Научная статья / Original research article
УДК 316.77:004.056
DOI:10.31660/1993-1824-2025-3-33-47
EDN: RMTXTN

Информационная безопасность в политическом дискурсе современной России

А. А. Попкова*, К. В. Парфенов

Тюменский индустриальный университет, Тюмень, Россия
**popkovaaa@tyuiu.ru*

Аннотация. Одним из значимых дискурсов в современной информационной повестке России является информационная безопасность, которая в условиях геополитических и внутриполитических трансформаций приобретает все большее значение. В статье анализируется эволюция концепции информационной безопасности в выступлениях основных политических акторов России за период 2022–2024 годов, выделяются основные тенденции и трансформации в государственной политике. Цель статьи — определение содержательных компонентов дискурса информационной безопасности и их трансформация в публичных выступлениях президента Российской Федерации, представителей законодательной и исполнительной власти страны. Авторы применяют дискурсивный анализ для изучения публичных выступлений представителей органов власти, включая президента, правительство и Совет Федерации. Основное внимание уделяется таким аспектам, как цифровой суверенитет, киберугрозы, регулирование интернет-пространства и защита данных. Авторы подчеркивают, что дискурс информационной безопасности служит инструментом политической мобилизации, формируя общественное сознание и оправдывая жесткие регуляторные меры. Результаты исследования демонстрируют, как технологические, правовые и идеологические компоненты объединяются в единую стратегию обеспечения национальной безопасности. Статья будет полезна специалистам в области политологии, социологии и информационных технологий, а также всем, кто интересуется вопросами цифрового суверенитета и государственной политики.

Ключевые слова: информационная безопасность, цифровой суверенитет, киберугрозы, политический дискурс, государственное регулирование

Для цитирования: Попкова, А. А. Информационная безопасность в политическом дискурсе современной России / А. А. Попкова, К. В. Парфенов. – DOI 10.31660/1993-1824-2025-3-33-47 // Известия высших учебных заведений. Социология. Экономика. Политика. – 2025. – № 3. – С. – С. 33–47. – EDN: RMTXTN

Information security in the political discourse of contemporary Russia

Alena A. Popkova*, Konstantin V. Parfenov

Industrial University of Tyumen, Tyumen, Russia
* *popkovaaa@tyuiu.ru*

© А. А. Попкова, К. В. Парфенов, 2025

Abstract. One of the meaningful discourses in Russia's current information agenda is information security, which has become increasingly important amid geopolitical and domestic political changes. This paper analyzes the evolution of the concept of information security in the speeches of key political actors in from 2022 to 2024, highlighting major trends and shifts in state policy. The aim of the paper is to identify the main components of the information security discourse and examine how they have transformed in public statements made by the President of the Russian Federation, as well as representatives from the legislative and executive branches. The authors use discourse analysis to study public speeches by government officials, including the President, the Government, and the Federation Council. The study focuses on aspects such as digital sovereignty, cyber threats, internet regulation, and data protection. The authors underline that the information security discourse acts as a tool for political mobilization, shaping public awareness and justifying strict regulatory measures. The results show how technological, legal, and ideological elements combine into a cohesive strategy for national security. This paper will be beneficial for experts in political science, sociology, and information technology, as well as anyone interested in digital sovereignty and state policy.

Keywords: information security, digital sovereignty, cyber threats, political discourse, state regulation

For citation: Popkova, A. A., & Parfenov, K. V. (2025). Information security in the political discourse of contemporary Russia. Proceedings of Higher Educational Institutions. Sociology. Economics. Politics, (3), pp. 33-47. (In Russian). DOI: 10.31660/1993-1824-2025-3-33-47

Введение

Современная эпоха цифровой трансформации принесла не только новые технологические возможности, но и беспрецедентные вызовы в сфере информационной безопасности. Для России, активно развивающей цифровую экономику и внедряющей технологии в государственное управление, защита от киберугроз становится ключевым элементом национальной безопасности. Статистика последних лет демонстрирует тревожную динамику: киберпреступность растет, атаки становятся все более изощренными, а их последствия — все более разрушительными. В 2024 году в России было зарегистрировано 765,4 тыс. киберпреступлений, что составляет 40 % от их общего числа [1]. Эти цифры свидетельствуют о том, что цифровое пространство превратилось в новое поле борьбы, где угрозы носят не только криминальный, но и стратегический характер. Рост киберпреступности в России приобретает масштабы национальной угрозы. По данным Следственного комитета Российской Федерации (РФ), в 2024 году было расследовано более 24 тыс. преступлений, совершенных с применением цифровых технологий, что на 10 % больше, чем в предыдущем году [2]. Особую тревогу вызывает тот факт, что практически каждое пятое преступление в сфере информационной безопасности совершается несовершеннолетними, что говорит о необходимости усиления не только технической, но и социально-правовой защиты.

