Северо-Кавказский юридический вестник. 2024. № 4. С. 153–161
North Caucasus Legal Vestnik. 2024;(4):153–161
Проблемы уголовного и процессуального права
Научная статья
УДК 343.85
https://doi.org/10.22394/2074-7306-2024-1-4-153-161 EDN TMXBMC

Актуальные проблемы проведения оперативно-розыскных мероприятий, направленных на раскрытие публичных призывов к осуществлению террористической деятельности посредством сети Интернет

Владимир Федорович Попов[1], Оксана Андреевна Полещук[2], Валентин Геннадьевич Выстропов[3]

[1, 2]Федеральное государственное казенное учреждение дополнительного профессионального образования «Всероссийский институт повышения квалификации сотрудников Министерства внутренних дел Российской Федерации», Домодедово, Россия
[3]Академия управления МВД России, Москва, Россия

[1]popov19102791@mail.ru
[2]oxanapoleshchuk@gmail.com
[3]mvd_vystropov@mail.ru

Аннотация. За последние несколько лет наблюдается устойчивый рост преступлений, предусмотренных ст. 205.2 УК РФ. По этой причине возникла необходимость совершенствования методики проведения оперативно-розыскных мероприятий, основанной на глубинных исследованиях механизма совершения исследуемого преступного деяния, присущего на сегодняшний день.

В первую очередь необходимо проанализировать состав публичных призывов к осуществлению террористической деятельности, публичных оправданий терроризма или пропаганды терроризма, выявить его отличительные черты от смежных преступных деяний и дать ему оперативно-розыскную характеристику.

Далее авторами статьи предлагаются к рассмотрению те оперативно-розыскные мероприятия, которые по их мнению обладают большей эффективностью для раскрытия указанного преступления.

Согласно статистическим данным подавляющая часть публичных призывов к осуществлению террористической деятельности совершается посредством сети Интернет, по этой причине приобретает актуальность разработка инновационных компьютерных программ, позволяющих проводить мониторинг огромного потока информации с целью выявления признаков рассматриваемого преступного деяния. При этом важно не только выявить информацию о фактах преступления, но осуществить наблюдение в рамках проведения оперативно-розыскных мероприятий за пользователем определённого сайта, с целью получения его изображения, определения его местонахождения и привлечения к уголовной ответственности.

Ключевые слова: оперативно-розыскные мероприятия, оперативно-розыскная характеристика, публичные призывы, терроризм, способ совершения преступления, информационное пространство, сеть Интернет, целевая аудитория, оперативно-розыскной мониторинг, искусственный интеллект, наблюдение, инновационное программное обеспечение

Для цитирования: Попов В. Ф., Полещук О. А., Выстропов В. Г. Актуальные проблемы проведения оперативно-розыскных мероприятий, направленных на раскрытие публичных призывов к осуществлению террористической деятельности посредством сети Интернет // Северо-Кавказский юридический вестник. 2024. № 4. С. 153–161. https://doi.org/10.22394/2074-7306-2024-1-4-153-161. EDN TMXBMC

Problems of Criminal and Procedural Law

Original article

Actual problems of conducting operational search activities aimed at uncovering public calls for terrorist activities via the Internet

Vladimir F. Popov[1], Oksana A. Poleshchuk[2], Valentin G. Vystropov[3]

[1, 2]Federal State Institution of Additional Professional Education "All-Russian Institute for Advanced Training of Employees of the Ministry of Internal Affairs of the Russian Federation", Domodedovo, Russia

[3]Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia

[1]popov19102791@mail.ru

[2]oxanapoleshchuk@gmail.com

[3]mvd_vystropov@mail.ru

Abstract. Over the past few years, there has been a steady increase in crimes under Article 205.2 of the Criminal Code of the Russian Federation. For this reason, there was a need to improve the methodology of conducting operational investigative measures based on in-depth studies of the mechanism of committing the investigated criminal act, which is inherent today.

First of all, it is necessary to analyze the composition of public calls for terrorist activities, public justifications of terrorism or propaganda of terrorism, identify its distinctive features from related criminal acts and give it an operational investigative characteristic.

