

А. В. Кутузов

**ПРАВОВОЕ РЕГУЛИРОВАНИЕ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ ИНТЕРНЕТ
В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ**

5

Исследуются правовые основы осуществления оперативно-розыскной деятельности в информационно-телекоммуникационной сети Интернет, уделяется внимание положениям федеральных законов «О связи», «Об информации, информационных технологиях и о защите информации», «Об оперативно-розыскной деятельности» в контексте противодействия экстремизму. В работе анализируются особенности проведения оперативно-розыскных мероприятий в сети Интернет с точки зрения их технической и юридической природы.

В рамках научного исследования осуществлен анализ законодательных основ проведения оперативно-розыскных мероприятий в сети Интернет с целью оперативно-розыскного противодействия экстремистской преступности. Обосновано отличие оперативно-розыскного мероприятия «получение компьютерной информации» от иных оперативно-розыскных мероприятий в сети Интернет.

В ходе исследования использовались формально-логический, логико-юридический и сравнительно-правовой методы, которые применялись при исследовании правовых норм и выработке предложений по совершенствованию проведения оперативно-розыскных мероприятий в сети Интернет при раскрытии преступлений экстремистской направленности.

Акцентируется внимание на отличиях оперативно-розыскных мероприятий в сетях связи и в сети Интернет как их разновидности, а также соответствующей правовой регламентации в противодействии экстремистской преступности. Для устранения противоречий в законодательных актах, регламентирующих данную деятельность, обоснованы предлагаемые автором изменения в законодательство.

In the current article, the author explores the legal basis for investigation activities on Internet, paying particular attention to the provisions set forth in the Federal Laws "On Communications," "On Information, Information Technologies and the Information Security", "On the Investigative Search activities" in the context of countering extremism. The article analyzes the technical and legal features of online investigation measures.

The author analyzes the legislation on the investigation measures on the Internet aiming at counteracting extremist. The difference of the operational-search measures "obtaining computer information" from other operational-search measures on the Internet is justified.

The research used formal-logical, logical-legal and comparative-legal methodology to study legal norms and to work out the proposals on improving the investigation measures on the Internet when dealing with extremist crimes.



Particular attention is paid to the differences in investigation in telecommunication networks and the Internet as their certain kind, as well as the relevant legal regulation in countering extremist crimes. To eliminate possible contradictions in the legislative acts regulating this activity, amendments to the current legislation are proposed.

Ключевые слова: правоохранительные органы, противодействие экстремизму, сеть Интернет, оперативно-розыскная деятельность, правовая основа, оперативно-розыскные мероприятия.

Keywords: law enforcement agencies, countering extremism, the Internet, investigation activity, legal basis, investigation measures.

Эволюция социума сопровождается и советующими изменениями общественных отношений. Новые знания, умения и технологии предоставляют дополнительные возможности для удовлетворения потребностей индивидов, их защиты от внутренних и внешних угроз. Стремительное развитие информационных технологий с конца прошлого века, которое продолжается и в наши дни, существенно повлияло на жизнь каждого человека, общества и государства. Компьютерные технологии и Интернет, с одной стороны, предоставили неограниченный потенциал и ресурсы для свободного создания, распространения и хранения информации, а с другой — расширили возможности манипулирования информацией в противоправных целях. Интернет стал средой, где экстремисты, террористы, представители организованной преступности осуществляют явный или, как правило, скрытый обмен информацией, а также товарами и услугами, оборот которых запрещен на территории Российской Федерации.

Необходимость использования новейших технологий в оперативно-розыскной деятельности ранее неоднократно отражалась в научных исследованиях [1; 2]. В последнее время государственные органы принимают значительные усилия по усовершенствованию законодательных основ информационной деятельности в сети Интернет, что отражено в соответствующих изменениях в федеральные законы «О связи», «Об информации»; введена юридическая ответственность за использование информационной сети в деструктивных целях. Данный процесс обусловлен как широким распространением и использованием сети Интернет в экстремистской деятельности, так и значительными пробелами в правовом регулировании оперативно-розыскной деятельности в информационно-телекоммуникационной сети (далее — ИТКС). Существующие методики противодействия экстремизму уже не отвечают современным требованиям и обуславливают необходимость осуществления коренных изменений, активизации усилий при проведении целого комплекса оперативно-розыскных мероприятий (далее — ОРМ) в цифровой среде, что, в свою очередь, должно обеспечиваться и соответствующей правовой основой.