Финансовые последствия кибератак также становятся все более тяжелыми. Если в 2019 году средний размер выкупа, который компании платили злоумышленникам, составлял относительно небольшие суммы, то к 2024-му он вырос более чем в десять

раз, достигнув 10–15 млн рублей за один инцидент [3]. Это создает серьезные риски для бизнеса, особенно для малых и средних предприятий, которые не всегда обладают достаточными ресурсами для защиты. Следовательно, существенная роль в системе их защиты принадлежит также государству и зависит от эффективности проводимой политики обеспечения информационной безопасности.

Наибольшую опасность с позиции обеспечения информационной безопасности представляют атаки на организации критической информационной инфраструктуры, на которые в 2024 году пришлось 64 % всех инцидентов. Эти объекты обеспечивают функционирование ключевых отраслей экономики и безопасности государства, и их повреждение может привести к катастрофическим последствиям. Распределение атак по отраслям показывает, что наиболее уязвимыми остаются: промышленные предприятия (31% всех атак, 28 % высококритичных инцидентов), государственные учреждения (15 % атак), финансовый сектор (13–17 % атак), телекоммуникации (10 %), транспорт и логистика (11 %) [4].

Такая концентрация атак на стратегически важных секторах свидетельствует о том, что киберпреступность все чаще носит не просто криминальный, но и геополитический характер. В условиях санкционного давления и цифровой конфронтации с Западом Россия сталкивается не только с действиями отдельных хакеров, но и со скоординированными кампаниями, направленными на дестабилизацию экономики и государственного управления.

В связи с этими вызовами политика информационной безопасности становится одним из ключевых направлений государственной стратегии. Органы государственной власти РФ активно развивают нормативно-правовую базу, усиливают контроль критической информационной инфраструктуры, внедряют новые технологии защиты данных. Однако растущая сложность киберугроз требует не только технических мер, но и формирования общественного сознания, повышения цифровой грамотности, а также международного сотрудничества в борьбе с трансграничной киберпреступностью.

В последние годы политический дискурс вокруг информационной безопасности значительно активизировался: представители силовых структур, регуляторов и высшего руководства страны все чаще публично обсуждают вопросы кибербезопасности. Это отражает осознание того, что информационная безопасность — задача не только технологическая, но и политическая, напрямую связанная с суверенитетом и стабильностью государства. Укрепление обороны цифрового пространства, защита и надежная работа информационных систем, безопасность работы сайтов государственных органов власти, угрозы утечек конфиденциальной информации и персональных данных все чаще проявляется в качестве основных тем политического дискурса главы государства и федеральных органов власти.

Требование комплексного подхода к политике информационной безопасности определяется ростом киберпреступности, усилением атак на критическую инфраструк-

туру и увеличение финансовых потерь бизнеса. Необходимы не только новые законы и технологии, но и консолидация усилий государства, бизнеса и общества. В условиях цифровой эпохи безопасность данных и информационных систем становится таким же приоритетом, как и традиционные виды безопасности, что делает развитие политики информационной безопасности одной из ключевых задач современной России.

Публичные выступления представителей органов государственной власти по вопросам информационной безопасности позволяют выявить основные направления государственной политики в этой сфере, определить разрабатываемую и реализуемую систему мер по предотвращению социально-политических и экономических последствий киберугроз, а также сформировать в обществе социальную коммуникацию, ориентированную на развитие общественного сознания противодействия информационным угрозам.

Повышение осведомленности общества о потенциальных угрозах, влияние на цифровое поведение граждан, мобилизация общественной поддержки, формирование доверия в реализуемой политике информационной безопасности, профилактика панических настроений в условиях постоянных информационных угроз выступают системообразующими факторами, определяющими публичность дискурса об информационной безопасности в современной политической среде нашего государства.

Материалы и методы

В Стратегии национальной безопасности РФ «развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия» выступает национальным интересом и основой политики информационной безопасности. Многокомпонентность категории «информационная безопасность» в государственной политике определяется через задачи ее обеспечения, реализуемые путем формирования безопасной среды оборота достоверной информации, защиты информационной инфраструктуры, выявления и предупреждения угроз, предотвращения деструктивного воздействия на объекты критической инфраструктуры, предупреждения, выявления и пресечения преступлений с использованием информационно-телекоммуникационных технологий, повышения защищенности информационно-коммуникационной инфраструктуры, защиты информации и персональных данных, предотвращения ущерба от деятельности технической разведки иностранных государств, развития инструментов информационного противоборства, приоритетности использования в информационной сфере отечественного оборудования и технологий [5]. В Доктрине информационной безопасности Российской Федерации под информационной безопасностью понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором 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 безопас-

ность государства» [6]. Правовой анализ базовых документов, определяющих политику информационной безопасности России, показал, что информационная безопасность — многомерная категория, включающая как технические аспекты использования информации, ее защищенность, так и социально-психологические аспекты, определяющие деструктивное воздействие информационных угроз на личность и государство, влекущие за собой существенные социальные, экономические и политические последствия.

