Научная статья
УДК 327.8
DOI: 10.20323/2658-428X-2025-2-27-43
EDN: NAURGJ

Национальная безопасность России в контексте когнитивной войны

Артемий Сергеевич Гринчевский
Аспирант кафедры социально-политических теорий, Ярославский государственный университет им. П. Г. Демидова, г. Ярославль
grinchevsky@gmail.com, https://orcid.org/0009-0008-3626-5082

Аннотация. Государственная информационная политика представляет собой ключевую область государственного управления, особенно в современных условиях, характеризующихся глобализацией, цифровизацией и растущей зависимостью общества от информационных технологий. Ее значение возрастает ввиду необходимости противодействия новым вызовам, таким как дезинформация, киберугрозы, информационные и когнитивные войны. Информационная политика России направлена на обеспечение национальной безопасности, защиту государственного суверенитета и формирование эффективного взаимодействия между органами власти и обществом. В статье рассматриваются угрозы национальной безопасности России в сфере когнитивного противостояния и роль отечественных СМИ в обеспечении информационной безопасности. Анализируются теоретические основы когнитивного противостояния, классификация и источники угроз, а также потенциальные последствия для различных сфер жизни общества и государства. Методологическую основу данного исследования составляет сочетание различных методов научного познания, такие как системный анализ, сравнительный метод и контент-анализ материалов СМИ. Особое внимание уделяется функциям СМИ в структуре государственной информационной политики, текущему состоянию отечественной медиасферы и вызовам, стоящим перед ней. Социальные сети и интернет-платформы стали ключевыми каналами распространения информации, что существенно усложнило процессы контроля и фильтрации контента. Современные технологии машинного обучения позволяют создавать индивидуализированный контент, учитывающий психологические особенности и предпочтения каждого пользователя. Это открывает беспрецедентные возможности для точечного воздействия на различные группы населения. Все эти факторы формируют новый информационный ландшафт, где традиционные методы защиты от манипуляций становятся малоэффективными, а необходимость в развитии новых механизмов информационной безопасности становится все более актуальной.

Ключевые слова: когнитивное противостояние; когнитивная война; информационная безопасность; национальная безопасность; средства массовой информации; манипуляция сознанием; информационные угрозы; медиаграмотность; информационная политика

Для цитирования: Гринчевский А. С. Национальная безопасность России в контексте когнитивной войны // Социально-политические исследования. 2025. № 2 (27). С. 43–58. http://dx.doi.org/10.20323/2658-428X-2025-2-27-43. https://elibrary.ru/NAURGJ.

Original article

Russian national security in the context of cognitive warfare

Artemiy S. Grinchevskiy
Post-graduate student at department of socio-political theories, Yaroslavl state university named after P. G. Demidov, Yaroslavl
grinchevsky@gmail.com, https://orcid.org/0009-0008-3626-5082

Abstract. Public information policy is a key area of public administration, especially in today's environment characterized by globalization, digitalization and the growing dependence of society on information technologies. Its importance is increasing due to the need to counter new challenges such as disinformation, cyber threats, information and cognitive wars. Russia's information policy is aimed at ensuring national security, protecting state sovereignty and creating effective interaction between the authorities and society. The article considers the threats to Russia's national security in the sphere of cognitive confrontation and the role of domestic media in ensuring information security. The theoretical foundations of cognitive confrontation, classification and sources of threats, as well as potential consequences for various spheres of life of society and the state are analyzed. The methodological basis of this study is a combination of various methods of scientific knowledge, such as system analysis, comparative method and content analysis of media materials. Special attention is paid to the functions of the media in the structure of information security, the current state of the domestic media sphere and the challenges facing it. Social networks and Internet platforms have become the key channels of information dissemination, which has significantly complicated the processes of content control and filtering. Modern machine learning technologies make it possible to create individualized content that takes into account the psychological characteristics and preferences of each user. This opens up unprecedented opportunities for targeted influence on different population groups. All these factors are shaping a new information landscape where traditional methods of protection against manipulation are becoming ineffective, and the need to develop new information security mechanisms is becoming more and more urgent.

Key words: cognitive confrontation; cognitive warfare; information security; national security; mass media; mind manipulation; information threats; media literacy; information policy

For citation: Grinchevskiy A. S. Russian national security in the context of cognitive warfare. *Social and political researches*. 2025;2(27): 43–58. (In Russ). http://dx.doi.org/10.20323/2658-428X-2025-2-27-43. https://elibrary.ru/NAURGJ.

Введение

В эпоху стремительного развития информационных технологий и глобализации коммуникационных процессов проблема обеспечения национальной безопасности в контексте

когнитивного противостояния приобретает особую актуальность для Российской Федерации. Современные геополитические вызовы и усиливающееся информационное противоборство между государствами создают новые угрозы, направленные на подрыв национальных интересов, манипулирование общественным сознанием и дестабилизацию социально-политической обстановки.