Further, the authors of the article propose for consideration those operational investigative measures that, in their opinion, are more effective in solving the specified crime.

Taking into account the fact that most of the public calls for terrorist activities are committed on the Internet, it becomes relevant to develop innovative computer programs that allow monitoring a huge flow of information in order to identify signs of the criminal act in question. At the same time, it is important not only to identify information about the facts of the crime, but to carry out surveillance within the framework of operational investigative measures for the user of a certain site, in order to obtain his image, determine his location and bring him to criminal responsibility.

Keywords: operational investigative measures, operational investigative characteristics, public appeals, terrorism, method of committing a crime, information space, Internet, target audience, operational investigative monitoring, artificial intelligence, surveillance, innovative software, artificial intelligence

For citation: Popov V. F., Poleshchuk O. A., Vystropov V. G. Actual problems of conducting operational search activities aimed at uncovering public calls for terrorist activities via the Internet. *North Caucasus Legal Vestnik.* 2024;(4):153–161. (In Russ.). https://doi.org/10.22394/2074-7306-2024-1-4-153-161. EDN TMXBMC

Введение

Вопрос относительно обеспечения информационной безопасности представляет собой главенствующее направление внешней политики Российской Федерации. Любое государство стремится поддержать информационную безопасность, поскольку она опосредует его положение на международной арене, в связи с чем правительство нашей страны особо подходит к решению этой задачи.

Распространение и насаждение идеологии антиценностей, терроризма, экстремизма в информационном пространстве представляет такую же степень общественной опасности, например, как незаконный оборот запрещенных веществ.

Электронные и информационно-телекоммуникационных сети в качестве способа совершения преступления значительно увеличивают его степень общественной опасности, так как использование такого механизма обеспечивает простоту реализации преступного умысла, повышает возможности сокрытия преступных лиц, увеличивает их поток, способствует оперативному распространению информации негативного характера, в том числе террористической направленности.

За последнее время количество публичных призывов к осуществлению террористической деятельности, публичных оправданий терроризма или пропаганды терроризма (ст. 205.2 УК РФ)

выросло в разы (преимущественно совершены с использованием сети Интернет, социальных сетей мессенджеров и др.). Весомый вклад в этой связи составляют социальные сети, отличающиеся своей простотой и доступностью для осуществления коммуникации, с возможностью оставаться инкогнито на протяжении длительного периода времени, что необходимо для целей реализации террористических умыслов.

Так только за 2022 год подлежало регистрации около 983 преступлений, совершенных указанным способом[1]. В 2023 году в период с января по декабрь было зарегистрировано 548 преступлений по ст. 205 УК РФ[2], и хотя это количество уменьшилось, преобразованию подлежали способы маскировки их совершения посредством сети и выявления.

В настоящем исследовании авторы рассматривают наиболее привлекательные с точки зрения эффективности оперативно-розыскные мероприятия, способствующие раскрываемости публичных призывов к осуществлению террористической деятельности, совершённых в сети Интернет, и основные подходы к их организации.

Признак публичности

На сегодняшний день практически каждое развитое государство сталкивается с теми или иными преступными проявлениями террористического характера. Общественная опасность публичных призывов к осуществлению террористической деятельности заключается в непредсказуемости последствий, их масштабном характере. В связи с этим надлежит организовать проведение оперативно-розыскные мероприятий, таким образом, чтобы уже на стадии приготовления к совершению этого преступления, пресечь преступную деятельность. Относительно уже совершённого деяния, первостепенной задачей стоит зафиксировать обстоятельства при которых оно было совершено, а затем предстоит выявить и установить лиц, задействованных в его совершении.

Очевидно, что выбор определённых оперативно-розыскные мероприятий происходит исходя из учёта специфических черт объективной стороны конкретного состава преступления. Знания относительно оперативно-розыскных характеристик преступного деяния расширяет возможности оперативных сотрудников в построении оперативно-розыскной версии содеянного.