Многокомпонентность категории «информационная безопасность» определила дифференциацию предмета исследования у современных ученых, занимающихся проблемами информационной безопасности. Так, например, суверенизацию интернета как ответ на геополитическую конфронтацию достаточно подробно исследуют В. А. Луцкий и Т. А. Полякова [7, 8]. Исследованием гибридных угроз как проявлением информационно-психологического воздействия в результате кибератак занимается С. П. Расторгуев [9]. Технологические и политические аспекты импортозамещения для обеспечения информационной безопасности рассматривают в своих работах А. Г. Вепрев и С. В. Козлов. [10, 11]. А. В. Баранов представляет подробный обзор юридических аспектов международного опыта борьбы за цифровой суверенитет [12].

В качестве основного метода исследования применялся дискурсивный анализ, представляющий собой междисциплинарный метод, направленный на анализ социального контекста, выявление скрытых смыслов, властных отношений и идеологических структур в текстах и коммуникативных практиках.

В рамках политической социологии дискурс понимается как система институционализированных речевых практик, формирующих политическую реальность [13–15]. Применение дискурс-анализа в исследовании информационной безопасности позволяет выявить такие ключевые политические характеристики, как: механизмы легитимации политических решений, структуры властных отношений, способы конструирования социальных проблем в системе политики информационной безопасности. Благодаря именно этому подходу могут быть определены характерные составляющие системы власти, формирующей современную реальность через анализ идеологических сдвигов, способов легитимации политических решений, трансформаций содержательных характеристик.

Основу методологического исследования с применением дискурс-анализа составляют анализ тематических репрезентаций, выявление дискурсивных стратегий, деконструкцию бинарных оппозиций.

Материалами для исследования в дискурс-анализе послужили однотипные текстовые — публичные выступления представителей органов государственной власти разных ветвей:

- стенограммы посланий Президента Российской Федерации к Федеральному Собранию в 2023–2024 годах (2024 — объем текстового материала — 20 тыс. слов, доля текста по тематике информационной безопасности 1,5 % от общего объема, 2023 — объем текстового материала — 10,5 тыс. слов, доля текста по тематике информационной безопасности 1 %, 2022 — не было выступления с посланием) [16, 17];

- стенограммы выступления Председателя Правительства РФ с ежегодным отчетом Правительства перед Государственной Думой Федерального Собрания за 2022–2024 годы (2024 — объем текстового материала — 47,5 тыс. слов, доля текста по тематике информационной безопасности 0,3 % от общего объема, 2023 — объем текстового материала — 34 тыс. слов, доля текста по тематике информационной безопасности 1,5 %, 2022 — объем текстового материала — 48,7 тыс. слов, доля текста по тематике информационной безопасности 2,1 %) [18–20];
- ежегодные доклады Комиссии по защите государственного суверенитета и предотвращения вмешательства во внутренние дела Российской Федерации Совета Федерации Федерального Собрания за 2022–2024 годы (2024 — объем текстового материала — 42,5 тыс. слов, доля текста по тематике информационной безопасности 12 % от общего объема, 2023 — объем текстового материала — 35 тыс. слов, доля текста по тематике информационной безопасности 15 %, 2022 — объем текстового материала — 37 тыс. слов, доля текста по тематике информационной безопасности 10 %) [21–23].

Результаты и обсуждение

Политический дискурс информационной безопасности в России за последние годы стал ключевым элементом политической риторики. За период 2022–2024 годов он демонстрирует динамику, отражающую изменения внешнеполитического контекста, технологических вызовов и внутренних приоритетов государства. Для анализа текстов выступления в контексте информационной безопасности были выделены следующие аспекты: основная угроза, изменения законодательства, приоритетные технологии, используемые органами власти, ключевые целевые аудитории и характер риторики. На основе анализа официальных докладов и выступлений фиксируются ключевые тенденции и изменения в риторике выступлений политических акторов по вопросам информационной безопасности (табл. 1). Целесообразно отметить, что в анализируемых материалах президент, Совет Федерации и правительство выражают общие тенденции, эволюция которых особенно заметна в 2022–2024 годах.

Таблица 1

Эволюция дискурса «Информационная безопасность» в 2022–2024 годах

Аспект	2022	2023	2024
Основная угроза	Гибридная война	Иностранное влияние	Искусственный интеллект и дипфейки
Законодательство	Контроль иностранных компаний	Регулирование «агентов»	Защита выборов
Технологии	Импортозамещение	Развитие НИОКР	Цифровые платформы и искусственный интеллект
Целевые аудитории	Молодежь (соцсети)	Блогеры и наблюдатели	Избиратели и госслужащие
Риторика	«Защита от Запада»	«Цифровая диктатура»	«Электоральный суверенитет»

Политическая риторика по этим аспектам не отражает системности в деятельности органов государственной власти. Напротив, политический дискурс существенно меняется и каждый год в системе информационной безопасности расставляются новые акценты, которые отчасти зависят от геополитической ситуации и политических процессов, происходящих в России, более того не являются производными предыдущего этапа реализации политики в данной сфере. Это свидетельствует о постоянном поиске новых эффективных решений, конкретных действий в политике обеспечения информационной безопасности России.

