

Эволюция политики обеспечения информационной безопасности России в условиях геополитической турбулентности¹

Выходец Р. С. *, Щербань А. В.

Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация

* e-mail: marketing812@mail.ru

ORCID: 0000-0002-5910-9815

РЕФЕРАТ

Настоящее исследование посвящено анализу трансформации ключевых периодов российской политики информационной безопасности, в котором рассматриваются изменение восприятия вызовов и угроз, а также институциональное и концептуальное оформление данной сферы.

Цель и задачи. Выявить этапы развития системы информационной безопасности России в контексте влияния технологических и геополитических факторов. Проанализировать основные концептуальные документы и нормативно-правовые акты, а также охарактеризовать деятельность ключевых ведомств, ответственных за реализацию обеспечения политики в области информационной безопасности. **Методология.** В ходе исследования авторами использовались следующие методы: хронологический подход, метод анализа документов, метод системного анализа, институциональный анализ и контент-анализ. **Результаты.** Авторы выявили четыре основных периода формирования политики информационной безопасности России. Начальный этап (1992–1999 гг.) связан с разработкой нормативно-правовой базы в области защиты информации, институционализации органов государственного управления. Второй этап (2000–2014 гг.) ознаменовал начало доктринального оформления политики информационной безопасности, а также разработку мер защиты технических систем, связанных с масштабными процессами компьютеризации. Третий этап (2014–2022 гг.) за информационным пространством закрепляет статус самостоятельного домена международных конфликтов. Россия проводит комплексную политику по обеспечению информационной безопасности, которая учитывает технологические и психологические аспекты. Четвертый этап (с 2022 г.) характеризуется усилением внимания к обеспечению информационно-психологической безопасности, в котором учитывается влияние высоких технологий. **Выводы.** Российская политика информационной безопасности формировалась в логике постоянной адаптации к трансформации системы международных отношений и развития технологий. В условиях геополитической турбулентности, связанной с продолжением специальной военной операции, Россия взяла курс на обеспечение технологического суверенитета и усиление механизмов защиты информационно-психологического компонента безопасности.

Ключевые слова: информационная безопасность России, гибридные угрозы, цифровой суверенитет, информационное противоборство, цифровизация, информационное воздействие

Для цитирования: Выходец Р. С., Щербань А. В. Эволюция политики обеспечения информационной безопасности России в условиях геополитической турбулентности // Евразийская интеграция: экономика, право, политика. 2026. Т. 20, № 1. С. 164–174. EDN: XCGOIJ

¹ Работа выполнена при поддержке СПбГУ, шифр проекта 116471555.

The Evolution of Russia's Information Security Policy in the Context of Geopolitical Turbulence

Roman S. Vykhodets*, Anastasia V. Shcherban

Saint Petersburg State University, Saint Petersburg, Russian Federation

* e-mail: marketing812@mail.ru

ORCID: 0000-0002-5910-9815

ABSTRACT

This study is devoted to the analysis of the transformation of key periods of the Russian information security policy, which examines the changing perception of challenges and threats, as well as the institutional and conceptual design of this area. **Aim and tasks.** To identify the stages of development of the Russian information security system in the context of the influence of technological and geopolitical factors. To analyze the main conceptual documents and regulatory legal acts, as well as to characterize the activities of key departments responsible for the implementation of information security policy.

Methods. In the course of the research, the authors used the following methods: chronological approach, document analysis method, system analysis method, institutional analysis and content analysis. **Results.**

The authors have identified four main periods of the formation of Russia's information security policy: The initial stage (1992–1999) was associated with the development of a regulatory framework in the field of information protection and the institutionalization of public administration. The second stage (2000–2014) marked the beginning of the doctrinal formulation of information security policy, as well as the development of measures to protect technical systems associated with large-scale computerization processes. The third stage (2014–2022) establishes the status of an independent domain of international conflicts for the information space. Russia is pursuing a comprehensive information security policy that takes into account technological and psychological aspects. The fourth stage (from 2022) is characterized by increased attention to information and psychological security, which takes into account the impact of high technology. **Conclusions.** The analysis of these stages allows us to conclude that the Russian information security policy was formed in the logic of constant adaptation to the transformation of the system of international relations and the development of technology. In the context of the geopolitical turbulence associated with the continuation of its military operations, Russia has embarked on ensuring technological sovereignty and strengthening mechanisms to protect the information and psychological component of security.

Keywords: Russia's information security, hybrid threats, digital sovereignty, information warfare, digitalization, information impact

For citation: Vykhodets R. S., Shcherban A. V. The Evolution of Russia's Information Security Policy in the Context of Geopolitical Turbulence // Eurasian Integration: Economics, Law, Politics. 2026. Vol. 20, No. 1. P. 164–174 (In Russ.). EDN: XCGOIJ

Введение

В современном мире научно-технологический прогресс оказывает значимое влияние на все сферы жизни, включая область международных отношений. На это есть несколько причин. Прежде всего, динамичный рост пользователей интернет-пространства продолжает общемировые тенденции формирования глобального информационного общества, в котором быстрый обмен информацией играет ключевую роль [13, р. 9–10]. Только по последним данным 68% населения Земли являются активными пользователями интернета. Примечательно, что, используя сеть для поиска информации, чтения новостей, общения и развлечений, человек в среднем проводит онлайн более шести с половиной часов в день [11]. Это говорит о том, что интернет наряду с традиционными СМИ, образованием, воспитанием и социумом выступает ключевым элементом в формировании картины мира человека.

