

Дата поступления рукописи в редакцию: 13.06.2026 г.  
Дата принятия рукописи в печать: 11.07.2026 г.

DOI: 10.24412/2782-3849-2026-7-46-49

**МИСРОКОВ Тенгиз Замирович,**

кандидат юридических наук, старший преподаватель кафедры ГиГПД Северо-Кавказского института  
повышения квалификации (филиал) Краснодарского университета МВД России,

e-mail: mail@law-books.ru

## ИНФОРМАЦИОННЫЙ АСПЕКТ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ЭКСТРЕМИЗМА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА

**Аннотация.** В статье анализируются особенности использования цифровых технологий экстремистскими организациями, а также основные направления по противодействию данным угрозам. Отдельное внимание уделяется роли общественных институтов и потенциалу образовательных организаций в вопросах борьбы с экстремистскими угрозами в цифровом пространстве, а также отмечается важность повсеместного повышения цифровой грамотности населения. Указывается необходимость постоянного совершенствования нормативно-правового регулирования в сфере информационного противодействия экстремизму и использование технических решений для защиты населения России от киберугроз, связанных с деятельностью экстремистских организаций. Автором подчеркивается важность достижения оптимального баланса при реализации конституционных прав населения Российской Федерации и обеспечением их безопасности, что является условием успешного развития общества и раскрытия потенциала каждого человека, проживающего в нашей стране.

**Ключевые слова:** противодействие экстремизму, цифровизация общества, информационная безопасность, технологии нейросетей, защита граждан от цифровых угроз, информационная компетентность, цифровая грамотность, экстремистские угрозы в цифровом пространстве.

**MISROKOV Tengiz Zamirovich,**

candidate of law sciences Senior lecturer of the state, civil and law disciplines chair of the North-Caucasian  
Advanced Training Institute (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia

## INFORMATION ASPECT OF COUNTERING THE DISSEMINATION OF EXTREMISM IN THE CONDITIONS OF DIGITALIZATION OF MODERN SOCIETY

**Annotation.** The article analyzes the features of the use of digital technologies by extremist organizations, as well as the main directions for countering these threats. Special attention is paid to the role of public institutions and the potential of educational organizations in combating extremist threats in the digital space, and the importance of increasing the digital literacy of the population is noted. The article highlights the need for continuous improvement of legal and regulatory frameworks in the field of information counteraction to extremism and the use of technical solutions to protect the Russian population from cyber threats associated with the activities of extremist organizations. The author emphasizes the importance of achieving an optimal balance between the implementation of the constitutional rights of the Russian population and ensuring their safety, which is essential for the successful development of society and the realization of the potential of every individual living in our country.

**Key words:** counteraction to extremism, digitalization of society, information security, neural network technologies, protection of citizens from digital threats, information competence, digital literacy, and extremist threats in the digital space.

Противодействие экстремизму является одной из ключевых задач на пути к обеспечению национальной безопасности Российской Федерации и международной безопасности всего современного мирового сообщества. Экстремистские проявления чрезвычайно

разнообразны, они трансформируются, а экстремистские организации быстро адаптируются к изменяющимся условиям, стремительно беря на вооружение последние достижения в области цифровых технологий, информации и связи. В сложившихся условиях

противодействие экстремизму становится невозможным без обеспечения информационной составляющей противодействия его распространению, которая в условиях неизбежной и ускоряющейся цифровизации современного общества требует комплексных мер. В числе прочих, к подобным мерам относят те, что направлены на нейтрализацию деструктивного контента, профилактику радикализации и повышение цифровой грамотности населения. Современная цифровая среда не только расширяет возможности для коммуникации, но и активно используется радикальными структурами для распространения экстремистских идеологий. Сложно не согласиться с мнением Пачиной Н.Н. и Касенова А.Д., утверждающих, что: «Сложность борьбы с информационным экстремизмом частично обусловлена его технологическим оснащением. Ошибочно думать, что под информационными экстремистами понимаются только неорганизованные хакеры или энтузиасты компьютерных технологий. Данные группы характеризуются дисциплинированностью и конспиративностью, их действия в информационной сфере тщательно спланированы» [2].

Рассматривая проблему использования цифровых технологий экстремистскими организациями и отдельными злоумышленниками, занимающимися распространением экстремистской идеологии, необходимо учитывать ряд особенностей. Прежде всего, транснациональный характер деятельности экстремистских организаций влечёт за собой юридические проблемы, связанные с невозможностью каждой отдельной страны противостоять их деструктивной деятельности в цифровом пространстве в одиночку, в виду использования преступниками географических и правовых барьеров, объективно существующих между государствами и недостаточной готовностью ряда государств к конструктивному и взаимовыгодному сотрудничеству в сфере борьбы с экстремизмом.

В настоящее время информационно-телекоммуникационная сеть «Интернет» и функционирующие в её цифровом пространстве социальные сети и мессенджеры являются основными платформами для распространения экстремистского контента, площадками для вербовки новых сторонников, ведения экстремистской пропаганды, а также финансирования экстремистских организаций и управления их структурными ячейками.

Экстремистские организации используют технологии нейросетей для быстрой генерации деструктивного контента, мгновенного создания новых сайтов и аккаунтов в социальных сетях,

обхода защитных мер в форме модерации и обнаружения запрещенного национальным законодательством контента.

Ряд передовых технологий, таких как «Deepfake», позволяют генерировать поддельные видео- и аудиоматериалы, дискредитирующие органы государственной и муниципальной власти, группы лиц или конкретных людей. Качество подобных недостоверных материалов стремительно улучшается, что влечёт за собой значительное усложнение проверки их подлинности и возможности их разоблачить и опровергнуть.