Когнитивное противостояние, как форма информационного воздействия на индивидуальное и массовое сознание, становится одним из ключевых инструментов в межгосударственных конфликтах и геополитической конкуренции. В этих условиях роль отечественных средств массовой информации (*далее СМИ*) в обеспечении информационной безопасности страны значительно возрастает. СМИ выступают не только как источник информации, но и как инструмент формирования общественного мнения, сохранения культурной идентичности и противодействия внешним информационным угрозам. Современные изменения в информационном пространстве требуют от государства постоянной адаптации стратегий, направленных на защиту граждан и государственных интересов, а также на поддержку отечественных IT-компаний и технологий.

Цель данного исследования заключается в рассмотрении угроз национальной безопасности России в сфере когнитивного противостояния, анализе роли отечественных СМИ в структуре государственной информационной политики (*далее ГИП*) и выработке предложений по противодействию выявленным угрозам.

Методологическую основу исследования составляет комплексный подход, сочетающий в себе различные методы научного познания: системный анализ, позволяющий рассматривать угрозы национальной безопасности, нормативно-правовую базу и роль СМИ в ГИП; сравнительный метод, применяемый для сопоставления различных подходов к обеспечению информационной безопасности и противодействию когнитивным угрозам; контент-анализ материалов отечественных СМИ для оценки их роли в формировании общественного мнения и противодействии информационным угрозам. Работа включает исследование теоретических основ, современных подходов, а также международного опыта в этой сфере, что позволит выявить ключевые проблемы и предложить направления для их решения.

Теоретические основы когнитивного противостояния

В современном мире, характеризующемся стремительным развитием информационных технологий и глобализацией коммуникационных процессов, когнитивное противостояние становится одним из ключевых факторов, влияющих на национальную безопасность государств. Для глубокого понимания этого феномена необходимо рассмотреть его теоретические основы, особенности проявления в современных условиях и влияние на различные аспекты

национальной безопасности. Когнитивное противостояние представляет собой комплексное явление в сфере информационного взаимодействия, направленное на воздействие процессов восприятия, мышления и принятия решений целевой аудитории [Зиновьева, 2018; Ottewell, 2020; Whiteaker, 2022].

В научной литературе нет единого общепринятого определения данного термина, однако, опираясь на работы ведущих исследователей в области информационной безопасности и психологии, можно сформулировать следующее определение: *когнитивное противостояние – это форма информационного противоборства, целью которого является изменение системы знаний, убеждений и поведенческих паттернов противника путем целенаправленного воздействия на когнитивные процессы индивидов и социальных групп с использованием информационно-психологических технологий и средств массовой коммуникации*. В современном мире когнитивное противостояние приобретает ряд специфических черт, обусловленных развитием технологий и изменением глобального информационного ландшафта [Кефели, 2017].

Глобализация информационного пространства, связанная с развитием интернет-технологий и социальных сетей, значительно расширила возможности для проведения когнитивных операций в планетарном масштабе. Технологическая эволюция, включающая использование искусственного интеллекта, больших данных и алгоритмов машинного обучения, позволяет более точно таргетировать аудиторию и персонализировать информационные воздействия. Феномен «постправды» и распространение фейковых новостей приводят к размыванию границ между правдой и ложью, что усложняет процесс верификации информации для целевой аудитории. Согласно А. В. Манойло, феномен «постправды» относится к механизму психологического влияния, направленному на изменение восприятия и глубинных убеждений человека. Этот процесс способен кардинально изменить человеческое мнение об уже произошедших важных событиях в социально-политической сфере, которые ранее были оценены и восприняты обществом определенным образом [Манойло, 2020].

В 2020 г. глава Инновационного центра НАТО Франсуа дю Клозель опубликовал научную работу, посвященную когнитивному противостоянию. В рамках своего исследования дю Клозель анализирует, как стратегическое информационное воздействие может служить инструментом достижения политических и военных целей без прямого военного вмешательства [du Clozel, 2020]. Дю Клозель утверждает, что путем выборочной подачи информации, акцентов на конфликтах и проблемах внутри страны, возможно подорвать авторитет России на международной арене, а также внутри самой страны. [du Clozel, 2020].

Особенностью современного когнитивного противостояния является его мультимодальность: воз-

действие осуществляется через различные каналы коммуникации, включая традиционные СМИ, социальные сети и мессенджеры. Важно отметить асимметричность когнитивных операций, которые могут проводиться негосударственными акторами, что усложняет процесс атрибуции и противодействия. Кроме того, результаты когнитивного воздействия могут проявляться в течение длительного времени, что затрудняет оценку их эффективности и разработку мер противодействия [Баканова, 2020].

Анализ угроз национальной безопасности России в сфере когнитивного противостояния

В современных условиях геополитической напряженности и информационного противоборства анализ угроз национальной безопасности России в сфере когнитивного противостояния приобретает особую актуальность. Когнитивные угрозы представляют собой многогранное явление, требующее комплексного подхода к их изучению и противодействию. *Классификация угроз национальной безопасности в контексте когнитивного противостояния может быть проведена по различным основаниям* [Зиновьева, 2018].

По источнику возникновения выделяются внешние и внутренние угрозы. Внешние угрозы исходят от иностранных государств, международных организаций и транснациональных корпораций, стремящихся оказать влияние на внутреннюю и внешнюю политику России. Внутренние угрозы связаны с деятельностью отдельных групп и индивидов внутри страны, которые, осознанно или неосознанно, могут способствовать распространению деструктивных идей и информации [Алексеев, Алекссева, 2021].

