УДК 327.8 **DOI: 10.34670/AR.2026.99.37.006**

Проблемы и перспективы повышения эффективности региональной антитеррористической политики в условиях цифровизации и информационных войн

Девятов Александр Андреевич

Аспирант,
Воронежский филиал
Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации,
394005, Российская Федерация, Воронеж, просп. Московский, 143;
e-mail: kafppu@vrn.ranepa.ru

Слинько Александр Анатольевич

Доктор политических наук, профессор,
Воронежский филиал
Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации,
394005, Российская Федерация, Воронеж, просп. Московский, 143;
e-mail: kafppu@vrn.ranepa.ru

Аннотация

Автор рассматривает в статье, какие перспективы региональной антитеррористической деятельности в РФ открываются в условиях информатизации и цифровизации. Цифровизация общественных процессов, распространение социальных сетей создали новые каналы террористической пропаганды, что требует модернизации методов информационного противодействия на региональном уровне.

Для цитирования в научных исследованиях

Девятов А.А., Слинько А.А. Проблемы и перспективы повышения эффективности региональной антитеррористической политики в условиях цифровизации и информационных войн // Теории и проблемы политических исследований. 2026. Том 15. № 5А. С. 54-60. DOI: 10.34670/AR.2026.99.37.006

Ключевые слова

Антитеррористическая деятельность, региональная антитеррористическая политика, цифровизация, информационные войны, онлайн-радикализация, кибербезопасность, цифровая профилактика.

Введение

Современный этап развития общества характеризуется масштабной цифровизацией всех сфер жизни, проникновением информационных технологий в политику, экономику, социальные отношения. Цифровая трансформация создает не только новые возможности для развития, но и новые угрозы безопасности, включая террористические. Террористические организации активно используют цифровые технологии для планирования атак, вербовки сторонников, финансирования деятельности, пропаганды радикальной идеологии. Информационные войны, ведущиеся в цифровом пространстве, включают распространение дезинформации, манипулирование общественным сознанием, дестабилизацию социально-политической ситуации. Региональная антитеррористическая политика сталкивается с необходимостью адаптации к цифровым вызовам, разработки новых методов противодействия, внедрения технологических решений. [[Раджабли, Слинько, 2024, с.142].

Использование интернета и социальных сетей террористическими организациями качественно изменило характер террористических угроз. Если ранее вербовка в террористические организации осуществлялась преимущественно через личные контакты, то в цифровую эпоху интернет стал основным каналом распространения радикальной идеологии, поиска и вербовки сторонников. Террористические организации создают профессионально оформленные сайты, аккаунты в социальных сетях, каналы в мессенджерах, через которые транслируют пропагандистский контент, инструкции по совершению терактов, призывы к насилию. Анонимность интернета, трансграничный характер цифрового пространства затрудняют выявление и пресечение террористической деятельности онлайн [Пинкевич, Зубалова, 2020, с. 65].

Региональная антитеррористическая политика в Российской Федерации

Феномен онлайн-радикализации, когда индивиды, не имевшие ранее связей с террористическими организациями, под влиянием интернет-пропаганды самостоятельно принимают решение о совершении террористических актов, представляет серьезный вызов. «Одинокие волки», радикализировавшиеся в интернете, сложнее выявляются спецслужбами, поскольку не входят в известные террористические сети, не контактируют с известными экстремистами. Региональные антитеррористические структуры сталкиваются с необходимостью мониторинга цифрового пространства, выявления признаков радикализации в онлайн-поведении, разработки методов профилактического воздействия на лиц, подверженных влиянию экстремистской идеологии.

Мессенджеры с шифрованием, анонимные сети, криптовалюты создают возможности для конспиративной деятельности террористических организаций. Планирование терактов, координация действий, передача инструкций осуществляются через зашифрованные каналы, недоступные для контроля спецслужб. Финансирование терроризма через криптовалюты затрудняет отслеживание финансовых потоков, выявление источников и получателей средств. Противодействие данным угрозам требует развития технологических возможностей правоохранительных органов, привлечения специалистов в области информационных технологий, международного сотрудничества с IT-компаниями [Зубарев, 2022, с. 178].