Проблематика законодательного регулирования оперативно-розыскной деятельности (далее — ОРД) является одним из наиболее важных предметов для пристального научного исследования специали-



стов. Данные вопросы рассматривались в отечественной литературе в трудах В. М. Аتماжитова, В. Г. Боброва, Е. А. Доли, И. А. Климова, Р. В. Кулешова, А. Г. Маркушина, Л. А. Осипенко, Л. Л. Тузова, А. Ю. Шумилова и др. Принимая во внимание значительный вклад указанных ученых в науку об ОРД и не преуменьшая его бесспорного значения, отметим, что вопросы законодательного регулирования использования сети Интернет при проведении ОРМ в силу различных причин фактически не нашли должного научного отражения. Это связано со стремительностью развития сети Интернет, а также динамическим характером содержащейся в ней информации, что обуславливает и широкий спектр сценариев поведения пользователей, которые активно меняются в зависимости от появления новых программных продуктов, способов коммуникации, ввода и получения данных. Существующая неурегулированность проведения ОРМ в сети Интернет, по мнению исследователей, также приводит к хаотичному толкованию имеющихся правовых норм [3, с. 69].

На наш взгляд, очерченные положения свидетельствуют о необходимости систематизации имеющихся подходов к пониманию правовой природы использования сети Интернет в оперативно-розыскном противодействии преступлениям экстремистского характера, в частности, при проведении ОРМ как на стадии получения первичной информации о подготавливаемых преступлениях, так и при оперативно-розыском сопровождении уголовных дел указанных категорий.

Целью научной работы является изучение законодательных основ регулирования оперативно-розыскной деятельности в сети Интернет в раскрытии преступлений экстремистской направленности для последующей выработки рекомендаций по усовершенствованию существующей правовой базы, что напрямую влияет на повышение эффективности ОРД в цифровой среде.

В широком смысле правовое регулирование ОРД представляет собой специфическую деятельность государства, его органов и должностных лиц по упорядочению общественных отношений путем установления правовых норм и принятия в необходимых случаях индивидуально-регламентирующих решений в соответствии с этими нормами по юридически значимым вопросам, которые возникают в процессе таких отношений [4, с. 80]. С позиции законодательства такое регулирование осуществляется в соответствии со ст. 4 ФЗ «Об оперативно-розыскной деятельности» [5]. На наш взгляд, в правовую основу использования сети Интернет при проведении оперативно-розыскных мероприятий следует включать Конституцию РФ, федеральные конституционные законы, федеральный закон «Об оперативно-розыскной деятельности» и другие федеральные законы, касающиеся регулирования различных сфер ОРД, а также подзаконные нормативные акты.

В свое время А. Ю. Шумилов, изучая правовое регулирование ОРД, выделял в нем 4 уровня: конституционный, международный, законодательный и подзаконный [6, с. 50–51]. Принимая во внимание значение



Конституции в соблюдении прав и свобод граждан при проведении ОРМ, считаем необходимым очертить основные положения, прямо влияющие на их проведение. Так, ст. 2 Основного закона закрепляет в качестве обязанности государства и его приоритета соблюдение и защиту прав и свобод человека и гражданина. В свою очередь, разд. 2 Конституции Российской Федерации провозглашает основные права и свободы человека и гражданина, что ограничивает вмешательство правоохранительных органов в частную (личную) жизнь гражданина. В частности, положения ст. 23 и 25 Конституции закрепляют право на тайну переписки, телефонных разговоров, почтовой, телеграфной и другой корреспонденции, неприкосновенность жилища, личности, право передвижения и выбора места жительства и другие права и свободы. Ограничения таких прав возможно только на основании судебного решения [7].

Законность методов и средств ОРД в традиционном понимании хорошо изучена в теории ОРД, однако, на наш взгляд, определенные сложности возникают при сборе информации из сети Интернет. В большинстве случаев пользователь сам размещает личную информацию о себе, фактически разрешая любому лицу (или определенным группам в случае ограничения настроек приватности) получать информацию о его личной жизни. В то же время утечки данных граждан, размещение фото- и видеофайлов другими пользователями без согласия собственника, обнародование переписок лиц в различных мессенджерах прямо нарушают положения ст. 24 Конституции, запрещающие сбор, хранение, использование и распространение информации о частной жизни лица без его согласия [7].