Не менее важным аспектом является факт того, что технологическое развитие становится новым критерием в определении лидерских позиций государств на арене международных отношений [4, с. 7]. Первая четверть XXI в. ознаменовала начало технологической гонки между КНР и США, которая привела к формированию вокруг них двух ИТ-пространств. В таких условиях страны, оценивая риски и возможности, стремятся примкнуть к более приемлемой модели высокотехнологического прогресса [2, с. 262]. С одной стороны, данное обстоятельство способствует росту экономических показателей инновационных государств-сателлитов, с другой — создает дополнительный рычаг давления и ограничивает технологический суверенитет.

Все вышеизложенное свидетельствует о том, что стремительная цифровизация и широкое распространение информационных технологий актуализирует проблему их противоправного использования. В настоящее время для реализации своих политических амбиций международные акторы все чаще прибегают к совершению атак, мишенью которых становятся не только информационно-коммуникационные системы, но и мировоззренческие установки граждан, системы общественного мнения и даже психика отдельного человека [6, с. 78].

С началом специальной военной операции (СВО) на территории Украины страны коллективного Запада усилили информационное противоборство против России. В нынешних условиях наметилась опасная тенденция проведения информационно-психологических операций, направленных на дискредитацию действий Москвы и формирование негативного образа государства в глазах мировой общественности. В таких обстоятельствах указанные последствия технологического прогресса демонстрируют значимость выстраивания эффективной системы информационной безопасности, поскольку она неразрывно связана с вопросами суверенитета России и обеспечением национальной безопасности.

Материалы и методы

Источниковая база исследования сформирована рядом официальных российских документов, затрагивающих вопросы обеспечения информационной безопасности. Теоретическую основу статьи составляют весомые отечественные и зарубежные работы по данной теме.

В ходе исследования хронологический метод позволил выделить ключевые этапы в развитии системы обеспечения информационной безопасности России. Осуществив институциональный и нормативно-правовой анализ, авторы смогли оценить возможность реализации законов и определить компетенции ключевых государственных ведомств. Для исследования основных доктрин и концепций был применен контент-анализ. Благодаря системному анализу установлены факторы влияния международной напряженности и развития технологий на обеспечение информационной безопасности России.

Обсуждение и результаты

События февраля 2022 г. выступили мощным катализатором процессов мировой деглобализации, положив начало становлению новой системы международного порядка. Такая трансформация нарушила устойчивость привычных моделей глобального взаимодействия, что привело к усилению *геополитической турбулентности* — состоянию международных отношений, в котором традиционные практики управления утратили свою силу, а новые еще не обрели институционального оформления [1, с. 43]. Как следствие, происходит обострение международных конфликтов, в которых информационное пространство в настоящее время выступает обособленным измерением, сочетающим борьбу на информационно-технологическом и информационно-психологическом направлениях. В этих условиях обеспечение информационной безопасности становится стратегическим приоритетом защиты национальных интересов государства.

При этом некоторые исследователи указывают на существующие проблемы, связанные с разработкой эффективной модели информационной безопасности [10, р. 449–450]. В большинстве случаев государства не создают принципиально новые механизмы защиты информационного пространства,

а стремятся адаптировать традиционные практики безопасности к условиям цифровизации. Такой подход не всегда способен гарантировать возможность адекватного ответа на вызовы и угрозы цифровой эпохи.

Этапы становления политики информационной безопасности России

Современная система информационной безопасности России сложилась в результате поэтапной трансформации подходов к восприятию вызовов и угроз в информационной среде. Существенное влияние на ее формирование оказал ряд факторов, включающих процессы геополитической турбулентности, динамичного развития высоких технологий и смещения межгосударственного противоборства в информационное пространство.

В истории развития политики информационной безопасности России целесообразно выделить четыре основных этапа.

Первый этап: 1992–2000 гг. В этот период была заложена нормативно-правовая база, которая в будущем станет основой для разработки доктринальных документов, регламентирующих вопросы обеспечения информационной безопасности.

Впервые термин «информационная безопасность» в российском официальном дискурсе встречается в Законе РФ «О безопасности» от 05.03.1992¹ (в настоящее время утратил силу). Анализируя ст. 13 этого документа, можно отметить, что, несмотря на указание необходимости обеспечения информационной безопасности, в положении отсутствует ее определение и четкая конкретизация границ.