В 2022 году доминирующей рамкой осмысления информационной безопасности стала концепция «гибридной войны», внутри которой цифровые угрозы рассматривались как составная часть комплексного противостояния с западными странами. Этот период характеризовался активным формированием концепта «цифрового суверенитета» как основы национальной безопасности. В нормативной сфере были приняты важные решения, в частности Федеральный закон № 236-ФЗ, регулирующий деятельность иностранных IT-компаний [24]. Особое внимание уделялось вопросам импортозамещения, что выразилось в создании национальных цифровых решений, таких как RuStore, и разработке системы льгот для отечественного IT-сектора.

К 2023 году произошла заметная институционализация контроля в информационной сфере. Принятие Федерального закона «О контроле за деятельностью лиц, находящихся под иностранным влиянием» от 14.07.2022 N 255-ФЗ обозначило новый этап в регулировании цифрового пространства [25]. В этот период наблюдается конкретизация воспринимаемых угроз — от абстрактных кибератак к более специфическим формам вмешательства, таким как использование блогеров для информационно-психологических операций. Важной новацией стало включение в дискурс темы цифровой грамотности населения как элемента системы противодействия угрозам. Параллельно активизировалась работа по развитию научно-технического потенциала, что нашло отражение в значительном расширении реестра российского программного обеспечения.

Прошедший 2024 год ознаменовался появлением новых технологических вызовов, в первую очередь связанных с развитием искусственного интеллекта. В фокусе внимания оказались такие явления, как создание дипфейков и персонализированное воздействие на участников избирательного процесса. Это потребовало совершенствования защитных механизмов, включая оптимизацию системы блокировки противоправного контента и введение специальных мер ответственности за посягательство на «электоральный суверенитет». Одновременно были сформулированы долгосрочные стратегические ориентиры, предполагающие создание комплексных цифровых платформ во всех ключевых отраслях к 2030 году и достижение самодостаточности в сфере искусственного интеллекта.

Эволюция дискурса демонстрирует последовательное усложнение концептуального аппарата и расширение регуляторного поля. Если в 2022 году акцент делался на противодействии внешним угрозам в рамках парадигмы «гибридной войны» и это обусловлено началом специальной военной операции, то к 2024-му сформировалась более комплексная система взглядов, интегрирующая технологические, правовые и идеологические компоненты национальной безопасности. Особого внимания заслуживает концепт «электорального суверенитета», отражающий усиление внимания к защите политических процессов в цифровой среде.

Необходимо отметить, что за три года российский дискурс информационной безопасности претерпел значительную трансформацию — от реактивных мер по противодействию внешним угрозам к формированию целостной системы взглядов, сочетающей технологическое развитие с комплексной защитой национального цифрового пространства. Эта эволюция отражает как изменение характера самих угроз, так и трансформацию подходов к обеспечению информационной безопасности в условиях быстро меняющейся технологической и геополитической реальности.

Исследование политического дискурса современной России по вопросу информационной безопасности позволило выделить ключевые акторы, его формирующие. К ним относятся президент, Совет Федерации Федерального собрания и правительство.

Таблица 2

Анализ акцентов в сфере информационной безопасности среди политических акторов России в 2022–2024 годах

Актор	Главные цитаты	Основные темы	Цель	Инструмент
Совет Федерации	*«Гибридная война с Западом», «12 млн кибератак на ЦИК»*	Внешние угрозы, контроль информации	Легитимация контроля	Законы, блокировки контента
Президент РФ	*«Защита детей от деградации», «Самодостаточность в ИИ»*	Идеологическая защита, технологический суверенитет	Идеологическая консолидация	Риторика «защиты»
Правительство РФ	*«80 % зарубежных решений имеют аналоги», «RuStore с 8 млн пользователей»*	Технологическое развитие, импортозамещение	Технологическая независимость	Льготы, RuStore, реестр ПО

Анализ официальных документов позволяет выявить специфику риторических стратегий различных институтов власти в области информационной безопасности. Со-

вет Федерации в своих докладах последовательно выстраивает нарратив о «тотальной гибридной войне с Западом», используя конкретные цифры кибератак (12 млн на ЦИК в 2024 году) для обоснования необходимости усиленного контроля (табл. 2). Эта позиция находит отражение в законодательных инициативах, таких как закон о равных условиях для IT-компаний, где подчеркивается обязанность государства противодействовать «распространению фальшивых сообщений».

Правительство, со своей стороны, делает акцент на практических аспектах технологического суверенитета. В отчетах подчеркиваются достижения в импортозамещении («80 % зарубежных решений имеют аналоги») и конкретные показатели развития цифровой инфраструктуры, такие как 8 млн пользователей RuStore. Особое внимание уделяется планам цифровой трансформации, выраженным в тезисе о необходимости сформировать «цифровые платформы во всех ключевых отраслях к 2030 году».

