

Когнитивные науки в информационном обществе / Cognitive Sciences in the Information Society <https://knio.ru/>

2025, Том 5, № 2 / 2025, Vol. 5, Iss. 2 <https://knio.ru/issue-2-2025.html>

URL статьи: <https://knio.ru/PDF/06KN225.pdf>

2.3.8. Информатика и информационные процессы

**Ссылка для цитирования этой статьи:**

Матиашвили, Г. Н. Гибридные угрозы как внешняя угроза национальной безопасности России: политико-правовые аспекты / Г. Н. Матиашвили // Когнитивные науки в информационном обществе. — 2025. — Том 5. — № 2. — URL: <https://knio.ru/PDF/06KN225.pdf>.

**For citation:**

Matiashvili G.N. Hybrid threats as an external threat to Russia's national security: political and legal aspects. *Cognitive Sciences in the Information Society*. 2025;5(2): 06KN225. Available at: <https://knio.ru/PDF/06KN225.pdf>. (In Russ., abstract in Eng.).

**Матиашвили Георгий Нугзарович**

ФГБОУ ВО «Московский государственный лингвистический университет», Москва, Россия

E-mail: [geo.matiashvili@gmail.com](mailto:geo.matiashvili@gmail.com)

## **Гибридные угрозы как внешняя угроза национальной безопасности России: политико-правовые аспекты**

**Аннотация.** Современные межгосударственные отношения характеризуются существенными противоречиями в вопросах реализации суверенных прав внутри цифрового пространства. Уникальная природа виртуальной среды, характеризующаяся отсутствием физических барьеров и осязаемых элементов, обуславливает необходимость кардинального переосмысления существующих механизмов определения государственной юрисдикции. При этом, концептуальные различия между западным и российским пониманием государственного суверенитета проявляются через призму регулирования информационного пространства. Законодательный механизм Российской Федерации определяет юрисдикцию над информационной инфраструктурой строго по территориальному признаку. Нормативная система страны устанавливает правовой режим для всех технических компонентов обработки информации в пределах государственных границ. Правовое регулирование фокусируется исключительно на материальных объектах информационной среды внутри России, оставляя за рамками вопросы управления ресурсами на внешней инфраструктуре.

Анализ гибридных угроз в Интернете подчеркивает негативное влияние процессов глобализации на национальные культуры и экономику стран. Современные информационные технологии используются для манипуляции массовым сознанием, способствуя разрушению традиционных ценностей и формированию потребительского мировоззрения. Особую опасность представляют социальные сети, провоцируя агрессию среди молодежи и увеличивая случаи кибербуллинга. Исследования показывают, что представители восточноазиатских культур менее склонны к агрессивному поведению благодаря коллективистской ориентации и моральному воспитанию. В то же время такие страны как Россия или Китай предпринимают в отношении ЕС и других стран активные меры по защите своего информационного пространства, осознавая важность киберзащиты для сохранения суверенитета и национальной безопасности.

**Ключевые слова:** национальная безопасность; внешние угрозы национальной безопасности; гибридные угрозы; киберугрозы; кибербезопасность; критическая инфраструктура

Стратегический характер кибернетических средств воздействия приобретает особую значимость при обеспечении защищенности ключевых инфраструктурных объектов государства, становясь механизмом сдерживания наравне с ядерным арсеналом. Мировое сообщество стремится криминализировать целенаправленные кибератаки на значимые объекты инфраструктуры, несмотря на отсутствие сформированной нормативно-правовой базы цифрового взаимодействия между странами. Существующие международные правовые нормы демонстрируют недостаточную адаптивность к современным вызовам информационной безопасности.

Фундаментальные разногласия между ведущими технологическими державами, где доминирующую роль занимают Соединенные Штаты Америки, определяют политическую составляющую цифрового пространства. Западные эксперты подчеркивают многогранность проблематики через призму военно-стратегических, экономических, дипломатических и социальных компонентов международного взаимодействия [1].