При этом появление электронных возможностей обработки, передачи и хранения данных, а также растущая зависимость государства от технологий продиктовали необходимость создания механизма координации мер защиты на федеральном уровне. С этой целью в 1992 г. была образована Государственная технологическая комиссия при Президенте РФ (в настоящее время — Федеральная служба по техническому и экспортному контролю (ФСТЭК)), осуществлявшая контроль в сфере технической защиты информации².

В то же время нельзя не отметить ряд принятых нормативно-правовых актов, в которых информация рассматривается в качестве объекта обеспечения безопасности:

- ФЗ «О средствах массовой информации» 1991 г.³ — регулирует вопросы информационной политики государства в целях обеспечения национальной безопасности. Документ закрепляет положение о недопустимости цензуры, а также устанавливает запрет на разглашение сведений, входящих в государственную тайну, открытых призывов к смене конституционного режима, пропаганде терроризма и экстремизма;
- ФЗ «О государственной тайне» 1993 г.⁴ — дает представление об информации, составляющей государственную тайну. Данный документ является первым законодательным актом, в котором защита информации напрямую связана с обеспечением государственных интересов;
- ФЗ «Об информации, информатизации и защите информации» 1995 г.⁵ (документ утратил силу) — координирует вопросы производства и распространения информации, устанавливает правила обработки и защиты информации, а также закрепляет права граждан на защиту своей конфиденциальной информации.

¹ Закон РФ «О безопасности» от 05.03.1992 № 2446-1 [Электронный ресурс] // Мэрия города Новосибирска. Департамент образования. URL: https://do.nios.ru/sites/do.nios.ru/files/no_2446-1_ot_05.03.92_o_bezopasnosti.pdf (дата обращения: 25.08.2025).

² Указ Президента Российской Федерации от 05.01.1992 № 9 «О создании Государственной технической комиссии при Президенте Российской Федерации» [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/acts/bank/706> (дата обращения: 21.10.2025)

³ Закон РФ от 27.12.1991 № 2124-1 (ред. от 23.07.2025) «О средствах массовой информации» [Электронный ресурс] // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения: 30.10.2025).

⁴ Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.08.2024) «О государственной тайне» [Электронный ресурс] // Консультант Плюс. URL: https://rpn.gov.ru/upload/iblock/d30/qjw6klw1pa2yif6ljqkh6y91lebabpsu/Zakon-RF-ot-21.07.1993-N-5485_1-O-gosudarstvennoy-tayne.pdf (дата обращения: 25.08.2025).

⁵ Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» [Электронный ресурс] // Правительство России. URL: <http://government.ru/docs/all/95876/> (дата обращения: 25.08.2025).

Отдельного внимания заслуживает ФЗ «Об участии в международном информационном обмене» 1996 г.¹ (документ утратил силу), поскольку именно в нем было дано первое официальное определение «информационной безопасности»: состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В 1998 г. по инициативе Комитета Государственной Думы по информационной политике и связи был разработан проект Концепции государственной информационной политики [7], в которой подчеркивалась необходимость «защиты информационных ресурсов и информационно-телекоммуникационной инфраструктуры от информационного оружия». Это стало первым примером артикуляции на уровне официального политического дискурса качественно нового вида вызов и угроз.

В том же году Россия обозначает национальные усилия в области обеспечения информационной безопасности на международном уровне. В октябре 1998 г. Российская Федерация внесла на рассмотрение Генеральной Ассамблеи ООН проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», который впоследствии был принят (в декабре 1999 г.)². В документе подчеркивалась необходимость совместных усилий мирового сообщества в предотвращении неправомерного использования информационных технологий в преступных и террористических целях.

Таким образом, на начальном этапе были заложены нормативно-правовые основы для выстраивания системы обеспечения информационной безопасности, а также предприняты первые политические шаги в этом направлении на национальном и международном уровнях.

Второй этап: 2000–2014 гг. В 2000 г. в России была принята Доктрина информационной безопасности РФ — первый официальный документ, который, по сути, придал информационной среде статус самостоятельного домена национальной безопасности. В Преамбуле подчеркивалось, что Доктрина «развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере»³. Поэтому с 2000 г. национальная безопасность России обрела самостоятельное информационное измерение.

Интенсификация процессов цифровизации отношений между гражданами и государством, чему во многом способствовала утвержденная Правительством в 2002 г. Федеральная целевая программа «Электронная Россия»⁴, потребовала системных мер по обеспечению безопасности процессов сбора, хранения и передачи персональной информации. Для решения этой задачи в 2006 г. Государственная Дума принимает Закон «О персональных данных»⁵, который определил основные принципы и подходы к обработке персональных данных граждан, что спустя двадцать лет, в эпоху искусственного интеллекта, станет одним из столпов обеспечения информационной безопасности.

Наряду с этим динамичное распространение информационно-коммуникационных технологий и ежегодный рост киберпреступности во всем мире продиктовали необходимость многоуровневого развития государственных механизмов контроля исполнения мер по обеспечению политики информационной безопасности. Так, в 2004 г. вопросы защиты критической информационной инфраструктуры, а также выдачи лицензионных сертификатов стали входить в компетенцию ФСТЭК⁶.

