

**Прокопьева А. В.** – доцент кафедры философии и социально-гуманитарных дисциплин Восточно-Сибирского института МВД России (Россия, г. Иркутск)

## **ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В ИНТЕРНЕТ-СРЕДЕ**

### **DIGITAL TECHNOLOGIES IN COUNTERING ONLINE EXTREMISM**

**Аннотация.** В статье исследуется роль цифровых технологий в системе противодействия экстремизму в интернет-среде. Автор анализирует трансформацию информационно-коммуникационного пространства в ключевую площадку для распространения радикальных идеологий, вербовки и координации противоправной деятельности. Рассматриваются действующие правовые и организационные механизмы мониторинга и блокировки запрещенного контента, включая взаимодействие с Роскомнадзором. Особое внимание уделено уязвимости молодежной аудитории и региональному опыту профилактической работы. В заключение обосновывается необходимость комплексного подхода, сочетающего развитие технологий искусственного интеллекта для проактивного выявления угроз, совершенствование межведомственного взаимодействия и масштабирование просветительских программ по формированию цифровой грамотности и критического мышления.

**Ключевые слова:** экстремизм, интернет, цифровые технологии, искусственный интеллект, киберпространство, профилактика, молодежь, Роскомнадзор, информационная безопасность.

**Abstract.** The article explores the role of digital technologies in countering extremism in the online environment. The author analyzes the transformation of the information and communication space into a key platform for the spread of radical ideologies, recruitment, and the coordination of illegal activities. The article examines the existing legal and organizational mechanisms for monitoring and blocking prohibited content, including cooperation with Roskomnadzor. Special attention is given to the vulnerability of young audiences and regional experiences in preventive work. In conclusion, the paper substantiates the need for a comprehensive approach that combines the development of artificial intelligence technologies for proactive threat detection, improving interagency cooperation, and scaling up educational programs to promote digital literacy and critical thinking.

**Keywords:** extremism, internet, digital technologies, artificial intelligence, cyberspace, prevention, youth, roskomnadzor, information security.

Стремительная цифровизация общества привела к переносу значительной части социальных, экономических и политических процессов в виртуальное пространство. Данная трансформация, наряду с несомненными преимуществами, породила новые серьезные вызовы в сфере национальной безопасности. Интернет-среда, характеризующаяся глобальностью, анонимностью и высокой скоростью распространения информации, стала основным каналом для пропаганды экстремистских и террористических идеологий, вербовки сторонников и координации их действий. Это обуславливает актуальность исследования современных цифровых технологий не только как инструмента деструктивных сил, но и как ключевого элемента системы противодействия им.

### **1. Информационно-коммуникационная среда как ключевая площадка современных экстремистских угроз.**

В начале XXI века кардинально изменилась среда распространения деструктивных идеологий. «С началом нового века именно информационно-коммуникационная среда стала плодородной почвой для экспансии радикальных взглядов, популяризации деструктивных идей, апробации новых способов вербовки неофитов и манипулирования общественным сознанием, совершения кибератак на государственные IT-ресурсы и банковский сектор, модернизации приемов содействия экстремизму и терроризму в обход традиционной финансовой системы и т. д.» [2, с. 188]. Данная трансформация обусловлена глобальным характером сети Интернет, ее анонимностью, скоростью распространения информации и способностью точно воздействовать на целевую аудиторию.

Ключевой особенностью экстремизма в цифровую эпоху является его публичная природа. Как отмечают исследователи: «Важнейшим определяющим признаком экстремистских проявлений в информационном поле является публичность, обеспечиваемая выступлением на открытых площадках с участием двух и более человек, а также средств массовой информации и виртуальных площадок, действующих на базе сети Интернет» [3, с. 9]. Таким образом, сеть Интернет, являясь по сути глобальной публичной площадкой, не только облегчает коммуникацию между сторонниками радикальных идей, но и выступает инструментом рекрутирования и пропаганды, формируя видимость массовости и легитимности маргинальных течений.

### **2. Правовые и организационные механизмы противодействия цифровому экстремизму.**

Эффективное противодействие указанным вызовам требует комплексного подхода, сочетающего технологические решения и правовое регулирование. На законодательном уровне одним из центральных инструментов является ведение специализированного реестра запрещенных материалов. В этой связи подчеркивается, что «Мониторинг социальных сетей

на наличие в них экстремистских и террористических материалов должен осуществляться во взаимодействии с Роскомнадзором, который ведет Реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие призывы к массовым беспорядкам, осуществлению экстремистской и террористической деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка» [1, с. 297].

Данный механизм создает правовую основу для ограничения доступа к опасному контенту. Однако оперативность выявления и блокировки таких материалов остается серьезной практической задачей, учитывая лавинообразный рост объема информации и использование экстремистскими группами зашифрованных каналов связи и ресурсов в даркнете. Это актуализирует необходимость развития систем автоматизированного мониторинга на основе технологий искусственного интеллекта, способных анализировать семантику текстов, изображений и видео.

### **3. Профилактика экстремизма в молодежной среде: региональный аспект.**

Особое внимание в системе противодействия экстремизму уделяется молодежи как наиболее уязвимой социальной группе. Исследователи констатируют, что «В современных условиях Интернет необходимо отнести к одному из основных каналов массовой информации, который с высокой степенью эффективности может воздействовать на молодых людей, не определившихся в своих идеологических приоритетах, чьи ценности, ориентации и смысловые установки еще неустойчивы, а их жизненные траектории могут склониться как в зону принимаемых обществом моделей поведения, так и асоциальных, антиобщественных действий, а также тех, кто входит в состав террористических бандформирований и экстремистских группировок» [5]. Психологическая податливость, поиск идентичности и активное использование цифровых технологий делают молодое поколение первостепенной мишенью для вербовщиков.