По характеру воздействия угрозы можно разделить на прямые и косвенные. Прямые угрозы направлены на немедленное изменение общественного мнения или поведения целевых групп, например, через распространение дезинформации о текущих событиях. Косвенные угрозы ориентированы на долгосрочные изменения в системе ценностей и мировоззрении общества, что может проявляться в попытках переписывания истории или подрыва традиционных культурных основ.

По масштабу воздействия выделяются локальные, региональные и глобальные угрозы [Баранова, 2014]. Локальные угрозы затрагивают отдельные социальные группы или географические районы. Региональные угрозы охватывают более широкие территории или сферы общественной жизни. Глобальные угрозы направлены на подрыв позиций России на международной арене и изменение ее роли в мировом сообществе.

Основными источниками угроз в сфере когнитивного противостояния выступают иностранные спецслужбы, международные неправительственные организации, транснациональные медиакорпорации, а также экстремистские и террористические группировки. Эти акторы используют широкий спектр инструментов

для реализации своих целей, включая социальные сети, онлайн-платформы, традиционные СМИ и образовательные программы.

Особую роль в генерации и распространении угроз играют технологические факторы. Развитие искусственного интеллекта и технологий обработки больших данных позволяет создавать все более изощренные методы манипуляции общественным сознанием [Dahl, 2022]. Использование ботов, технологий deepfake и алгоритмов персонализированной подачи контента в социальных сетях значительно усложняет задачу выявления и нейтрализации информационных угроз [Плашенков, 2022; Norton, 2021].

Потенциальные последствия реализации угроз национальной безопасности России в сфере когнитивного противостояния могут быть крайне серьезными и долгосрочными. В политической сфере это может привести к подрыву доверия к государственным институтам, росту социальной напряженности и политической нестабильности [Bjorgul, 2021]. Возможно усиление сепаратистских настроений в отдельных регионах и обострение межнациональных конфликтов. В экономической области когнитивные атаки могут спровоцировать панику на финансовых рынках, подорвать инвестиционную привлекательность страны и стимулировать отток капитала [Баранова, 2014]. Распространение ложной информации об экономической ситуации способно привести к нерациональному поведению экономических агентов и дестабилизации рынков. В области обороны и безопасности когнитивные атаки могут быть направлены на снижение престижа военной службы, дискредитацию вооруженных сил и подрыв морального духа личного состава. В критических ситуациях это может негативно сказаться на обороноспособности страны [Lanata, 2022].

Государственная информационная политика в структуре национальной безопасности

В рамках Указа Президента РФ «О стратегии национальной безопасности Российской Федерации» *информационная безопасность рассматривается как приоритетная задача, направленная на защиту государственных интересов и поддержку устойчивого развития страны в условиях цифровизации* [Указ … № 400, 2021]. Стратегия подчеркивает необходимость создания эффективной системы по защите информации, включая противодействие иностранному вмешательству и предотвращение распространения недостоверной информации, способной дестабилизировать социально-политическую обстановку.

ГИП представляет собой совокупность правовых, экономических и организационных мер, направленных на регулирование информационных процессов в обществе, обеспечение информационной безопасности и защиту интересов государства. В условиях современной цифровизации и глобализации, которые оказывают существенное влияние на внутреннюю и внешнюю политику, роль информационной политики

значительно возрастает. Многие российские ученые подчеркивают, что информационная политика выступает важным инструментом контроля и влияния, одновременно защищая общество от информационных угроз и обеспечивая стратегическое развитие информационной инфраструктуры. В условиях активного развития интернет-технологий и массового распространения социальных сетей данная функция информационной политики приобретает особую актуальность, так как становится возможным не только управлять информационными потоками, но и воздействовать на общественное сознание [Шалак, 2021].

В. С. Горбатов также делает акцент на том, что успешная реализация ГИП зависит от создания правового поля, регулирующего не только внутренние, но и международные информационные отношения. По его мнению, ГИП должна служить инструментом внешнеполитического влияния, позволяя государству представлять свою позицию на международной арене и защищать национальные интересы в глобальном информационном пространстве. В условиях цифрового противостояния и информационных войн эта роль становится крайне важной, особенно для обеспечения объективного освещения событий, касающихся России и ее внешнеполитических интересов [Горбатов, 2022].

Одним из ключевых направлений ГИП России является регулирование интернет-пространства и деятельности СМИ. В последние годы российское законодательство ужесточило меры для борьбы с фейковыми новостями, экстремистскими материалами и контентом, угрожающим общественной безопасности. Так, Федеральный закон «О средствах массовой информации» и Федеральный закон «О противодействии экстремистской деятельности» предусматривают меры для предотвращения распространения деструктивного контента в онлайн-среде [ФЗ … № 2124-1, 1991; ФЗ … №114, 2002].

По мнению А. А. Акишева и И. А. Калиева, регулирование интернет-пространства является важным элементом защиты национальных интересов, поскольку интернет стал инструментом влияния на массовое сознание. Авторы указывают, что в условиях возрастающего влияния иностранных медиа и платформ на российское общество необходимо создать единое информационное пространство, свободное от внешнего воздействия, и поддерживать независимые российские СМИ [Акишев, 2021].

