**Научная статья**
**https://doi.org/10.24412/2220-2404-2026-3-1**
**УДК 349**



# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СТРАТЕГИЧЕСКИЙ НАЦИОНАЛЬНЫЙ ПРИОРИТЕТ РОССИИ

**Алкесов Р.Т.**
Майкопский государственный технологический университет

***Аннотация***. *В статье на основе анализа доктринальных документов (Доктрина информационной безопасности, Стратегия национальной безопасности, Концепция внешней политики) раскрывается динамика усиления роли информационной безопасности в России. Особое внимание уделяется анализу комплекса объективных факторов и вызовов, которые обусловили отнесение информационной безопасности к стратегическим национальным приоритетам России наравне с обороноспособностью и территориальной целостностью. Информационная безопасность рассматривается как необходимое условие для технологического развития и экономического роста. Обозначены ключевые направления комплексной системы обеспечения информационной безопасности. Автором обосновывается тезис о том, что включение информационной безопасности в число стратегических приоритетов свидетельствует о понимании государством фундаментальной важности цифрового и технологического суверенитета. По мнению автора, ключевыми векторами развития информационной безопасности в России являются достижение информационного суверенитета, продвижение международно-правовых механизмов регулирования и защита общества от деструктивного информационного воздействия.*

***Ключевые слова:*** *информационная безопасность, национальная безопасность России, стратегические национальные приоритеты, технологический суверенитет, информационный суверенитет, информационные угрозы.*

***Финансирование****: инициативная работа.*

# INFORMATION SECURITY AS A STRATEGIC NATIONAL PRIORITY OF RUSSIA

**Ruslan T. Alkesov**
Maikop State Technological University

***Abstract.*** *This article, based on an analysis of doctrinal documents (the Information Security Doctrine, the National Security Strategy, and the Foreign Policy Concept), explores the dynamics of the growing role of information security in Russia. Particular attention is given to an analysis of the complex of objective factors and challenges that have led to the inclusion of information security among Russia's strategic national priorities, alongside defense capability and territorial integrity. Information security is viewed as a prerequisite for technological development and economic growth. Key areas of a comprehensive information security system are outlined. The author substantiates the thesis that the inclusion of information security among strategic priorities demonstrates the state's understanding of the fundamental importance of digital and technological sovereignty. According to the author, the key vectors for the development of information security in Russia are achieving information sovereignty, promoting international legal regulatory mechanisms, and protecting society from destructive information influences.*

***Keywords:*** *information security, national security of Russia, strategic national priorities, technological sovereignty, information sovereignty, information threats.*

***Funding****: Independent work.*

**Введение**.

В современном мире, который часто называют эпохой цифровой экономики и гибридных войн, понятие «национальная безопасность» вышло далеко за рамки традиционной защиты границ и военной мощи.

Одним из ключевых факторов суверенитета и устойчивого развития государства стала информационная безопасность. В Российской Федерации этот тезис закреплен на высшем законодательном уровне: информационная безопасность официально отнесена к числу стратегических национальных приоритетов. Это обусловлено объективными процессами цифровизации и ростом геополитической напряженности, где информационная сфера стала ареной противостояния.

Политика, направленная на обеспечение информационного суверенитета, защиту критической инфраструктуры и ограждение граждан от деструктивного влияния, является необходимой мерой для сохранения российской государственности и устойчивого развития в условиях глобальной нестабильности.

Закрепление информационной безопасности в качестве одного из стратегических национальных приоритетов России явилось закономерным решением, адекватно отражающим возрастающую угрозу современных вызовов в цифровом пространстве. Ученые солидарны в этом и подчеркивают, что «включение информационной безопасности в число стратегических национальных приоритетов Российской Федерации в базовом документе стратегического планирования в

области безопасности стало важным и своевременным шагом со стороны политического руководства России, отвечающим на возросшую опасность вызовов цифровой среды» [1, с. 227].

**Обсуждение.**

Вслед за юристами мы полагаем, что «информационная безопасность выражается в обеспечении защиты интересов личности, общества и государства от очевидных и скрытых угроз, при использовании информационного пространства и технологий» [2, с. 213].