Ответом на эту угрозу должны стать не только репрессивные, но в первую очередь профилактические меры, реализуемые на всех уровнях. Положительный опыт такой работы накоплен в регионах. Например: «Молодежному аспекту в рамках экстремизма уделяется большое внимание в Иркутской области. Так, каждый год проводятся дни лекций, на которых говорится о важности вовлечения молодого поколения в борьбу с экстремизмом» [4, с. 93].

Подобные просветительские инициативы, направленные на формирование правовой грамотности и критического мышления, являются важным элементом построения устойчивого иммунитета общества к радикальной идеологии. Их тиражирование и адаптация с учетом местной специфики представляется одним из ключевых направлений профилактической работы.

Эффективность мониторинга и нейтрализации противоправного контента напрямую зависит от слаженности действий всех субъектов, задействованных в этой работе. Взаимодействие правоохранительных органов с Роскомнадзором, который ведет реестр запрещенных ресурсов, является необходимым, но не достаточным условием. Для повышения оперативности требуется создание единых межведомственных платформ обмена данными в режиме реального времени, которые объединили бы усилия МВД России, ФСБ России, Роскомнадзора и генеральной прокуратуры. Подобная централизация позволит не только быстро блокировать уже выявленные ресурсы, но и проводить проактивный анализ цифровых следов для выявления сетевых структур и пресечения деятельности распространителей экстремистских материалов на ранних стадиях.

Важнейшим направлением совершенствования является внедрение передовых технологий анализа данных. Современные системы на основе искусственного интеллекта и машинного обучения способны автоматически выявлять семантические паттерны, характерные для экстремистской пропаганды, анализировать мультимедийный контент (изображения, видео, аудио) и отслеживать связи между пользователями в закрытых сообществах и мессенджерах. Однако развитие таких технологий сопряжено с этическими и правовыми вызовами, связанными с необходимостью защиты персональных данных и недопущения цензуры легитимных форм выражения мнения.

Параллельно с развитием технологий контроля необходимо активно формировать цифровую грамотность и правосознание у пользователей, особенно среди молодежи. Просветительские программы и кампании в медиасреде должны не просто информировать о запретах, но и развивать критическое мышление, умение распознавать манипулятивные техники и противостоять им.

Таким образом, комплексный подход, сочетающий жесткие меры по пресечению противоправной деятельности с мягкими мерами по воспитанию устойчивого иммунитета к радикальной идеологии, представляется наиболее сбалансированной и перспективной стратегией в долгосрочной борьбе с цифровым экстремизмом.

### **Библиографический список**

1. Берова Д. М., Карданов Р. Р. Противодействие использованию сети Интернет в террористических целях // Проблемы экономики и юридической практики. 2021. Т. 17, № 3. С. 295–298.
2. Опалев А. В. Современные информационные технологии как инструмент деятельности экстремистских и террористических организаций // Вестник Московского университета МВД России 2022. № 5.

3. Применение информационных технологий в профилактике экстремизма в молодежной среде : учебно-методическое пособие / П. Е. Суслонов, А. Н. Старостин, В. Л. Назаров [и др.] ; под общ. ред. В. Л. Назарова ; Министерство науки и высшего образования Российской Федерации. Екатеринбург : Изд-во Урал.ун-та, 2021. 140 с.

4. Прокопьева А. В. Экстремизм и его угрозы в отношении молодежи Иркутской области // Экстремизм: новые вызовы региональной безопасности : сборник научных трудов по итогам международной научно-практической конференции (Барнаул, 27 марта 2025 года). Барнаул : Барнаульский юридический институт МВД России, 2025. С. 93–95.

5. Профилактика экстремизма в сети Интернет // Международный институт компьютерных технологий. URL: <https://iict.ru/> (дата обращения: 28.02.2026).

© Прокопьева А. В., 2026

УДК 323.28:343.85

**Рябчиков С. А.** – доцент кафедры криминалистики Уфимского юридического института МВД России (Россия, г. Уфа)

## **ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОФИЛАКТИКЕ ЭКСТРЕМИЗМА: ТЕХНОЛОГИЧЕСКИЕ ВОЗМОЖНОСТИ И ПРАВОВЫЕ ОГРАНИЧЕНИЯ**

### **ARTIFICIAL INTELLIGENCE IN EXTREMISM PREVENTION: TECHNOLOGICAL CAPABILITIES AND LEGAL RESTRICTIONS**

**Аннотация.** В статье проводится комплексный анализ применения технологий искусственного интеллекта в профилактике экстремистской деятельности в цифровой среде. Исследуются современные технологические решения для мониторинга, выявления и пресечения распространения экстремистских материалов в сети Интернет, отмечается положительный опыт Российской Федерации. Подробно рассматриваются правовые ограничения, связанные с использованием искусственного интеллекта в деятельности сотрудников правоохранительных органов, включая защиту персональных данных, прозрачности алгоритмов и соблюдения фундаментальных прав человека. На основе сравнительного анализа международных и национальных правовых норм формулируются рекомендации по сбалансированному развитию практических подходов, позволяющих реализовать потенциал искусственного интеллекта по профилактике экстремизма.