Цели ГИП в России определены также в ряде нормативно-правовых актов. В частности, Закон «О безопасности» и Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» формируют правовую основу для регулирования информационной сферы и обеспечения информационной безопасности [ФЗ … № 149, 2006]. Эти нормативные акты подчёркивают важность защиты информации от несанкционированного доступа и угроз кибербезопасности, а также поддерживают развитие ин-

формационной инфраструктуры. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» устанавливает правовую основу для защиты объектов, чья деятельность критически важна для национальной безопасности и общественного благополучия [ФЗ … № 187, 2017]. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646, подчеркивает необходимость предотвращения кибератак и иных угроз, направленных на нарушение работы критических объектов информационной инфраструктуры [Указ … № 646, 2016].

На современном этапе важной целью ГИП является поддержка и развитие национальных IT-компаний и технологий. В условиях санкционного давления и растущей зависимости от импортных решений Россия вынуждена стимулировать создание и развитие отечественных технологий. Одним из направлений является поддержка российских социальных сетей, поисковых систем и других платформ, способных конкурировать с иностранными аналогами. Китай представляет собой ценный пример надежной, самодостаточной медиа-экосистемы, которая эффективно обслуживает свою внутреннюю аудиторию. Такие платформы, как WeChat, QQ и Douyin, доказали свою высокую функциональность и даже расширили свой глобальный охват. В отличие от западных платформ, эти платформы удовлетворяют разнообразные потребности пользователей в Китае, предлагая все – от социальных сетей до электронной коммерции [Чэнь, 2019].

ГИП также направлена на защиту информационных прав граждан, что включает как обеспечение свободы слова, так и защиту персональных данных. Важным документом в этой области является Федеральный закон «О персональных данных», который регламентирует порядок обработки и защиты данных, а также предусматривает меры ответственности за их утечку [ФЗ … № 152, 2006].

П. У. Кузнецов отмечает, что защита персональных данных в условиях цифровизации становится одним из важнейших направлений ГИП, поскольку данные граждан становятся мишенью для злоумышленников и объектов государственного контроля. По его мнению, государственная политика должна учитывать баланс между правом граждан на частную жизнь и необходимостью государственного контроля за критически важной информацией [Кузнецов, 2021].

ГИП Российской Федерации на современном этапе представляет собой комплекс мер, направленных на формирование устойчивого информационного пространства, защищенного от внешнего влияния, и обеспечение национальных интересов. В условиях цифровизации и глобализации ключевыми направлениями такой политики стали регулирование интернет-пространства и СМИ, обеспечение кибербезопасности, поддержка национальных

IT-компаний и технологий, а также защита информационных прав граждан. Одним из ключевых направлений ГИП России является регулирование интернет-пространства и деятельности СМИ.

Согласно Е. И. Казакевич и Е. П. Губину, регулирование интернет-пространства выступает элементом защиты национальных интересов, поскольку интернет стал инструментом влияния на массовое сознание. Он подчеркивает, что создание безопасного информационного пространства требует независимых национальных медиаплатформ [Казакевич, 2022].

В. В. Штоль указывает, что защита критической информационной инфраструктуры является неотъемлемой частью национальной безопасности и важнейшим элементом ГИП. По его мнению, обеспечение кибербезопасности требует не только технологических решений, но и выстраивания сотрудничества между государственными и частными структурами [Штоль, 2024].

Н. Н. Нестерова и О. Ю. Смыслова отмечают, что защита персональных данных в условиях цифровизации становится одним из важнейших направлений ГИП, поскольку данные граждан становятся мишенью для злоумышленников и объектов государственного контроля. По их мнению, государственная политика должна учитывать баланс между правом граждан на частную жизнь и необходимостью государственного контроля за критически важной информацией [Нестерова, 2022].

Одной из ключевых проблем является сложность правового регулирования информационного пространства. Законодательство, регулирующее информационную политику, в частности Федеральный закон «О средствах массовой информации» и Федеральный закон «О персональных данных», часто обновляется, однако процесс внедрения правовых норм остается медленным [ФЗ … № 2124-1, 1991; ФЗ … № 152, 2006].

Роль отечественных СМИ в структуре ГИП

Функции СМИ в обеспечении информационной безопасности многогранны и охватывают широкий спектр задач. Прежде всего, СМИ выступают как основной источник достоверной информации для населения, противодействуя распространению дезинформации и фейковых новостей. Они играют важную роль в формировании национальной повестки дня, определяя приоритетные темы общественного дискурса и способствуя консолидации общества вокруг национальных интересов. Кроме того, СМИ выполняют образовательную функцию, повышая медиаграмотность населения и развивая критическое мышление, что является важнейшим элементом информационной безопасности в эпоху информационных войн. Отечественные СМИ также служат инструментом «мягкой силы» на международной арене, формируя позитивный образ России за рубежом и противодействуя антироссийской пропаганде [Панарин, 2019]. Они выступают площадкой для общественного диа-

лога, способствуя снижению социальной напряженности и предотвращению конфликтов. Не менее важна роль СМИ в обеспечении информационной прозрачности деятельности государственных органов, что повышает доверие граждан к власти и укрепляет национальную безопасность.

