Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2024, 2: 133–139

EDN IWFNXE
DOI 10.26163/GIEF.2024.57.81.018
УДК 343.9

И.С. Репин

ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИСТСКИМ ПРОЯВЛЕНИЯМ В СЕТИ ИНТЕРНЕТ

Иван Сергеевич Репин – начальник отделения Центра по противодействию экстремизму (ЦПЭ) УМВД России по Ярославской области, капитан полиции, г. Ярославль; **e-mail: 1234567890076@bk.ru**.

Аннотация. *Статья посвящена проблеме борьбы с экстремизмом в интернете и стратегиям, которые могут помочь в ее решении. Проанализированы различные подходы в аспекте исследуемой проблемы, включая правовые меры, социальную мобилизацию и технические средства для блокировки неприемлемых контентов. Освещена необходимость эффективного сотрудничества между правительственными и неправительственными организациями, странами в целях совместного противодействия экстремизму. Рассмотрены данные и исследования в контексте темы статьи, что делает ее актуальной и ценной для научного общества и всех, кто заботится о безопасности и стабильности в сети Интернет.*

Ключевые слова: *экстремистская деятельность; сеть Интернет; противодействие; подходы; оперативные подразделения; мониторинг; сотрудничество.*

I.S. Repin

ON COMBATING EXTREMIST MANIFESTATIONS ON INTERNET

Ivan Repin – Head, the Department of the Centre for Combating Extremism, Russian Ministry of Internal Affairs for the Yaroslavl region, Captain of Police, Yaroslavl; **e-mail: 1234567890076@bk.ru**.

Annotation. *The article focuses on the relevant issue of fighting extremism on the Internet as well as on related strategies which might help on addressing the challenge. The paper presents analysis of a variety of approaches in the context of the matters under research including legal measures, social mobilization and technical aids for blocking unacceptable content. The author highlights the need for an effective cooperation between governmental and non-governmental organizations and states so that to ensure joint combating extremism. The article touches upon appropriate data and researches in the context of the article's topic which make it relevant and valuable for scientific society and for all who cares about security and stability on the Internet.*

Keywords: *extremist activity; Internet; countering; approaches; operational units; monitoring; cooperation.*

Современная информационная среда, в которой функционирует общество, служит источником новых возможностей и вызовов. Вместе с тем развитие технологий способствует и распространению экстремистских, террористических идей, которые находят отражение в сети Интернет.

Экстремистская деятельность в интернете – актуальная проблема в современном обществе. Это проявляется в форме распространения ненавистной риторики, призывов к насилию и дискриминации, а также силовых действий и террористических актов. Для противодействия указанной проблеме на международном и национальном уровнях принимают законы и политические меры. Однако проблема остается острой, так как экстремистская

деятельность в сети Интернет продолжает развиваться и проникать в сферы, ранее считавшиеся безопасными. Профилактика и пресечение экстремистской деятельности в данной сфере видится сложной задачей, требующей комплексного подхода и совместных усилий государства и общества в целом.

Информационно-телекоммуникационные сети, включая сеть Интернет, стали основным средством связи для экстремистских организаций, которое они используют для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии[1]. Исходя из этого, возникает необходимость акцентирования особого внимания на вопросы борьбы с данным видом преступлений в интернете. Благодаря техническим возможностям глобальной сети, именно в ней совершено доминирующее количество преступлений, связанных с экстремизмом. Согласно сводным статистическим сведениям о деятельности федеральных судов общей юрисдикции и мировых судей, за отчетный период 2020 г. в суды по статьям экстремистской направленности, в частности ст. 280, 280.1, 282–282.3 Уголовного кодекса Российской Федерации (УК РФ), на рассмотрение поступило 378 уголовных дел, за отчетный период 2021 г. – 573 уголовных дела, за отчетный период 2022 г. – 617 уголовных дел. На основании статистических данных с 2020 по 2022 г. можно сделать вывод, свидетельствующий о динамике роста преступлений экстремистской направленности.

