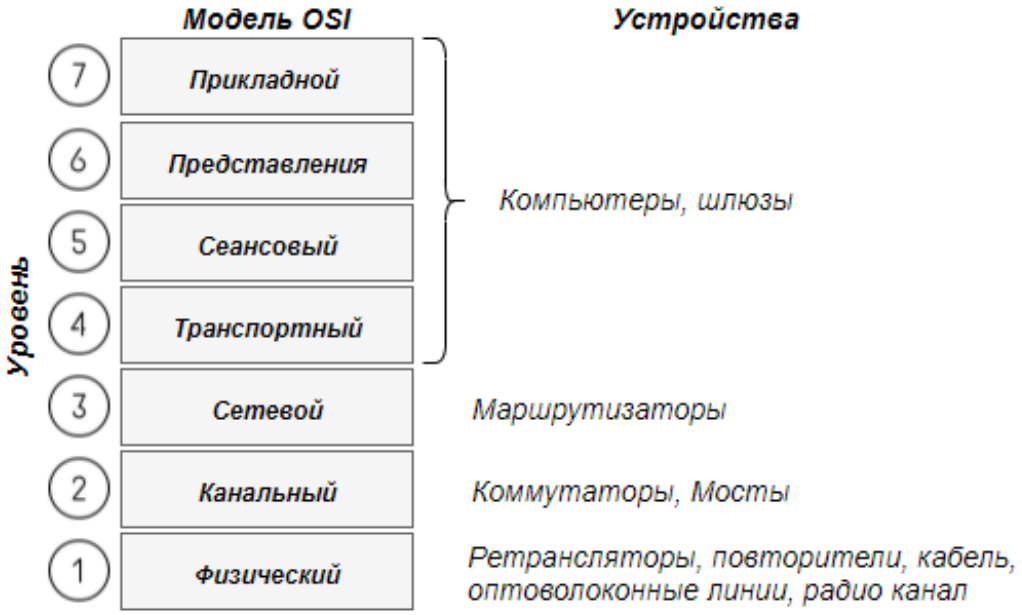

Рисунок – 2 Устройства, поддерживающие каждый уровень OSI

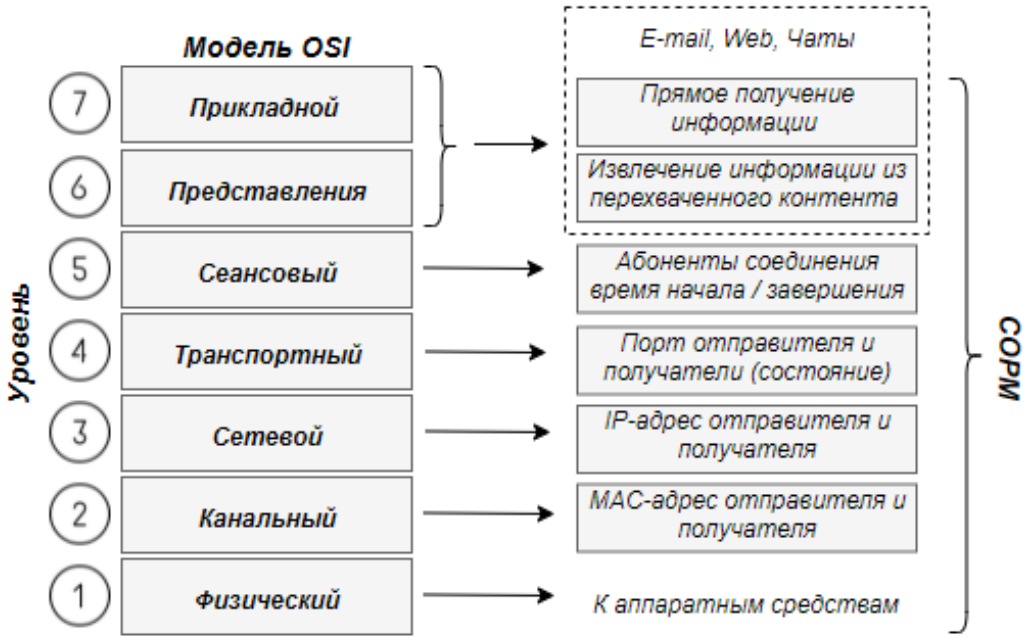

Рисунок – 3 Связь уровней OSI с информацией, получаемой при перехвате и извлечении данных

Темпы развития информационных технологий и интеграция в социальные отношения сети Интернет значительно опережают законодательство. Сегодня очень часто при осуществлении оперативно-розыскной деятельности возникает необходимость получения информации со средств ее хранения, обработки и передачи. В современных реалиях некоторые способы документирования преступной деятельности не в полной мере соотносятся с содержательной частью оперативно-розыскных мероприятий.