¹ Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» [Электронный ресурс] // Правительство России. URL: <http://government.ru/docs/all/95876/> (дата обращения: 25.08.2025).

² Резолюция Генеральной Ассамблеи ООН № 53/70 от 04.01.1999 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Электронный ресурс] // Организация Объединенных Наций. URL: <https://docs.un.org/ru/A/RES/53/70> (дата обращения: 25.08.2025).

³ Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) [Электронный ресурс] // Контур Норматив. URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=40613> (дата обращения: 25.08.2025).

⁴ Постановление Правительства РФ от 28.01.2002 № 65 «О федеральной целевой программе “Электронная Россия (2002–2010 годы)”» [Электронный ресурс] // Гарант.ру. URL: <https://base.garant.ru/184120/> (дата обращения: 25.08.2025).

⁵ Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [Электронный ресурс] // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 31.07.2025).

⁶ Сведения о полномочиях ФСТЭК России; перечень нормативных правовых актов, определяющих эти полномочия [Электронный ресурс] // Федеральная служба по техническому и экспортному контролю. URL: <https://fstec.ru/obshchaya-informatsiya/polnomochiya> (дата обращения: 03.08.2025).

Вместе с тем российское государство остро нуждалось в развитии надежной и безопасной системы правительственной связи и повышении уровня защиты информационной инфраструктуры. Реализация этих мер была включена в перечень полномочий Спецсвязи и Федеральной службы безопасности. Отдельно необходимо отметить деятельность Роскомнадзора, который осуществляет контроль соблюдения законодательных актов России в области связи, информационно-коммуникационных технологий (ИКТ) и СМИ¹.

В это время по странам постсоветского пространства и Ближнего Востока прокатилась волна «цветных революций» под идеологической вывеской распространения западных ценностей и построения многовекторной внешней политики, нацеленной на сближение с США и ЕС [5, с. 71]. Как указывают некоторые исследователи, существует достаточно широкий диапазон в оценках феномена «цветных революций». Если в отечественной науке господствует точка зрения о внешнем вмешательстве во внутреннюю политику страны, то для западного социально-политического дискурса характерно рассмотрение данных событий в категориях ненасильственного сопротивления и демократизации государственных процессов [9, с. 947]. Так или иначе, и российские, и западные исследователи едины в том, что основным инструментом в подогревании протестных настроений и мобилизации оппозиционно настроенных граждан сыграли социальные сети. В частности, после массовых протестов в Молдове в 2009 г. в широкий обиход вошел термин «твиттер²-революция»³.

В результате этого как на уровне экспертов, так и на уровне политической власти становится очевидным, что некоммерческие организации, электронные СМИ, лидеры мнений, в распоряжении которых находится весь арсенал современных средств коммуникации, обладают достаточными ресурсами по дестабилизации социально-политической обстановки в любой стране мира, а действуя в интересах внешнего субъекта, они становятся влиятельными игроками в международных конфликтах. Осознание этого факта привело к закреплению самостоятельного статуса информационной безопасности в системе национальной безопасности и потребовало от России дальнейших шагов по защите своего суверенитета и национальных интересов в информационной сфере.

Третий этап: 2014–2022 гг. Началом нового этапа формирования в России целостной системы обеспечения информационной безопасности послужила «Крымская весна». В 2014 г. в результате государственного переворота, произошедшего на Украине при активной поддержке западных политиков и спецслужб, Республика Крым вошла в состав Российской Федерации. Данное событие послужило спусковым крючком к резкому обострению геополитической обстановки, многие годы остававшейся напряженной. В ответ на это коллективный Запад начинает активно применять тактику гибридной войны [12, р. 18] в отношении России, которую он открыто обозначает в качестве своей основной угрозы⁴.

Примечательно, что годом ранее, выступая в Академии военных наук, генерал В. Герасимов поднимал проблему расширения театра боевых действий и появления новых форм конфликтов. Основные положения его доклада дополнили новую редакцию Военной доктрины РФ (2014 г.)⁵. В документе отмечалось, что наметилась тенденция смещения межгосударственного противоборства в сферу информационного пространства и увеличения числа эпизодов использования ИКТ для дестабилизации внутриполитической обстановки.

События на территории Украины 2014 г., а также последующее участие Вооруженных сил РФ на стороне правительственных войск Сирии в 2015 г. дали старт разворачиванию Западом масштабных информационных кампаний по очернению и дискредитации России на международной арене.

¹ Публичная декларация целей и задач Роскомнадзора [Электронный ресурс] // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: <https://rkn.gov.ru/about/public-declaration/> (дата обращения: 03.08.2025).

² Социальная сеть X (ранее Twitter) заблокирована на территории Российской Федерации по решению Генпрокуратуры от 24 февраля 2022 г. на основании ст. 15.3 закона об информации, информтехнологиях и о защите информации.

