Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2019. – Т. 5 (71). № 2. – С. 154-162.

УДК 323.283:343.1

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СЕТЬ ИНТЕРНЕТ КАК ПРИОРИТЕТНЫЙ ИСТОЧНИК ПОЛУЧЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

Кутузов А. В.

Ростовский юридический институт Министерства внутренних дел Российской Федерации

В статье обоснована необходимость использования информационно-телекоммуникационной сети Интернет при раскрытии преступлений, в особенности экстремистской направленности. Проанализированы преимущества и недостатки информационных возможностей ресурсов сети Интернет при противодействии экстремизму. Особое внимание уделено достоверности сведений, размещенных на ресурсах информационно-телекоммуникационной сети Интернет. Предоставлены предложения по улучшению деятельности подразделений полиции в части поиска оперативно-значимой информации в сети Интернет.

Ключевые слова: Правоохранительные органы, противодействие экстремизму, сеть Интернет, информационно-телекоммуникационные сети, оперативно-значимая информация.

На сегодняшний день внедрение и использование информационных технологий занимает одно из приоритетных направлений государственной политики, в том числе и в правоохранительной сфере. Это обусловлено, тем фактом, что информационные процессы, происходящие в мире, оказывают значительное влияние не только на научно-техническую сферу, но и на широкий круг общественных отношений.

Значительные темпы роста информатизации общества расширяют спектр выполняемых задач по противодействию преступности органами внутренних дел. В частности, в последнее десятилетие, таковым является борьба с проявлениями экстремизма в общества, в частности противодействие преступлениям экстремистской направленности. В отличие от сотрудников правоохранительных органов, субъекты преступлений экстремистской направленности более обширно и предметно используют информационные технологии при осуществлении своей противоправной деятельности [4, с. 42]. Это вызывает необходимость применения возможностей информационно-телекоммуникационной сети Интернет в рамках борьбы с отдельными видами преступности, особенно экстремистского характера.

Вполне закономерно, что эффективность деятельности органов внутренних дел в сфере противодействия преступности напрямую зависит от своевременного реагирования на различные изменения в социально-культурных процессах, происходящих в обществе. В настоящее время одним из перспективных направлений деятельности оперативных подразделений полиции является широкое использование альтернативных источников приобретения оперативно-значимой информации. Данное положение обусловлено необходимостью получения наиболее полных сведений о субъекте преступления, его связях (как криминальных, так и социально-бытовых), способах и методах совершения преступления, а также выяснения иных обстоятель-

ств, информацию о которых невозможно или затруднительно добыть с помощью традиционных средств и методов оперативно-розыскной деятельности.

Невзирая на снижение количества зарегистрированных преступлений экстремистского характера в последнее время [1], не следует недооценивать социальную опасность данного вида преступного посягательства на общественные отношения. В связи с тем, что официальная статистика, в частности Генеральной прокуратуры Российской Федерации, не учитывает способ и место совершения преступлений экстремистской направленности, а только приводит количество возбужденных и направленных в суд уголовных дел, представляется затруднительным достоверно определить данные о способах совершения экстремистских преступлений. В то же время, по мнению подавляющего большинства исследователей, одним из наиболее распространенных способов распространения идей экстремизма является широкое использование возможностей сети «Интернет» [3]. Отдельно отметим, что согласно анализа материалов уголовных дел, возбужденных по ст. 280 УК РФ (публичные призывы к осуществлению экстремистской деятельности), проведенного А.В. Петриняном [9], в 87,5 % случаев, то есть в 7 из 8 случаев, экстремистские материалы распространялись именно с использованием сети Интернет.

Значительная роль в необходимости всестороннего использования возможностей сети Интернет при раскрытии и расследовании преступлений экстремистской направленности проявляется самой конструкцией уголовно-правовой нормы, изложенной в ст. 280 УК РФ. Так, дефиниция части 2 указанной статьи указывает на квалифицирующий признак «те же деяния, совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет» [11]. Учитывая способ и место совершения экстремистских преступлений и существенную роль сети Интернет при подготовке и осуществлении преступлений данной категории [10, с. 62-63], сотрудники полиции должны эффективнее применять на практике оперативно-розыскной инструментарий. По нашему мнению, таковым является как сама сеть Интернет, так и её ресурсы, доступные среднестатистическому пользователю.

