Научная статья
УДК 004.056.5
EDN: AUNUKF

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ЭТНОКОНФЕССИОНАЛЬНЫЕ РИСКИ И СИСТЕМЫ МОНИТОРИНГА

Андрей Андреевич МАКОВСКИЙ

Псковский государственный университет
Псков, Россия
aamakovsky@mail.ru
https://orcid.org/0000-0002-5505-3295

Аннотация. Цель статьи – исследование феномена информационной безопасности через призму политической проблематики этноконфессиональных угроз.

Методология исследования включает кейс ситуации в Республике Дагестан в 2023 г., связанной с массовыми волнениями, которые вызвали распространение фейковых новостей в мессенджерах. Анализ событий осуществлен исходя из данных контент-анализа Telegram-канала и политической реакции в субъекте РФ. При этом внимание акцентируется на применении инструментов цифровой мобилизации и формировании протестных и радикальных настроений в онлайн-пространстве.

В результате исследования проанализированы этноконфессиональные риски в цифровой среде, возникающие в результате политических спекуляций религиозного характера, распространения радикальных идей, а также разжигания межнациональной розни и ненависти. В работе изучаются механизмы мониторинга этноконфессиональной ситуации в сети Интернет. Рассматривается также деятельность центров управления регионами (ЦУР) как эффективных институтов, способных оперативно выявлять и нейтрализовать потенциальные этноконфессиональные угрозы в информационном пространстве субъектов РФ.

Ключевые слова: Информационная безопасность, экстремизм, социальные сети, религия, государственно-конфессиональные отношения, мониторинг, межнациональное согласие.

Заявление о конфликте интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: *Маковский А.А.* Информационная безопасность: этноконфессиональные риски и системы мониторинга // Вестник Поволжского института управления. 2025. Т. 25, № 4. С. 59–71. EDN: AUNUKF

Original article

INFORMATION SECURITY: ETHNIC-CONFESSIONAL RISKS AND MONITORING SYSTEMS

Andrey A. MAKOVSKY

Pskov State University
Pskov, Russia
aamakovsky@mail.ru
https://orcid.org/0000-0002-5505-3295

Abstract. The aim of the article is to study the phenomenon of information security through the prism of political issues of ethno-confessional threats.

The research methodology is based on the case of the situation in the Republic of Dagestan in 2023, associated with mass popular unrest, which caused the spread of fake news in messengers. The author analyzes the events based on the data of content analysis of Telegram channel and political reaction in the subject of the Russian Federation, focusing on the use of digital mobilization tools and the formation of protest and radical sentiments in the online space.

As a result of the study ethno-confessional risks in the digital environment arising from political speculation on religious topics, the spread of radical ideas, as well as incitement of interethnic discord and hatred are analyzed. The paper also studies the mechanisms of monitoring the ethno-confessional situation on the Internet. Activities of Regional Management Centers (RMCs) as effective institutions capable of promptly identifying and neutralizing potential ethno-confessional threats in the information space of the constituent entities of the Russian Federation is considered.

Keywords: information security, extremism, social networks, religion, state-confessional relations, monitoring, interethnic harmony.

Conflicts of interest. The author declares no conflicts of interest.

For citation: *Makovsky, A.A.* Information Security: Ethnic-Confessional Risks and Monitoring Systems // Bulletin of the Volga Institute of Management. 2025. Vol. 25, №. 4. P. 59–71. EDN: AUNUKF

Введение. В условиях цифровизации почти всех сфер общественной жизни проблемы информационной безопасности приобретают сугубо политический характер, выходя за рамки исключительно технического или правового измерения. Сегодня информационное пространство становится ареной геополитического противоборства, межэтнических и межконфессиональных конфликтов, что актуализирует комплексный анализ системы информационной безопасности. Вмешательство иностранных акторов в политическую повестку через цифровые платформы, распространение радикальных идеологий и религиозного экстремизма, манипуляция общественным сознанием с использованием национальных и культурных ярлыков — все это формирует новые угрозы устойчивости и безопасности государства. В связи с этим исследование информационной безопасности в контексте политико-национальных и религиозных вызовов становится не только научно значимым, но и практически необходимым для формирования эффективной государственной политики в сфере обеспечения информационной безопасности.