Ключевое место среди правоохранительных органов в борьбе с преступлениями экстремистской направленности занимают оперативные подразделения по противодействию экстремизму МВД России и оперативные подразделения уголовного розыска, наделенные данными полномочиями. В свою очередь, эти подразделения выполняют следующие задачи в сфере противодействия экстремистской деятельности:

– осуществляют мониторинг экстремистских сообществ и сайтов в интернете для выявления пропаганды и призывов к экстремистской деятельности;

– проводят анализ информации, распространяемой экстремистскими группами в интернете для установления связей и выявления ключевых фигур;

– сотрудничают с провайдерами интернет-услуг для получения данных о пользователях, распространяющих экстремистские материалы;

– используют технические средства для контроля за сетевым трафиком и блокировки нежелательных сайтов и сообществ;

– проводят информационную работу с населением, в том числе образовательные мероприятия, направленные на профилактику экстремизма в интернете;

– занимаются совершенствованием методов и средств борьбы с экстремизмом в сети Интернет в соответствии с изменяющимися технологиями и методами работы экстремистов;

– осуществляют ряд комплексных оперативно-розыскных мероприятий, направленных на изобличение экстремистов и дальнейшее привлечение их к установленной законом ответственности и др.

Помимо МВД России, противодействие экстремистской деятельности в сети Интернет на стадии выявления осуществляют и другие правоохранительные органы. Согласно отчету МВД России, с января по декабрь 2020 г. выявлено 833 преступления экстремистской направленности, в том числе:

– сотрудниками Следственного комитета РФ – девять преступлений;

– сотрудниками МВД России – 500 преступлений;

– сотрудниками ФСБ России – 324 преступления[2].

[1] Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года: указ Президента РФ от 29 мая 2020 г. № 344 // Президент России: офиц. сайт. URL: http://www.kremlin.ru/acts/bank/45555 (дата обращения: 01.02.2024).

[2] Краткая характеристика состояния преступности в России за январь – декабрь 2020 года // МВД России: офиц. сайт. 2021. 21 января. URL:

Согласно отчету МВД России, с января по декабрь 2021 г. выявлено 1 057 преступлений экстремистской направленности (+26,9% к 2020 г.), в том числе:

– сотрудниками Следственного комитета РФ – 15 преступлений (+66,7% к 2020 г.);

– сотрудниками МВД России – 567 преступлений (+13,4% к 2020 г.);

– сотрудниками ФСБ России – 475 преступлений(+46,6% к 2020 г.)[3].

Согласно отчету МВД России, с января по декабрь 2022 г. выявлено 1566 преступлений экстремистской направленности (+48,2% к 2021 г.), в том числе:

– сотрудниками Следственного комитета РФ – 63 преступления (+320% к 2021 г.);

– сотрудниками МВД России – 863 преступления (+52,2% к 2021 г.);

– сотрудниками ФСБ России – 640 преступлений (+34,7% к 2021 г.)[4].

Иные федеральные органы исполнительной власти, включая министерства, агентства и службы (Минцифры России, Роскомнадзор и др.), некоммерческие организации (например, межрегиональная общественная организация «Центр содействия государству в противодействии экстремистской деятельности» и др.), выполняют лишь профилактическую функцию противодействия экстремистской деятельности, за исключением прокуратуры. Так, согласно приказу Генеральной прокуратуры России от 21 марта 2018 г. № 156 «Об организации прокурорского надзора за исполнением законов о противодействии экстремистской деятельности», Управлению по надзору за исполнением законов о федеральной безопасности, межнациональных отношениях, противодействии экстремизму и терроризму Генеральной прокуратуры РФ необходимо систематически организовывать мониторинг средств массовой информации, в том числе сети Интернет, в целях недопущения распространения экстремистской деятельности, а также постоянно организовывать взаимодействие с подразделением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций[5]. При обнаружении в интернете материалов, внесенных в Федеральный список экстремистских материалов, в установленном порядке прокуратура РФ обязана направить полученную информацию в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций или ее территориальное подразделение для осуществления ограничительных мер к информационному ресурсу. В случаях выявления подразделениями прокуратуры РФ в сети Интернет информации, свидетельствующей о призывах к экстремистской деятельности или призывах к участию в массовых беспорядках, сотрудники прокуратуры обязаны направить имеющиеся материалы в следственные органы по подследственности для решения вопроса о возбуждении уголовного дела. При выявлении информационных материалов, связанных с иностранной или международной неправительственной организацией, деятельность которой признана нежелательной на территории РФ, на основании и в соответствии с Федеральным законом от 28 декабря 2012 г. № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации»[6] сотрудники прокурату-

https://xn--b1aew.xn--p1ai/reports/item/22678184/?ysclid=lvgcs90k2q474056772 (дата обращения: 01.02.2024).