Согласно февральскому докладу 2023 года, аналитические материалы Европейской внешнеполитической службы (ЕВС) демонстрируют масштабные угрозы информационного вмешательства со стороны двух государств — Российской Федерации и Китайской Народной Республики. Документ характеризует деятельность КНР как комплексную систему воздействия, охватывающую широкий спектр методов: от легальных инструментов публичной дипломатии до нелегитимных практик давления на критически настроенных лиц. Европейские эксперты подчеркивают синергетический эффект китайских манипулятивных стратегий, сочетающих информационное влияние с экономическим принуждением. Представленные в отчете данные мониторинга свидетельствуют о сохранении за КНР статуса источника гибридных угроз для европейского пространства.<sup>1</sup>

Политизация экономического взаимодействия между странами становится ключевым элементом внешней политики в том числе и Европейского союза при его противостоянии зарубежному влиянию. Рыночная конкуренция закономерно порождает столкновение бизнес-интересов различных участников международной торговли. Дискурс о гибридных угрозах переводит экономическое соперничество в сферу политических решений на высшем государственном уровне, что негативно сказывается на социальной стабильности и материальном положении граждан. Вытеснение компаний из России и Китая с европейских рынков под лозунгами борьбы с гибридными угрозами способствует укреплению позиций американского и местного бизнеса, одновременно поддерживая политические амбиции проатлантических элит [2]. Ограничение международного сотрудничества существенно снижает потенциал стратегической автономии европейских союзников США. Прибалтийский регион рассматривается атлантическими группами влияния как ключевая зона российского гибридного воздействия, связанного с энергетической зависимостью этих стран от поставок из России [3].

Современные межгосударственные отношения характеризуются существенными противоречиями в вопросах реализации суверенных прав внутри цифрового пространства. Уникальная природа виртуальной среды, характеризующаяся отсутствием физических барьеров и осязаемых элементов, обуславливает необходимость кардинального переосмысления существующих механизмов определения государственной юрисдикции. Так, научные разработки британских специалистов Цагуриаса и Бучана представляют альтернативную

---

<sup>1</sup> 1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence. 02.2023. URL: <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf> (дата обращения: 25.08.2025).

модель экстерриториального правоприменения в киберпространстве, преодолевающую ограничения традиционной территориальной парадигмы [4].

При этом, концептуальные различия между западным и российским пониманием государственного суверенитета проявляются через призму регулирования информационного пространства. Законодательный механизм Российской Федерации определяет юрисдикцию над информационной инфраструктурой строго по территориальному признаку. Нормативная система страны устанавливает правовой режим для всех технических компонентов обработки информации в пределах государственных границ. Правовое регулирование фокусируется исключительно на материальных объектах информационной среды внутри России, оставляя за рамками вопросы управления ресурсами на внешней инфраструктуре [5].

Локальное размещение информационно-технологических компонентов российской цифровой инфраструктуры формирует базовый элемент защиты национального киберпространства. Географическая концентрация вычислительных мощностей и сетевых узлов внутри российских границ обеспечивает комплексный контроль над цифровыми процессами. Многоуровневая система мониторинга виртуального пространства существенно снижает риски кибератак, предупреждая различные формы злонамеренной активности — от хакерских вторжений до межгосударственного противоборства в цифровой среде [6].

Существующая архитектура глобальной системы доменных имен отражает существенный территориальный дисбаланс распределения корневых серверов DNS между регионами мира [7], при котором американские информационные центры, включающие десять ключевых узлов, доминируют над европейскими и азиатскими локациями [8]. Создание национальных серверных кластеров разными странами не устраняет зависимость мировых информационных потоков от центрального маршрутизационного комплекса, расположенного на территории Соединенных Штатов Америки [9].