Информационные войны в цифровом пространстве включают распространение

дезинформации, фейковых новостей, манипулятивного контента, направленного на дестабилизацию социально-политической ситуации, подрыв доверия к власти, разжигание межнациональной и межконфессиональной розни. Информационные атаки могут предшествовать или сопровождать террористические акты, усиливая их психологический эффект, создавая панику, дезориентируя общество. Региональная антитеррористическая политика требует развития систем мониторинга информационного пространства, оперативного выявления и опровержения дезинформации, информирования населения о реальной ситуации.

Блокирование экстремистского контента в интернете составляет важное направление цифрового противодействия терроризму. Российское законодательство предусматривает механизмы блокирования сайтов, содержащих материалы экстремистского характера, призывы к терроризму. Роскомнадзор на основании решений судов или по требованию Генеральной прокуратуры осуществляет блокирование доступа к таким ресурсам. Вместе с тем эффективность блокирования ограничена техническими возможностями обхода блокировок, использованием зарубежных хостингов, быстрым созданием новых ресурсов взамен заблокированных. Более эффективным представляется комплексный подход, сочетающий блокирование с созданием позитивного контента, дискредитацией экстремистской идеологии, формированием критического мышления пользователей [Лебедева, 2021, с. 211].

Создание систем мониторинга социальных сетей, выявления экстремистского контента, лиц, распространяющих радикальную идеологию, требует использования технологий искусственного интеллекта, машинного обучения, больших данных. Автоматизированные системы могут анализировать огромные объемы информации в социальных сетях, выявлять ключевые слова, фразы, образы, характерные для экстремистского контента. Вместе с тем полностью автоматизированный мониторинг недостаточен, требуется участие специалистов-аналитиков, способных интерпретировать контекст, отличать реальные угрозы от ложных тревог, принимать обоснованные решения о необходимости реагирования.

Региональные антитеррористические комиссии сталкиваются с проблемой недостаточных технологических и кадровых ресурсов для эффективного противодействия цифровым угрозам. Большинство сотрудников аппаратов комиссий не обладают специализированными компетенциями в области информационных технологий, цифровой безопасности, анализа больших данных. Привлечение IT-специалистов, создание специализированных подразделений, занимающихся мониторингом цифрового пространства, повышение квалификации сотрудников в области цифровых технологий представляются необходимыми мерами. Взаимодействие с IT-компаниями, научными организациями, занимающимися исследованиями в области цифровой безопасности, расширяет возможности региональных структур [Романов, 2022, с. 245].

Цифровая профилактика терроризма включает создание позитивного онлайн-контента, альтернативного экстремистской пропаганде. Антитеррористические комиссии координируют создание информационных ресурсов, социальных сетей, каналов, транслирующих идеи толерантности, межнационального согласия, традиционных ценностей. Привлечение популярных блогеров, лидеров мнений, молодежных активистов к созданию и распространению позитивного контента повышает его охват и влияние. Использование современных форматов – видеороликов, подкастов, интерактивных проектов – делает профилактический контент привлекательным для целевой аудитории, особенно молодежи.

Образовательные программы по цифровой грамотности, критическому мышлению, безопасному поведению в интернете способствуют формированию иммунитета к экстремистской пропаганде. Включение в школьные и вузовские программы курсов по

медиаграмотности, анализу информации, распознаванию манипулятивных техник готовит молодое поколение к безопасному использованию цифровых технологий. Проведение тренингов, семинаров, конкурсов по цифровой безопасности для педагогов, родителей, самих учащихся расширяет охват профилактической работы. Формирование навыков критического анализа информации, проверки источников, распознавания фейков снижает уязвимость к информационным манипуляциям [Соколов, 2021, с. 267].