³ Moldova's Twitter revolution is NOT a myth [Электронный ресурс] // Foreign policy. 10.04.2009 URL: <https://foreignpolicy.com/2009/04/10/moldovas-twitter-revolution-is-not-a-myth/> (дата обращения: 28.12.2025).

⁴ Заявление глав государств и правительств, участвующих в заседании Североатлантического союза в Уэльсе — 4–5 сентября 2014 г. [Электронный ресурс] // NATO. 05.12.2014. URL: https://www.nato.int/cps/ru/natohq/official_texts_112964.htm (дата обращения: 29.07.2025).

⁵ Военная доктрина Российской Федерации (утверждена Президентом Российской Федерации 25.12.2014 № Пр-2976) [Электронный ресурс] // Совет Безопасности РФ. URL: <http://www.scrf.gov.ru/security/military/document129/#> (дата обращения: 03.08.2025).

Неоднократно фиксировавшиеся в это время спланированные атаки на российские информационные системы и множественные кампании в информационной среде, направленные на усиление экстремистских настроений в обществе, разжигание национальной и религиозной розни, делигитимацию политического руководства страны, способствовали концептуальной дифференциации информационной безопасности и началу обособления двух ее сфер: информационно-технической и информационно-психологической.

В качестве ответных мер по укреплению информационно-технической составляющей в 2016 г. широкую огласку получили два федеральных закона, № 374-ФЗ и № 375-ФЗ, более известные как «пакет Яровой». Их основные положения касаются упрощения технических возможностей по идентификации личности в информационном пространстве. В частности, провайдерам и операторам связи предписывалось хранить весь пользовательский трафик в установленный период и предоставлять данную информацию по запросу правоохранительных органов¹.

В дополнение к этому в июле 2017 г. были приняты поправки в Федеральный закон «О связи»², целью которых являлось пресечение распространения SIM-карт без предоставления реальных паспортных данных абонента. А в октябре 2021 г. Правительство РФ приняло Постановление, которое определило порядок идентификации пользователей организаторами сервисов обмена мгновенными сообщениями. В частности, операторы обязаны идентифицировать личность при регистрации в мессенджерах, используя данные оператора мобильной связи³.

2016 г. ознаменовался началом милитаризации киберпространства. По итогам Варшавского саммита НАТО за киберпространством был закреплен статус самостоятельной сферы проведения стратегических операций⁴. В конце этого же года МИД РФ публикует обновленную Доктрину информационной безопасности⁵, в которой нашли отражение окончательно сложившиеся к тому моменту изменения геополитических реалий, а также форм и методов современных международных конфликтов. Прежде всего, в качестве объективных условий в документе констатировалось появление новых видов информационных угроз.

В качестве первых шагов по обеспечению информационно-психологической безопасности выступают принятые в 2019 г. изменения в КоАП РФ, предусматривающие ответственность за распространение в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информации, которая оскорбляет человеческое достоинство и общественную нравственность⁶.

Стремительные изменения структуры мирового порядка, а также непрекращающиеся попытки дестабилизации политической обстановки в стране послужили катализатором разработки нового стратегического документа в области обеспечения национальной безопасности. В 2021 г. В. В. Путиным была утверждена обновленная Стратегия национальной безопасности РФ, которая закрепляла положение о том, что реализация национальных интересов России невозможна без объединения усилий в приоритетных направлениях, к которым относится сфера информационной безопасности⁷.

¹ Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» от 06.07.2016 № 375-ФЗ (последняя редакция) [Электронный ресурс] // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_201087/#dst0 (дата обращения: 05.08.2025); Федеральный закон «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» от 06.07.2016 № 374-ФЗ (последняя редакция) [Электронный ресурс] // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_201078/#dst0 (дата обращения: 05.08.2025).

² Федеральный закон от 29.07.2017 № 245-ФЗ «О внесении изменений в Федеральный закон «О связи»» [Электронный ресурс] // Консультант Плюс. URL: <https://www.consultant.ru/law/hotdocs/50478.html> (дата обращения: 01.08.2025).

³ Постановление Правительства Российской Федерации от 20.10.2021 № 1801 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями» [Электронный ресурс] // Правительство России. URL: <http://government.ru/docs/all/137122/> (дата обращения: 09.09.2025).

⁴ Warsaw Summit Communiqué [Электронный ресурс] // NATO URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communication> (дата обращения: 17.10.2025).

⁵ Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Министерство иностранных дел Российской Федерации. URL: https://www.mid.ru/ru/foreign_policy/official_documents/1539546/ (дата обращения: 29.07.2025).

⁶ Федеральный закон от 18.03.2019 № 28-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/acts/bank/44089> (дата обращения: 09.09.2025).

⁷ Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/acts/bank/47046> (дата обращения: 01.08.2025).

Итогом третьего этапа стало формирование целостной системы идентификации личности в информационном пространстве, создание нормативно-правовой основы по противодействию распространению дезинформации, а в концептуальном аспекте наметилась четкая тенденция по обособлению информационно-технической и информационно-психологической сфер информационной безопасности.