Для оперативно-розыскных мер, осуществляемых в рамках расследования публичных призывов к осуществлению террористической деятельности, присущи такие характерные черты как: поисково-справочный и наблюдательно – обследовательский характер, реализация посредством специальных негласных и гласных методов, использование средств, ориентируемых на обнаружение орудий преступления, иных обстоятельств, имеющих особое значение для целей построения следственной версии относительно уже совершённых деяний, его подробностей и предпосылок, лежащих в основе причинного комплекса, поиска причастных лиц, находящихся в розыске.

Как справедливо отмечает А. С. Синельников [1, с. 425] в процессе раскрытия публичных призывов к осуществлению террористической деятельности, недостаточно установить сам факт призыва в публичной форме. Вместе с тем он образует обязательный признак рассматриваемого состава, заключающийся в донесении информации хотя бы минимум двум людям, в любой доступной для восприятия форме. На практике аудитория гораздо шире и не приравнивается к пару человек, однако как отмечает И. А. Анисимова [2, с. 5] важно соблюсти формальный подход, достаточно чтобы информация, содержащая призывы поступила хотя бы до двух человек.

Относительно состава рассматриваемого преступного деяния отметим, что на его наличие не влияет тот факт получилось ли у виновного лица в результате его призывов вызвать готовность осуществлять террористическую деятельность хотя бы у одного человека или нет. Важно подчеркнуть, что призывы не имеют персонифицированный характер, а направлены на сознание широкой аудитории, рассчитаны воздействовать на массы. Вместе с тем, полагаем, что невозможно признать массовую рассылку СМС-сообщений, писем по электронной почте и т. д. в качестве публичного призыва, так как признак публичности не равен по содержанию такому признаку как массовость. Всё-таки нам близок подход тех правоведов, которые полагают, что массовость больше имеет

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 г. Официальный сайт МВД России. Доступно: мвд.рф/героГз/йет/35396677/ [Дата обращения: 12 октября 2024 г.].
[2] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 г. Официальный сайт МВД России. Доступно в://мвд.рф/героГз/йет/35396677/ [Дата обращения: 12 октября 2024 г.].

отношение к количеству, в то время как публичность – к качеству. Хотя бы один публичный призыв, воспроизведённый перед аудиторией, одновременно доступен для восприятия всем – это и есть качественный признак рассматриваемого явления.

На практике такой признак как публичность по рассматриваемой статье УК РФ[1] возможно доказать, если удастся найти более трёх свидетелей совершения преступного деяния, один из которых не являлся представителем его аудитории, что даст возможность провести отграничение публичных призывов к осуществлению террористической деятельности от смежных составов. Указанный признак детально изучается в научных кругах правоведов и потому является поводом для споров.

Фиксация содержания призыва

Крайне принципиально корректно зафиксировать содержание и призыва, для дальнейшего его изучения экспертами и дачи заключения относительно содержания в нём признаков объективной стороны либо их отсутствия. Именно исследование экспертами языковых единиц позволяет обнаружить элементы враждебности, влекущие пропаганду насилия, ненависти, дискриминации по признакам расы, национальности и пр.. Вместе с тем сам факт их обнаружения в ходе работы эксперта не даёт ещё полной картины относительно мотивов автора, его целей и задач, знания последствий, которые могут возникнуть в результате формулирования его мыслей посредством именно такого языкового приёма. Именно поэтому её результаты рассматриваются в суде в совокупности с другими доказательствами по уголовному делу.

Представляется универсальным для публичных призывов, а также для сообщений, направленных на оправдание или пропаганду терроризма, признак, состоящий в потенциальной опасности совершения хотя бы одного преступного деяния террористического характера. Однако не каждое обращение, хотя и направленное по факту на побуждение к совершению террористических преступлений, подлежит квалификации по ст. 205.2 УК РФ. Так как массово пользуются сетью Интернет именно лица молодёжного возраста, то вполне допустимо, что они необдуманно в силу возраста, а порой и спонтанно, могут разместить на своей страничке в социальной сети изображение, аудио- или видеофайл, текстовый файл, включающий в себя элементы экстремизма или терроризма, но, если не будет установлен умысел, характерный для анализируемой нормы, то привлечь их к уголовной ответственности представляется невозможным.