Взаимодействие с IT-компаниями, владельцами социальных сетей, интернет-платформ представляет важное направление цифрового противодействия терроризму. Крупные технологические компании обладают ресурсами и технологиями для выявления и удаления экстремистского контента, блокирования аккаунтов террористических организаций, предотвращения использования их платформ в террористических целях. Некоторые компании разработали автоматизированные системы модерации контента, используют технологии искусственного интеллекта для выявления запрещенных материалов. Вместе с тем сотрудничество государственных органов и IT-компаний сталкивается с проблемами конфиденциальности данных, различиями в правовых системах, политическими разногласиями.

Международное сотрудничество в цифровой сфере критически важно для эффективного противодействия транснациональному онлайн-терроризму. Террористический контент размещается на серверах в различных странах, террористы используют платформы, зарегистрированные в разных юрисдикциях. Эффективное противодействие требует международной координации, обмена информацией, совместных действий по блокированию и удалению экстремистского контента. Россия участвует в международных инициативах по борьбе с онлайн-терроризмом, взаимодействует с зарубежными правоохранительными органами, выступает за выработку международных норм регулирования цифрового пространства. [Москалец, Слинько, 2024, с.50].

Таблица 1 – Цифровые угрозы и меры противодействия в региональной антитеррористической политике

Цифровая угроза	Проявления	Меры противодействия	Проблемы реализации
Онлайн-вербовка	Распространение экстремистской пропаганды в соцсетях, мессенджерах	Мониторинг соцсетей, блокирование контента, создание альтернативного контента	Анонимность, зашифрованные каналы, трансграничность
Онлайн-радикализация	«Одинокие волки», самостоятельная радикализация через интернет	Цифровая профилактика, выявление признаков радикализации, работа с группами риска	Сложность выявления, отсутствие явных связей с террористами
Информационные войны	Дезинформация, фейки, манипулятивный контент	Мониторинг инфопространства, опровержение фейков, медиаграмотность населения	Скорость распространения фейков, массовость аудитории
Киберфинансирование	Использование криптовалют для финансирования терроризма	Отслеживание крипто-транзакций, регулирование криптовалют, международное сотрудничество	Анонимность криптовалют, сложность регулирования

Правовое регулирование цифрового пространства в контексте противодействия терроризму представляет сложную задачу, требующую баланса между безопасностью и защитой прав и свобод граждан. Меры по мониторингу интернета, блокированию контента, сбору данных о пользователях должны осуществляться в правовых рамках, с соблюдением конституционных прав на свободу слова, неприкосновенность частной жизни, тайну переписки. Чрезмерное

регулирование может приводить к ограничению свободы информации, цензуре, нарушению прав граждан. Выработка сбалансированного правового регулирования, обеспечивающего эффективное противодействие цифровым террористическим угрозам при соблюдении прав человека, остается актуальной задачей [Устинов, 2020, с. 203].

Развитие технологий искусственного интеллекта открывает новые перспективы для антитеррористической деятельности. Системы искусственного интеллекта способны анализировать огромные массивы данных, выявлять паттерны поведения, характерные для террористической деятельности, прогнозировать угрозы. Использование технологий распознавания лиц, анализа поведения может способствовать выявлению подозрительных лиц в местах массового скопления людей, на транспорте, критически важных объектах. Вместе с тем использование таких технологий вызывает этические вопросы, опасения относительно тотальной слежки, нарушения приватности [Шевченко, 2022, с. 298].

Перспективы повышения эффективности региональной антитеррористической политики в цифровую эпоху связаны с комплексным подходом, включающим технологическую модернизацию, развитие кадрового потенциала, совершенствование правового регулирования, международное сотрудничество, партнерство с бизнесом и гражданским обществом. Создание региональных центров мониторинга цифрового пространства, оснащенных современными технологиями и укомплектованных квалифицированными специалистами, повысит возможности оперативного выявления цифровых террористических угроз. Развитие системы подготовки специалистов в области цифровой безопасности, проведение научных исследований цифровых аспектов терроризма, распространение лучших практик цифрового противодействия обеспечат устойчивое развитие потенциала региональной антитеррористической системы.