Анализ текущего состояния отечественных СМИ обозначает ряд тенденций, имеющих непосредственное влияние на информационную безопасность страны. С одной стороны, наблюдается усиление государственного контроля над крупнейшими медиаресурсами, что позволяет более эффективно координировать ГИП в интересах национальной безопасности. С другой стороны, это вызывает опасения относительно снижения плюрализма мнений и независимости СМИ. Происходит активная цифровая трансформация медиаландшафта: традиционные СМИ адаптируются к новым форматам потребления информации, развивают онлайн-платформы и присутствие в социальных сетях [Сулейманова, 2019]. Это расширяет возможности для оперативного реагирования на информационные угрозы, но одновременно создает новые вызовы в области кибербезопасности и защиты информационной инфраструктуры.

Отмечается тенденция к персонализации контента и развитию нишевых медиа, что позволяет более точно таргетировать аудиторию, но также может способствовать фрагментации информационного пространства и формированию «эхо-камер» [John Hopkins … , 2021]. В условиях информационного противоборства российские СМИ активно развивают международное вещание, стремясь донести альтернативную точку зрения на глобальные события до зарубежной аудитории. Однако перед отечественными СМИ стоит ряд серьезных проблем и вызовов, которые могут ослабить их роль в обеспечении информационной безопасности [Манойло, 2018].

Одним из главных вызовов является снижение доверия аудитории к традиционным медиа, особенно среди молодежи, которая все чаще обращается к альтернативным источникам информации в интернете и социальных сетях. Это создает риски распространения непроверенной информации и повышает уязвимость общества к информационным манипуляциям. Экономические трудности, усугубленные падением рекламных доходов и конкуренцией с глобальными интернет-платформами, ставят под угрозу финансовую устойчивость многих СМИ, особенно региональных и независимых изданий. Это может привести к снижению качества журналистики и ослаблению способности СМИ выполнять свои функции по обеспечению информационной безопасности.

Заключение

В результате проведенного исследования были рассмотрены ключевые аспекты угроз национальной безопасности России в сфере когнитивного противостояния и роль отечественных СМИ в структуре ГИП. Анализ показал, что когнитивное

противостояние представляет собой комплексную угрозу, затрагивающую различные сферы жизни общества и государства. Выявлено, что основными источниками угроз выступают как внешние акторы (иностранные государства, международные организации), так и внутренние факторы (деструктивная деятельность отдельных групп и индивидов). Особую опасность представляют технологические факторы, связанные с развитием искусственного интеллекта и методов манипуляции информацией.

Исследование подтвердило ключевую роль отечественных СМИ в структуре ГИП. СМИ выполняют функции источника достоверной информации, инструмента формирования общественного мнения и противодействия дезинформации [Федоров, 2015]. Однако перед ними стоит ряд серьезных вызовов, включая снижение доверия аудитории, экономические трудности и необходимость адаптации к новым технологическим реалиям.

Итогом анализа выступает то, что для России целесообразно развивать адаптивный подход к информационной политике, сочетающий черты западной модели защиты прав граждан с элементами цифрового суверенитета, характерными для азиатского региона. Повышение координации между ведомствами, развитие национальных технологий и активное участие в международных инициативах по кибербезопасности могут укрепить информационную безопасность России. Выстраивание комплексной информационной политики позволит стране не только защитить цифровой суверенитет, но и создать условия для безопасного и устойчивого развития в условиях глобальной цифровизации.

Выявленные проблемы реализации информационной политики в России, такие как недостаточная координация между ведомствами, правовые пробелы и угрозы дезинформации, требуют дальнейшей разработки эффективных мер для их преодоления.

Библиографический список

1. Акишев А. А. Национальные интересы в информационной сфере как объект информационной безопасности в Республике Казахстан / А. А. Акишев, И. А. Калиев // Norwegian Journal of Development of the International Science. 2021. №. 66. С. 36–39.

2. Алексеев А. П. Цифровизация и когнитивные войны / А. П. Алексеев, И. Ю. Алексеева // Философия и общество. 2021. № 4 (101). С. 39–51.

3. Баканова А. С. Информационные угрозы национальной безопасности России в эпоху современных информационных войн // Информационные войны. 2020. № 1(53). С. 79–83.

4. Баранова Н. А. Информационное пространство современного общества и проблемы информационной безопасности / Н. А. Баранова, Г. О. Федоров // Социальные отношения. 2014. №. 3. С. 41–45.

5. Горбатов В. С. Кибербезопасность сетевого периметра объекта критической информационной инфраструктуры / В. С. Горбатов [и др.] // Безопасность информационных технологий. 2022. Т. 29, №. 4. С. 12–26.

6. Закон РФ «О безопасности» от 05.03.1992 №2446-1. URL: https://www.consultant.ru/document/cons_doc_LAW_376/ (дата обращения 27.02.2025).

7. Зиновьева Е. С. Цифровая дипломатия, международная безопасность и возможности для России // Вестник МГИМО-Университета. 2018. № 6 (63). С. 25–40.