В соответствии с п. 21 постановления Пленума Верховного суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности»[2], по ч. 2 ст. 205.2 УК РФ надлежит подвергать оценке деяния, имеющие связь с призывами, подлежащими размещению на сайтах, форумах и блогах, а также в социальных сетях и мессенджерах. Судебная коллегия по делам военнослужащих Верховного Суда Российской Федерации закрепила в своём кассационном определении 08.07.2021 г.[3] вывод о том, что момент окончания преступления по ч. 2 ст. 205.2 УК РФ связан с фактическим размещением публичных призывов в сети Интернет.

Во многих случаях в ходе проведения оперативно-розыскных мероприятий возможно обнаружить совокупность нескольких признаков преступлений различной направленности, например, террористического и экономического характера либо террористического и экстремистского. В связи с этим сотрудникам становится всё труднее их выявить в огромном потоке информации в сети, что доказывает существование необходимости разработки новых инструментариев их эффективного обнаружения и фиксирования. Это позволит минимизировать риски, связанные с допущением юридических ошибок в процессе определения признаков конкретного состава, отграничения преступного деяния от других смежных составов.

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.10.2024) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

[2] Постановление Пленума Верховного Суда РФ от 09.02.2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (в ред. от 03.11.2016 г.) // Бюллетень Верховного Суда РФ. 2012. № 4.

[3] Кассационное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 08.07.2021 № 222-УД21-25-А6 Приговор: По ч. 2 ст. 205.2 УК РФ за публичное оправдание и пропаганду терроризма, совершенные с использованием информационно-телекоммуникационной сети Интернет, по двум эпизодам // Документ опубликован не был. СПС КонсультантПлюс. – URL https://online11. consultant.ru (дата обращения: 08.11.2024).

В этой связи Вугар Эдвар-оглы Гаджиев и М.Л. Демина [3, с. 67] отмечают, что оперативным работникам буквально приходится бороться за информацию в каждом отдельно взятом случае. Очевидно, что в настоящее время вручную не представляется возможным проводить обработку информации, равно как и посредством примитивных программ для компьютера, имевших успех скажем лет десять назад. Так как со временем претерпевают преобразования преступные проявления, то соответственно алгоритмы программ, созданные для выявления признаков публичных призывов к террористической деятельности должны подлежать изменению.

Приведём пример недавней разработки поисковой системы пермской компании «Сеуслаб» на основе датасета пермского ученого А. Рабчевского, с помощью которой представляется возможным произвести идентификацию пользователей социальных сетей, занимающихся распространением материалов экстремистского характера и выявить их роли[1]. Но как отмечает учёный математические модели, лежащие в основе системы, позволяют выявлять и пользователей, распространяющий такой деструктивный материал, как террористический. Она способна анализировать посты, лайки и комментарии. В основе такой системы лежат ключевые слова, при этом для каждого негативного явления составлен свой список слов. Отмечается, что рассматриваемая поисковая система уже используется более чем в половине территориальных управлений МВД РФ.

Сотрудники правоохранительных органов, имея представление относительно имеющихся способов обрабатывания огромного потока информации, установления соответствующих фильтров, ввиду колоссального массива информации могут просто не заметить значимые элементы сведений, носящих террористический оттенок.

Учитывая этот факт в научной литературе бытует представление о целесообразности организовать мониторинг социальных сетей в непрерывном автоматическом режиме, используя имеющиеся возможности инновационного специализированного программного обеспечения, дающего возможность сократить энергозатраты сотрудников и расширить диапазон интересующей информации.

Раскрытие преступных деяний, совершённых в сети Интернет осложнено рядом факторов: использование при совершении программного обеспечения, исключающего определение пользователя; своевременное очищение администрацией сайта ресурсов, материалов, имеющих террористический характер, а также данных благодаря которым правоохранительным органам представлялась возможность идентифицировать пользователя; сбои технического характера, например, оборудования аккумулирующего и хранящего информацию, дающего возможность идентифицировать пользователя и изобличить объективную сторону их преступных деяний. На этот счёт В. В. Бычков и В. А. Прорвич [4, с. 56] высказывают предложение использовать возможности некоторых компонентов искусственного интеллекта, возможности которого они раскрывают в своих научных трудах.