Отметим, что в ряде случаев, сведения, полученные об объекте оперативного интереса из открытых источников, являются более информативными и представляют не меньший интерес, чем данные, содержащиеся в ведомственных базах данных. В связи с этим, в современных условиях информационно-аналитическое обеспечение деятельности подразделений полиции позиционируется как важнейший элемент своевременного информационного противодействия и борьбы с экстремистскими проявлениями, так и преступностью в общем.

Использование современных Интернет-технологий, в частности поисковых систем, социальных сетей, мессенджеров и иных ресурсов Глобальной Сети является необходимым условием для эффективной деятельности по предупреждению и раскрытию преступлений. В то же время, необходимо признание факта применения Интернет-ресурсов в оперативно-розыскной и криминалистической науке с последующим распространением в иные сферы научной деятельности.

В связи с повсеместным распространением сети Интернет, сотрудники правоохранительных органов в своей практике все чаще используют возможности глобальной международной информационной сети для выполнения задач, возложенных на них. Как отмечает В.И. Шаров, сотрудники полиции при использовании ре-

сурсов Интернет не опираются на какие-либо разработанные методики, а руководствуются в большей степени интуицией [13, с. 114]. В частности, применяют базовые навыки, полученные в ходе обучения в общеобразовательных и высших учебных заведениях. Следует обратить внимание на то, что согласно результатам проведенного исследования [13, с. 113], сотрудники оперативных подразделений системы МВД России в рамках работы по оперативным делам используют сеть Интернет «довольно часто» или «часто» (в 56,8% случаях).

Процессы интернетизации представляют субъектам оперативно-розыскной деятельности дополнительную возможность установления обстоятельств событий, поиска очевидцев, выявления и анализа фото- и видеоматериалов, получения первичной информации в отношении правонарушителя. Отметим, что данная информация не всегда соответствует требованиям допустимости в рамках уголовного процесса и не в полной мере может является доказательством [7], но в тоже время может использоваться исключительно как ориентирующая информация для оперативного сотрудника или следователя.

Исходя из вышеизложенного, необходимо более предметно очертить основные источники информации, размещенные в ресурсах сети Интернет, которые целесообразно использовать при раскрытии преступлений экстремистского характера. Таковыми являются:

1) поисковые системы: «ya.ru», «rambler.ru», «google.com» и другие. Отметим, что в зависимости от региональных особенностей (настроек), данные поисковые сервисы порой могут предоставлять диаметрально противоположные результаты поиска, что обуславливает необходимость их применения в конкретной ситуации, тщательной перепроверки полученных результатов;

2) специальные базы данных, доступные для любого пользователя Сети: сервисы Государственной инспекции безопасности дорожного движения МВД России (проверка транспортного средства, административные правонарушения и другое), Федеральной налоговой службы (проверка идентификационного номера налогоплательщика), Федеральной службы судебных приставов (наличие исполнительных производств в отношении конкретного гражданина), иных государственных органов власти, находящихся в свободном доступе. Принимая во внимание тенденции государственной политики в части повышения доступности государственных услуг населению и курса на цифровизацию экономики [14], можно сделать вывод о том, что количество таких сервисов будет только увеличиваться;

3) сайты-справочники, энциклопедии, досье о личности сотрудника (например, резюме, сопроводительные и рекомендационные письма, размещенные на ресурсах поиска работы с указанием значительного объема персональных данных), компании, организации: сайты-справочники, агрегаторы, собирающие сведения о лице в автоматическом режиме;

4) официальные сайты органов государственной власти, хозяйствующих субъектов, политических и общественных организаций, а также сайты информационных агентств;

5) форумы, чаты, блоги и социальные сети.

Вместе с тем, нельзя не отметить тот факт, что в ряде случаев, возможности сети Интернет в контексте поиска информации, необходимой при раскрытии и расследовании преступлений, особенно экстремистской направленности, лишены недостат-

ков, присущих базам данных, находящихся в распоряжении сотрудников полиции и формируемых подразделениями МВД России. К таковым несовершенствам целесообразно отнести следующее: узкоспециализированный, ведомственный характер поступления и накопления информации, отсутствие возможности получения и объединения сведений из разных ведомственных источников в автоматическом режиме, сложность в комплексной обработке и детализированном анализе интересующих данных в режиме онлайн, а также ограниченный доступ (по субъекту и порядку обработки). Таким образом, использование ИТКС Интернет в ряде случаев позволяет решить данные проблемы при раскрытии и расследовании преступлений.