В связи с этим Федеральным законом от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон о противодействии терроризму и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» были внесены изменения в ряд законодательных актов, среди которых, добавлено оперативно-розыскное мероприятие «получение компьютерной информации». В соответствии с пунктом 4 ст. 6 Федерального закона от 12.08.1995 № 144-ФЗ данное оперативно-розыскное мероприятие должно проводится только при участии оперативно-технических подразделений органов федеральной службы безопасности и органов внутренних дел. Также согласно ст. 8 того же федерального закона, проведение нового вида ОРМ может затрагивать права человека и гражданина на тайну переписки, телефонных переговоров, почтовых и телеграфных отправлений, а также иных

сообщений, передаваемых по сетям Интернет. Поэтому в числе обязательных условий при проведении оперативно-розыскного мероприятия наличие судебного решения.

Оперативно-розыскное мероприятие «получение компьютерной информации» имеет достаточно широкую трактовку, что создает размытость границ с проводимыми мероприятиями. Основная проблема заключается в том, что необходимо относить к компьютерной информации и выделять в качестве ее источника. Согласно ст. 272 УК РФ от 13.06.1996 № 63-ФЗ компьютерная информация – это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Что в целом не дает точного понимания.

Понятие компьютера определено в ГОСТ 15971 – 90 «Системы обработки информации», вычислительная машина (компьютер) – совокупность технических средств, создающая возможность проведения обработки информации и получение результата в необходимой форме. Кроме того, дано понятие ЭВМ – вычислительная машина, основные функциональные устройства которой выполнены на электронных компонентах. Также в указанном стандарте выделены следующие виды компьютеров: супер – ЭВМ; ЭВМ общего назначения; мини – ЭВМ; микро ЭВМ; персональная ЭВМ; специализированная ЭВМ; бортовая ЭВМ [4]. Указанная компьютерная техника в современной терминологии это – ноутбук, смартфон, планшетный компьютер, сервер и т.д.

К одному из ключевых понятий компьютерной техники и информационных технологий можно отнести данные. В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ информация – сведения (сообщения, данные) независимо от формы их представления [1]. Также можно обратиться к ГОСТ 15971-90, где информация – это сведения о фактах, концепциях, объектах, событиях и идеях, которые в данном контексте имеют вполне определенное значение, а данные – информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека [4]. Таким образом в области использования компьютерной техники значение информации и данных имеют одно значение.

Вполне очевидно, что к объектам ОРМ «получение компьютерной информации» можно отнести информацию (данные) о преступной деятельности в виде, пригодном для обработки автоматическими средствами. В качестве цели будет получение информации (данных) с указанных видов компьютерной техники. Можно отметить что, условие ограничения конституционных прав говорит о том, что при проведении

ОРМ «Получение компьютерной информации» могут использоваться специальные технические средства для негласного получения информации с технических средств ее хранения, обработки и передачи [5], а также возможного использования средств преодоления механизмов защиты информации.

Заключение.

В результате проведенного анализа можно выделить две группы специальных технических средств для получения компьютерной информации: дистанционного доступа к компьютерной системе и физического доступа к компьютерной системе или электронному носителю информации.

Дистанционной доступ к компьютерной системе может быть осуществлен посредством технологий компьютерной разведки.

При физическом доступе к компьютерной системе или электронному носителю информации можно использовать специальные технические средства с блокировкой записи (программы или устройства, не позволяющие вносить изменения на исходный носитель информации). Указанные технические средства позволяют использовать полученную информацию в судопроизводстве. Неизменность содержания полученной информации может быть обеспечена путем расчёта контрольных сумм (хэша) с указанием значения в соответствующих документах. Современные способы расчета контрольных сумм основаны на сложных алгоритмах криптографического хэширования что сводит к минимуму вероятность фальсификации полученной информации.

При проведении указанных в статье оперативно розыскных мероприятий неотъемлемым компонентом является взаимодействие органов, осуществляющих оперативно-розыскную деятельность с операторами связи и провайдерами хостинга. Также необходимо разграничить ряд технических средств для реализации каждого вида ОРМ проводимого в сети Интернет.

Сравнительный анализ показал наличие общих черт в содержательной части описанных оперативно-розыскных мероприятий. Это дает возможность предположить, что проведение их может в большинстве случаев проводится комплексно.