Отметим, что согласие лица на сбор, хранение и обработку информации о нем не требуется при проведении ОРМ, дознания и следствия в соответствии с положениями ФЗ «Об оперативно-розыскной деятельности» [5] и УПК РФ [8].

Вторая группа нормативно-правовых актов, составляющих основу ОРД, — нормы международно-правового характера. Базовым международно-правовым договором, регулирующим вопросы обмена электронными данными, является Конвенция о защите лиц в отношении автоматической обработки личных данных, заключенная Советом Европы в 1981 г. и вступившая в силу в 1985 г. [9]. Конвенция содержит правила сбора, обработки и передачи личных данных по компьютерным сетям. В данную группу относятся и решения Еврокомиссии, регламентирующие защиту персональных данных физических лиц и сбор таких сведений, факультативные протоколы к Конвенции, ведомственные и иные международно-правовые акты, имеющие непосредственное отношение к вопросам осуществления ОРД, функционирования ИТКС, проведения ОРМ в целях получения оперативно-значимой информации в цифровом пространстве. В рамках исследования отметим, что отдельные положения Декларации о свободе общения в сети Интернет (2003) [10], рекомендации Парламентской ассамблеи Совета Европы №1706 (2005) «Средства массовой информации и терроризм»



[11], рекомендации №R (2001) Комитета министров Совета Европы «О вопросах регулирования виртуального содержания от 5 сентября 2001 г.» [12], также являются фундаментальной международно-правовой основой регламентацией ОРД в сети Интернет [12].

Обращает на себя внимание и тот факт, что в ряде стран сбор информации, размещенной в открытых источниках, может классифицироваться как посягательство на неприкосновенность частной жизни. В частности, Европейским судом по правам человека по делу «Сегерстедт-Виберг и другие против Швеции» [14] действия полиции по сбору информации, которая является открыто доступной для пользователей сети Интернет, квалифицированы как нарушение права на неприкосновенность частной жизни, гарантированное ст. 8 конвенции Совета Европы «О защите прав человека и основных свобод» от 4 ноября 1950 г. [15]. Систематический сбор информации расценивается как вмешательство в частную жизнь в связи с тем, что лицо, размещающее информацию, рассчитывает на хранение сведений и отсутствие мониторинга его профиля. Сбор сведений является допустимым только по закону и в целях борьбы с преступностью (ст. 8 (2) Конвенции).

Третий (законодательный) уровень правового регулирования ОРД включает в себя нормы, отраженные в соответствующих ординарных законах, определяющих направления и формы борьбы с преступностью экстремистской направленности как специальной сферы государственной деятельности. В данной группе следует указать федеральные законы «Об оперативно-розыскной деятельности» [5], «О связи» [17], «Об информации, информационных технологиях и о защите информации» [18], «О противодействии экстремистской деятельности» [19], федеральные законы, регулирующие группы общественных отношений в ОРД и их отдельные виды.

Проведение ОРМ в сети Интернет неразрывно связано с информацией, в ней размещенной. Так, федеральный закон «Об информации, информационных технологиях и о защите информации» содержит только определение информации как таковой, не конкретизируя понятие «компьютерной информации». В 2011 г. в УК РФ законодателем была разъяснена суть данного термина: под «компьютерной информацией» понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [20]. В настоящее время в подавляющем большинстве случаев, пользователь сталкивается с общедоступной информацией (любые сведения, кроме отнесенных законом к информации с ограниченным доступом) [18]. Общедоступная информация может быть использована любым лицом по его усмотрению, однако при соблюдении ограничений или условий, установленных законодательством. Статья 7 указанного закона предусматривает, что в случае, если информация размещена правообладателем в сети Интернет в форме, предусматривающей автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, она является общедоступной информацией, размещаемой в форме открытых данных [18].



Учитывая изложенное, закономерно приходим к выводу, что оперативные работники вправе накапливать обезличенную открытую информацию, в том числе в инициативном порядке, а сбор сведений в отношении отдельных лиц допустим только в пределах и в порядке, предусмотренных соответствующими федеральными законами.

Рассмотрев виды информации, в том числе распространяемой в сети Интернет, считаем целесообразным очертить различие сетей связи и ИТКС Интернет, что прямо зависит от видов ОРМ, особенностей и порядка их проведения.