[3] Краткая характеристика состояния преступности в России за январь – декабрь 2021 года // МВД России: офиц. сайт. 2022. 18 января. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/?ysclid=lvgctzforz219189718 (дата обращения: 01.02.2024).

[4] Краткая характеристика состояния преступности в России за январь – декабрь 2022 года // МВД России: офиц. сайт. 2023. 20 января. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677?ysclid=lvgcvvsm16422567205 (дата обращения: 01.02.2024).

[5] Об организации прокурорского надзора за исполнением законов о противодействии экстремистской деятельности: приказ Генпрокуратуры России от 21 марта 2018 г. № 156 (в ред. от 24.03.2023) // Справ.-правовая система «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_298172/?ysclid=lvgcq8atlv411511976 (дата обращения: 01.02.2024).

[6] О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод челове-

ры уполномочены на составление протокола об административном правонарушении, предусмотренном ст. 20.33 Кодекса РФ об административных правонарушениях (КоАП РФ). В случаях выявления материалов, связанных с возбуждением ненависти либо вражды, а равно унижением человеческого достоинства, сотрудники прокуратуры уполномочены на составление административного протокола о правонарушении, предусмотренном ст. 20.3.1 КоАП РФ. Таким образом, можно сделать вывод о том, что МВД России и Генеральная прокуратура РФ наделены функциями противодействия экстремизму, связанными с выявлением, пресечением и профилактикой экстремистских проявлений в сети Интернет. На практике в зоне ответственности прокуратуры РФ – лишь административные правонарушения экстремистской направленности.

Кроме того, содействие в борьбе с экстремизмом в интернете оказывают компании и организации, предоставляющие сервисы связи и хранения данных (например, социальные сети, почтовые сервисы, облачные хранилища и т.д.). Эффективные меры противодействия с экстремистской деятельностью в сети Интернет особенно значимы в современном обществе. Ни одна страна в мире не остается в стороне от проблем экстремизма и терроризма, в настоящее время получающих все большее распространение в информационно-телекоммуникационном пространстве, объединяя субъектов в одну общую мировую сеть.

В первую очередь важным видится сохранение социальной стабильности в обществе. Экстремистская деятельность может стать причиной возникновения конфликтов между отдельными группами людей, искажения общественного мнения и нарушения прав человека и гражданина, других негативных явлений. Нельзя не упомянуть о том, что экстремистская деятельность в интернете имеет широкую аудиторию, которую можно легко мобилизовать и которой можно манипулировать. Это предоставляет экстремистам мощное средство для распространения своих идей и привлечения новых сторонников, среди которых могут быть и молодежь, и люди, искренне считающие, что они принимают участие в борьбе за свободу или справедливость.

Важно обеспечить безопасность существующих и будущих поколений. Несмотря на то, что интернет открывает широкие возможности для развития и саморазвития, он способен стать и средством введения молодых людей в круги экстремистов. Это может привести к нежелательным изменениям в их жизни, как в личностном, так и профессиональном аспекте, отрицательно отразиться на развитии общества в целом.

Учитывая вышеизложенное, можно заключить, что основные меры по противодействию экстремистской деятельности в сети Интернет осуществляются специальными службами и иными органами государственной власти. В частности, могут быть проведены следующие мероприятия:

– общий мониторинг сети Интернет, основанный на различных формах и сферах направленности экстремистских проявлений (социальной, религиозной, политической, международной, экологической, иной);

– мониторинг за активностью лиц, ранее привлекавшихся к ответственности за совершение преступлений и административных правонарушений экстремистской направленности;

– выявление сторонников и участников существующих экстремистских организаций, дальнейший анализ степени вовлеченности участников в деятельность экстремистских организаций и сообществ, а также уровня убежденности и солидарности сторонников сообществ;

– мониторинг социальных сетей, форумов и других сетевых ресурсов (наблюдение за активностью пользователей и их проявлениями, связанными с экстремизмом), который может осуществляться с помощью специальных программных средств, мониторящих интернет-трафик и обнару-

ка, прав и свобод граждан Российской Федерации: федер. закон от 28 декабря 2012 г. № 272-ФЗ // Собрание законодательства РФ. 2012. № 53 (ч. I). Ст. 7597.