Цифровая трансформация антитеррористической деятельности должна сопровождаться развитием межведомственного взаимодействия, поскольку эффективное противодействие цифровым угрозам требует координации усилий спецслужб, правоохранительных органов, регуляторов цифровой сферы, IT-компаний, образовательных учреждений, гражданского общества. Создание единых цифровых платформ для обмена информацией, координации действий, мониторинга ситуации повысит оперативность и эффективность взаимодействия. Формирование культуры цифровой безопасности в обществе, осознание гражданами цифровых угроз и способов защиты, активное участие общества в противодействии цифровому терроризму составят прочную основу обеспечения безопасности в цифровую эпоху [Ярочкин, Бузанова, 2021, с. 287].

Заключение

Таким образом, цифровизация и информационные войны создают качественно новые вызовы для региональной антитеррористической политики, требующие адаптации стратегий, методов, технологий. Террористические организации активно используют цифровые технологии для вербовки, планирования, пропаганды, что требует развития цифровых возможностей противодействия. Региональные антитеррористические структуры сталкиваются с проблемами недостаточных технологических и кадровых ресурсов, правового регулирования, международной координации. Перспективы повышения эффективности связаны с технологической модернизацией, развитием кадрового потенциала, совершенствованием правовых механизмов, цифровой профилактикой, взаимодействием государства, бизнеса и гражданского общества в обеспечении цифровой безопасности и противодействии

террористическим угрозам в цифровом пространстве.

Библиография

1. Зубарев С.М. Информационные технологии в деятельности террористических организаций / С.М. Зубарев // Информационное общество. — 2022. — № 3. — С. 174-184.
2. Лебедева Н.С. Блокирование экстремистского контента: правовые и технические аспекты / Н.С. Лебедева // Информационное право. — 2021. — № 4. — С. 207-217.
3. Москалец А.В. Новые политические и экономические феномены в мировой политике / А.В. Москалец, А.А. Слинько // Теории и проблемы политических исследований. — 2024. — Т. 13. — № 2-1. — С. 47-53.
4. Пинкевич Т.В. Современное состояние экстремизма и терроризма в условиях развития цифровых технологий / Т.В. Пинкевич, О.А. Зубалова // Юристъ-Правоведъ. — 2020. — № 3 (94). — С. 64-68.
5. Раджабли О.Ю. Внутренняя политика Российской Федерации по противодействию террористической угрозе: принципы и эффективность / О.Ю. Раджабли, А.А. Слинько // Регион: системы, экономика, управление. — 2024. — № 3 (66). — С. 142-147.
6. Романов Д.А. Кадровое обеспечение антитеррористической деятельности / Д.А. Романов // Управление персоналом и интеллектуальными ресурсами в России. — 2022. — № 2. — С. 241-250.
7. Соколов И.А. Цифровая грамотность как фактор профилактики экстремизма / И.А. Соколов // Образование и наука. — 2021. — № 7. — С. 263-276.
8. Устинов В.В. Правовые основы противодействия терроризму / В.В. Устинов. — М.: Юстиция, 2020. — 336 с.
9. Шевченко С.Н. Искусственный интеллект в антитеррористической деятельности / С.Н. Шевченко // Информационные технологии. — 2022. — № 5. — С. 294-305.
10. Ярочкин В.И. Международный опыт противодействия терроризму / В.И. Ярочкин, С.А. Бузанова. — М.: Ось-89, 2021. — 368 с.