Анализ стратегических документов последних лет позволяет проследить четкую динамику усиления роли информационной безопасности. Основополагающим документом, определяющим курс государства в этой сфере, является «Стратегия национальной безопасности Российской Федерации» (утверждена Указом Президента РФ 2 июля 2021 г.) [3]. В этом документе четко обозначены девять стратегических национальных приоритетов, среди которых отдельной строкой выделена «Защита российского общества от деструктивного информационного воздействия», что, по сути, является основным элементом информационной безопасности.

Ключевым документом, задавшим парадигму развития отрасли, является Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.), которая детализирует угрозы, цели и задачи государства в данной области. В отличие от предшествующих редакций, данная доктрина закрепила расширительное толкование понятия «информационная безопасность». Это не просто состояние защищенности данных, а состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются суверенитет, территориальная целостность и устойчивое социально-экономическое развитие [4].

Анализ текста Доктрины позволяет выделить три принципиально важных новации:

- расширение субъектного состава угроз. В качестве источников угроз рассматриваются не только хакеры или киберпреступники, но и иностранные государства, использующие информационно-коммуникационные технологии для вмешательства во внутренние дела;

- включение информационно-психологического компонента. Отдельное внимание уделяется противодействию попыткам размывания исторических основ и патриотических традиций, что сближает задачи информационной безопасности с задачами культурной и исторической политики;

- приоритет развития собственной IT-индустрии. Снижение зависимости от зарубежного программного обеспечения провозглашено не экономической, а именно стратегической национальной задачей.

Дальнейшее развитие доктринальные положения получили в Концепции внешней политики РФ 2023 г., в которой защита российского общества от деструктивного иностранного информационно-психологического воздействия выделена в качестве пятого из девяти национальных интересов во внешнеполитической сфере [5]. Важной новацией является положение о том, что враждебные действия с использованием информационно-коммуникационных технологий могут быть основанием для принятия симметричных и асимметричных ответных мер. Это юридически закрепляет понимание кибератак не просто как криминальных действий, а как угрозы суверенитету, приравнивая их к традиционным военным угрозам [5].

Именно обозначенные стратегические документы формируют понимание того, почему информационной сфере уделяется внимание наравне с обороной страны и экономическим ростом.

**Результаты.**

Отнесение информационной безопасности к стратегическим приоритетам России продиктовано комплексом объективных факторов и вызовов:

Во-первых, информационно-психологическое воздействие. Современные конфликты все чаще ведутся не только на поле боя, но и в сознании людей. Деструктивная информация, направленная на размывание традиционных российских духовно-нравственных ценностей, фальсификация истории, призывы к экстремизму и сепаратизму рассматриваются как реальная угроза конституционному строю и общественному согласию.

Во-вторых, техногенные факторы и зависимость. Критическая информационная инфраструктура (энергетика, финансы, транспорт, связь) становится мишенью для кибератак. Рост числа компьютерных атак на российские ресурсы со стороны зарубежных хакерских групп требует создания надежных систем защиты и технологической независимости.

В-третьих, информационное противоборство. В условиях геополитической напряженности Россия сталкивается с масштабными информационными кампаниями в зарубежных и глобальных СМИ, направленными на формирование негативного образа страны. Противодействие такой политике требует активной работы по донесению объективной информации до мировой аудитории.

В-четвертых, технологический суверенитет. Использование иностранного программного обеспечения и оборудования в государственных органах и стратегических отраслях создает риски шпионажа и управляемых сбоев. Переход на отечественные решения (импортозамещение) стал важнейшей задачей для обеспечения независимости страны в цифровую эпоху.

В рамках данной статьи следует также подчеркнуть, что включение задач информационной безопасности в новый национальный проект «Экономика данных и цифровая трансформация государства» [6] подтверждает, что информационная безопасность рассматривается как необходимое условие для технологического развития и экономического роста.