ЛИТЕРАТУРА

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

2. Федотов Н.Н., Форензика – компьютерная криминалистика. 2007 – 432С.
3. ГОСТ 22348-86 «Сеть связи автоматизированная единая. Термины и определения».
4. ГОСТ 15971-90 «Системы обработки информации. Термины и определения».
5. Постановление Правительства РФ от 01.07.1996 № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности».
6. ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель».
7. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 19.02.2018).
8. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ.
9. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ.
10. Федеральный закон «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» от 06.07.2016 № 374-ФЗ.
11. Постановление Правительства РФ от 27.08.2005 N 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность».
12. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
13. Aqsacom Document No. 040451 Lawful Interception for IP Networks White Paper 2010 – 40С.

14. Чечетин А.Е., Основы оперативно-розыскной деятельности органов внутренних дел: учеб. пособие /Дальневосточный юрид. ин-т МВД РФ. – Хабаровск: РИО ДВЮИ МВД РФ, 2014. – 264с.

E.S. Polikarpov, M.A. Ledovskaya, S.G. Klyuev, A.G. Aleksandrov

COMPARATIVE ANALYSIS OF SINGLE TYPES OF OPERATIVE-INVESTIGATIVE ACTION IN THE INTERNET

Krasnodar University of the Ministry of the Interior of the Russian Federation, Krasnodar,Russia

The article provides a comparative analysis of certain types of operational-search measures related to obtaining information from the means of its processing and storage. The following types of operational search activities carried out in the information and telecommunication Internet network are analyzed: "surveillance"; "removal of information from technical communication channels"; "getting computer information." Considered changes in legislation in this area and the legal basis of the operational-search event "Obtaining computer information". The implementation of the first two types of operational-search measures, in part or in whole, can be replaced by a new type of operational-search measures. Analyzed the regulatory framework of individual operational-search activities. The basic concepts and terms in the field of building data transmission channels are considered: hosting provider, information owner, website owner on the Internet, communication channel, node of the secondary network, information, computer information, computer, computer concept. The basic reference model of open systems interaction is also considered. It consists of seven interaction levels: application layer, presentation layer, session layer, transport layer, network layer, channel and physical layer. Submitted technical means corresponding to each of the levels. The types of information obtained at each level are considered. Two groups of means for obtaining computer information are proposed: means of remote access to a computer system and means of physical access to a computer system or electronic information carrier. A general characteristic of the substantive part of the operational-search event "obtaining computer information" is proposed.

Keywords: getting computer-data, operatively-search activity, Internet, technical communication, network operator, hosting provider.

REFERENCES

1. Federal Law «On Information, Information Technologies and Information Protection» of 27.07.2006 N 149-FZ.
2. Fedotov NN, Forensic - computer forensics. 2007 – 432P.
3. GOST 22348-86 «Automated unified communication network. Terms and Definitions».
4. GOST 15971-90 «Information processing systems. Terms and Definitions».
5. Decree of the Government of the Russian Federation of 01.07.1996 No. 770 «On approval of the Regulation on licensing the activities of individuals and legal entities not authorized to conduct operational search activities related to

the development, production, sale, purchase for the purpose of sale, import into and out of the Russian Federation its limits of special technical means intended (developed, adapted, programmed) for secretly receiving information, and the List of special technical means, intended (developed, adapted, programmed) for secretly receiving information in the process of carrying out operational-search activity».

6. GOST R ISO / IEC 7498-1-99 «Information technology (IT). Interconnection of open systems. Basic reference model. Part 1. The basic model»
7. The Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ (as amended on 19.02.2018).
8. Federal Law «On Operative-Search Activity» of 12.08.1995 N 144-FZ.
9. Federal Law «On Communications» of 07.07.2003 N 126-FZ.
10. The Federal Law «On Amendments to the Federal Law on Countering Terrorism and Certain Legislative Acts of the Russian Federation on the Establishment of Additional Measures to Counter Terrorism and Ensure Public Security» of 06.07.2016 No. 374-FZ.
11. Decree of the Government of the Russian Federation of 27.08.2005 No. 538 «On Approval of the Rules for the Interaction of Communication Operators with Authorized State Authorities Performing Operational Investigative Activities».
12. GOST R 50922-2006 «Information protection. Basic terms and definitions».
13. Aqsacom Document No. 040451 Lawful Interception for IP Networks White Paper 2010 – 40P.
14. Chechetin A.E. Fundamentals of operative-search activity of law enforcement bodies: Textbook. allowance / Far Eastern jurist. in-t of the Ministry of Internal Affairs of the Russian Federation. - Khabarovsk: RIO of the TWO Ministry of Internal Affairs of the Russian Federation, 2014. – 264P.