Необходимо обеспечить оперативных работников доказанными с научной точки зрения правовыми инструментами, раскрывающими возможности оперативным способом проводить обработку высокоскоростных потоков информации в режиме онлайн и обнаруживать признаки состава преступления.

С практической точки зрения важно грамотно подходить к процессу организации проведения оперативно-розыскных мероприятий, преследующих своей целью раскрыть публичные призывы к осуществлению террористической деятельности. Оперативным работникам надлежит учитывать следующие моменты на стадии организации оперативно-розыскных мероприятий: объём необходимых правоограничений относительно лица, в отношении которого они планируют проводиться; направленность его мотивов; способ, посредством которого было совершено преступное деяние; изучение тесного круга общения лица, которое представляет оперативный интерес; учёт требований о раздельном содержании подозреваемых, обвиняемых и осужденных; ряд других моментов и условий.

Для исключения втягивания к осуществлению террористической деятельности новой аудитории, сторонников, на наш взгляд, следует организовать постоянную работу по осуществлению защиты информационно-телекоммуникационных сетей, в том числе сети Интернет, на комплексной основе. Современный терроризм в условиях информационной пропаганды безусловно опасен для нашего общества. Ввиду этого назрела необходимость защиты современных средств коммуникации от их использования в качестве орудия пропаганды террористических идей террористами, использующими всё новые подходы и методы воздействия на сознание людей [5, с. 247].

[1] Российскими учеными создана система для выявления экстремистов в соцсетях. Интернет-портал СНГ пространство интеграции. Доступно в: https://e-cis.info/news/569/122492/ [Дата обращения: 08 ноября 2024 г.].

Оперативно-розыскной мониторинг

Сеть Интернет привлекательна для террористов своей открытостью, в связи с чем актуален её мониторинг в режиме нон-стоп. Ряд исследователей определяют оперативно-розыскной мониторинг (интернет-мониторинг) как перспективную разновидность направления оперативного поиска в сетевом информационном пространстве, представляющую собой комплексную систему оперативно-розыскных мероприятий, которые обеспечивают наблюдение за состоянием криминальных процессов в сетевой социальной среде, базирующуюся на применении средств и методов оперативно-розыскной деятельности [6, с. 236–237]. Мониторинг такого вида может опираться на реализацию оперативно-розыскных мероприятий, проводимых в сети, к примеру: опросы, наведение справок, непосредственное наблюдение и прочее.

Оперативно-розыскной мониторинг сетевых информационных ресурсов, представляющих интерес с точки зрения оперативно-розыскной работы осуществляется благодаря автоматизированному поиску, оперативно-розыскному изучению и наблюдению за общением, скрытым от других пользователей и имеющим элементы преступной деятельности.

С практической точки зрения будет полезен просмотр уведомлений о размещенных новостях в сомнительных сообществах, группах, «пабликах». В процессе проведения мониторинга следует делать акцент на данные об участии лиц, которые являются выходцами из регионов Северного Кавказа и Средней Азии; новостных «постах» религиозной и национальной тематики; информации, подлежащей размещению в информационных блоках аккаунтов – «Стена», «Аудиозаписи», «Видеозаписи», «Фотографии», «Сохраненные фотографии».

Иные оперативно-розыскные мероприятия

Необходимо не только отследить соответствующие сайты, заблокировать и удалить их в установленном законом порядке, а провести такие оперативно-розыскные мероприятия, как «Наблюдение» и «Оперативный эксперимент» [3, с. 67], поскольку спустя некоторое время преступники создадут новые сайты. Проведение указанных оперативно-розыскных мероприятий даст преимущество, заключающееся в возможности в ходе их проведения изобличить преступника посредством его фото либо видеоизображения и своевременно возбудить уголовное дело. Также оперативными сотрудниками может быть организовано непосредственное общение в онлайн режиме с автором или авторами призывов, но для определения их местонахождения также требуется проведение соответствующих оперативно-розыскных мероприятий.