Данная проблематика рассматривалась как отечественными, так и зарубежными исследователями, преимущественно на пересечении политологии, социологии и юриспруденции. Значительный вклад в разработку теоретических основ информационной безопасности внесли исследования, в которых изучались политические манипуляции и деструктивные информационные потоки как угроза национальной безопасности [1—3]. Ряд работ в рамках государственной стратегии информационной безопасности, где анализировались механизмы распространения политически мотивированной дезинформации и роль социальных сетей в трансформации общественно-политической повестки, был подготовлен научными коллективами РАНХиГС, МГИМО, МГУ [4]. В рамках этноконфессиональных проблем информационная безопасность чаще всего рассматривается с точки зрения информационных угроз этноконфессиональному миру [5, с. 89], распространения ксенофобии [6], цифрового религиозного экстремизма [7, с. 145], этноконфессиональных фейк-ньюс [8, с. 156], кибердджихадизма [9. с. 118], радикализации молодежи [10].

Однако, несмотря на большое количество научных работ по указанной проблематике, современные механизмы мониторинга этноконфессиональной ситуации в информационном пространстве российских регионов изучены недостаточно. Именно поэтому цель настоящей работы — обобщение и анализ систем мониторинга этноконфессиональных угроз информационной безопасности в условиях гибридной войны, при которой информационное пространство используется в качестве инструмента целенаправленного воздействия на массовое созна-

ние, а также на процессы формирования мировоззрения этнических и религиозных сообществ — представляется весьма актуальной. Исследовательский интерес заключается в необходимости осмысления эффективных механизмов мониторинга цифровых рисков и манипулятивных воздействий посредством цифровых коммуникационных каналов.

Основным научным подходом исследования избрана теория исторического неоинституционализма, основанная на явлении «троп зависимости», определяющем исторический контекст современных институциональных взаимодействий. При таком подходе оказываются задействованными реперные исторические точки в формировании этноконфессиональных отношений в России, так как возникает необходимость «сужения» объекта исследования ввиду обширности проблематики этнических и религиозных рисков. Ярким примером этноконфессионлаьных рисков и работы системы мониторинга явилась ситуация в Республике Дагестан в 2023 г., в ходе которой было предпринято посягательство прозападных сил на информационную безопасность Российской Федерации. Отметим, что применение контент-анализа по методу О. Хольсти Telegram-источников — медиаматериалов, публикаций в социальных сетях, агитационных текстов — позволяет выявить структуру и характер информационного воздействия на целевые аудитории, включая этнические и конфессиональные сообщества.

Теоретико-правовые основы информационной безопасности: этноконфессиональная проблематика. Термин «информационная безопасность» неизменно остается предметом активной научной дискуссии, что объясняется как многообразием акторов и объектов рассматриваемых отношений, так и сложной, междисциплинарной природой самого феномена. В академическом дискурсе можно обнаружить различные интерпретации — от юридических до философских и социологических подходов. В рамках настоящего анализа представляется целесообразным сосредоточиться на ряде исследовательских позиций, сформулированных в политологической науке. Так, А.Д. Урсул и Т.Н. Цырдя рассматривают информационную безопасность как способность государства, общества, социальных групп и отдельных индивидов с определенной степенью вероятности противодействовать информационным угрозам и опасностям. Под рисками такого характера понимаются деструктивные воздействия на общественное и индивидуальное сознание, психоэмоциональное состояние граждан, а также на инфраструктуру цифровой и технической среды, включая компьютерные сети и системы хранения и передачи данных [11].

О.М. Манжуева отмечает, что фундаментальная природа безопасности любой системы заключается в ее способности сохранять структур-

ную и функциональную целостность, а также обеспечивать устойчивое развитие в условиях внешнего давления, включая конфликты, риски и неопределенность. Система обеспечения безопасности, в частности информационная, представляет собой механизм реализации адаптивного потенциала системы в изменчивой среде. В этом контексте информационная безопасность должна трактоваться одновременно как защита объекта в условиях информационного взаимодействия, так и поддержание устойчивости самой информационной среды — ее структур, потоков и институциональных рамок [12].