Геополитический дисбаланс цифрового суверенитета между Россией и западными державами обнажает фундаментальные противоречия современного информационного пространства. Локализация российской цифровой инфраструктуры в пределах государственных границ создает существенные ограничения для реализации национальных интересов на международной арене. Масштабное присутствие американских и европейских серверных мощностей определяет характер глобального информационного взаимодействия. Опыт функционирования платежной системы МИР наглядно продемонстрировал недостатки текущей архитектуры — зависимость от иностранных процессинговых центров существенно ограничила возможности противодействия санкционному давлению [10].

Разведывательная деятельность иностранных держав, активно использующих передовые информационные технологии, представляет серьезную угрозу безопасности Российской Федерации [11], что подтверждается Доктриной информационной безопасности 2016 года. Масштабное внедрение цифровых систем наблюдения и контроля создает дополнительные вызовы для сохранения политической стабильности, территориальной целостности и суверенных прав государства. Комплексный характер современных разведывательных операций требует принятия превентивных мер по защите национальных интересов страны в информационном пространстве.<sup>2</sup>

Многообразие подходов к защите значимых государственных объектов обусловлено различными трактовками критической инфраструктуры в мировой практике. Концептуальное видение США характеризует данную систему как совокупность физических и цифровых

<sup>2</sup> Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 06.12.2016.

активов стратегического значения, повреждение которых может нанести существенный урон обороноспособности, экономике и социальной стабильности государства. Американская модель критической инфраструктуры охватывает шестнадцать стратегических секторов, от химической промышленности и энергетики до транспортных сетей и государственного управления.

Европейская концепция рассматривает критическую инфраструктуру как комплекс жизненно важных объектов, расположенных в странах-участницах ЕС, обеспечивающих базовые потребности общества. Нарушение работоспособности данных систем несет прямую угрозу социальному благополучию, здравоохранению, оборонному потенциалу и экономической устойчивости государств европейского сообщества. Модель критической инфраструктуры Евросоюза включает девять приоритетных направлений, охватывающих энергетику, транспорт, водоснабжение, здравоохранение, телекоммуникации, финансовый сектор, государственное управление, сельское хозяйство, медиа-пространство и культурное достояние [12].

Нормативно-правовое регулирование защиты стратегических информационных ресурсов Российской Федерации претерпело значительную модернизацию с момента принятия основополагающих документов. Утверждённая Доктрина информационной безопасности 2016 года определила концептуальные принципы охраны государственных цифровых активов. Законодательный акт о защите критической информационной инфраструктуры 2017 года закрепил юридические механизмы и понятийный аппарат для обеспечения сохранности ключевых информационных объектов.<sup>3</sup> Президентский указ того же года модернизировал государственную систему противодействия цифровым угрозам, внедрив протоколы экстренного реагирования на масштабные кибератаки.

Российское законодательство создало многоуровневую систему координации действий государственных структур при выявлении, блокировании и устранении последствий информационных атак. Нормативные акты сформировали актуальный терминологический базис, охватывающий сферу информационной безопасности, критически важных объектов и компьютерных инцидентов. Законодательные меры фокусируются на защите стратегических элементов инфраструктуры, образующих отдельную категорию охраняемых государством объектов. Основной вектор правового регулирования направлен на укрепление защищенности национальной информационной инфраструктуры.

Комплексная структура критической информационной инфраструктуры, согласно федеральному законодательству, представляет собой многоуровневую систему взаимодействующих элементов, охватывающую автоматизированные комплексы управления, телекоммуникационные сети и специальные каналы связи, обеспечивающие непрерывное функционирование стратегических объектов государственного значения.

Законодательный аппарат РФ не включает формального определения понятия «критическая инфраструктура». Федеральное законодательство о защите населения при чрезвычайных ситуациях природного и техногенного характера выделяет две взаимосвязанные категории объектов. Критически важные объекты характеризуются потенциальным риском дестабилизации экономических процессов на различных административных уровнях, возможностью возникновения необратимых последствий или существенного снижения безопасности граждан. Потенциально опасные объекты определяются как архитектурно-

---

<sup>3</sup> Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации <http://pravo.gov.ru>, 26.07.2017.