Президентская риторика объединяет технологическую и идеологическую составляющие. С одной стороны, подчеркивается необходимость «самодостаточности в искусственном интеллекте», с другой — звучат призывы к защите традиционных ценностей от «деградации». Характерно использование эмоционально окрашенных формулировок об «агрессивных информационных атаках», которые «извращают исторические факты», что усиливает информационное воздействие, определяя напряженность и угрозы в системе информационной безопасности.

Сравнительный анализ показывает, что при различии акцентов все институты используют сходный набор риторических приемов: апелляцию к статистике, подчеркивание внешних угроз, демонстрацию достижений в области технологического развития. Это создает целостный, но многослойный дискурс, где технологические аспекты безопасности тесно переплетаются с вопросами идеологии и государственного суверенитета.

Таким образом, разные акторы дополняют друг друга, формируя единый, но многослойный дискурс, где технологические меры одного сочетаются с силовой риторикой другого и объединяются идеологией третьего актора, где дискурс информационной безопасности становится инструментом политики обеспечения и защиты суверенитета государства.

Результаты проведенного исследования материалов также показывают, что основные содержательные темы дискурса информационной безопасности в политическом информационном поле включают цифровой суверенитет, киберугрозы, дезинформацию, регулирование интернета и защиту данных. Конструкцию дискурс-анализа определили следующие составляющие: содержание понятий «информационная безопасность» и «цифровой суверенитет»; используемые механизмы власти для регулирования информационного пространства; угрозы информационной безопасности России; обоснование реализуемых политических мер.

С 2022 года в российском политическом дискурсе информационная безопасность тесно связана с концепцией «цифрового суверенитета». Этот термин использует-

ся для обозначения независимости России в цифровой сфере, особенно в условиях «гибридной войны с Западом». В докладе комиссии Совета Федерации Федерального собрания РФ определяется необходимость «обеспечения цифрового суверенитета России в условиях тотальной гибридной войны с Западом», а в отчете правительства подчеркивается, что «создание и внедрение собственных технологий и решений — это один из наших важнейших приоритетов». Исходя из позиции того, что, по утверждению Фуко, дискурс формирует «режимы истины», которые определяют, что считается допустимым или недопустимым в обществе, то в данном контексте цифровой суверенитет представлен как необходимость, обусловленная внешними угрозами. Это создает нарратив, где зависимость от зарубежных технологий опасна, а переход на отечественные аналоги — единственно верный путь обеспечения информационной безопасности.

Также исследование определило, что основными мерами, которые государство активно применяет для контроля информационного пространства, являются принимаемые законы, такие как Федеральный закон от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации» и Федеральный закон «О контроле за деятельностью лиц, находящихся под иностранным влиянием» от 14.07.2022 N 255-ФЗ, которые направлены на регулирование деятельности иностранных IT-компаний и противодействие «иностранному влиянию». Таким образом, власть проявляется через дисциплинарные практики — законы и нормативные акты. Эти меры не только ограничивают деятельность иностранных компаний, но и формируют систему надзора, где государство определяет, какая информация допустима. Например, выявленная в дискурсе информационной безопасности информация о блокировке «противоправного контента» проявляется в 2024 году как инструмент контроля.

В дискурсе информационной безопасности Запад представлен как главный источник угроз, через кибератаки, дезинформацию и вмешательство во внутренние дела государства. Нарратив отражен в материалах Совета Федерации Федерального собрания РФ в 2022– 2023 годах, например, в следующих высказываниях: «информационная война... ведется по всем линиям, в том числе в социальных сетях и мессенджерах», «зарубежные оппоненты стараются использовать возможности общественных наблюдателей... для дискредитации избирательной системы». Это явление характерно для конструирования дискурса за счет создания бинарных оппозиций («мы» vs «они»). Здесь Запад — это «другой», который угрожает стабильности России. Такой нарратив оправдывает жесткие меры контроля, поскольку они подаются как защита от внешней агрессии.

Для обоснования мер информационной безопасности в выступлениях должностных лиц и представителей органов государственной власти используются данные о кибератаках, дезинформации и успехах отечественных технологий: «общее количество отраженных атак на портал ЦИК России... превысило пять миллионов», «уже почти 80 % зарубежных решений имеют отечественные аналоги». В этом случае использова-

ние фактологического материала позволяет ставить акценты на успехи в импортозамещении, что доказывает эффективность проводимой политики. Однако эти данные редко подвергаются независимой проверке, что делает их частью контролируемого конструируемого дискурса.

Хотя официальный дискурс подчеркивает успехи в цифровом суверенитете, в докладах также отмечаются проблемы, такие как недостаток отечественных платформ или сложности с качеством отечественного программного обеспечения. Однако эти вопросы подаются как временные трудности, которые будут преодолены: «В России до сих пор не созданы в необходимом количестве отечественные медиаплатформы», «сейчас заботимся об их качестве» (в контексте замены зарубежных IT-решений). Включение в дискурс элементов самокритики осуществляется для укрепления основного нарратива. Здесь признание проблем лишь усиливает аргумент о необходимости дальнейшего контроля и поддержки отечественных разработок.