Опираясь на представленные научные подходы, можно сформулировать интегральное понимание сущности информационной безопасности, включающее три взаимосвязанных аспекта:

— защиту самой информации как стратегического ресурса;

— обеспечение безопасности субъектов информационного взаимодействия от деструктивных или манипулятивных воздействий;

— формирование и поддержание безопасного состояния информационной среды, необходимого для удовлетворения легитимных информационных потребностей общества, институтов и личности.

Согласно Стратегии национальной безопасности Российской Федерации от 2 июля 2021 г., национальные интересы Российской Федерации и ее стратегические приоритеты неразрывно связаны с формированием устойчивого и безопасного информационного пространства, способного противостоять деструктивному информационно-психологическому воздействию на общество [13]. Защита этих интересов обеспечивается посредством консолидации усилий органов публичной власти, институтов гражданского общества и профильных организаций, ориентированных на реализацию приоритетных направлений государственной политики, среди которых ключевое место занимает информационная безопасность как системообразующий элемент национальной безопасности в целом.

Исходя из Доктрины информационной безопасности Российской Федерации, информационная безопасность в юридическом поле рассматривается как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при которой обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [14].

Обеспечение информационной безопасности трактуется как целенаправленная и системная деятельность, включающая взаимосвязанный комплекс правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, ин-

формационно-аналитических, кадровых, экономических и иных мероприятий, направленных на прогнозирование, выявление, сдерживание, предотвращение и отражение информационных угроз, а также на ликвидацию их последствий.

Следует отметить, что именно прогнозирование и сдерживание являются основополагающим механизмом купирования конфликтов в цифровом информационном пространстве. Отечественные исследователи выделяют ряд этноконфессиональных вызовов для информационной безопасности, актуальных на территории России в силу «троп зависимости» и международного информационного противостояния. Р.Р. Карданов наряду с другими авторами выделяет угрозу активности террористических и экстремистских структур в онлайн-среде [15, с. 89]. Это проблема усложняется новыми вызовами: киберджихадизмом, кибершейхизмом (квазирелигиозные проповедники) [16, с. 113]; киберрелигиями (новыми религиозными направлениями), киберсектами (радикальными информационными сообществами, основанными на культе личности проповедника). В.Э. Волков освещает проблему информационного сепаратизма, возникновение которой обусловлено информационно-психологическим давлением на национальные и религиозные меньшинства [17, с. 17].

Исходя из исследовательских позиций, можно предположить, что информационная безопасность в контексте этноконфессиональных угроз — это состояние защищенности информационного пространства государства от деструктивного воздействия информации, направленной на разжигание межнациональной и межконфессиональной розни, подрыв межэтнического и межрелигиозного согласия, дестабилизацию общественно-политической обстановки и манипулирование идентичностями.

В результате анализа этноконфессиональных процессов сущность информационной безопасности можно определить как ряд определенных функций:

— предотвращение распространения экстремистских идеологий, радикальных религиозных учений в информационном поле;

— защита общества от манипулятивных попыток внешних и внутренних акторов использовать этноконфессиональную тематику для политического давления или сепаратизма;

— мониторинг и нейтрализация фейков, направленных на подрыв межнационального и межконфессионального доверия.

По мнению С.Р. Хайкина и С.Б. Бережковой, главное значение в обеспечении информационной безопасности принадлежит системе мониторинга [18, с. 104], которая включает регулярный анализ и оценку состояния сетевого и медийного пространства, социальных сетей, мес-

сенджеров, видеохостингов и других коммуникационных платформ. Мониторингу подлежит содержание, связанное с политическими событиями, религиозной и этнической тематикой, а также динамика общественного мнения, проявления радикализма, конфликтные сообщения, распространение фейков, призывы к насилию и сепаратизму. Особое внимание уделяется анализу активности деструктивных акторов, выявлению сетей распространения информации, координированных кампаний, а также фальсифицированного или манипулятивного контента.