В соответствии со ст. 2 ФЗ «О связи», сетью связи является технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи [18]. В свою очередь, ИТКС — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Интернет же является разновидностью ИТКС, представляет собой всемирную сеть и предназначен для общего пользования. Следовательно, отождествлять проведение ОРМ в сетях связи с ОРМ в сети Интернет некорректно ввиду иного порядка доступа и использования.

Так, ч. 2 ст. 64 закона «О связи» [18] предусматривает проведение ОРМ в сетях связи субъектами ОРД с соблюдением требований к установленному порядку использования сетей и средств связи, а также без разглашения организационных и тактических приемов проведения данных ОРМ. Из этого следует, что закон «О связи» предусматривает только проведение ОРМ, ограничивающих права и свободы граждан. Автор исследования приходит к мнению, что проведение иных мероприятий возможно в соответствии с законом «Об оперативно-розыскной деятельности». Отметим, что приведенные положения являются довольно новыми и введены только с июля 2017 г. Фактически проведение отдельных ОРМ именно в сети Интернет четко регламентировано лишь несколько лет назад.

Федеральный закон «Об оперативно-розыскной деятельности» [5] не содержит ни одного упоминания такого понятия, как «Интернет», однако исходя из расширительного уяснения его положений можно прийти к логическому выводу о возможности осуществления ОРД в сети Интернет и ее соответствия действующему законодательству. Данный тезис обосновывает необходимость внесения изменений в положения ст. 6 ФЗ «Об оперативно-розыскной деятельности», закрепляющих возможность использования не только информационных систем, но и ИТКС для решения задач ОРД.

Статья 4 Федерального закона формулирует правовую основу проведения ОРМ, включая в нее нормативные акты, регламентирующие организацию и тактику проведения ОРД, издаваемые органами, осуществляющими ОРД в пределах своих полномочий в соответствии с законодательством РФ. В ст. 6 законодатель подчеркивает, что в ходе проведения ОРМ используются в том числе информационные системы, а также другие технические и иные средства, не наносящие ущерба



жизни и здоровью людей и не причиняющие вреда окружающей среде. Мероприятия, ограничивающие конституционные права граждан, должны проводиться только на основании судебного решения [5].

Рассматривая сеть Интернет как среду совершения преступлений, в том числе экстремистской направленности, и как современный способ распространения информации, большинство ОРМ, перечисленных в ст. 6 возможно проводить в ее условиях (опрос, наведение справок, отождествление личности и др.).

Считаем, что в цифровой среде при сборе информации в целях раскрытия преступлений экстремистской направленности целесообразно проводить следующие ОРМ:

- оперативный опрос с использованием социальных сетей, чатов, форумов и мессенджеров;

- наведение справок, имеющее черты оперативно-розыскного мониторинга сети Интернет, поиска сведений в поисковых интернет-системах (Google, Yandex, Baidu и др.), а также сбор информации с помощью иных программных продуктов и сервисов сети Интернет;

- отождествление личности, при котором используется специализированное, зачастую общедоступное программное обеспечение (например, идентификация пользователей по фотографиям, задействующая массив социальных сетей) для преодоления потенциального криминального противодействия правоохранительным органам.

Данный список не является исчерпывающим, однако приведенные примеры свидетельствуют о необходимости их более детального законодательного урегулирования в отношении используемых методов, технических средств, порядка проведения и способа фиксации полученных результатов.

Заметим, что введение в 2016 г. в ФЗ «Об оперативно-розыскной деятельности» нового вида оперативно-розыскного мероприятия «Получение компьютерной информации» [21] не сняло вопросов о конкретизации таковых сведений и оставляет данную дефиницию на усмотрение правоприменителя. На наш взгляд, показателен тот факт, что указанное ОРМ введено для установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности. Под получением компьютерной информации, по мнению А.Л. Осипенко, следует понимать специфический способ получения сведений, как правило, с применением специальных технических средств для добытия сведений, недоступных оперативному сотруднику без использования таковых [22, с. 85].

Отсюда возникает вопрос, является ли получение сведений из сети Интернет разновидностью соответствующего ОРМ или выступает разновидностью иных ОРМ (например, наведение справок). Учитывая приведенные выше аргументы, считаем, что по своей сути указанное ОРМ может проводиться и в интернет-среде. В случае если добывание оперативной информации происходит в процессе проведения иных ОРМ (например, опрос), но используется интернет-среда, без приме-



ния специальных технических средств фиксации информации, таковое ОРМ, на наш взгляд, не является «получением компьютерной информации».