Четвертый этап: с 2022 г. В феврале 2022 г., с началом проведения Россией специальной военной операции на территории Украины, стало ясно, что вооруженный конфликт на ограниченной территории является частью комплексного противоборства Москвы с коллективным Западом. В этом обострившемся противостоянии вполне отчетливо обозначались несколько фронтов: военный, финансово-экономический и информационный.

Обладая подавляющим преимуществом в контроле над глобальным медиапространством, странам Запада удалось сформировать необходимую для них в сложившихся обстоятельствах антироссийскую информационную повестку, которая позволяла на протяжении нескольких лет поддерживать негативное общественное мнение по поводу российских действий.

С момента начала СВО западные СМИ и социальные сети наполнились ярко выраженными русофобскими нарративами, активно создавались и тиражировались фейки в отношении действий российских военных на территории Украины, подверглись блокировке многие пророссийские каналы на популярных видеохостингах и группы в социальных сетях. Это дало основания говорить о развернутой против России полномасштабной информационно-психологической войне.

Ответные шаги Москвы не заставили себя ждать. В марте 2022 г. на территории России произошла блокировка продуктов компании Meta¹. Данное решение было обусловлено тем, что контролируемые ею социальные платформы официально сняли запрет на призывы к насилию в отношении российских военных.

На законодательном уровне также были предприняты необходимые шаги по укреплению информационно-психологического компонента информационной безопасности страны. В частности, введен контроль за деятельностью иностранных агентов². Документ предусматривал необходимость маркировки информации, производимой и (или) распространяемой иностранным агентом.

Безответственная популяризация нарративов, направленных на искажение сознания граждан и формирование ложных ценностных ориентиров, акцентировала необходимость дополнения законодательства. Так, была установлена уголовная ответственность за фейки о действиях Вооруженных Сил РФ, а также их дискредитацию³. На государственном уровне введен запрет пропаганды нетрадиционных семейных отношений⁴, а также запрет размещения рекламы на ресурсах с ограниченным доступом⁵.

Существующие проблемы, связанные с вербовкой и травлей детей, вовлечением их в преступную деятельность, а также распространением материалов с возрастными ограничениями посредством социальных платформ, потребовали разработки системных мер по созданию безопасной информационной среды. В 2023 г. Правительство РФ утвердило Концепцию информационной безопасности детей⁶, в которой закреплялась необходимость включения в образовательный процесс учебных дисциплин по информационной безопасности и цифровой грамотности.

¹ Компания Meta Platforms Inc. признана в России экстремистской организацией и запрещена.

² Федеральный закон «О контроле за деятельностью лиц, находящихся под иностранным влиянием» от 14.07.2022 № 255-ФЗ (последняя редакция) [Электронный ресурс] // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_421788/ (дата обращения: 04.09.2025).

³ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 01.09.2025) [Электронный ресурс] // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/1aa9268e7d3bd57bcbd46a3016641c5af64b9c87/ (дата обращения: 04.09.2025).

⁴ Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 06.09.2025) [Электронный ресурс] // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/5b103e878283a04f8ea2130f38e19f10b516b626/ (дата обращения: 04.09.2025).

⁵ Федеральный закон от 07.04.2025 № 72-ФЗ «О внесении изменений в статью 12 Федерального закона «О противодействии экстремистской деятельности» и Федеральный закон «О рекламе»» [Электронный ресурс] // Официальное опубликование правовых актов. URL: <http://publication.pravo.gov.ru/document/0001202504070018> (дата обращения: 04.09.2025).

⁶ Правительство утвердило Концепцию информационной безопасности детей [Электронный ресурс] // Правительство РФ. URL: <http://government.ru/docs/48416/> (дата обращения: 11.12.2025).

Вхождение в состав Российской Федерации Донецкой и Луганской Народных Республик, Запорожской и Херсонской областей выступило фактором совершенствования механизмов по интеграции местного населения в единое социокультурное пространство страны. Это положение в полной мере отражается в Стратегии государственной национальной политики РФ на период до 2036 года. Особая роль в документе отводится укреплению единства многонационального народа при сохранении этнического и языкового многообразия. В то же время русский язык занимает центральное место в формировании общероссийской гражданской идентичности¹.

Несмотря на существующую геополитическую напряженность, Россия продолжает развивать международное сотрудничество в области формирования системы международной информационной безопасности, что входит в число приоритетных задач Концепции внешней политики РФ². Ввиду этого можно отметить активизацию российских усилий в данном вопросе на региональных площадках. Так, в рамках деятельности ПА ОДКБ Российская Федерация и Республика Беларусь являются лидерами в продвижении инициатив, направленных на пресечение попыток фальсификации истории и реабилитации нацизма [3, с. 206]. В условиях непрекращающегося информационного давления против России такие предложения способствуют укреплению компонента информационно-психологической безопасности государства, поскольку защищают патриотическо-ценностные установки граждан и подвиг советского народа.