Выводы

Выступления российских политических акторов по вопросам информационной безопасности играют ключевую роль в формировании информационной компоненты существования российского общества. Они повышают осведомленность граждан о киберугрозах, объясняют необходимость защитных мер и формируют общественную поддержку государственной политики.

Наличие в публичных выступлениях вопроса информационной безопасности — это не просто информирование населения, а важный инструмент формирования культуры общества и обеспечения поддержки государственной политики в сфере обеспечения информационной безопасности, встроенный в общегосударственную стратегию управления как неотъемлемый элемент сохранения государственного суверенитета и основа развития страны.

Дискурс информационной безопасности в современной России, анализируемый через призму фукианского подхода, представляет собой сложную систему власти, контроля и конструирования реальности. Проведенный анализ позволяет проследить существенную трансформацию концепции информационной безопасности в российском политическом дискурсе. За три года сложилась комплексная система взглядов, отражающая новые технологические и геополитические реалии. Цифровой суверенитет становится центральным элементом политической риторики, оправдывающим жесткие меры регулирования. Законодательные инициативы служат инструментами дисциплинарной власти, ограничивающими свободу информации. Образ Запада как врага используется для консолидации общества вокруг государственной политики. Технологии истины через статистические данные и демонстрацию успеха укрепляют доверие к официальному дискурсу, минимизируя альтернативные точки зрения.

Этот дискурс не только отражает политику государства, но и активно формирует общественное сознание, определяя, что считать угрозой, а что — безопасностью. В будущем, вероятно, он будет развиваться в сторону ужесточения контроля, особенно в связи с активным использованием в 2024 году искусственного интеллекта и дипфейков, что усилит роль государства в информационной сфере.

Из результатов анализа следует, что дискурс информационной безопасности в России служит инструментом привлечения населения к значению этой проблемы для государства и общества, переопределяет границы допустимого в публичной сфере, создает новые формы социального контроля.

Эволюция дискурса отражает переход от реактивных мер к системному подходу, где технологические решения сочетаются с правовым регулированием и идеологической защитой. Это свидетельствует о формировании целостной концепции информационной безопасности как элемента государственного суверенитета в цифровую эпоху.

Список источников

1. На кибермошенничества в РФ пришлось 40 % от всех преступлений в 2024 года. – URL: https://www.interfax.ru/russia/1003799 (дата обращения: 25.05.2025). – Текст : электронный.
2. Преступления с криптовалютой в России участились. Что предлагают власти. – URL: https://www.rbc.ru/crypto/news/67b7487c9a79471c2dd2c1f5?from=copy (дата обращения: 17.05.2025). – Текст : электронный.
3. Эксперты оценили в $150 тыс. средний выкуп, требуемый хакерами у бизнеса. – URL: https://www.rbc.ru/technology_and_media/05/02/2025/67a38a279a 79475e6c238ee7?ysclid=mcvonijb54397324156 (дата обращения: 17.05.2025). – Текст : электронный.
4. С КИИ — бди: большинство кибератак приходится на критическую инфраструктуру. – URL: https://iz.ru/1822780/sergei-guranov/s-kii-bdi-bolsinstvo-kiberatak-prihoditsa-na-kriticeskuu-infrastrukturu (дата обращения: 17.06.2025). – Текст : электронный.
5. Стратегия национальной безопасности Российской Федерации – URL: http://www.kremlin.ru/acts/bank/47046/page/1 (дата обращения: 17.06.2025). – Текст : электронный.
6. Доктрина информационной безопасности Российской Федерации. – URL: https://base.garant.ru/71556224/?ysclid=mdd1g7o37b960463043 (дата обращения: 17.06.2025). – Текст : электронный.
7. Луцкий, В. А. Кибербезопасность и государство: правовые основы информационного суверенитета / В. А. Луцкий. – Москва : Юстицинформ, 2022. – 288 с. – Текст : непосредственный.
8. Полякова, Т. А. Информационная безопасность: государственные стратегии противодействия угрозам / Т. А. Полякова. – Москва : МГИМО-Университет, 2021. – 416 с. – Текст : непосредственный.
9. Расторгуев, С. П. Информационная война как инструмент геополитики / С. П. Расторгуев. – Москва : Академический проект, 2020. – 352 с. – Текст : непосредственный.
10. Вепрев, А. Г. Политика информационной безопасности в условиях цифровой трансформации / А. Г. Вепрев, П. А. Толстых. – Москва : Русайнс, 2023. – 180 с. – Текст : непосредственный.
11. Козлов, С. В. Государственное управление информационной безопасностью в РФ / С. В. Козлов, А. А. Смирнов. – Москва : Проспект, 2021. – 240 с. – Текст : непосредственный.

12. Баранов, А. В. Национальные интересы России в киберпространстве / А. В. Баранов. – Санкт-Петербург : Изд-во СПбГУ, 2022. – 320 с. – Текст : непосредственный.