Говоря о необходимости использования ресурсов ИТКС Интернет как источника информации в оперативно-розыскной деятельности, необходимо определить, соответствует ли она критериям, выработанным наукой оперативно-розыскной деятельности, предъявляемой к оперативно-розыскной информации. Данные требования были сформулированы С.С. Овчинским, согласно которому оперативно-разыскная информация представляет собой вид социальной информации, специфичной по цели получения (борьба с преступностью), методам получения и режиму использования, обеспечивающему конспирацию, надежную зашифровку источников, возможность проверки сообщаемых сведений и их применение в целях профилактики, предупреждения и пресечения преступной деятельности [6, с. 33].

Учитывая приведенные выше положения можно сделать вывод, что информация, получаемая из открытых источников, в том числе из сети Интернет, отвечает очерченным требованиям конспирации и зашифровки источников, как с помощью технических средств (vpn-сервисы, анонимайзеры и другое), так и с помощью легендированных учетных записей на различных сайтах. Таким образом, выделим основные преимущества использования сети Интернет как источника оперативно-значимой информации при раскрытии преступлений, в том числе экстремистской направленности:

Финансовые затраты и скорость применения. Информационные системы ОВД нуждаются в комплексном техническом сопровождении и обслуживании, которые обусловливают значительные материальные затраты. Обработка информации с ограниченным доступом требует дополнительной установки технических средств защиты и категорирования в установленном Законом порядке. В отличие от этого, материальные затраты, связанные с использованием возможностей ресурсов Интернет, ограничиваются только необходимым количеством компьютеров, подключенных к сети Интернет, оплатой доступа и трафика (объема полученной информации). Также немаловажным фактором является мобильность и скорость Интернет-соединения, что прямо отражается на возможности получения необходимых сведений в достаточном объеме и режиме реального времени, текущего и перспективного планирования оперативно-розыскных и следственных мероприятий.

Динамический характер информации. Интернет позволяет получить как информацию о событиях, имевших место несколько лет назад (как правило – первоисточник), так и актуальную информацию при её появлении, либо изменении. В частности, речь идет о связях лиц, представляющих оперативный интерес, их образе жизни и будущих планах. В ряде случаев, сотрудник полиции может целенаправленно не отслеживать активность пользователя вручную, а использовать push-

уведомления, рассылки посредством электронной почты и встроенные инструментарий различных сайтов.

Интуитивность использования. Как правило, подавляющее большинство сайтов создаются для возможности использования среднестатистическими пользователями, не имеющие технического или иного специального образования. Сотрудник полиции не нуждается в специальной подготовке по поиску необходимой информации, так как в ряде случаев он использует аналогичные сервисы и приложения в своей повседневной жизни. В то же время, для достижения качественных и действенный результатов необходимо постоянное усовершенствование методических разработок по использованию ресурсов Сети на базе учебных заведений системы МВД России в тесном взаимодействии с оперативно-аналитическими подразделениями территориальных органов полиции.

Невзирая на неоспоримые преимущества ИТКС Интернет при поиске информации в интересах субъектов ОРД, необходимо указать и на ряд недостатков, присущих информации, размещенной в сети, а именно:

Информация в сети Интернет не всегда соответствует высоким стандартам достоверности. В ряде случаев, пользователи преднамеренно искажают сведения о себе на различных сайтах, в частности социальной направленности: указывают неверные установочные данные, публикуют фотографии мест и людей, не связанных с ними. Результаты исследований, проведенные независимыми экспертными организациями в разный период времени, свидетельствуют об этом. Например, по данным ВЦИОМ, каждый второй пользователь социальных сетей и блогов, как минимум 1 раз сообщал о себе неправду. Отметим, что наиболее часто это делают пользователи в возрасте от 18-24 лет [5]. Также стоит привести данные «Лаборатории Касперского», согласно которым, пользователи сайтов знакомств, в 58 % случаев не менее 1 раза указывали неверную информацию о себе, в том числе фотографию (75 % респондентов), что намного выше общемирового показателя (54 %), искаженные сведения о возрасте (50%) и семейном положении (40 %) [2].

Представленные результаты обусловлены, как правило, желанием сохранить анонимность в сети, выдать желаемые сведения за действительность, либо по иным причинам. В частности, лица, причастные к преступной деятельность, в том числе экстремистского характера, имеют возможность намеренно искажать данные с целью введения в заблуждение правоохранительных органов, сокрытия информационных следов, имеющих решающее значение при раскрытии преступлений. Указанные положения также подтверждают тезис, предполагающий необходимость учета возрастных особенностей пользователей Глобальной сети, степени владения техническими средствами. Таким образом, можно прийти к выводу, что не всякая информация, размещенная в сети Интернет является надежной и может быть использована в оперативно-розыскной и следственной деятельности.