8. Казакевич Е. И. Защита прав и свобод человека при обработке персональных данных в период цифровой трансформации / Е. И. Казакевич, Е. П. Губин // Уральский журнал правовых исследований. 2022. №. 4 (21). С. 36–46.

9. Кефели И. Ф. Информационно-психологическая и когнитивная безопасность / И. Ф. Кефели, Р. М. Юсупова. Санкт-Петербург : ИД «Петрополис», 2017. 300 с.

10. Кузнецов П. У. Цифровая трансформация государственного управления как этап развития информатизации в России // Вестник Южно-Уральского государственного университета. Серия: Право. 2021. Т. 21, №. 1. С. 84–95.

11. Манойло А. В. Государственная информационная политика в особых условиях. Москва : МИФИ, 2018. 388 с.

12. Манойло А. В. Цепные реакции каскадного типа в современных технологиях вирусного распространения «фейковых новостей» // Российский социально-гуманитарный журнал. 2020. № 3. С. 75–107.

13. Нестерова Н. Н. Государственная информационная политика в новых условиях развития современного общества / Н. Н. Нестерова, О. Ю. Смыслова // ЭФО: Экономика. Финансы. Общество. 2022. №. 1. С. 6–18.

14. Панарин И. Н. Основы теории «гибридной войны» // Международное сотрудничество евразийских государств: политика, экономика, право. 2019. №. 4. С. 58–71.

15. Плашенков Д. Д. Фейки как технология информационной войны против России: понятие и политика противодействия / Д. Д. Плашенков, Г. И. Авцинова // Социальные и гуманитарные науки в условиях вызовов современности. Комсомольск-на-Амуре : Изд-во Комсомольский-на-Амуре государственный университет, 2022. С. 289–293.

16. Сулейманова Ш. С. Информационные войны: история и современность / Ш. С. Сулейманова, Е. А. Назарова. Москва : Международный издательский центр «Этносоциум», 2019. 124 с.

17. Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О стратегии национальной безопасности Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 27.02.2025).

18. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения 27.02.2025).

19. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 27.02.2025).

20. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 27.02.2025).

21. Федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 №114-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_37867/ (дата обращения 27.02.2025).

22. Федеральный закон «О средствах массовой информации» от 27.12.1991 № 2124-1. URL: https://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения: 27.02.2025).

23. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 27.02.2025).

24. Федоров А. В. Медиаобразование: история и теория. Москва : Информация для всех, 2015. 450 с.

25. Чэнь Цзюньшуай. Цифровая реальность и права граждан в Китае // Право и государство: теория и практика. № 2 (170). 2019. С. 92–96.

26. Шалак А. В. Приоритеты в области защиты информационно-культурного пространства: историко-геополитическая интерпретация // Вопросы теории и практики журналистики. 2021. Т. 10, №. 1. С. 157–173.

27. Штоль В. В. Стратегическое партнёрство в условиях вызовов информационной безопасности // Обозреватель-Observer. 2024. №. 5. С. 134–145.

28. Bjorgul L. Cognitive warfare and the use of force // Stratagem. 3.11. 2021. URL: https://www.stratagem.no/ cognitive-warfare-and-the-use-of-force/ (дата обращения: 24.08.2024).

29. Claverie B., du Cluzel F. The cognitive warfare concept. Innovation Hub. URL: https://www.innovationhubact.org/sites/default/files/202202/CW%20article%20Claverie%20du%20Cluzel%20final_0.pdf (дата обращения: 22.08.2024).

30. Dahl A. Considering a cognitive warfare framework. URL: https://www.jstor.org/stable/pdf/ resrep13807.9.pdf (дата обращения: 21.08.2024).

31. Du Cluzel F. Cognitive warfare. Innovation Hub. URL: https://www.innovationhubact.org/sites/default/files/202101/20210122_CW%20Final.pdf (дата обращения: 22.08.2024).

32. Hopkins J. University & Imperial College London. Countering cognitive warfare: Awareness and resilience. NATO Review. 2021. URL: https://www.nato.int/docu/review/articles/2021/05/20/ countering-cognitive-warfare-awareness-and-resilience/index.html (дата обращения: 22.08.2024).

33. Lanata A. (2022). Cognitive Warfare. 1.04. 2022. URL: https://hal.science/hal-03635872/document (дата обращения: 21.08.2024).

34. Norton B. Behind NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries. 2021. URL: https://mronline.org/2021/10/13/behind-natos-cognitive-warfare-battle-for-your-brain-waged-by-westernmilitaries/ (дата обращения: 22.08.2024).

35. Ottewell P. Defining the cognitive domain // OTH. 2020. URL: https://othjournal.com/2020/12/07/defining-the-cognitive-domain/ (дата обращения: 24.08.2024).

36. Whiteaker J., Valkonen S. Cognitive warfare: complexity and simplicity // HAL. 2022. URL: https://hal. archives-ouvertes.fr/hal-03635948/document (дата обращения: 24.08.2024).