13. Фуко, М. Археология знания / М. Фуко. – Санкт-Петербург : ИЦ «Гуманитарная Академия»; Университетская книга, 2004. – 416 с. – Текст : непосредственный.

14. Савельева, Е. Б. О взглядах Мишеля Фуко на теорию дискурса / Е. Б. Савельева. – Текст : непосредственный // Вестник Московского института лингвистики. – 2015. – № 2. – С. 92–95.

15. Родина, В. В. Дискурс: генезис, природа и содержание, обзор научных школ / В. В. Родина. – Текст : непосредственный // Известия Санкт-Петербургского государственного экономического университета. – 2018. – № 1 (109). – С. 101–111.

16. Послание Президента Федеральному Собранию в 2024 году. – Текст: электронный // Президент России : официальный сайт. – 2024. – 29 фев. – URL: http://www.kremlin.ru/events/president/transcripts/messages/73585 (дата обращения: 20.06.2025).

17. Послание Президента Федеральному Собранию в 2023 году. – Текст : электронный // Президент России : официальный сайт. – 2023. – 21 фев. – URL: http:// www.kremlin.ru/events/president/transcripts/messages/70565 (дата обращения: 20.06.2025).

18. Ежегодный отчет Правительства в Государственной Думе. – 26 марта 2025. – URL: http://government.ru/news/54597/ (дата обращения: 21.06.2025). – Текст : электронный.

19. Ежегодный отчет Правительства в Государственной Думе. – 3 апреля 2024. – URL: http://government.ru/news/51246/ (дата обращения: 21.06.2025). – Текст : электронный.

20. Ежегодный отчет Правительства в Государственной Думе. – 23 марта 2023. – URL: http://government.ru/news/48055/ (дата обращения: 21.06.2025). – Текст : электронный.

21. Ежегодный доклад Комиссии по защите государственного суверенитета и предотвращению вмешательства во внутренние дела Российской Федерации за 2024 год. – URL: http://council.gov.ru/structure/commissions/iccf_def/plans/163959/ (дата обращения: 17.06.2025). – Текст : электронный.

22. Ежегодный доклад Комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела Российской Федерации. – 13 декабря 2023. – URL: http://council.gov.ru/structure/commissions/iccf_def/plans/151215/ (дата обращения: 17.06.2025). – Текст : электронный.

23. Ежегодный доклад Временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела Российской Федерации. – 23 декабря 2022. – URL: http://council.gov.ru/structure/commissions/iccf_def/plans/ 141465/ (дата обращения: 17.06.2025). – Текст : электронный.

24. Российская Федерация. Законы. О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации: Федеральный закон № 236-ФЗ [принят Государственной Думой 17 июня 2021 года : одобрен Советом Федерации 23 июня 2021 года]. – Москва, 2021. – URL: https://ivo.garant.ru/#/document/401414628/paragraph/1/doclist/1686/2/0/0/%D1%84%D0%B7%202 36:1 (дата обращения: 20.05.2025). – Текст : электронный.

25. Российская Федерация. Законы. О контроле за деятельностью лиц, находящихся под иностранным влиянием: Федеральный закон от 14 июля 2022 г. № 255-ФЗ [принят Государственной Думой 29 июня 2022 года : одобрен Советом Федерации 8 июля 2022 года]. – Москва, 2022. – URL: https://base.garant.ru/404991865/?ysclid=mct75kur2v299857741 (дата обращения: 20.05.2025). – Текст : электронный.

References

1. Cyber fraud accounted for 40 % of all crimes in Russia in 2024. (In Russian). Available at: https://www.interfax.ru/russia/1003799

2. Cryptocurrency-related crimes have increased in Russia. What authorities propose. (In Russian). Available at: https://www.rbc.ru/crypto/news/67b7487c9a79471c2dd2 c1f5?from=copy

3. Experts estimate average ransom demanded by hackers from businesses at $150 thousand. (In Russian). Available at: https://www.rbc.ru/technology_and_media /05/02/2025/67a38a279a79475e6c238ee7?ysclid=mcvonijb54397324156

4. Critical infrastructure alert: majority of cyber attacks target critical infrastructure. (In Russian). Available at: https://iz.ru/1822780/sergei-guranov/s-kii-bdi-bolsinstvo-kiberatak-prihoditsa-na-kriticeskuu-infrastrukturu

5. The National Security Strategy of the Russian Federation. (In Russian). Available at: http://www.kremlin.ru/acts/bank/47046/page/1

6. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii. (In Russian). Available at: https://base.garant.ru/71556224/?ysclid=mdd1g7o37b960463043

7. Lutskiy, V. A (2022). Kiberbezopasnost' i gosudarstvo: pravovye osnovy informatsionnogo suvereniteta. Moscow, Yustitsinform Publ., 288 p. (In Russian).

8. Polyakova, T. A. (2021). Information Security: State Strategies for Countering Threats. Moscow: MGIMO-University Publ., 416 p. (In Russian).