инженерные комплексы повышенной ответственности с возможной единовременной концентрацией свыше пяти тысяч человек.<sup>4</sup>

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» устанавливает ключевые сферы экономики, требующие повышенных мер защиты. Статья 2 данного нормативного акта включает стратегически значимые отрасли: медицинскую сферу, научно-исследовательский сектор, транспортную систему, телекоммуникации, энергообеспечение, финансово-кредитную отрасль. Особое внимание уделяется промышленным комплексам: нефтегазовому, атомному, оборонному, аэрокосмическому, добывающему, металлургическому, химическому производству.

Комплексный анализ международных практик и передовых технологических разработок служит основой для совершенствования нормативно-правовой базы по защите стратегических объектов инфраструктуры. Формирование автономных информационных систем совместно с развитием конкурентных отечественных разработок определяет уровень национальной кибербезопасности. Технологическая зависимость российского производственного сектора от зарубежных программных решений существенно сдерживает экономический рост и создает уязвимости перед внешнеполитическим давлением.

Результативная цифровая защита национальных интересов достигается путем стратегического партнерства государств через реализацию согласованных программ развития. Расширение механизмов информационного взаимодействия между участниками СНГ и ЕАЭС обеспечивает надежную защиту от актуальных вызовов цифровой безопасности.

Таким образом, комплексное исследование киберпространства выявляет деструктивные последствия глобализационных процессов для самобытности национальных культур и экономического развития стран третьего мира. Манипулятивные технологии массовой коммуникации способствуют размыванию традиционных ценностных ориентиров общества, насаждая философию потребления. Платформы социальных медиа становятся катализатором агрессивных проявлений среди подростков, многократно усиливая масштабы сетевой травли. Многолетние наблюдения демонстрируют меньшую склонность представителей восточноазиатских обществ к деструктивному поведению благодаря укорененности коллективистских установок. Отдельные страны, к примеру, Россия и КНР, реализуют комплексные программы защиты национального информационного суверенитета от внешнего вмешательства, признавая стратегическую значимость кибербезопасности для сохранения государственности.

## ЛИТЕРАТУРА

1. Вильданов М., Башкиров Н. Международно-правовые аспекты защиты инфраструктуры государств от киберугроз // Зарубежное военное обозрение. 2019. № 7. С. 3–10 // [http://factmilcom/publ/soderzhanie/informacionnye\\_vojny/mezhdunarodno\\_pravovye\\_aspekty\\_zashhity\\_infrastruktury\\_gosudarstv\\_ot\\_kiberugroz\\_2019/107-1-0-1659](http://factmilcom/publ/soderzhanie/informacionnye_vojny/mezhdunarodno_pravovye_aspekty_zashhity_infrastruktury_gosudarstv_ot_kiberugroz_2019/107-1-0-1659) (дата обращения 15.08.2025).
2. Данилов Д.А. Глобальные горизонты атлантического альянса: "вакцина" Байдена // Современная Европа. 2021. № 5. С. 19–31 // 10.15211/soveurope520211931 (дата обращения: 26.08.2025). DOI: 10.15211/soveurope520211931 (EDN: DGNGXP).

<sup>4</sup> Федеральный закон от 21.12.1994 № 68-ФЗ (ред. от 08.08.2024) «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (с изм. и доп., вступ. в силу с 26.11.2024) // Российская газета. № 250. 24.12.1994.