Информация не имеет структурированной каталогизации (описание содержания и формы), а содержит только минимальную структуру информационных материалов, носит фрагментарный характер. Для успешного достижения поставленных задач, оперуполномоченный или следователь должен иметь представление о принципах поиска информации в сети, от особенностей конкретных социальных сетей до критериев запросов в поисковых системах. Кроме того, учитывая осведомленность злоумышленников о проведении в отношении них оперативно-розыскных

и следственных мероприятий, получение необходимых сведений становится более затруднительным.

Динамический характер сведений. В ряде случаев, информация на сайте может быть удалена в кратчайшие сроки (по требованию администрации сайта, жалобе лица, вследствие технических трудностей, др.). Одним из возможных вариантов решения данных проблем, на наш взгляд, является использование т.н. «кэша» страниц для их последующей обработки или использование возможностей Интернет-архива, например, Wayback Machine (https://archive.org) или инструментариев поисковых систем (yandex, google).

В контексте поиска информации и лицах, возможно причастных к экстремистской деятельности, по нашему мнению, целесообразно выделить еще одну особенность Глобальной сети – **ограниченный доступ к персональной информации пользователей**. Так, чтобы получить доступ к личным кабинетам на различных сайтах и Интернет-сервисах необходимо иметь логин и пароль, а в ряде случаев пройти и многоуровневую аутентификацию пользователя. В то же время, для преступников не представляет особой сложности получить ключи доступа к учетным записям пользователей в социальных сетях, аккаунтам к мобильным телефонам и прочей конфиденциальной информации, используя ресурсы т.н. «Даркнета» (Сегмент сети Интернет, не индексируемый обычными поисковыми машинами) [12]. Базы данных, формируемые сайтами продаются за сравнительно небольшую плату и позволяют получить детальные сведения о лице. В свою очередь, правоохранительные органы могут получить такие сведения только в установленном Законом порядке, что занимает несравнимо большее количество времени, чем у преступников. Кроме того, «взломанные» профили лиц на сайтах, могут содержать недостоверную информацию, а большая часть в конечном счете будет удалена или заблокирована.

Принимая во внимание неоспоримые преимущества сети Интернет и негативные явления, возникающие в связи с этим, очертим основные направления использования ресурсов всемирной информационно-телекоммуникационная сети при раскрытии и расследования преступлений экстремистского характера:

- Мониторинг сети Интернет для предупреждения и раскрытия преступлений (выявление сайтов, с помощью которых распространяются экстремистские материалы, обнаружение противоправного контента и другое). По мнению ученых, занимающихся разработкой данной проблематики, мониторинг сети целесообразно проводить в автоматическом режиме с использованием специализированного программного обеспечения [8, с. 14], что позволяет не только более рационально использовать человеческие ресурсы, но и охватить наибольший объем информации с учетом значительной динамики ее увеличения;
- Поиск информации на тематических сайтах, форумах, в социальных сетях о готовящихся и совершенных преступлениях. К таковым возможно отнести закрытые форумы, группы в социальных сетях, каналы в мессенджерах, где происходит пропаганда идей, проводится агитационная и вербовочная деятельность участниками запрещенных организаций и сообществ;
- Сбор сведений о лицах, представляющих оперативный интерес для сотрудников полиции (как о фигурантах уголовных дел, так и об их связях из близкого

окружения). Особое внимание необходимо уделять социальным сетям и сведениям, содержащиеся в них для последующего анализа и планирования дальнейших поисковых мероприятий.

Подводя итог, следует подчеркнуть, что в настоящее время, возможности ресурсов Интернет не столь широко и активно используются в отечественной правоохранительной деятельности, в частности при раскрытии и расследовании преступлений экстремистского характера. В современных условиях деятельность правоохранительных органов должна основываться на синтезе традиционных и новейших методов предупреждения и раскрытия преступлений, повышения возможностей оперативного реагирования на изменяющиеся условия окружающей действительности. В данном контексте сеть Интернет позволяет своевременно и эффективно противодействовать проявлениям преступности, в т.ч. экстремистской направленности.

Невзирая на очевидные преимущества применения возможностей ресурсов ИТКС Интернет при поиске оперативно-значимой информации для решения задач ОРД, остаются и проблемы, нуждающиеся в оперативном решении. Среди таковых необходимо выделить значительные объемы информации, подлежащей квалифицированной аналитической обработке, а также т.н. «информационный шум» и умышленное искажение событий, позволяющее ввести в заблуждение как обычных пользователей, так и представителей правоохранительных органов.