Таким образом, на текущем этапе в России завершается формирование целостной системы информационной безопасности, включающей информационно-техническую и информационно-психологическую сферы. При этом, как указывают некоторые авторы, в настоящее время самостоятельный статус начинает обретать когнитивная безопасность, связанная с противодействием вызовам и угрозам индивидуальной человеческой психике, основанная на передовых информационных технологиях, прежде всего, искусственном интеллекте [8, с. 317, 320]. На этом этапе обеспечение информационной безопасности обрело статус одного из ключевых элементов в сфере обеспечения технологического суверенитета России. Так, Концепция технологического развития на период до 2030 года придает приоритетное значение вопросам обеспечения безопасности высокотехнологических систем и защите информации. Что позволяет рассматривать информационную безопасность в качестве системообразующего элемента обеспечения технологической независимости России.

Заключение

Исследуя российскую модель информационной безопасности, авторы выделили четыре периода в истории ее становления. *Ранний этап — 1992–2000 гг.* — представляет собой принятие нормативных документов, которые заложили основу будущего формирования политики информационной безопасности. *В период с 2000 по 2014 г.* информационная безопасность обрела самостоятельность в системе национальной безопасности и получила доктринальное закрепление. Это объясняется активными процессами цифровизации и развитием ИКТ, которые стали инструментом и площадкой для проведения информационно-психологических операций, направленных на дестабилизацию внутривнутриполитической обстановки.

В период 2014–2022 гг. происходит геополитическая конфронтация между Россией и странами Запада, нашедшая воплощение в проведении информационной политики по дискредитации образа РФ на международной арене и росте прецедентов использования ИКТ в противоправных целях. Ответными мерами России была разработка новой доктрины и законодательных актов, регулирующих вопросы обеспечения информационной безопасности.

На современном этапе, с момента начала Россией СВО на территории Украины, произошел новый виток геополитической конфронтации, в котором информационное противоборство стало самостоятельной ареной проведения стратегических операций. Масштабное проведение кибератак, информа-

¹ Указ Президента Российской Федерации от 25.11.2025 № 858 «О Стратегии государственной национальной политики Российской Федерации на период до 2036 года» [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/acts/bank/52615> (дата обращения: 13.12.2025).

² Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 31 марта 2023 г.) [Электронный ресурс] // Министерство иностранных дел РФ. URL: https://www.mid.ru/fr/foreign_policy/official_documents/1860586/?lang=ru (дата обращения: 03.08.2025).

ционно-психологическое давление на российских военных и гражданских лиц и проведение такого рода стратегических операций, злонамеренное применение технологий искусственного интеллекта представило понимание серьезности вопросов обеспечения информационно-психологической безопасности и необходимости обретения цифрового суверенитета для обеспечения защиты технологических систем.

Список литературы

1. Балацкий Е. В. Россия в эпицентре геополитической турбулентности: накопление глобальных противоречий // Экономические и социальные перемены: факты, тенденции, прогноз. 2022. Т. 15, № 4. С. 42–59. EDN: LOGPEF. DOI: 10.15838/esc.2022.4.82.3
2. Выходец Р. С. Большие ИИ-пространства и стратегия России в условиях санкционной войны // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22. № 2. С. 256–270. EDN: FYNWU. DOI: 10.22363/2313-0660-2022-22-2-256-270
3. Выходец Р. С., Тюменцев И. О. Вопросы информационно-психологической безопасности в ракурсе Программы деятельности Парламентской Ассамблеи Организации Договора о коллективной безопасности на 2026–2030 годы // Вестник Волгоградского государственного университета. Серия 4. История. Регионоведение. Международные отношения. 2025. Т. 30, № 3. С. 201–211. EDN: YLZKPB. DOI: 10.15688/jvolsu4.2025.3.18
4. Караганов С. А., Лукьянов Ф. А. Россия в мире силы XXI века // Россия и мусульманский мир. 2014. № 5 (263). С. 5–13. EDN: SGGZKJ
5. Карпович О. Г., Манойло А. В. Цветные революции. Теория и практика демонтажа современных политических режимов. М. : ЮНИТИ-ДАНА: Закон и право. 2015. 111 с. ISBN: 978-5-238-02631-2. EDN: TBWKDJ
6. Кефели И. Ф. Асфатроника: на пути к теории глобальной безопасности. СПб. : ИПЦ СЗИУ РАНХиГС, 2020. 228 с. ISBN: 978-5-89781-676-7. EDN: JSTIQP
7. Концепция государственной информационной политики / под общ. ред. О. А. Финько. М. : 1999. 47 с.
8. Прологомены когнитивной безопасности. Коллективная монография / под ред. И. Ф. Кефели. СПб. : ИД «Петрополис», 2023. 487 с. ISBN: 978-5-9676-1526-9. EDN: MRECBE
9. Цветкова Н. А. Дискурс «цветных революций» // Постсоветские исследования. 2019. Т. 2, № 2. С. 940–950. EDN: ZAQKFV
10. Foulon M., Meibauer G. How Cyberspace Affects International Relations: The Promise of Structural modifiers // Contemporary Security Policy. 2024. Vol. 45, No. 3. P. 426–458. DOI: 10.1080/13523260.2024.2365062
11. Kemp S. Digital 2025: Global Overview Report. 05.02.2025. URL: <https://datareportal.com/reports/digital-2025-global-overview-report>
12. Mattis J., Hoffman F. Future Warfare: The Rise of Hybrid Wars // Proceedings Magazine. 2005. Vol. 132. Issue: November. P. 18–19. URL: <https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars>
13. Webster F. Theories of the Information Society. 3th ed. London : Routledge, 2006. 314 p. ISBN: 978-0-415-40633-8. DOI: 10.4324/9780203962824

