

Дата поступления рукописи в редакцию: 22.05.2025 г.
Дата принятия рукописи в печать: 02.06.2025 г.

DOI: 10.24412/2076-1503-2025-5-557-561

ОСМАНОВ Мухамед Мартинович,
старший преподаватель кафедры
организации правоохранительной деятельности
Северо-Кавказского института повышения
квалификации сотрудников МВД (филиал)
Краснодарского университета МВД России,
кандидат педагогических наук,
подполковник полиции,
e-mail: muhamedosmanov8@gmail.com

ВСЕМИРНАЯ СЕТЬ ИНТЕРНЕТ КАК ПЛОЩАДКА ДЛЯ ПРОПАГАНДЫ ЭКСТРЕМИСТКОЙ ИДЕОЛОГИИ: МАСШТАБЫ И КАНАЛЫ РЕАЛИЗАЦИИ

Аннотация. Автор в своем исследовании уделяется особое внимание каналам, источникам и масштабам распространения преступными сообществами радикальной идеологии и пропаганды информации экстремистского характера с применением информационных технологии в глобальной сети Интернет и применяемым правоохранительными органами мерам противодействия ее проявления интернет пространстве.

Ключевые слова: виртуализация, агитация, анонимность, глобальная площадка, экстремизм, интернет-каналы, интернет технологии, дезинформация, преступление, социальная сеть, единый центр, противодействие, ресурс.

OSMANOV Mukhamed Martinovich,
Senior Lecturer at the Department of Organization of Law
Enforcement Activities of the North Caucasus Institute
for Advanced Training of Ministry of Internal Affairs Officers (branch)
of the Krasnodar University of the Ministry of Internal Affairs of Russia,
Candidate of Pedagogical Sciences,
Police Lieutenant Colonel.

THE WORLD WIDE WEB AS A PLATFORM FOR PROPAGANDA OF EXTREMIST IDEOLOGY: SCALE AND CHANNELS OF IMPLEMENTATION

Annotation. The author in his study pays special attention to the channels, sources and scale of distribution of radical ideology and propaganda of extremist information by criminal communities using information technology in the global Internet and the measures taken by law enforcement agencies to counteract its manifestation in the Internet space.

Key words: virtualization, agitation, anonymity, global platform, extremism, Internet channels, Internet technologies, disinformation, crime, social network, single center, counteraction, resource.

Динамично развивающееся информационное общество на базе информационно-телекоммуникационных технологий относится к общемировым тенденциям современности. Информационное пространство предоставляет широкие возможности, такие как общедоступность, высокая скорость передачи информации, независимость от местонахождения, анонимность и многие другие.

Данные преимущества, в том числе – трудность в осуществлении контроля со стороны органов правопорядка, привлекают внимание и криминальных структур, и они активно используют это в своей преступной деятельности, что позволяет им стать менее уязвимыми для правоохранительных органов.

Построение современных экстремистских групп организовано по принципу сетевой струк-

туры, которая обеспечивает функционирование единых центров и информационно-коммуникационных каналов.

Экстремистскими идеологами широко используются средства психологической войны, включающие такие, как дезинформация, подмена понятий и фактов, манипуляция общественным сознанием.

Современные информационно-коммуникационные возможности глобальной сети позволяют виртуализированным экстремистским решениям беспрепятственно и бесконтрольно проникать в наиболее подверженную деструктивному влиянию молодежную среду.

Сегодня проявления экстремизма и терроризма в глобальном информационном пространстве представляют угрозу безопасности многих стран и их граждан, затрагивают всё человечество и деструктивно влияют на всё мировое сообщество.

Важно отметить, что ряды экстремистских группировок обычно пополняют люди, являющиеся социальными аутсайдерами, которые в силу различных причин не смогли реализоваться в современных условиях. К отмеченной категории относятся, как правило, лица, не имеющие работы; молодые люди, не имеющие образования и достойного уровня жизни.

Преступные идеологи для ведения пропаганды, вербовки новых сторонников и увеличения количества «сочувствующих» используют широко-масштабную аудиторию глобальной сети, большую часть пользователей которой составляют молодые люди в возрасте от 12 до 30 лет.

В частности по отношению к несовершеннолетним, в качестве методов, террористами могут применяться различные игры в реальном времени, условием которого является выполнение каких-либо конкретных действий или выполнение отдельных заданий, представляют и сравнивают их с положительными персонажами различных предоставляемых на обозрение жанров, что способствует тому, что несовершеннолетние вдохновляются различными идеями, повышается их самооценка, стараются заслужить уважение, повысить свой статус в обществе, начинают подражать преступному элементу, целью которых является добиться именно этого эффекта.