Очерченные положения позволяют говорить о необходимости правовой регламентации проведения оперативно-розыскных мероприятий в сети Интернет, дальнейшей разработки специализированных методик выявления преступлений экстремистского характера с использованием сети Интернет, механизмов поиска дополнительной оперативно-значимой информации на Интернет-ресурсах в отношении лиц, представляющих интерес для оперативных сотрудников, а также её комплексный и всесторонний анализ, в том числе с использованием автоматизированных программно-технических комплексов.

Список литературы

1. Генеральная прокуратура Российской Федерации. Состояние преступности в России. URL: https://genproc.gov.ru/upload/iblock/2b7/sbornik_8_2018.pdf (дата обращения: 10.01.2019).
2. Кругом обман: «Лаборатория Касперского» рассказала об опасностях на сайтах знакомств. URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-investigates-dangers-of-dating-sites (дата обращения: 10.01.2019).
3. Миц Д. С. Противодействие экстремизму в современной России // Вестник Прикамского социального института. 2017. №2 (77). URL: https://elibrary.ru/download/elibrary_30102229_98910653.pdf (дата обращения: 15.01.2019).
4. Нерубенко А.С., Елисеева Е.С. Экстремизм как социально-правовое явление: распространение экстремистских материалов в сети Интернет // Вестник БелЮИ МВД России. 2018. №1. – С. 41-44.
5. О чем врут пользователи социальных сетей? URL: https://wciom.ru/index.php?id=236&uid=1742 (дата обращения: 10.01.2019).
6. Овчинский А. С. Информация и оперативно-розыскная деятельность: Монография / Под ред. заслуженного юриста Российской Федерации, доктора юридических наук, профессора В.И. Попова. — М.: ИНФРА-М, 2002. - 97 с.
7. Озеров И. Н., Черкасова Е. А., Капустина И. Ю. Допустимость доказательств в уголовном судопроизводстве: сущность и значение // ППД. 2013. №2. URL: https://cyberleninka.ru/article/n/dopustimost-dokazatelstv-v-ugolovnom-sudoproizvodstve-suschnost-i-znachenie (дата обращения: 14.01.2019). с 67-69.
8. Осипенко А. Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник ВИ МВД России. 2015. №2. - С. 13-19.
9. Петрянин А. В. Уголовно-правовые, оперативно-разыскные и криминалистические механизмы противодействия экстремизму в телекоммуникационных сетях и сети «Интернет»: на примере статьи 280 УК РФ // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. №1 (33). URL: https://cyberleninka.ru/article/n/ugolovno-pravovye-operativno-razysknye-i-

kriminalisticheskie-mehanizmy-protivodeystviya-ekstremizmu-v-telekommunikatsionnyh-setyah-i (дата обращения: 14.01.2019).
10. Самошин А.В., Горовой В.В. Особенности предупреждения распространения экстремистских материалов в молодежной среде по глобальной сети Интернет // Труды Академии управления МВД России. 2016. №3 (39). – С. 61-65.
11. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 10.01.2019).
12. Узденов Р. М. «Новые границы киберпреступности» // Всероссийский криминологический журнал. 2016. [Электронный ресурс]. – URL:https://cyberleninka.ru/article/n/novye-granitsy-kiberprestupnosti (дата обращения:
10.01.2019).
13. Шаров В.В. Интернет как источник оперативно-разыскной и процессуальной информации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. №3 (35). – С. 111-114.
14. Юдина Т. Н. Цифровизация как тенденция современного развития экономики российской Федерации: Pro y contra // Государственное и муниципальное управление. Ученые записки СКАГС. 2017. №3. URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-kak-tendentsiya-sovremennogo-razvitiya-ekonomiki-rossiyskoy-federatsii-pro-y-contra (дата обращения: 14.01.2019).

Kutuzov A. V. Internet as a priority source of operational-relevant information in the disclosure of crimes of an extremist nature // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2019. – T. 5 (71). № 2. – P. 154-162.

The article substantiates the need to use Internet technologies in detecting crimes, especially related to extremism. The strengths and flaws of the information capacity of the Internet resources are also covered in the article. Special attention is given to the reliability of the information published on the Internet. There are suggestions proposed for improvement of the police forces activities in search for essential operational information on the Internet.