Исходя из своих стратегических целей, Россия выстраивает комплексную систему обеспечения информационной безопасности по нескольким ключевым направлениям:

- совершенствования законодательства: принятие законов, направленных на защиту персональных данных, регулирование деятельности иностранных интернет-платформ, создание «суверенного Рунета» – механизмов, гарантирующих работу российского сегмента сети даже в случае отключения от глобальной инфраструктуры;

- развития отечественных технологий: стимулирование производства российского программного обеспечения и других разработок;

- защиты культурного пространства: блокировка ресурсов, пропагандирующих противоправное поведение, суициды, наркотики, а также деструктивные идеологии. Воспитание у граждан навыков критического мышления;

- международного сотрудничества: продвижение на международных площадках (ООН, БРИКС, ШОС) идеи справедливого управления интернетом и выработки глобальных правил ответственного поведения государств в информационном пространстве.

**Заключение.**

В течение последнего десятилетия в Российской Федерации произошла кардинальная трансформация взглядов на природу угроз в информационной сфере. Если в начале 2000-х годов информационная безопасность воспринималась, преимущественно, как защита государственных секретов и критической инфраструктуры от технических атак, то к середине 2020-х годов она заняла место в числе высших национальных приоритетов наравне с обороноспособностью и территориальной целостностью.

Российская научная школа информационного права, представленная ведущими институтами (Институт государства и права РАН, МГЮА им. О.Е. Кутафина) внесла значительный вклад в теоретическое обоснование включения информационной безопасности в число стратегических приоритетов [7]. Ключевым концептом здесь выступает **информационный суверенитет, под которым понимается** «способность страны самостоятельно формировать информационную политику и возможность обеспечивать безопасность в информационной сфере независимо от внешнего влияния» [8, с. 89].

Несмотря на принимаемые меры, реализация анализируемого приоритета сопряжена с рядом сложностей. Скорость развития технологий часто опережает возможности регулирования. Кроме того, поиск баланса между обеспечением безопасности и соблюдением конституционных прав граждан на свободу слова и доступ к информации остается сложной задачей.

Тем не менее, факт включения информационной безопасности в число стратегических приоритетов свидетельствует о понимании государством фундаментальной важности цифрового и технологического суверенитета.

В XXI веке способность защитить свое информационное поле и обеспечить безопасность критической инфраструктуры становится таким же условием выживания и развития нации, как и наличие современной армии. Россия, провозглашая этот приоритет, встраивается в общемировой тренд, одновременно предлагая собственное видение того, как должно быть устроено безопасное цифровое будущее.

Таким образом, информационная безопасность в российской стратегической политике окончательно оформилась как компонент национальной безопасности и стратегический национальный приоритет. Она объединяет:

- оборону (стратегическое сдерживание в киберпространстве);

- политику (борьба с иностранным вмешательством);

- экономику (технологический суверенитет);

- социальную сферу (защита от деструктивного контента).

В условиях, когда информация превратилась в стратегический ресурс, обеспечение информационной безопасности перестало быть исключительно задачей технических специалистов. Сегодня это – неотъемлемая часть системы национальной безопасности, влияющая на обороноспособность, экономический суверенитет и социальную стабильность государства.

Включение информационной безопасности в число стратегических приоритетов России является результатом осознания фундаментальных сдвигов в природе современного геополитического противостояния. Сегодня этот приоритет закреплен на высшем доктринальном уровне и обеспечен системной научно-правовой базой.

Ключевыми векторами развития информационной безопасности являются достижение информационного суверенитета, продвижение международно-правовых механизмов регулирования и защита общества от деструктивного информационного воздействия. Более того, в условиях реализации национального проекта «Экономика данных и цифровая трансформация государства» информационная безопасность перестает быть исключительно защитной функцией и становится фактором развития, обеспечивающим устойчивость цифровой инфраструктуры и доверие к цифровой экономике.

**Конфликт интересов**

Не указан.

**Рецензия**

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

**Conflict of Interest**

None declared.