Таким образом, информационная безопасность в современных условиях является неотъемлемой составляющей национальной безопасности, отражающей как устойчивость информационного пространства, так и способность государства и общества противостоять внутренним и внешним угрозам, включая этноконфессиональные риски. Эффективность обеспечения информационной безопасности определяется не только уровнем технологического развития, но и своевременностью выявления этноконфессиональных рисков и их нейтрализацией. К числу наиболее значимых вызовов в данной сфере относятся следующие: распространение идей религиозного экстремизма, этнонационалистический сепаратизм, киберджихадизм, кибершиизм, межконфессиональная вражда, радикализация молодежи в цифровой среде, деструктивное влияние псевдорелигиозных сообществ, вмешательство иностранных акторов в конфессиональные процессы, информационно-психологическое давление на национальные и религиозные меньшинства.

Инструменты мониторинга этноконфессиональных угроз в региональном политическом пространстве. Предупреждение религиозных конфликтов и проявления ксенофобии возможно за счет мониторинга общественной напряженности [19, с. 102]. Данная технология помогает выявлять изменения в отношениях между различными этническими и религиозными группами, обнаруживать ранние признаки напряженности и принимать меры для предотвращения вероятных конфликтов. Результаты мониторинга используются для информирования государственных органов и правоохранительных структур, чтобы они могли разрабатывать и реализовывать эффективные программы по поддержанию межнационального и межконфессионального мира. Оперативный сбор и анализ информации о потенциальных угрозах, таких как экстремистская деятельность, дискриминация или рост ксенофобии, позволяют своевременно принимать меры для их нейтрализации [20, с. 260].

Целевые опросы общественного мнения, определяющие состояние межнациональных и межконфессиональных отношений, проводятся профильными министерствами субъектов РФ, ФСБ РФ и ФСО РФ. Ежегодно органами государственной власти субъектов РФ осуществляется

проведение социологических исследований по методам звонка, онлайн-опроса, подомового опроса [21].

Особо продуктивен мониторинг региональных центров управления регионами (ЦУР) [22], которые юридически выражены в АНО «Диалог Регионы» как дочерняя структура АНО «Диалог» [23]. ЦУР — это специальная структура, созданная для координации и управления процессами в регионах (социальные сети, сайты, мессенджеры) с целью повышения эффективности взаимодействия между гражданами и органами власти. ЦУР централизованно принимают, обрабатывают и передают обращения граждан в соответствующие органы власти для решения возникающих проблем. Это повышает скорость и эффективность реагирования на запросы населения. Центры занимаются сбором и анализом данных, что позволяет делать прогнозы и принимать обоснованные управленческие решения, направленные на развитие региона и улучшение качества жизни граждан.

К компетенции ЦУР относятся координация работ по мониторингу и обработке всех видов обращений и сообщений российских граждан, взаимодействие с гражданами через социальные сети, оперативное реагирование по направлениям и тематикам и, конечно, мониторинг информационных ресурсов, социальных сетей в целях выявления сообщений, направленных на разжигание межнациональной и межрелигиозной вражды [24].

ЦУР может использовать несколько методов для мониторинга социальных сетей. Самый распространенный — использование автоматизированных инструментов. Для мониторинга социальных медиа, отслеживания упоминаний, хештегов и ключевых слов, выявления тенденций и важных событий используется программное обеспечение ИАС «Инцидент менеджмент» компании «Медиалогия», созданной в 2018 г. [22].

В межнациональной и межрелигиозной тематике проводится мониторинг таких тем, как неуважение традиций, бытовые конфликты на межнациональной почве, разжигание межнациональной розни и т.д.

ЦУР проводит сбор и анализ больших объемов данных для выявления паттернов и трендов. Этот процесс включает в себя анализ тональности сообщений и выявление ключевых тем. В случае экстренной ситуации специалисты могут вручную просматривать сообщения и посты в социальных сетях для выявления потенциальных угроз или важных новостей [23].

Таким образом, в регионах России сформировалась эффективная технология мониторинга этноконфессиональной ситуации. Следует выделить возможность прямого обращения граждан, социологические

опросы, проводимые на постоянной основе профильными органами государственной власти. Особое значение для информационной безопасности имеет работа центров управления регионами, которые в социальных сетях оперативно находят очаги социального возгорания, в том числе по этноконфессиональной проблематике. Нередко вольно или невольно межнациональные и религиозные конфликты разжигает молодежь, то есть люди младше 35 лет. Весь негатив они выплескивают в социальные сети и тем самым привлекают внимание специалистов. Мониторинг позволяет выявить конфликт на начальной стадии и своевременно его купировать.