Problems and Prospects for Increasing the Efficiency of Regional Anti-Terrorist Policy in the Context of Digitalization and Information Wars

Aleksandr A. Devyatov

Postgraduate Student,
Voronezh Branch
of the Russian Presidential Academy of National Economy
and Public Administration,
394005, 143, Moskovskiy ave., Voronezh, Russian Federation;
e-mail: kafppu@vrn.ranepa.ru

Aleksandr A. Slin'ko

Doctor of Political Sciences, Professor,
Voronezh Branch
of the Russian Presidential Academy of National Economy
and Public Administration,
394005, 143, Moskovskiy ave., Voronezh, Russian Federation;
e-mail: kafppu@vrn.ranepa.ru

Abstract

The author examines in the article what prospects for regional anti-terrorist activities in the Russian Federation are opening up in the context of informatization and digitalization. The

digitalization of social processes and the spread of social networks have created new channels for terrorist propaganda, which requires the modernization of information counteraction methods at the regional level.

For citation

Devyatov A.A., Slin'ko A.A. (2026) Problemy i perspektivy povysheniya effektivnosti regional'noy antiterroristicheskoy politiki v usloviyakh tsifrovizatsii i informatsionnykh voyn [Problems and Prospects for Increasing the Efficiency of Regional Anti-Terrorist Policy in the Context of Digitalization and Information Wars]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 15 (5A), pp. 54-60. DOI: 10.34670/AR.2026.99.37.006

Keywords

Anti-terrorist activities, regional anti-terrorist policy, digitalization, information wars, online radicalization, cybersecurity, digital prevention.

References

1. Lebedeva, N.S. (2021). Blokirovaniye ekstremistskogo kontenta: pravovyye i tekhnicheskiye aspekty [Blocking Extremist Content: Legal and Technical Aspects]. Informatsionnoye pravo, (4), 207-217.
2. Moskalec, A.V., & Slinko, A.A. (2024). Novyye politicheskiye i ekonomicheskiye fenomeny v mirovoy politike [New Political and Economic Phenomena in World Politics]. Teorii i problemy politicheskikh issledovaniy, 13(2-1), 47-53.
3. Pinkevich, T.V., & Zubalova, O.A. (2020). Sovremennoye sostoyaniye ekstremizma i terrorizma v usloviyakh razvitiya tsifrovykh tekhnologiy [The Current State of Extremism and Terrorism in the Context of Digital Technology Development]. Yurist-Pravoved, (3(94)), 64-68.
4. Radzhabli, O.Y., & Slinko, A.A. (2024). Vnutrennyaya politika Rossiyskoy Federatsii po protivodeystviyu terroristicheskoy ugroze: printsipy i effektivnost [Domestic Policy of the Russian Federation on Countering the Terrorist Threat: Principles and Effectiveness]. Region: sistemy, ekonomika, upravleniye, (3(66)), 142-147.
5. Romanov, D.A. (2022). Kadrovoye obespecheniye antiterroristicheskoy deyatelnosti [Personnel Support of Anti-Terrorist Activities]. Upravleniye personalom i intellektualnymi resursami v Rossii, (2), 241-250.
6. Shevchenko, S.N. (2022). Iskusstvennyy intellekt v antiterroristicheskoy deyatelnosti [Artificial Intelligence in Anti-Terrorist Activities]. Informatsionnyye tekhnologii, (5), 294-305.
7. Sokolov, I.A. (2021). Tsifrovaya gramotnost kak faktor profilaktiki ekstremizma [Digital Literacy as a Factor in Preventing Extremism]. Obrazovaniye i nauka, (7), 263-276.
8. Ustinov, V.V. (2020). Pravovyye osnovy protivodeystviya terrorizmu [Legal Foundations of Countering Terrorism]. Yustitsiya.
9. Yarochkin, V.I., & Buzanova, S.A. (2021). Mezhdunarodnyy opyt protivodeystviya terrorizmu [International Experience in Countering Terrorism]. Os-89.
10. Zubarev, S.M. (2022). Informatsionnyye tekhnologii v deyatelnosti terroristicheskikh organizatsiy [Information Technologies in the Activities of Terrorist Organizations]. Informatsionnoye obshchestvo, (3), 174-184.