Несмотря на прямое отсутствие в законе «Об оперативно-розыскной деятельности» упоминания о проведении ОРМ в сети Интернет, федеральные законы «Об информации, информационных технологиях и о защите информации» и «О связи» подразумевают проведение таковых.

В свою очередь, противодействие экстремизму в обществе также основывается на специально принятом правовом акте, относящемся к правовой основе ОРД в сети Интернет в условиях противодействия экстремизму. Так, ФЗ «О противодействии экстремистской деятельности» определяет противодействие экстремизму как приоритетную задачу уполномоченных органов. В рамках данного исследования привлекает внимание ст. 12 упомянутого Федерального закона, запрещающая использование сетей общего доступа для осуществления экстремистской деятельности. В случае использования указанных сетей в деструктивной деятельности применяются меры, указанные в Законе [19]. Исходя из того, что в данном случае Интернет выступает местом совершения преступления, документирование противоправных действий также будет осуществляться с его использованием с учетом всех доступных средств и методов ОРД.

Рассмотрев основные вопросы законодательного регулирования использования сети Интернет в оперативно-розыском противодействии преступлениям экстремистской направленности, целесообразно сформулировать следующие выводы.

Проанализированные нами нормативные правовые акты напрямую не предусматривают проведение ОРМ в сети Интернет, однако в широком смысле и не запрещают проведение таковых при условии соблюдения конституционных прав и свобод граждан или особого порядка получения таких данных при проведении ОРМ, определенных Федеральным законом.

Считаем, что отождествление проведения ОРМ в сети Интернет с таковыми на сетях сотовой связи или иных телекоммуникационных сетях ошибочно в силу существенных отличий их построения и функционирования. В то же время Интернет является разновидностью ИТКС ввиду своей природы и основ функционирования, что предполагает иной порядок проведения ОРМ в отличие от таковых мероприятий в сетях связи.

На наш взгляд, сеть Интернет выступает в первую очередь средой проведения таких мероприятий, требующей кардинально иного подхода к пониманию принципов получения информации, ее распространения и обработки. С учетом изложенного приходим к выводу о том, что сбор сведений в сети Интернет в целях противодействия преступности, в частности, экстремистской направленности, является допустимым и законным, а текущая правовая регламентация, несмотря на отсутствие единого подхода законодателя, достаточна для проведения соответствующих ОРМ.



В целях устранения потенциальных противоречий в правоприменительной практике при противодействии преступности, в том числе экстремистского характера, считаем целесообразным предусмотреть в ФЗ «Об оперативно-розыскной деятельности» возможность осуществления оперативно-розыскной деятельности в сети Интернет. Так, В. И. Шаров предлагает дополнить ст. 6 следующим абзацем: «Оперативно-розыскные мероприятия могут проводиться в сети Интернет в порядке и при соблюдении условий, определяемых настоящим Законом» [24, с. 85]. Данное предложение, на наш взгляд, является дискуссионным, так как не в полной мере учитывает специфику получения данных, их обработку и способы взаимодействия между пользователями в сети. В то же время такая формулировка очерчивает возможность проведения ОРМ в сети Интернет и не вступает в противоречие с духом и буквой Закона. Частично соглашаясь с данным мнением, считаем необходимым предусмотреть возможность проведения ОРМ не только в сети Интернет, но и в цифровой среде в целом, где Интернет выступает одним из важнейших компонентов. Таким образом, целесообразно дополнить приведенную выше статью абзацем следующего содержания: «Оперативно-розыскные мероприятия могут проводиться в цифровой среде в порядке и при соблюдении условий, определяемых настоящим Законом».

Кроме того, для конкретизации возможности использования сети Интернет в реализации задач ОРД представляется целесообразным дополнить ст. 6 ФЗ «Об оперативно-розыскной деятельности» и изложить абз. 3 в следующей редакции: «В ходе проведения оперативно-розыскных мероприятий используются информационные системы, информационно-телекоммуникационные сети, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде».

Данные предложения в законодательство, на наш взгляд, с одной стороны, конкретизируют возможность использования сети Интернет при проведении устоявшихся в правоохранительной деятельности ОРМ, а с другой — открываются новые перспективы для оперативного внедрения новейших технологий в ОРД.