Reference list

1. Akishev A. A. Nacional'nye interesy v informacionnoj sfere kak ob#ekt informacionnoj bezopasnosti v Respublike Kazahstan = National interests in the information sphere as an object of information security in the Republic of Kazakhstan / A. A. Akishev, I. A. Kaliev // Norwegian Journal of Development of the International Science. 2021. №. 66. S. 36–39.

2. Alekseev A. P. Cifrovizacija i kognitivnye vojny = Digitalization and cognitive wars / A. P. Alekseev, I. Ju. Alekseeva // Filosofija i obshhestvo. 2021. № 4 (101). S. 39–51.

3. Bakanova A. S. Informacionnye ugrozy nacional'noj bezopasnosti Rossii v jepohu sovremennyh informacionnyh vojn = Information threats to Russia's national security in the era of modern information wars // Informacionnye vojny. 2020. № 1(53). S. 79–83.

4. Baranova N. A. Informacionnoe prostranstvo sovremennogo obshhestva i problemy informacionnoj bezopasnosti = Information space of modern society and information security problems / N. A. Baranova, G. O. Fedorov // Social'nye otnoshenija. 2014. №. 3. S. 41–45.

5. Gorbatov V. S. Kiberbezopasnost' setevogo perimetra ob#ekta kriticheskoj informacionnoj infrastruktury = Cybersecurity of the network perimeter of a critical information infrastructure facility / V. S. Gorbatov [i dr.] // Bezopasnost' informacionnyh tehnologij. 2022. T. 29. №. 4. S. 12–26.

6. Zakon RF «O bezopasnosti» ot 05.03.1992 №2446-1 = Law of the Russian Federation “On Safety” dated 05.03.1992 No. 2446-1. URL: https://www.consultant.ru/document/cons_doc_LAW_376/ (data obrashhenija 27.02.2025).

7. Zinov'eva E. S. Cifrovaja diplomatija, mezhdunarodnaja bezopasnost' i vozmozhnosti dlja Rossii = Digital diplomacy, international security and opportunities for Russia // Vestnik MGIMO-Universiteta. 2018. № 6 (63). S. 25–40.

8. Kazakevich E. I. Zashhita prav i svobod cheloveka pri obrabotke personal'nyh dannyh v period cifrovoj transformacii = Protection of human rights and freedoms in the processing of personal data during the period of digital transformation / E. I. Kazakevich, E. P. Gubin // Ural'skij zhurnal pravovyh issledovanij. 2022. №. 4 (21). S. 36–46.

9. Kefeli I. F. Informacionno-psihologicheskaja i kognitivnaja bezopasnost' = Information-psychological and cognitive safety / I. F. Kefeli, R. M. Jusupova. Sankt-Peterburg : ID «Petropolis», 2017. 300 s.

10. Kuznecov P. U. Cifrovaja transformacija gosudarstvennogo upravlenija kak jetap razvitija informatizacii v Rossii = Digital transformation of public administration as a stage in the development of informatization in Russia // Vestnik Juzhno-Ural'skogo gosudarstvennogo universiteta. Serija: Pravo. 2021. T. 21, №. 1. S. 84–95.

11. Manojlo A. V. Gosudarstvennaja informacionnaja politika v osobyh uslovijah = State information policy in special conditions. Moskva : MIFI, 2018. 388 s.

12. Manojlo A. V. Cepnye reakcii kaskadnogo tipa v sovremennyh tehnologijah virusnogo rasprostranenija «fejkovyh novostej» = Cascade-type chain reactions in modern technologies of viral distribution of “fake news” // Rossijskij social'no-gumanitarnyj zhurnal. 2020. № 3. C. 75–107.

13. Nesterova N. N. Gosudarstvennaja informacionnaja politika v novyh uslovijah razvitija sovremennogo obshhestva = State information policy in the new conditions of modern society development / N. N. Nesterova, O. Ju. Smyslova // JeFO: Jekonomika. Finansy. Obshhestvo. 2022. №. 1. S. 6–18.

14. Panarin I. N. Osnovy teorii «gibridnoj vojny» = The basics of the theory of “hybrid war” // Mezhdunarodnoe sotrudnichestvo evrazijskih gosudarstv: politika, jekonomika, pravo. 2019. №. 4. S. 58–71.

15. Plashenkov D. D. Fejki kak tehnologija informacionnoj vojny protiv Rossii: ponjatie i politika protivodejstvija = Fakes as an information warfare technology against Russia: the concept and policy of counteraction / D. D. Plashenkov, G. I. Avcinova // Social'nye i gumanitarnye nauki v uslovijah vyzovov sovremennosti. Komsomol'sk-na-Amure : Izd-vo Komsomol'skij-na-Amure gosudarstvennyj universitet, 2022. S. 289–293.

16. Sulejmanova Sh. S. Informacionnye vojny: istorija i sovremennost' = Information wars: history and modernity / Sh. S. Sulejmanova, E. A. Nazarova. Moskva : Mezhdunarodnyj izdatel'skij centr «Jetnosocium», 2019. 124 s.

17. Ukaz Prezidenta Rossijskoj Federacii ot 02.07.2021 g. № 400 «O strategii nacional'noj bezopasnosti Rossijskoj Federacii» = Decree of the President of the Russian Federation of 02.07.2021 No. 400 “On the National Security Strategy of the Russian Federation”. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (data obrashhenija: 27.02.2025).