Этноконфессиональные вызовы системе информационной безопасности. С развитием цифровых технологий Интернет стал не только пространством для свободного обмена мнениями и культурного диалога, но и средой для распространения деструктивных идей, включая разжигание национальной розни. Анонимность, скорость распространения информации и слабая модерация на онлайн-платформах создают благоприятную почву для формирования и усиления ксенофобских настроений, дискриминации по национальному признаку и дестабилизации общественного сознания.

Особую тревогу вызывает то, что подобные проявления все чаще выходят за рамки виртуального пространства, влияя на реальные межэтнические отношения, формируя предвзятое восприятие целых групп населения и способствуя росту социальной напряженности. В условиях многонационального государства подобные процессы представляют серьезную угрозу не только для межкультурного диалога, но и для национальной безопасности в целом.

Проиллюстрируем это на примере беспорядков, которые произошли в Республике Дагестан в 2023 г. во время рейса из Израиля. В то время функционировал телеграм-канал «Утро Дагестан», который привлек множество подписчиков и завоевал популярность среди местного населения. В ходе анализа информационной активности телеграм-канала «Утро Дагестан» в период, предшествующий и сопровождающий события в аэропорту Махачкалы в октябре 2023 г., можно выделить отчетливую координационную и мобилизационную направленность ряда публикаций. За период с 25 по 29 октября 2023 г. в данном телеграм-канале было размещено более пятидесяти сообщений, прямо или косвенно связанных с темой приезда пассажиров из страны Ближнего Востока, поддержки Палестины, призывов к действиям, распространения дезинформации и эмоционально нагруженных заявлений, носящих антисемитский характер.

Используя категориальный анализ по О. Хольсти [25], были выделены

следующие тематические группы: 1) информационно-мобилизационные посты (30); 2) религиозно-политическая пропаганда (4); 3) эмоционально заряженные лозунги и образы (31); 4) сообщения с дезинформацией или манипулятивными интерпретациями (11). Наиболее часто встречались категории 1 и 3, что указывает на преобладание оперативной агитации и эмоционального воздействия над попытками рационального объяснения событий.

Информация канала в этот период выполняла не только роль информирования, но и функцию непосредственной мобилизации граждан на действия в реальном физическом пространстве, что стало катализатором незаконного проникновения в здание аэропорта и нарушения режима безопасности объекта. Телеграм-канал фактически превратился в инструмент координации спонтанного насилия, что соответствует типу «воспламеняющей коммуникации» в рамках концепций массовых беспорядков.

Прозападными силами была использована политическая технология раскачки общественного мнения, которая представляет собой набор методов и стратегий, направленных на формирование общественных настроений и мобилизацию людей для участия в протестных акциях. Технология включает в себя мониторинг настроений и поиск острых социальных или политических проблем, создание или усиление информационных поводов, которые вызывают недовольство, злость, гнев у целевой аудитории, распространение в соцсетях мемов, постов, видео, которые эмоционально затрагивают людей (вирусный контент). Использовались также призывы через закрытые чаты в мессенджерах и вовлечение лидеров мнений.

Ответом послужила работа центра управления регионом во взаимодействии с Правительством РФ и правоохранительными органами. В рамках мониторинга осуществлялся сбор и анализ данных из цифровых сред, включая социальные сети, мессенджеры и новостные платформы. Это позволило оперативно выявить очаги деструктивной активности, в том числе источники дезинформации и провокационных призывов. На основе полученной информации была сформулирована консолидированная позиция, направленная на стабилизацию общественных настроений. Своевременное информирование населения через проверенные каналы коммуникации позволило снизить уровень напряженности и предотвратить эскалацию конфликта.