Специальные средства и активное использование возможностей посредством таких социальных сетей и мессенджеров, как «Telegramm», «WhatsApp», «ВКонтакте», «Одноклассники», «Facebook» и «Instagram»), способствует распространению экстремистской идеологии.

По итогам мониторинга российских и иностранных социальных платформ, осуществленного правоохранительными органами в сети

Интернет, были обнаружены текстовые, фото и видеоматериалы экстремистского характера. зачастую помогают им создать защищенные каналы связи, незаметные для органов правопорядка.

Преступные сообщества умеют разрабатывать разные страницы и сайты в Интернете, для распространения своих идей с максимальной скоростью и большим охватом аудитории, к ним можно отнести такие как: бесплатные хостинги, страницы в социальных сетях, профессиональные сайты на платных хостингах.

Стремительно возрастающее год от года количество активных пользователей сети Интернет, детерминирует необходимость выработки соответствующих мер обеспечения информационной безопасности глобального информационного пространства, в частности, противодействия активизировавшемуся распространению идей экстремизма и терроризма в глобальной сети.

Основной и важной задачей вышеуказанных ресурсов, является преподнесение определенной информации для их сторонников в ускоренной форме, постоянно меняя демонстрируют реакцию на различные мировые события и новости.

Сайты могут быть акцентированы на различную публику и подразделяться на разные категории, такие как: по возрастным категориям, по интересам определенных граждан, на социальные группы, по национальным признакам, по различным пользователям определенной информации.

За частую преступники хорошо прорабатывают и техническую составляющую, для эффективного распространения информации.

Для реализации вышеуказанных целей, осуществляют регистрацию сайтов на зарубежных серверах, применяют для этого услуги подставных лиц, имеют возможности, предоставляющие возможность сохранить доступ к информации, как страхового варианта обеспечения функционирования и доступа, при непредвиденных ситуациях связанных с блокировкой сайта или иной ситуации, тем самым обеспечивают бесперебойный доступ пользователя к информации.

Зачастую сеть Интернет и специальные различные программы позволяют обеспечить анонимность информации, посредства его шифрования, что является очень важным для злоумышленников в процессе пропаганды различной негативной информации.

Преступники в большинстве случаев в ускоренной форме осуществляют процессы передачи информации, осуществляют обмен информацией, поддерживают диалог с большой аудиторией и пользователями в удаленном пространстве, в том числе и вне зависимости от их месторасположе-

ния и в такого рода случаях Интернет, становится удобной площадкой и каналам распространения преступной идеологии и развития преступности на международном уровне.

Глобальное информационное пространство, благодаря широкой распространенности и всеобщей доступности, безусловно, является очень удобным и эффективным источником информации.

Вследствие этого использование безграничных возможностей обмена общедоступной информацией во всемирной сети не вызывает никаких споров и сомнений. Однако, в киберпространстве также осуществляется размещение информации, доступ к которой запрещен в целях обеспечения общественной и государственной безопасности.

Вместе с тем, наравне с откровенными сайтами содержащими террористическую и иную экстремистскую идеологию, в сети функционирует множество новостных порталов и сайтов информационного характера так или иначе не связанных с террористическими и преступными сообществами и группировками, однако в тот же момент и разделяющие их идеи и взгляды, тем самым оказывающие преступникам поддержку в различных сферах.

Современный информационный экстремизм ставит под угрозу безопасность общества, нарушая законные права человека, чиня препятствия достижению гражданского согласия, подрывая устои демократического и правового государства.

Исходя из чего, противодействие проявлению экстремистской идеологии в информационном пространстве становится приоритетной и первоочередной задачей стоящей перед органами государственной власти.

Профилактические и действенные меры по противодействию распространения преступной идеологии в сети Интернет, наряду с проявляющимися различного рода явлениями, носящими угрожающий характер национальной безопасности, обществу и государству носят невоенный характер призванные обеспечить эффективный способ достижения политических и стратегических целей и по своей результативности в большинстве случаев являются наиболее эффективными, нежели военные террористические средства и методы.

Основная проблема противодействия экстремизму в сети Интернет во многом объясняется наличием у преступных сообществ значительного научно-технического потенциала, поскольку они привлекают в свои ряды целые группы квалифицированных специалистов в области высоких технологий.