Указанные выше обстоятельства свидетельствуют о необходимости проведения работы, опираясь на новейшие методики мониторинга информационного пространства в сети Интернет. Следует направленно отслеживать лиц, склонных к реализации публичных призывов, с целью организации и проведения разъяснительно-предупредительной работы в индивидуальном порядке.

Успех деятельности оперативных подразделений в области пресечения функционирования подобных сайтов будет обеспечен при условии активного взаимодействия со специализированными органами, осуществляющими задачи по выявлению и пресечению интернет-сайтов, которые включают информационные материалы противоправного характера, включая террористические и экстремистские, а также лиц, имеющих отношение к их публикации.

Следует отметить, что организация проведения оперативно-розыскных мероприятий всегда представляет собой комбинацию мыслительного процесса над восприятием конкретной ситуации для последующего выбора способов действий, переплетающийся с психологией относительно внутренней убеждённости лица действовать определенным образом, а никак иначе [1, с. 426].

А. А. Гребенщиков [7, с. 464] отмечает, что технология раскрытия преступного деяния, предусмотренного ст. 205.2 УК РФ совмещает в себе как общие приёмы, способы оперативно-розыскной работы, так и специальные методы расследования цифрового характера. Указанные методы ориентированы на сбор, анализ, реконструкцию цифровых следов, изъятие и проведение экспертизы компьютерной техники, активное внедрение в исследование специализированного программного обеспечения, предназначенного для того, чтобы обработать полученные данные, что предъявляет высокие критерии к квалификации и обладанию узкоспециализированными знаниями, навыками оперативными сотрудниками. Поскольку темпы развития цифровых технологий стремительно растут, возникают новые формы киберугроз, что вызывает необходимость совершенствования уже имеющихся методик, систематического повышения квалификации сотрудников.

Обобщив изученный в рамках обозначенной тематики материал, можно выделить следующие оперативно-розыскные мероприятия, способствующие раскрытию исследуемого преступления: проведение опроса; наведение справок; осуществление исследования предметов и документов; наблюдение с применением специальных технических средств; снятие информации с технических каналов связи; оперативное внедрение (предполагает проникновение оперативного работника в криминальную среду лиц, вынашивающих террористические намерения или склонных к совершению подобных преступлений, и добывание нужных сведений от самих объектов в целях недопущения и пресечения их преступной деятельности).

Отметим, что на практике одновременно могут совершаться несколько из указанных оперативно-розыскных мероприятий, что отвечает требованиям целесообразности и эффективности. Приведём пример, одновременно с опросом, могут быть проведены наблюдение, а также сбор образцов для сравнительного исследования [1, с. 426].

Принимая во внимание тот факт, что проведение некоторых оперативно-розыскных мероприятий связаны с ограничительными мерами относительно некоторых прав человека и гражданина, провозглашённых в Конституции Российской Федерации[1], то значительно суживаются пределы приёмов тактики их осуществления. В этом случае их результативность будет также находиться в зависимости от грамотного сочетания гласных и негласных методов оперативно-розыскной деятельности.

Авторы статьи полагают, что ограничение конституционных прав граждан в процессе осуществления мониторинга сети Интернет, возможно только на основании решения суда, вступившего в законную силу, аналогично с иными оперативно-розыскными мероприятиями.

Алгоритм выявления публичных призывов в сети Интернет

Главенствующим аспектом выявления и раскрытия анализируемого преступного деяния выступает деятельность именно оперативных подразделений органов внутренних дел, направленная на выявление, проверку и дальнейшее использование достоверной первичной информации в соответствии со следующей последовательностью:

1. Установление имени интернет-ресурса, где подлежала размещению преступная информация или аккаунта пользователя.

2. Установление юридического лица, зарегистрировавшего доменное имя или пользователя, а также местонахождение сайта.

3. Получение сведений об администраторах сайта, благодаря наведению справок у организации, указанной в предыдущем пункте.

4. Установление IP-адреса, посредством которого распространялась информация террористического характера, а так же телефонные номера и другие данные.

5. Определение интернет-провайдера, за которым зарегистрированы IP-адреса, а также отработка иной оперативно-значимой информации.

6. Установление конечных сведений IP-адресов и оборудования [8, с. 137].