Использование религиозной, национальной символики, манипуляция чувствами аудитории, вовлечение лидеров мнений и слабая институциональная реакция создают благоприятную почву для реализации сценариев внешнего вмешательства и информационной дестабилизации. Это подтверждает необходимость системного подхода к инфор-

мационной безопасности в национальном и межэтническом контексте. В таких условиях ключевую роль играют проактивная работа с общественным мнением, быстрая реакция на провокации, информационное сопровождение острых событий и привлечение к коммуникации авторитетных общественных и религиозных лидеров.

Заключение. Информационная безопасность в современных условиях представляет собой комплексную и многослойную систему, охватывающую институциональные, технологические и содержательно-коммуникативные компоненты, направленные на защиту информационного пространства государства. В рамках этноконфессиональной проблематики информационная безопасность включает в себя профилактику распространения радикальных идеологий, религиозного экстремизма и этноцентричных нарративов, способных трансформироваться в инструменты социальной и политической дестабилизации. Одновременно она ориентирована на защиту публичного дискурса от манипулятивного влияния как со стороны внутренних, так и внешних акторов, стремящихся использовать этноконфессиональную тематику в целях давления, провоцирования сепаратистских настроений или поляризации общества.

В этих условиях система мониторинга этноконфессиональной ситуации в Российской Федерации приобретает характер превентивного механизма обеспечения общественной стабильности и социального мира. Основу системы составляет сбор и аналитическая обработка эмпирических данных, получаемых как через прямые каналы обратной связи (обращения граждан, экспертные оценки, социологические опросы и фокус-группы), так и посредством мониторинга цифровых пространств, включая социальные сети, новостные ресурсы и работу центров управления регионами.

Ситуация в 2023 г. в Республике Дагестан, связанная с массовыми волнениями на национальной почве, показала эффективность работы ЦУР в регионах России. Западные агенты с использованием информационно-мобилизационных постов, пропаганды, эмоционально заряженных лозунгов и фейков стремились раскачать общественное волнение на этнической основе. Работа ЦУР позволила оперативно выявить очаги конфликта и дезинформации, сформулировать убедительную позицию по гармонизации общественных настроений и донести ее до аудитории, тем самым купировав эскалацию.

Список источников

1. *Елин В.М.* Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом. М.: Московский институт государственного управления и права, 2016. 168 с. EDN: XRCLFL.

2. *Стрельцов А.А*. Проблемы укрепления суверенитета государства в среде информационно-коммуникационных технологий // Системы высокой доступности. 2024. Т. 20, № 3. С. 59–70. DOI: 10.18127/j20729472-202403-06. EDN: DVKHHF.

3. *Козлова Н.Ш., Довгаль В.А.* Кибербезопасность и информационная безопасность: сходства и отличия // Вестник Адыгейского государственного университета. Сер. 4: Естественно-математические и технические науки. 2021. Вып. 3 (286). С. 88–96. DOI: 10.53598/2410-3225-2021-3-286-88-97 EDN: VSEERU.

4. *Крутских А.В*. Международная информационная безопасность: теория и практика. М.: Аспект Пресс, 2021. 384 с. EDN: HHGIBH.

5. *Жаде З.А., Хуако З.Ю*. Информационная безопасность в контексте межэтнической напряженности // Вестник Адыгейского государственного университета. Сер.: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2016. Вып. 1 (174). С. 87–95. EDN: VXJJQV

6. *Шевченко О.М., Штофер Л.Л.* Ксенофобия как эффективная технология современных информационных войн // Гуманитарий Юга России URL: https://cyberleninka.ru/article/n/ksenofobiya-kak-effektivnaya-tehnologiya-sovremennyh-informatsionnyh-voyn/viewer.

7. *Сергеев А.В., Крысин М.В.* Религиозный экстремизм в информационном пространстве сети Интернет // Аграрное и земельное право. 2017. С. 144–148. EDN: YSRGYF.

8. *Дубень А.К.* Вопросы обеспечения информационной безопасности в условиях новых вызовов и угроз // Право и государство: теория и практика. 2021. № 11. С. 155–158. EDN: PUWCUQ.

9. *Круглова А.Ю*. Деструктивные исламистские и тюркско-исламистские сетевые структуры на Юге России как предмет социологических исследований // Гуманитарий Юга России. 2019. Т. 8, № 1. С. 3–7. DOI: 10.23683/2227-8656.2019.1.20. EDN: SSXBNB.