3. Смирнов П.Е. Эволюция политических приоритетов США в регионе Балтийского моря во втором десятилетии XXI века // Балтийский регион. 2020. Т. 12. № 3. С. 4–25 // 10.5922/2079-8555-2020-3-1 (дата обращения: 26.08.2025). DOI: 10.5922/2079-8555-2020-3-1 (EDN: IXULIM).
4. Tsagourias N., Buchan R. (eds.). Research Handbook on International Law and Cyberspace. Sheffield: Edward Elgar Publishing, 2015. 342 p.
5. Терентьева Л.В. Территориальный аспект юрисдикции и суверенитета государства в киберпространстве // LEX RUSSICA (РУССКИЙ ЗАКОН). 2022. № 4(149). С. 139–150 // <https://cyberleninka.ru/article/n/territorialnyy-aspekt-yurisdiksii-i-suvereniteta-gosudarstva-v-kiberprostranstve/viewer> (дата обращения: 15.08.2025).
6. Joubert V. Getting the Essence of Cyberspace: A Theoretical Framework to Face Cyber // Conference on Cyber Conflict Proceedings, Tallinn. 2010. 845 p.
7. Базаркина Д.Ю. Практика противодействия гибридным угрозам: опыт Европейского союза и его государств-членов // Современная Европа. 2022. № 2. С. 145–158. DOI: 10.31857/S020170832202011 EDN: NBQEZR.
8. Разумов Е.А. Киберсуверенитет как аспект системы национальной безопасности КНР // Россия и Китай: история и перспективы сотрудничества. Материалы VII международной научно-практической конференции. 2023. С. 707–710 // <https://elibrary.ru/item.asp?id=29191372> (дата обращения: 14.08.2025).
9. Башкиров Н. Обеспечение кибербезопасности электроэнергетической системы США // Зарубежное военное обозрение. 2022. № 3. С. 3–9. URL: [http://pentagonus.ru/publ/obespechenie\\_kiberbezopasnosti\\_ehlektroehnergetcheskoj\\_s\\_istemy\\_ssha\\_2022/19-1-0-2889](http://pentagonus.ru/publ/obespechenie_kiberbezopasnosti_ehlektroehnergetcheskoj_s_istemy_ssha_2022/19-1-0-2889) (дата обращения: 20.06.2025).
10. Катасонов В.Ю. «Китайский синдром» Путина. Прорыв или утопия? М.: Алгоритм, 2019. 465 с.
11. Калашников А.О., Сакрутина Е.А. Прогнозирование рискового потенциала объектов критической инфраструктуры атомных электростанций // Управление развитием крупномасштабных систем. М.: Институт проблем управления имени В.А. Трапезникова РАН. 2023. С. 245–247 // <https://elibrary.ru/item.asp?id=36620660> (дата обращения: 20.06.2025).
12. Михалевич И.Ф. Критические информационные инфраструктуры в контексте общей безопасности // Технологии информационного общества. М.: Медиа Паблишер, 2019. С. 370–372.

**Matiashvili Georgy Nugzarovich**

Moscow State Linguistic University, Moscow, Russia  
E-mail: [geo.matiashvili@gmail.com](mailto:geo.matiashvili@gmail.com)

## **Hybrid threats as an external threat to Russia's national security: political and legal aspects**

**Abstract.** Modern interstate relations are characterized by significant contradictions in the implementation of sovereign rights within the digital space. The unique nature of the virtual environment, characterized by the absence of physical barriers and tangible elements, necessitates a fundamental rethink of the existing mechanisms for determining state jurisdiction. At the same time, the conceptual differences between the Western and Russian understanding of state sovereignty are manifested through the prism of information space regulation. The legislative mechanism of the Russian Federation defines jurisdiction over the information infrastructure strictly on a territorial basis. The country's regulatory system establishes a legal regime for all technical components of information processing within state borders. Legal regulation focuses exclusively on the material objects of the information environment inside Russia, leaving out the issues of resource management on the external infrastructure.

The analysis of hybrid threats on the Internet highlights the negative impact of globalization processes on national cultures and economies. Modern information technologies are used to manipulate mass consciousness, contributing to the destruction of traditional values and the formation of a consumer worldview. Social networks are particularly dangerous, provoking aggression among young people and increasing cases of cyberbullying. Research shows that representatives of East Asian cultures are less prone to aggressive behavior due to their collectivist orientation and moral education. At the same time, countries such as Russia or China are taking active measures against the EU and other countries to protect their information space, realizing the importance of cyber defense to preserve sovereignty and national security.

**Keywords:** national security; external threats to national security; hybrid threats; cyber threats; cybersecurity; critical infrastructure