живающих признаки экстремизма, в зависимости от задаваемого критерия поиска.

При обнаружении экстремистской деятельности в социальных сетях, на форумах и других сетевых ресурсах производят анализ содержания информации с целью выявления участников, разместивших материалы экстремистского содержания, установление контекста размещенных материалов и дальнейшее документирование их противоправной деятельности. Первоначально документирование противоправной деятельности может заключаться в составлении акта осмотра интернет-ресурса, неотъемлемым критерием которого является наличие незаинтересованных в исходе проверки представителей общественности, необходимых для подтверждения факта размещения в сети Интернет информации экстремистского содержания.

Использование меры противодействия экстремистской деятельности в сети Интернет, такой как выявление экстремистской деятельности, через опосредованный мониторинг интернета не приводит к нарушению прав граждан на личную жизнь и свободу выражения мнения, поскольку мониторинг затрагивает публичную часть сети Интернет и предполагает выявление фактов распространения информации, направленной на неограниченный и неопределенный круг лиц. Факт размещения информации в публичном пространстве приравнивается к публичному провозглашению и служит моментом окончания преступления или административного правонарушения, а конституционные права лица, совершившего данное деяние, на стадии выявления не затрагиваются.

Сотрудничество с интернет-провайдерами играет важную роль в противодействии экстремистской деятельности в сети Интернет. Провайдеры не только выступают основными поставщиками услуг доступа в интернет, но и могут следить за активностью пользователей, находящихся на их серверах. При противодействии экстремистской деятельности интернет-провайдеры могут выполнять следующие функции:

– блокировать доступ к сайтам и ресурсам, на которых распространяется экстремистская информация;

– ограничивать доступ к сети индивидуальным пользователям, которые проявляют поведение, связанное с экстремистской деятельностью;

– предоставлять информацию о пользователях, которые могут быть связаны с экстремистской деятельностью, правоохранительным органам;

– сотрудничать с другими интернет-провайдерами, правоохранительными органами, иными заинтересованными сторонами для обмена информацией и координации операций по противодействию экстремистской деятельности.

В настоящее время большое развитие получили системы фильтрации запрещенного контента в социальных сетях, заключающиеся в создании автоматических систем выявления информации, направленные на «отлавливание» и блокировку. Такие системы работают на основе алгоритмов, которые анализируют контент, загружаемый в интернет, и определяют наличие в нем экстремистских идей и слов. Если сигнал об экстремистском контенте срабатывает, то система автоматически блокирует доступ к контенту, что позволяет предотвратить его распространение.

Противодействие экстремистским проявлениям в сети Интернет происходит на стадии профилактики недопущения наступления экстремистских проявлений посредством создания уполномоченными правоохранительными органами образовательных программ, проведения обучающих курсов для широкого круга лиц о том, как правильно вести себя в сети Интернет, с предоставлением информации о том, что является экстремизмом в интернете и как его распознать. В рамках таких программ пользователи получают необходимые знания о том, как защитить себя и свою семью от негативного влияния экстремистов, как распознать подозрительные и неправомерные действия в глобальной сети, как правильно сообщать о подобных случаях в соответствующие службы. В процессе обучения пользователи узнают о том, как действовать в ситуации конфликта, как не

попасться на уловки экстремистов-провокаторов, которые сами не совершают противоправных действий, но склоняют иных лиц к противоправным действиям, как противостоять пропаганде идеологий, которые призывают к насилию или экстремизму. В результате пользователи становятся более осознанными и ответственными участниками интернет-сообщества, что способствует снижению уровня экстремистских проявлений в сети Интернет.