**Review**

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

***Список источников:***

*1. Смирнов А.А. Четвертый приоритет: правовое закрепление задач обеспечения информационной безопасности в новой стратегии национальной безопасности Российской Федерации // Вестник Воронежского государственного университета. Серия: Право. 2021. № 3 (46). С. 222-228. DOI: 10.17308/vsu.proc.law.2021.3/3552 EDN: TYRBSC*

*2. Шишкина Е.В., Шобонов С.А. Особенности соотношения информационной безопасности и остальных стратегических национальных приоритетов Российской Федерации // Вестник экономической безопасности. 2022. № 2. С. 210-214. DOI: 10.24412/2414-3995-2022-2-210-214 EDN: QRJVQK*

*3. Указ Президента РФ от 02.07.2021 г. № 400 "О Стратегии национальной безопасности Российской Федерации". URL: http://www.kremlin.ru/acts/bank/47046?ysclid=mm0n0kfnih167576854 (дата обращения 12.02.2026).*

*4. Указ Президента Российской Федерации от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". URL: http://www.kremlin.ru/acts/bank/41460?ysclid=mm0mxz2cbw781766917 (дата обращения 12.02.2026).*

*5. Указ Президента Российской Федерации от 31.03.2023 г. № 229 "Об утверждении Концепции внешней политики Российской Федерации". URL: http://www.kremlin.ru/ (дата обращения 12.02.2026).*

*6. Национальный проект "Экономика данных и цифровая трансформация государства". URL: http://government.ru/rugovclassifier/923/about/ (дата обращения 12.02.2026).*

*7. Полякова Т.А., Минбалеев А.В., Наумов В.Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. 2025. № 1. С. 160-173. DOI: 10.31857/S1026945225010148 EDN: HKYGVI*

*8. Холодная Е.В. Об информационном суверенитете // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С.85-90. DOI: 10.17803/2311-5998.2024.122.10.085-090 EDN: EAXHXM*

***Reference:***

*1. Smirnov A.A. The fourth priority: the legal consolidation of the tasks of ensuring information security in the new national security strategy of the Russian Federation // Bulletin of Voronezh State University. Series: Law. 2021. No. 3 (46). pp. 222-228. DOI: 10.17308/vsu.proc.law.2021.3/3552 EDN: TYRBSC*

*2. Shishkina E.V., Shobonov S.A. Features of the correlation of information security and other strategic national priorities of the Russian Federation // Bulletin of Economic Security. 2022. No. 2. PP. 210-214. DOI: 10.24412/2414-3995-2022-2-210-214 EDN: QRJVQK*

*3. Decree of the President of the Russian Federation dated 07/02/2021 No. 400 "On the National Security Strategy of the Russian Federation". URL: http://www.kremlin.ru/acts/bank/47046?ysclid=mm0n0kfnih167576854 (accessed 12.02.2026).*

*4. Decree of the President of the Russian Federation dated 05.12.2016 No. 646 "On Approval of the Information Security Doctrine of the Russian Federation". URL: http://www.kremlin.ru/acts/bank/41460?ysclid=mm0mxz2cbw781766917 (accessed 12.02.2026).*

*5. Decree of the President of the Russian Federation dated 03/31/2023 No. 229 "On Approval of the Concept of Foreign Policy of the Russian Federation". URL: http://www.kremlin.ru / (accessed 12.02.2026).*

*6. National project "Data Economics and Digital Transformation of the State". URL: http://government.ru/rugovclassifier/923/about / (accessed 12.02.2026).*

*7. Polyakova T.A., Minbaleev A.V., Naumov V.B. Modern priorities for the development of information law: legal support for state sovereignty and information security in the information space of Russia // State and Law. 2025. No. 1. PP. 160-173. DOI: 10.31857/S1026945225010148 EDN: HKYGVI*

*8. Kholodnaya E.V. On information sovereignty // Bulletin of the O.E. Kutafin University (MGUA). 2024. No. 10. pp.85-90. DOI: 10.17803/2311-5998.2024.122.10.085-090 EDN: EAXHXM*

**Информация об авторе:**
**Алкесов Руслан Темботович**, кандидат социологических наук, старший преподаватель кафедры административного и уголовного права, ФБГОУ ВО «Майкопский государственный технологический университет», ruslan059305@mail.ru
**Ruslan T. Alkesov,** Candidate of Sociological Sciences, Senior Lecturer, Department of Administrative and Criminal Law, Maikop State Technological University

Статья поступила в редакцию / The article was submitted 25.02.2026;
Одобрена после рецензирования / Approved after reviewing 13.03.2026;
Принята к публикации / Accepted for publication 20.03.2026.
Автором окончательный вариант рукописи одобрен.