В настоящее время, подразделениями по противодействию экстремизму ведется монито-

ринг сети Интернет, а также различных социальных сетей с целью обнаружения экстремистских материалов и различного рода запрещенной информации.

В целях обеспечения информационной пропаганды и не допущения блокирования сайтов содержащих информацию преступного характера, разработчиками применяются различные усилия направленные на защиту непосредственно сайтов от воздействия со стороны правоохранительных органов, вследствие чего применяют различные закодированные и зашифрованные программы, маршруты и сервисы как площадки в сети.

В целях доступа к сети применяются программы, позволяющие изменить электронные адрес или исключают применение персонального компьютера в домашних условиях и используют услуги интернет-кафе, различных заведений, предоставляющие пароль от своего Wi-Fi, обезличенные или оформленные на третьих лиц сим-карты с выходом в Интернет.

В целях реализации вышеуказанных методов применяются специальные серверы различных стран, законодательство которых позволяет использовать подобные методы шифрования.

Одним из первых правовых актов, регламентирующих противодействие экстремизму и терроризму, был Указ Президента РФ 23.03.1995 № 310 «О мерах по обеспечению согласованных действий органов государственной власти в борьбе с проявлениями фашизма и иных форм политического экстремизма в Российской Федерации».

Современная нормативно-правовая база РФ в области противодействия терроризму и экстремизму в глобальной сети базируется на следующих положениях Конституции РФ:

- п.5, ст.13 (запрет на создание и функционирование объединений, деятельность которых направлена на разжигание социальной, расовой, национальной и религиозной розни);
- п.2 ст.29 (запрет на пропаганду или агитацию, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду).

В сфере противодействия экстремизму и терроризму в РФ, правоохранительными органами применяются:

- Федеральный закон РФ от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности»;
- Федеральный закон РФ от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- «Стратегия противодействия экстремизму в Российской Федерации до 2025 года» от 28 ноября 2014 г. № Пр-2753 (ред. от 29.05.2020);

- «Концепция противодействия терроризму в Российской Федерации» от 5 октября 2009 года.

Вместе с тем стоит отметить, что органы государственной власти уделяют большое внимание проблемам обеспечения технического противодействия экстремизму в глобальном информационном пространстве.

Этому свидетельствуют вносимые поправки в законодательные акты Российской Федерации.

Правоохранительные органы, также используют возможности сети Интернет с целью своевременного выявления и мониторинга деятельности террористических групп и организаций, проводят профилактические мероприятия по борьбе с преступлениями, проводят информирование населения, осуществляют периодический сбор доказательств о готовящихся или уже совершенных преступлениях, в том числе и совершенных в сети Интернет или с использованием современных электронных технологий.

В настоящее время, одной из приоритетных задач органов государственной власти является разработка и внедрение эффективных технологий, направленных на противодействие проявлениям экстремизма в сети Интернет.

Однако не смотря на применяемые меры продолжающаяся мировая информационно-технологическая революция создает новые потенциальные угрозы жизнедеятельности как государств, так и мирового сообщества в целом.

В наибольшей степени это относится к экстремизму и терроризму, мутация которых, по мнению экспертов, происходит именно в информационной сфере.

Поэтому эффективное решение данной проблемы требует координации усилий по дальнейшему совершенствованию технических средств и разработке новых методов информационного противодействия деятельности экстремистских организаций в информационно-телекоммуникационной сети.

Список литературы:

- [1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
- [2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 06.04.2024).
- [3] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 22.04.2024).
- [4] Об информации, информационных технологиях и о защите информации (с изм. и доп., вступ. в силу с 30.06.2018): федер. закон от 27

июля 2006г. № 149-ФЗ (ред. от 14.07.2022) // Рос. газ. – 2006. – № 165.

[5] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон от 06 июля 2016г.

№ 375-ФЗ // Рос.газ. – 2016. – № 150.

[6] Экстремизм представлен в основном возрастной группой. Молодежный экстремизм как одна из наиболее актуальных социально – политических проблем в России.

[7] Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ от 28 нояб. 2014г. № Пр-2753) / Правовая база <http://www.scrf.gov.ru> (дата обращения: 12.05.2024).

[8] Жукова О.С. Информационный экстремизм в современном государственно – правовом государстве [Текст] / О. С. Жукова,

Р. Б. Иванченко, В. В. Трухачёв. – Философия права. – Изд-во: Ростовский юридический институт МВД, 2010. – С. 105 -108.