Противодействие экстремистской деятельности в сети Интернет имеет ряд проблемных аспектов. Один из них – анонимность в сети Интернет, достижение которой становится возможным за счет использования специального программного обеспечения, позволяющего скрыть свою личность, местоположение и иную имеющую значение для правоохранительных органов информацию, способствующую установлению всех обстоятельств преступной деятельности.

Наиболее распространенным программным обеспечением, позволяющим создавать защищенные анонимные сетевые подключения, так называемые виртуальные туннели, является Tor Browser (The Onion Router). Данное программное обеспечение состоит из трехуровневого прокси-сервера, используя которое пользователь осуществляет выход в сеть Интернет через промежуточные узлы выхода, перенаправляя свой трафик, через произвольно выбранные ретрансляторы, находящиеся в иных государствах, скрывая первоначальный IP-адрес пользователя, IMEI (международный идентификатор мобильного оборудования), IMSI (международный идентификатор абонента подвижной сети), MAC (уникальный идентификатор оборудования сетей передачи данных), ICQ-идентификатор служб обмена сообщениями. Тем самым пользователю обеспечена необходимая анонимность, и исчезает возможность у подразделений по противодействию экстремизму устанавливать и документировать обстоятельства, имеющие оперативное значение.

Ограничение доступа к анонимным средствам связи является лишь одним из возможных путей решения проблемы анонимности, но, по мнению специалистов в сфере информационных технологий, требуется воплощение нормативно-правовых запретов [1, с. 135]. Блокирование использования Tor Browser, VPN и иных прокси-серверов, анонимных сетей связи, позволяющих пользователям сети Интернет осуществлять подмены, шифрования своих идентификационных данных и предоставлять возможность подключения к ресурсам, внесенным в список запрещенных на территории РФ, на практике не представляется возможным вследствие активного усовершенствования и усложнения алгоритмов этого программного обеспечения со стороны производителей и недостаточного материального, финансового обеспечения технических подразделений МВД России и ФСБ России со стороны государства, что сказывается на недостаточном уровне и скорости решения поставленных задач, отнесенных к их компетенции.

Необходимым видится улучшение технологий и алгоритмов идентификации, которые могут помочь выявить отдельных пользователей в анонимной сети. Например, использование расширенных технологий идентификации на основе нескольких факторов, таких как идентификация отпечатков браузера и устройства, использование анализа поведения, текущей локации или фильтрации URL-адресов посредством идентификации по ранее заданным критериям в виде конкретных слов, словосочетаний и словарных оборотов.

Образование и информирование населения может оказаться наиболее эффективным путем. Требуется разъяснение общественности информации о возможных рисках использования анонимных средств связи экстремистами с акцентом на важности принятия мер для защиты личной информации.

Организация полноценного взаимодействия правоохранительных органов, интернет-провайдеров и служб безопасности социальных сетей в направлении интенсивного мониторинга, своевременного обмена оперативно значимой информацией, предоставления оперативно значимой информации превентивного характера

позволили бы выявлять преступления экстремистской направленности на стадии планирования или подготовки. Но в настоящее время правоохранители поставлены в ситуацию, в которой информация поступает лишь по запросу правоохранительного органа и с существенным опозданием относительно процессуальных сроков ответов на запросы.

Таким образом, проблема борьбы с экстремизмом в сети Интернет не является новой. Однако с развитием технологий и социальных сетей она приобретает все большую актуальность. В статье нами рассмотрены основные подходы по борьбе с данным видом преступлений. Каждый из подходов имеет преимущества и недостатки, и только комплексное использование всех методов может дать эффективный результат. Одним из ключевых элементов таких способов является деятельность оперативных подразделений, которые способны своевременно реагировать на выявление экстремистского контента в интернете и осуществлять пресечение деятельности экстремистских организаций в сети. В заключение обратим внимание на то, что борьба с экстремизмом в интернете требует совместных усилий со стороны государства, производителей IT-технологий, сообщества онлайн-пользователей и каждого человека. Важно помнить о том, что это – сложная, многогранная проблема, и только совместными усилиями мы сможем достичь успеха в борьбе с экстремизмом в интернете.

ЛИТЕРАТУРА

1. *Васильев Б.Д.* Киберэкстремизм: проблемы противодействия и правового регулирования // Право и политика. 2019. Т. 8. № 1. С. 135–141.