10. *Пащенко И.В*. Технологии вовлечения в ИГИЛ: специфика пропаганды и методы противодействия // Манускрипт. URL: https://cyberleninka.ru/article/n/tehnologii-vovlecheniya-v-igil-8-spetsifika-propagandy-i-metody-protivodeystviya/viewer

11. *Урсул А.Д., Цырдя Т.Н*. Информационная безопасность. Сущность, содержание и принципы ее обеспечения URL: http://security.ase.md/publ/ru/pubru22.html

12. *Цырендоржиева Д.Ш., Манжуева О.М*. Феномен информационной безопасности. Улан-Удэ: Изд-во Бурятского госуниверситета, 2020. 308 с.

13. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. № 400. URL: http://www.kremlin.ru/acts/bank/47046

14. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 дек. 2016 г. № 646. URL: http://www.kremlin.ru/acts/bank/41460

15. *Карданов Р.Р*. Актуальные проблемы борьбы с экстремизмом в информационной среде // Пробелы в российском законодательстве. 2023. Т. 16, № 5. С. 87–91. EDN: FBNAMR.

16. *Дорошин И.А*. Цивилизационный «разлом» Поволжья: профилактика конфликта и пространство диалога // Вестник Поволжского института управления. 2014. № 2 (41). С. 111–117. EDN: SDXYXN

17. *Волков В.Э.* Глобальное отчуждение: информационный сепаратизм и права человека // Юридический вестник Самарского университета. 2016. Т. 2, № 2. С. 15–18. EDN: YKUACD.

18. *Хайкин С.Р., Бережкова С.Б.* Социологический мониторинг межнациональных и межконфессиональных отношений федерального агентства по делам национальностей // Мониторинг общественного мнения: экономические и социальные перемены. 2016. № 5. С. 97–110. DOI: 10.14515/monitoring.2016.5.07. EDN: YFOSQH.

19. *Топчиев М.С.* Специфика государственной политики регулирования конфессиональных отношений в полиэтничном регионе (на примере Астраханской области) // Каспийский регион: политика, экономика, культура. 2013. № 1. С. 99–106. EDN: PZJYEH.

20. *Слобожникова В.С., Суслов И.В.* Социальные технологии мониторинга религиозно-экстремистских настроений // Вестник Саратовской государственной юридической академии. 2020. № 6. С. 258–266. DOI: 10.24411/2227-7315-2020-10181. EDN: BVFFCN.

21. Сборник методических материалов для государственных служащих органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления. М.: Федеральное агентство по делам национальностей, 2019.

22. *Большакова К.Ю., Климова А.В.* Центры управления регионом как новая форма управленческой деятельности // Вестник Российского университета дружбы народов. Сер.: Государственное и муниципальное управление. 2022. Т. 6, № 4. С. 391–400. DOI: 10.22363/2312-8313-2022-9-4-391-400. EDN: BAXMSO.

23. ЦУР Псковской области: URL: https://t.me/s/tsur60

24. *Зотов В.В., Василенко Л.А.* Влияние цифровизации на трансформацию методологии публичного управления // Управленческое консультирование. 2021. № 5. С. 98–109. DOI: 10.22394/1726-1139-2021-5-98-109. EDN: UZWKWY.

25. *Holsti O.R.* Content Analysis for the Social Sciences and Humanities. Reading, Mass.: Addison-Wesley Pub Co, 1969. 235 p.

Сведения об авторе

МАКОВСКИЙ Андрей Андреевич,
кандидат политических наук,
доцент кафедры управления
Псковского государственного
университета
Псков, Россия
aamakovsky@mail.ru
https://orcid.org/0000-0002-5505-3295

The author

Andrey A. MAKOVSKY,
Candidate of Sciences (Politics),
Docent at the Management Department,
Pskov State University
Pskov, Russia
aamakovsky@mail.ru
https://orcid.org/0000-0002-5505-3295

Статья поступила в редакцию
21.04.2025

Одобрена после рецензирования
09.06.2025

Принята к публикации
20.07.2025

The article was submitted
21.04.2025

Approved after reviewing
09.06.2025

Accepted for publication
20.07.2025