Keywords: Law enforcement agencies, countering extremism, the Internet, information and telecommunication networks, operational-relevant information

Spisok literatury

1. General'naya prokuratura Rossijskoj Federacii. Sostoyanie prestupnosti v Rossii. URL: https://genproc.gov.ru/upload/iblock/2b7/sbornik_8_2018.pdf (data obrashcheniya: 10.01.2019).
2. Krugom obman: «Laboratoriya Kasperskogo» rasskazala ob opasnostyah na sajtah znakomstv. URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-investigates-dangers-of-dating-sites (data obrashcheniya: 10.01.2019).
3. Mic D. S. Protivodejstvie ehkstremizmu v sovremennoj Rossii // Vestnik Prikamskogo social'no-go instituta. 2017. №2 (77). URL: https://elibrary.ru/download/elibrary_30102229_98910653.pdf (data obrashcheniya: 15.01.2019).
4. Nerubenko A.S., Eliseeva E.S. EHkstremizm kak social'no-pravovoe yavlenie: rasprostranenie ehkstremistskih materialov v seti Internet // Vestnik BelYUI MVD Rossii. 2018. №1. – S. 41-44.
5. O chem vrut pol'zovateli social'nyh setej? URL: https://wciom.ru/index.php?id=236&uid=1742 (data obrashcheniya: 10.01.2019).
6. Ovchinskij A. S. Informaciya i operativno-rozysknaya deyatel'nost': Monografiya / Pod red. zasluzhennogo yurista Rossijskoj Federacii, doktora yuridicheskih nauk, professora V.I. Popova. — M.: INFRA-M, 2002. - 97 s.
7. Ozerov I. N., CHerkasova E. A., Kapustina I. YU. Dopustimost' dokazatel'stv v ugolovnom sudoproizvodstve: sushchnost' i znachenie // PPD. 2013. №2. URL: https://cyberleninka.ru/article/n/dopustimost-dokazatelstv-v-ugolovnom-sudoproizvodstve-suschnost-i-znachenie (data obrashcheniya: 14.01.2019). s 67-69.
8. Osipenko A. L. Novye tekhnologii polucheniya i analiza operativno-rozysknoj informacii: pravo-vye problemy i perspektivy vnedreniya // Vestnik VI MVD Rossii. 2015. №2. - S. 13-19.
9. Petryanin A. V. Ugolovno-pravovye, operativno-razysknye i kriminalisticheskie mekhanizmy protivodejstviya ehkstremizmu v telekommunikacionnyh setyah i seti «Internet»: na primere stat'i 280 UK RF // YUridicheskaya nauka i praktika: Vestnik Nizhegorodskoj akademii MVD Rossii. 2016. №1 (33). URL: https://cyberleninka.ru/article/n/ugolovno-pravovye-operativno-razysknye-i-kriminalisticheskie-mehanizmy-protivodeystviya-ekstremizmu-v-telekommunikatsionnyh-setyah-i (data obrashcheniya: 14.01.2019).
10. Samoshin A.V., Gorovoj V.V. Osobennosti preduprezhdeniya rasprostraneniya ehkstremistskih materialov v molodezhnoj srede po global'noj seti Internet // Trudy Akademii upravleniya MVD Rossii. 2016. №3 (39). – S. 61-65.

11. Ugolovnyj kodeks Rossijskoj Federacii ot 13.06.1996 N 63-FZ (red. ot 27.12.2018) (s izm. i dop., vstup. v silu s 08.01.2019) URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (data obrashche-niya: 10.01.2019).
12. Uzdenov R. M. «Novye granicy kiberprestupnosti» // Vserossijskij kriminologicheskij zhurnal. 2016. [EH-lektronnyj resurs]. – URL:https://cyberleninka.ru/article/n/novye-granitsy-kiberprestupnosti (data obrash-cheniya:
10.01.2019).
13. SHarov V.V. Internet kak istochnik operativno-razysknoj i processual'noj informacii // YUridi-cheskaya nauka i praktika: Vestnik Nizhegorodskoj akademii MVD Rossii. 2016. №3 (35). – S. 111-114.
14. YUdina T. N. Cifrovizaciya kak tendenciya sovremennogo razvitiya ehkonomiki rossijskoj Federa-cii: Pro y contra // Gosudarstvennoe i municipal'noe upravlenie. Uchenye zapiski SKAGS. 2017. №3. URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-kak-tendentsiya-sovremennogo-razvitiya-ekonomiki-rossiyskoy-federatsii-pro-y-contra (data obrashcheniya: 14.01.2019).
.