Информация, которую удалось получить в результате пошагового выполнения вышеуказанных действий, как правило, является достаточной для идентификации лица, которое осуществляет публичные призывы к террористической деятельности в сети Интернет и его дальнейшего привлечения к уголовной ответственности.

Завершающий этап оперативной проверки связан с осуществлением ряда оперативно-розыскных мероприятий и следственных действий, целью которых является фиксирование в установленной законом форме доказательственной информации о преступном деянии.

В качестве сдерживающего фактора в механизме минимизации уровня экстремистско-террористической опасности в информационной среде выступает применение предусмотренных действующим законодательством комплекса оперативно-розыскных мер по мониторингу социальных сетей с использованием современных информационно-коммуникационных технологий, преследующих цель выявления, пресечения и раскрытия преступлений экстремистской направленности и террористического характера.

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства Российской Федерации. 2022. №710. Ст. 7045.

В настоящее время и в обозримом будущем надлежит на законодательном уровне более детально проработать вопрос относительно обозначенной проблематики и выработать научным сообществом теоретические рекомендации по модернизации действующей правовой основы оперативно-розыскной деятельности.

Заключение

Анализ вопросов, связанных с организацией оперативно-розыскных мероприятий, направленных на раскрытие публичных призывов к осуществлению террористической деятельности показал, что в условиях сегодняшних реалий это очень трудоёмкий процесс, требующий учёта специфических черт состава указанного преступного деяния и использования инновационных средств обнаружения и мониторинга информации в сети Интернет.

Авторы статьи убеждены, что блокировать информацию с публичными призывами в киберпространстве на стадии проведения оперативно-розыскных мероприятий малоэффективный способ минимизации их проявления, целесообразно после выявления подобных сообщений осуществить наблюдение за каналом передачи данных для обнаружения лиц, непосредственно размещающих такого рода информацию и с помощью специальных технических средств определить их местоположение.

Проблемным моментом осуществления оперативно-розыскных мероприятий при раскрытии публичных призывов к террористической деятельности, бесспорно является наличие устаревших программных комплексов их обнаружения, поэтому в качестве перспективного направления стоит рассматривать внедрение инновационных специализированных компьютерных программ для целей проведения автоматического оперативного мониторинга, а также использование некоторых компонентов искусственного интеллекта в оперативно-розыскную деятельность для осуществления эффективного мониторинга потока информации в сети.

Полагаем позитивным образом отразится на практике повсеместное внедрение в практическую деятельность правоохранительных органов недавно разработанной поисковой системы на основе уникального датасета ученого А. Рабчевского, позволяющего произвести идентификацию пользователей социальных сетей, которые распространяют экстремистский и террористический материал.

Список источников

1. Синельников А. С. Особенности организации оперативно-розыскных мероприятий, направленных на раскрытие публичных призывов к осуществлению террористической деятельности в учреждениях УИС // Право и государство: теория и практика. 2023. № 7 (223). С. 424–427. doi: 10.47643/1815-1337_2023_7_424.

2. Анисимова И. А. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма: особенности предмета и объективной стороны преступления // Российско-азиатский правовой журнал. 2020. № 4. С. 3–8. doi: https://doi.org/10.14258/ralj(2020)4.1.

3. Гаджиев Вугар Эдвар-оглы, Демина М.Л. Оперативно-разыскная характеристика преступлений, связанных с содействием террористической деятельности // ГлаголЪ правосудия. 2018. № 2 (16). С. 65–70.

4. Бычков В. В., Прорвич В. А. Противодействие новым вызовам экстремистской деятельности с использованием информационно-сетевых технологий на уровне трансграничных экстремистских сообществ // Вестник Московского университета МВД России. 2022. № 5. С. 54–60.

5. Смолина А. И. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма: объективная сторона // Молодой ученый. 2023. № 14 (461). С. 245–247.

6. Кутузов А. В. Оперативно-розыскной мониторинг сети Интернет как элемент противодействия преступлениям экстремистской направленности // Вестник Костромского государственного университета. 2020. Т. 26. № 2. С. 235–241. doi: 10.34216/1998-0817-2020-26-2-235-241.