9. Rastorguev, S. P. (2020). Informatsionnaya voyna kak instrument geopolitiki. – Moscow, Akademicheskiy Proekt Publ., 352 p. (In Russian).

10. Veprev, A. G., & Tolstykh, P. A. (2023). Politika informatsionnoy bezopasnosti v usloviyakh tsifrovoy transformatsii. Moscow, Rusayns Publ., 180 p. (In Russian).

11. Kozlov, S. V., & Smirnov, A. A. (2021). Gosudarstvennoe upravlenie informatsionnoy bezopasnost'yu v RF. Moscow, Prospekt Publ., 240 p. (In Russian).

12. Baranov, A. V. (2022). Natsional'nye interesy Rossii v kiberprostranstve. St. Petersburg, SPbGU Publ., 320 p. (In Russian).

13. Foucault, M. The Archaeology of Knowledge. (2004). St. Petersburg, IC “Gumanitarnaya Akademiya”; Universitetskaya Kniga Publ., 416 p. (In Russian).

14. Savelieva, E. B. (2015). On the views Michel Foucaults theory of discourse // Vestnik Moskovskogo instituta lingvistiki, (2), pp. 92-95. (In Russian).

15. Rodina, V. V. (2018). Discourse: genesis, nature and content, review of scientific schools // Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta, 1(109), pp. 101-111. (In Russian).

16. Poslanie Prezidenta Federal'nomu Sobraniyu. (2024). (In Russian). Available at: http://www.kremlin.ru/events/president/transcripts/messages/73585

17. Poslanie Prezidenta Federal'nomu Sobraniyu. (2023). (In Russian). Available at: http://www.kremlin.ru/events/president/transcripts/messages/70565

18. Ezhegodnyy otchet Pravitel'stva v Gosudarstvennoy Dume. (2025). (In Russian). Available at: http://government.ru/news/54597/

19. Ezhegodnyy otchet Pravitel'stva v Gosudarstvennoy Dume. (2024). (In Russian). Available at: http:// government.ru/news/51246/

20. Ezhegodnyy otchet Pravitel'stva v Gosudarstvennoy Dume. (2023). (In Russian). Available at: http://government.ru/news/48055/

21. Ezhegodnyy doklad Komissii po zashchite gosudarstvennogo suvereniteta i predotvrashcheniyu vmeshatel'stva vo vnutrennie dela Rossiyskoy Federatsii za 2024 god. (In Russian). Available at: http://council.gov.ru/structure/commissions/iccf_def/plans/163959/

22. Ezhegodnyy doklad Komissii Soveta Federatsii po zashchite gosudarstvennogo suvereniteta i predotvrashcheniyu vmeshatel'stva vo vnutrennie dela Rossiyskoy Federatsii. (2023). (In Russian). Available at: http://council.gov.ru/structure/commissions/iccf_def/plans/151215/

23. Ezhegodnyy doklad Vremennoy komissii Soveta Federatsii po zashchite gosudarstvennogo suvereniteta i predotvrashcheniyu vmeshatel'stva vo vnutrennie dela Rossiyskoy Federatsii. (2022). (In Russian). Available at: http://council.gov.ru/ structure/commissions/iccf_def/plans/141465/

24. Rossiyskaya Federatsiya. Zakony. O deyatel'nosti inostrannykh lits v informatsionno-telekommunikatsionnoy seti "Internet" na territorii Rossiyskoy Federatsii: Federal'nyy zakon No 236-FZ. (2021). (In Russian). Available at: https://ivo.garant.ru/#/document/401414628/paragraph/1/doclist/1686/2/0/0/%D1%84%D0%B7%20236:1

25. Rossiyskaya Federatsiya. Zakony. O kontrole za deyatel'nost'yu lits, nakhodyashchikhsya pod inostrannym vliyaniem: Federal'nyy zakon ot 14 iyulya 2022 g. No 255-FZ. (2022). (In Russian). Available at: https://base.garant.ru/404991865/?ysclid=mct75kur2v299857741

Информация об авторах / Information about the authors

Попкова Алена Анатольевна, кандидат социологических наук, доцент кафедры маркетинга и муниципального управления, Тюменский индустриальный университет, г. Тюмень, popkovaaa@tyuiu.ru, ORCID: https: orcid.org/ 0000-0002-8507-8151

Парфенов Константин Владимирович, аспирант кафедры маркетинга и муниципального управления, Тюменский индустриальный университет, г. Тюмень

Alena A. Popkova, Candidate of Sociology, Associate Professor of the Department of Marketing and Government Administration, Industrial University of Tyumen, popkovaaa@tyuiu.ru, ORCID: https: orcid.org/ 0000-0002-8507-8151

Konstantin V. Parfenov, Postgraduate Student of the Department of Marketing and Government Administration, Industrial University of Tyumen

Статья поступила в редакцию 20.06.2025; одобрена после рецензирования 22.07.2025; принята к публикации 11.08.2025.
The article was submitted 20.06.2025; approved after reviewing 22.07.2025; accepted for publication 11.08.2025.