[9] Организация деятельности правоохранительных органов по противодействию экстремизму и терроризму: учебное пособие /

Е.Н. Быстрыков, Е.В. Ионова, Н.Л. Потапова, А.Б. Смушкин. - 2-е изд., стер. — Санкт-Петербург: Лань, 2022. - 176 с.

[10] Рапог А.И. Уголовно-правовое противодействие терроризму и экстремизму: учебное пособие/ А.И. Рапог, В.В. Палий. - Москва: Проспект, 2021. - 96 с.

[11] Сахнов И.П. Противодействие распространению идеологии экстремизма и терроризма и профилактика аддиктивного поведения в молодежной среде: учебно-методическое пособие / И.П. Сахнов. - Кострома: КГУ им. Н.А. Некрасова, 2021. - 147 с.

Spisok literatury:

- [1] Konstituciya Rossijskoj Federacii (prinyata vsenarodny`m golosovaniem 12.12.1993 s izmeneniyami, odobrenny`mi v xode obshherossijskogo golosovaniya 01.07.2020).
- [2] Ugolovny`j kodeks Rossijskoj Federacii ot 13.06.1996 N 63-FZ (red. ot 06.04.2024).
- [3] Kodeks Rossijskoj Federacii ob administrativny`x pravonarusheniyax ot 30.12.2001 N 195-FZ (red. ot 22.04.2024).
- [4] Ob informacii, informacionny`x texnologiyax i o zashhite informacii (s izm. i dop., vstup. v silu s 30.06.2018): feder. zakon ot 27 iyulya 2006g. № 149-FZ (red. ot 14.07.2022) // Ros.gaz. – 2006. – № 165.

[5] O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i Ugolovno-processualnyj kodeks Rossijskoj Federacii v chasti ustanovleniya dopolnitel'nyx mer protivodejstviya terrorizmu i obespecheniya obshhestvennoj bezopasnosti: feder. zakon ot 06 iyulya 2016g.

№ 375-FZ // Ros.gaz. – 2016. – № 150.

[6] E'kstremizm predstavljen v osnovnom vozrastnoj gruppoj. Molodezhnyj e'kstremizm kak odna iz naibolee aktual'nyx social'no – politicheskix problem v Rossii.

[7] Strategiya protivodejstviya e'kstremizmu v Rossijskoj Federacii do 2025 goda (utv. Prezidentom RF ot 28 noyab. 2014g. № Pr-2753) / Pravovaya baza <http://www.scrf.gov.ru> (data obrashheniya: 12.05.2024).

[8] Zhukova O.S. Informacionnyj e'kstremizm v sovremennom gosudarstvenno – pravovom gosudarstve [Tekst] / O. S. Zhukova,

R. B. Ivanchenko, V. V. Truxachyov. – Filosofiya prava. – Izd-vo: Rostovskij juridicheskij institut MVD, 2010. – S. 105 -108.

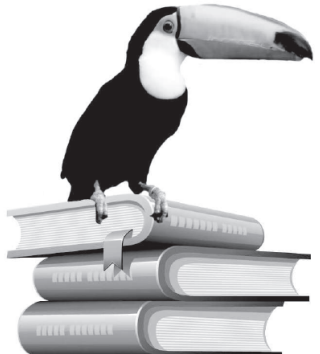
[9] Organizaciya deyatel'nosti pravooxranitel'nyx organov po protivodejstviyu e'kstremizmu i terrorizmu: uchebnoe posobie /

E.N. By'stryakov, E.V. Ionova, N.L. Potapova, A.B. Smushkin. - 2-e izd., ster. — Sankt-Peterburg: Lan', 2022. - 176 s.

[10] Rarog A.I. Ugolovno-pravovoe protivodejstvie terrorizmu i e'kstremizmu: uchebnoe posobie/ A.I. Rarog, V.V. Palij. - Moskva: Prospekt, 2021. - 96 s.

[11] Saxnov I.P. Protivodejstvie rasprostraneniyu ideologii e'kstremizma i terrorizma i profilaktika addiktivnogo povedeniya v molodezhnoj srede: uchebno-metodicheskoe posobie / I.P. Saxnov. - Kostroma: KGU im. N.A. Nekrasova, 2021. - 147 s.





Юридическое издательство

«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.

ЮРКОМПАНИ

www.law-books.ru