Применяемые алгоритмы подбора интересующего пользователей цифрового контента и системы рекомендаций могут, пусть и не всегда преднамеренно, но способствовать получению информации, которая бы подтверждала негативные тезисы и запросы лиц, которые потенциально могут попасть в орбиту деструктивного влияния экстремистских организаций, усиливая и подкрепляя радикальных характер распространяемой ими негативной повестки, основанной на предвзятости, манипуляциях, ложных посылах, стереотипах, информационных вбросах.

Изучение цифровых следов, оставляемых пользователями в сети «Интернет» позволяет экстремистским организациям и отдельным злоумышленникам проводить целевой поиск и последующую вербовку жертв среди наиболее уязвимых групп населения.

Кроме того, следует отметить, что современные цифровые технологии создают определенную, пусть и далеко не полную, анонимность, а также возможность шифрования передаваемой информации. Всё большее распространение получают различные мессенджеры и скрытые сети, доступ к которым возможен только с помощью определенного программного обеспечения.

Как мы видим, противодействие экстремизму в цифровом пространстве осложнено множеством факторов, которые в совокупности определяют необходимость системного противодействия, в основе которого должны лежать такие принципы как: 1) комплексность; 2) непрерывность; 3) адаптивность.

На сегодняшний день органы государственной власти предпринимают значительные усилия по пресечению деятельности экстремистской деятельности в цифровом пространстве. Наиболее ярко эти усилия проявляются в вопросах ограничения доступа к сайтам, аккаунтам, посредством которых осуществляется информационное сопровождение экстремистской деятельности.

Активные меры предпринимаются в направлении деанонимизации правонарушителей, что достигается усилением контроля за продажей SIM-карт и повышение требований, предъявляемых к пользователям при регистрации в различных цифровых сервисах.

Разумеется, отдельного внимания требует международное сотрудничество. Современное международное сообщество вступило в период глобального изменения привычных, потерявших актуальность форматов взаимодействия. Мир фрагментируется, возникают множественные центры консолидации сил и интересов различных государств. Информационное пространство нашего государства не существует в вакууме, оно переплетено с общей международной информационной средой, поэтому необходимо дальнейшее развитие международной правовой базы, формирующей общие подходы к определению экстремизма в цифровой среде и предлагающей системы защиты международного сообщества от цифровых угроз, носящих глобальный характер.

Говоря о борьбе с деструктивной идеологией, распространяемой экстремистскими организациями, следует понимать, что любой информационный вакуум неизбежно будет заполняться, поэтому необходимо, чтобы негативная и недостоверная информация не просто ограничивалась и удалялась из отечественного цифрового пространства, но и разоблачалась, опровергалась, а на смену ей быстро приходили социально полезные, гуманистические и патриотические идеи, подкрепляемые не только поддержкой органов государственной власти и местного самоуправления, но и образовательными организациями и общественными институтами. Взаимодействие с последними является одним из обязательных условий в профилактике экстремизма, поскольку те же школьные и иные образовательные учреждения занимают значительное место в повседневной жизни молодого поколения наших соотечественников.

Простор для вовлечения экстремистскими организациями в свои ряды населения, возникает в том числе и там, где наши соотечественники не знают, где найти единомышленников для совместного досуга, а также для интеллектуального и духовного развития. В особенности это касается молодёжи, которая в современных реалиях часто оказывается значительное время предоставлена сама себе, находясь по тем или иным причинам вне поля внимания родителей и иных старших родственников. В этой связи необходимо повсеместное привлечение различных категорий населения к культурным,

спортивным и иным массовым мероприятиям, где обеспечивалась бы реализация потребности наших соотечественников в социальной активности и самовыражении. Наряду с подобными масштабными формами взаимодействия населения, следует рассмотреть возможность повсеместного возрождения творческих, научных и иных кругов по интересам. С одной стороны, это будет способствовать поиску и выявлению новых талантов, а с другой стороны, это позволит продвигать посредством таких малых организаций патриотическое мышление, созидательные идеи, коллективизм и товарищество.

Говоря о защите населения Российской Федерации от деструктивного влияния экстремистских организаций в цифровом пространстве, всегда следует помнить о необходимости достижения оптимального баланса между обеспечением безопасности жителей нашей страны и реализацией их конституционных прав, в том числе, гарантированных статьёй 29 Конституции Российской Федерации, согласно которой: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» [1]. Лишь успешное выполнение обеих этих задач, позволит создать надлежащие условия для дальнейшего успешного развития нашего общества и реализации каждым человеком своих прав, свобод и законных интересов и наиболее полного раскрытия собственного интеллектуального, творческого и иного потенциала.

Подводя итог, необходимо отметить, что эффективное противодействие экстремизму в условиях цифровизации российского общества требует комплексного подхода, включающего правовые, технологические, образовательные и общественные меры, а также международное сотрудничество.

#### Список литературы:

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – Текст: электронный // Официальный интернет портал правовой информации. – URL: <http://pravo.gov.ru/>. – Дата публикации: 06.10.2022.

[2] Пачина Н.Н., Касенов А.Д. Стратегические направления, факторы и условия противодействия распространению информационного экстремизма // Известия ТулГУ. Гуманитарные науки. 2024. №4. С. 35-48.

#### References:

[1] The Constitution of the Russian

Federation (adopted by popular vote 12.12.1993 with amendments approved during the all-Russian vote 01.07.2020). - Text: electronic//Official Internet portal of legal information. – URL: <http://pravo.gov.ru/>. - Published on: 06.10.2022.

[2] Pachina N.N., Kasenov A.D. Strategic directions, factors and conditions for countering the spread of information extremism//Izvestia TulsU. Humanities. 2024. №4. S. 35-48.

---

---



**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](http://www.law-books.ru)*