7. Гребенщиков А. А. Некоторые проблемы расследования ст. 205.2 УК РФ // Вестник науки. 2024. №5 (74). С. 461–467.

8. Голяндин Н. П., Шериев А. М., Коломеец В. А. Вопросы выявления и проверки информации о совершении преступлений экстремистско-террористического характера в сети интернет // International Law Journal. 2019. Т. 2. № 4. С. 134–139.

References

1. Sinelnikov A.S. Features of the organization of operational investigative measures aimed at uncovering public calls for terrorist activities in criminal justice institutions. *Law and State: The Theory and Practice.* 2023;7(223):424–427. (In Russ.). doi: 10.47643/1815-1337_2023_7_424.
2. Anisimova I. A. Public calls to carry out terrorist activities, public justification of terrorism or propaganda of terrorism: features of the subject and objective side of the crime. *Russian-Asian Law Journal.* 2020;4(3-8). (In Russ). doi: https://doi.org/10.14258/ralj (2020)4.1.
3. Gadzhiev Vugar Edvar-ogly, Demina M.L. Operational investigative characteristics of crimes related to the promotion of terrorist activities. *Glagol Pravosudiya Magazine.* 2018;2(16):65–70. (In Russ).
4. Bychkov V.V., Prorvich V.A. Countering new challenges of extremist activity using information and network technologies at the level of cross-border extremist communities. *Vestnik of Moscow University of the Ministry of Internal Affairs of Russia.* 2022;(5):54–60. (In Russ).
5. Smolina A. I. Public calls to carry out terrorist activities, public justification of terrorism or propaganda of terrorism: the objective side. *Young Scientist.* 2023;14(461):245–247. (In Russ).
6. Kutuzov A.V. Operational investigative monitoring of the Internet as an element of countering extremist crimes. *Vestnik Of Kostroma State University.* 2020;26(2):235–241. (In Russ). doi: 10.34216/1998-0817-2020-26-2-235-241.
7. Grebenshchikov A. A. Some problems of investigation of Article 205.2 of the Criminal Code of the Russian Federation. *Vestnik nauki.* 2024;5(74):461–467. (In Russ.).
8. Golyandin N.P., Sheriev A.M. Kolomeets V.A. Issues of identification and verification of information about the commission of crimes of an extremist and terrorist nature on the Internet. *International Law Journal.* 2019;2(4):134–139. (In Russ.)

Информация об авторах

В. Ф. Попов – начальник Центра подготовки сотрудников полиции для подразделений по охране общественного порядка Федерального государственного казенного учреждения дополнительного профессионального образования «Всероссийский институт повышения квалификации сотрудников Министерства внутренних дел Российской Федерации».

О. А. Полещук – преподаватель кафедры подготовки сотрудников полиции для подразделений по охране общественного порядка и подразделений по вопросам миграции Федерального государственного казенного учреждения дополнительного профессионального образования «Всероссийский институт повышения квалификации сотрудников Министерства внутренних дел Российской Федерации».

В. Г. Выстропов – канд. юрид. наук, доцент кафедры управления органами внутренних дел в особых условиях центра командно-штабных учений Академии управления МВД России.

Information about the authors

V. F. Popov – Head of the Police Training Center for Public Order Units, Federal State Institution of Additional Professional Education "All-Russian Institute for Advanced Training of Employees of the Ministry of Internal Affairs of the Russian Federation".

O. A. Poleshchuk – Lecturer at the Department of Police Training for Public Order Units and Migration units, Federal State Institution of Additional Professional Education "All-Russian Institute for Advanced Training of Employees of the Ministry of Internal Affairs of the Russian Federation".

V.G. Vystropov – Cand. Sci. (Law), Associate Professor of the Department of Internal Affairs Management in special conditions of the Center for Command and Staff Exercises, Academy of Management of the Ministry of Internal Affairs of Russia.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 18.10.2024; одобрена после рецензирования 21.11.2024; принята к публикации 22.11.2024.
The article was submitted 18.10.2024; approved after reviewing 21.11.2024; accepted for publication 22.11.2024.