Об авторах:

Выходец Роман Сергеевич, доктор политических наук, доцент, профессор кафедры теории и истории международных отношений, Санкт-Петербургский государственный университет (Санкт-Петербург, Российская Федерация);
e-mail: marketing812@mail.ru; ORCID: 0000-0002-5910-9815

Щербань Анастасия Владимировна, аспирант, факультет международных отношений, Санкт-Петербургский государственный университет (Санкт-Петербург, Российская Федерация);
e-mail: n.shche@mail.ru

References

1. Balatsky, E. V. Russia in the Epicenter of Geopolitical Turbulence: Accumulation of Global Contradictions // Economic and Social Changes: Facts, Trends, Forecast. 2022. Vol. 15, No. 4. P. 42–59. (In Russ.) EDN: LOGPEF. DOI: 10.15838/esc.2022.4.82.3
2. Vykhodets, R. S. Large AI spaces and Russia's strategy in the context of the "Sanctions War" // Bulletin of the Peoples' Friendship University of Russia. Series: International Relations. 2022. Vol. 22, No. 2. P. 256–270. (In Russ.) EDN: FNYWU. DOI: 10.22363/2313-0660-2022-22-2-256-270.
3. Vykhodets, R. S., Tyumentsev, I. O. Issues of information and psychological security in the context of the Program of activities of the Parliamentary Assembly of the Collective Security Treaty Organization for 2026–2030 // Science Journal of Volgograd State University. History. Area Studies. International Relations 2025. Vol. 30, No. 3. P. 201–211. (In Russ.) EDN: YLZKPB. DOI: 10.15688/jvolsu4.2025.3.18
4. Karaganov, S. A., Lukyanov, F. A. Russia in the World of the Forces of the XXI Century // Russia and the Moslem World. 2014. No. 5 (263). P. 5–13. (In Russ.) EDN: SGGZKJ
5. Karpovich, O. G., Manoilo, A. V. Color Revolutions. Theory and Practice of Dismantling Modern Political Regimes. Moscow : Unity-Dana Publishing House. 2015. 111 p. (In Russ.). ISBN: 978-5-238-02631-2. EDN: TBWKDJ
6. Kefeli, I. F. Asphatronics: Towards a Theory of Global Security. St. Petersburg : Publishing and printing center of NWIM of RANEPa, 2020. 228 p. (In Russ.). ISBN: 978-5-89781-676-7. EDN: JSTIQP
7. The Concept of State Information Policy / ed. by of O. A. Finko. Moscow : 1999. 47 p. (In Russ.)
8. Prolegomena of Cognitive Security. Collective monograph / ed. by I. F. Kefeli. St. Petersburg: Petropolis, 2023. 488 p. ISBN: 978-5-9676-1526-9. (In Russ.) EDN: MRECBE
9. Tsvetkova, N. A. The Discourse of "Color Revolutions" // Post-Soviet Studies. 2019. Vol. 2, No. 2. P. 940–950. (In Russ.) EDN: ZAQKVF
10. Foulon, M., Meibauer, G. How Cyberspace Affects International Relations: The Promise of Structural Modifiers // Contemporary Security Policy. 2024. Vol. 45, No. 3. P. 426–458. DOI: 10.1080/13523260.2024.2365062
11. Kemp., S. Digital 2025: Global Overview Report. 05.02.2025. URL: <https://datareportal.com/reports/digital-2025-global-overview-report>
12. Mattis, J. Hoffman, F. Future Warfare: The Rise of Hybrid Wars // Proceedings Magazine. 2005. Vol. 132. Issue: November. P. 18–19. URL: <https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars>
13. Webster, F. Theories of the Information Society. 3th ed. London: Routledge. 2006. 314 p. ISBN: 978-0-415-40633-8. DOI: 10.4324/9780203962824

About the authors:

Roman S. Vykhodets, Doctor of Science (Political Sciences), Associate Professor, Professor of the Department of Theory and History of International Relations, St. Petersburg State University (Saint Petersburg, Russian Federation);
e-mail: marketing812@mail.ru; ORCID: 0000-0002-5910-9815

Anastasia V. Shcherban, PhD student, Faculty of International Relations, St. Petersburg State University (Saint Petersburg, Russian Federation);
e-mail: n.shche@mail.ru

Авторы заявляют об отсутствии конфликта интересов.

© Выходец Р. С., Щербань А. В., 2026