Список литературы

1. *Вязовец Р. Н.* Использование информационных технологий в оперативно-розыскной деятельности органов внутренних дел : автореф. дис. ... канд. юр. наук. М., 2010.
2. *Осипенко А. Л.* Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского Института МВД России. 2015. № 2. С. 10–13.
3. *Алябьев А. А., Лагуточкин А. В.* Проблемы осуществления оперативно-розыскных мероприятий в информационном пространстве сети Интернет // Проблемы правоохранительной деятельности. 2013. № 1. С. 66–69.
4. *Кулешов Р. В.* Правовое регулирование оперативно-боевого противодействия экстремистской и террористической деятельности // Вестник Санкт-Петербургского университета МВД России. 2013. № 1 (57). С. 80–83.



5. *Об оперативно-розыскной деятельности* : федер. закон от 12.08.1995 г. №144-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Шумилов А.Ю. Проблемы законодательного регулирования в оперативно-розыскной деятельности: десять лет спустя (конституционные, административные, уголовные, уголовно-процессуальные и уголовно-сыские аспекты) : монография. 2-е изд., испр. и доп. М., 2008.

7. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г., с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 г. №6-ФКЗ, от 30.12.2008 г. №7-ФКЗ, от 05.02.2014 г. №2-ФКЗ, от 21.07.2014 г. №11-ФКЗ). URL: <http://www.constitution.ru/> (дата обращения: 21.05.2020).

8. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. №174-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

10. Декларация о свободе обмена информацией в интернете (принята Комитетом Министров Совета Европы от 28 мая 2003 г. на 840-м заседании заместителей Министров). Доступ из справ.-правовой системы «КонсультантПлюс».

11. Средства массовой информации и терроризм: Рекомендации Парламентской ассамблеи Совета Европы №1706 (2005) ; Декларация Комитета министров Совета Европы о свободе выражения мнения и информации в СМИ в контексте борьбы с терроризмом (2005) // Журналистика и СМИ против террора. М., 2009. С. 269 – 274.

12. О вопросах саморегулирования виртуального содержания (саморегулирование и охрана пользователей от противоправного или причиняющего вред содержания новых информационных и коммуникационных услуг) : рекомендация №R (2001) 8 Комитета министров Совета Европы (принята 05.09.2001 г. на 762-м заседании представителей министров). Доступ из справ.-правовой системы «КонсультантПлюс».

13. Немкова Н.А. Особенности правового регулирования оперативно-розыскных мероприятий в сетях связи // Проблемы правоохранительной деятельности. 2009. №1-2. URL: <https://cyberleninka.ru/article/n/osobennosti-pravovogo-regulirovaniya-operativno-rozysknyh-meropriyatij-v-setyah-svyazi> (дата обращения: 20.05.2020).

14. *Case of Segerstedt-Wiberg and Others v. Sweden*. URL: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591> (дата обращения: 20.05.2020).

15. Конвенция о защите прав человека и основных свобод (заключена в Риме 04.11.1950 г., с изм. от 13.05.2004 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

16. Ташмагамбетов А.М. Оперативно-розыскные мероприятия с использованием социальных сетей: опыт Великобритании и Республики Казахстан // Наука и бизнес: пути развития. 2013. №11 (29). С. 129 – 133.

17. О связи : федер. закон от 07.07.2003 г. №126-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

18. Об информации, информационных технологиях и о защите информации : от 27.07.2006 г. №149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

19. О противодействии экстремистской деятельности : федер. закон от 25 июля 2002 г. №114-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

20. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».



21. 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 : федер. закон от 06.07.2016 г. №374-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

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

23. *Старичков М.В.* Понятие «Компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. 2014. №1 (68). URL: <https://cyberleninka.ru/article/n/ponyatie-kompyuternaya-informatsiya-v-rossiyskom-ugolovnom-prave> (дата обращения: 20.05.2020).

24. *Шаров В.И.* Оперативно-розыскные мероприятия в сети Интернет // Общество и право. 2018. №2 (64). С. 82 – 86.

Об авторе

Алексей Владимирович Кутузов – адъюнкт, Ростовский юридический институт Министерства внутренних дел Российской Федерации, Россия.

E-mail: kutuzovlist@yandex.ru

The author

Alexsei V. Kutuzov, adjunct, Rostov Law Institute of the Ministry of internal affairs of the Russian Federation, Russia.

E-mail: kutuzovlist@yandex.ru