18. Ukaz Prezidenta Rossijskoj Federacii ot 05.12.2016 № 646 «Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii» = Decree of the President of the Russian Federation of 05.12.2016 No. 646 “On approval of the Information Security Doctrine of the Russian Federation”. URL: http://www.kremlin.ru/acts/bank/41460 (data obrashhenija: 27.02.2025).

19. Federal'nyj zakon «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii» ot 26.07.2017 № 187-FZ = Federal Law “On Security of Critical Information Infrastructure of the Russian Federation” dated 26.07.2017 No. 187-FZ. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (data obrashhenija: 27.02.2025).

20. Federal'nyj zakon «O personal'nyh dannyh» ot 27.07.2006 № 152-FZ = Federal Law “On Personal Data” dated 27.07.2006 No. 152-FZ. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (data obrashhenija: 27.02.2025).

21. Federal'nyj zakon «O protivodejstvii jekstremistskoj dejatel'nosti» ot 25.07.2002 №114-FZ = Federal Law “On Countering Extremist Activities” of 25.07.2002 No. 114-FZ. URL: https://www.consultant.ru/document/cons_doc_LAW_37867/ (data obrashhenija: 27.02.2025).

22. Federal'nyj zakon «O sredstvah massovoj informacii» ot 27.12.1991 № 2124-1 = Federal Law “On Mass Media” dated 27.12.1991 No. 2124-1. URL: https://www.consultant.ru/document/cons_doc_LAW_1511/ (data obrashhenija: 27.02.2025).

23. Federal'nyj zakon «Ob informacii, informacionnyh tehnologijah i o zashhite informacii» ot 27 ijulja 2006 g. № 149-FZ = Federal Law “On Information, Information Technologies and Information Protection” dated July 27, 2006 No. 149-FZ. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (data obrashhenija: 27.02.2025).

24. Fedorov A. V. Mediaobrazovanie: istorija i teorija = Media education: history and theory. Moskva : Informacija dlja vseh, 2015. 450 s.

25. Chjen' Czjun'shuaj. Cifrovaja real'nost' i prava grazhdan v Kitae = Digital reality and citizens' rights in China // Pravo i gosudarstvo: teorija i praktika. № 2 (170). 2019. S. 92–96.

26. Shalak A. V. Prioritety v oblasti zashhity informacionno-kul'turnogo prostranstva: istoriko-geopoliticheskaja interpretacija = Priorities in the field of information and cultural space protection: historical and geopolitical interpretation // Voprosy teorii i praktiki zhurnalistiki. 2021. T. 10, №. 1. S. 157–173.

27. Shtol' V. V. Strategicheskoe partnjorstvo v uslovijah vyzovov informacionnoj bezopasnosti = Strategic partnership for information security challenges // Obozrevatel'-Observer. 2024. №. 5. S. 134–145.

28. Bjorgul L. Cognitive warfare and the use of force // Stratagem. 3.11. 2021. URL: https://www.stratagem.no/ cognitive-warfare-and-the-use-of-force/ (data obrashhenija: 24.08.2024).

29. Claverie B., du Cluzel F. The cognitive warfare concept. Innovation Hub. URL: https://www.innovationhubact.org/sites/default/files/202202/CW%20article%20Claverie%20du%20Cluzel%20final_0.pdf (data obrashhenija 22.08.2024).

30. Dahl A. Considering a cognitive warfare framework. URL: https://www.jstor.org/stable/pdf/ resrep13807.9.pdf (data obrashhenija: 21.08.2024).

31. Du Cluzel F. Cognitive warfare. Innovation Hub. URL: https://www.innovationhubact.org/sites/default/files/202101/20210122_CW%20Final.pdf (data obrashhenija: 22.08.2024).

32. Hopkins J. University & Imperial College London. Countering cognitive warfare: Awareness and resilience. NATO Review. 2021. URL: https://www.nato.int/docu/review/articles/2021/05/20/ countering-cognitive-warfare-awareness-and-resilience/index.html (data obrashhenija: 22.08.2024).

33. Lanata A. (2022). Cognitive Warfare. 1.04. 2022. URL: https://hal.science/hal-03635872/document (data obrashhenija: 21.08.2024).

34. Norton B. Behind NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries. 2021. URL: https://mronline.org/2021/10/13/behind-natos-cognitive-warfare-battle-for-your-brain-waged-by-westernmilitaries/ (data obrashhenija: 22.08.2024).

35. Ottewell P. Defining the cognitive domain // OTH. 2020. URL: https://othjournal.com/2020/12/07/defining-the-cognitive-domain/ (data obrashhenija: 24.08.2024).

36. Whiteaker J., Valkonen S. Cognitive warfare: complexity and simplicity // HAL. 2022. URL: https://hal. archives-ouvertes.fr/hal-03635948/document (data obrashhenija: 24.08.2024).

Статья поступила в редакцию 21.03.2025; одобрена после рецензирования 21.04.2025; принята к публикации 15.05.2025.
The article was submitted on 21.03.2025; approved after reviewing 21.04.2025; accepted for publication on 15.05.2025