На правах рукописи

НИКИТИН Никита Алексеевич

СОВРЕМЕННАЯ СТРАТЕГИЯ НАТО В КИБЕРПРОСТРАНСТВЕ

Специальность 5.5.4. Международные отношения, глобальные
и региональные исследования

Автореферат
диссертации на соискание ученой степени
кандидата политических наук

Москва – 2025

Работа выполнена на кафедре прикладного анализа международных проблем Федерального государственного бюджетного образовательного учреждения высшего образования «Дипломатическая академия Министерства иностранных дел России».

Научный руководитель:	**Иванов Олег Петрович** Доктор политических наук, профессор, заведующий кафедрой прикладного анализа международных проблем Дипломатической академии МИД России
Официальные оппоненты:	**Синдеев Алексей Александрович** Доктор исторических наук, профессор РАН, главный научный сотрудник Отдела европейской безопасности Федерального государственного бюджетного учреждения науки «Институт Европы Российской академии наук» **Надточей Юрий Иванович** Кандидат исторических наук, старший научный сотрудник Отдела Европы и Америки Федерального государственного бюджетного учреждения науки «Институт научной информации по общественным наукам Российской академии наук»
Ведущая организация	Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»

Защита состоится «___» _____ 202__ г. в _____ часов на заседании Диссертационного совета 05.2.001.01 в ФГБОУ ВО «Дипломатическая академия Министерства иностранных дел Российской Федерации» по адресу: 119021, г. Москва, ул. Остоженка, д. 53/2, стр. 1. С текстом диссертации можно ознакомиться в библиотеке ФГБОУ ВО «Дипломатическая академия Министерства иностранных дел Российской Федерации» по адресу: 119021, г. Москва, ул. Остоженка, д. 53/2, стр. 1 и на официальном сайте http://www.dipacademy.ru

Автореферат разослан «___» _____ 2025 г.

Ученый секретарь Диссертационного совета,
кандидат политических наук, доцент **А.Ш. Ногмова**

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

За последнее десятилетие крайне актуализировались проблемы обеспечения глобальной кибербезопасности. Геополитическое соперничество государств следует тенденции усиления противоборства в киберпространстве, включающего в себя информационно-коммуникационную сеть Интернет, ставшую наиболее популярным и всеобъемлющим источником информации и средством коммуникации. Концепции кибервойн прочно интегрировались в дискурс современного политического и общественного сознания.

В современной системе международных отношений НАТО, будучи военно-политическим блоком, включающим в себя 32 государства, является частью системы европейской и глобальной безопасности и одним из наиболее значимых международных институтов во всём мире, продолжает играть роль ключевого гаранта коллективной безопасности своих государств-членов, однако стратегическая парадигма и функциональное предназначение организации претерпели существенную трансформацию. После окончания Холодной войны Североатлантический альянс столкнулся с необходимостью легитимации своего существования в отсутствие советской угрозы, что привело к периоду экспансии на Восток к границам России и участию в операциях по кризисному регулированию за пределами собственной территории. Представляется возможным констатировать, что на современном этапе доминирующим вектором деятельности НАТО вновь становится сдерживание и оборона, что напрямую обусловлено возрождением глобального стратегического противоборства с Российской Федерацией. На современном этапе киберпространство стало ключевой сферой геополитической конкуренции, что подтверждает необходимость адаптации стратегий международных организаций к новым вызовам и угрозам. Сегодня целью коллективного Запада является нанесение стратегического поражения России без военного столкновения[1]. Киберпространство трансформируется в

[1] Истомин И.А. аналитическая записка Военно-политическая трансформация НАТО в контексте противоборства России и Запада. МГИМО 2024 г.

инструмент стратегического сдерживания и принуждения, где достижение политических или экономических целей осуществляется через паралич ключевых функций государства и подрыв доверия к его институтам, что по своим последствиям может быть сопоставимо с военным поражением. Будучи ведущим военно-политическим блоком, Североатлантический альянс активно трансформирует свою политику в киберпространстве, стремясь не только обеспечить коллективную кибербезопасность и противодействовать угрозам гибридного характера, но и проводить наступательные кибероперации. В условиях роста кибератак на критическую инфраструктуру и использования информационно-коммуникационных технологий в качестве инструмента политического и военного давления, Североатлантический альянс пересматривает доктринальные подходы, усиливает координацию между странами-членами и развивает собственный наступательный потенциал с использованием кибертехнологий.

Актуальность темы исследования обуславливается необходимостью изучения современной стратегии НАТО в киберпространстве в условиях постоянно трансформирующейся международной обстановки и структуры глобальной безопасности. Исследование данной проблематики позволяет дать объективную оценку современных приоритетов Североатлантического альянса в киберпространстве и идентифицировать основные тенденции стремительно развивающейся политики обеспечения кибербезопасности.

Объект исследования – киберпространство в качестве одной из ключевых сфер деятельности НАТО на современном этапе. **Предмет исследования** – политика НАТО в киберпространстве.

Источниковую базу исследования составляют официальные документы на русском и английском языках, которые можно разделить на три группы:

– Первая группа представлена ключевыми доктринальными документами Североатлантического альянса: Стратегическими концепциями НАТО 1991, 1999, 2010, 2022 гг., заявлениями по итогам встреч на высшем уровне

с 1999 по 2025 гг., Североатлантическим договором 1949 г., Декларацией Вашингтонского саммита НАТО 2024 г., Декларацией Гаагского саммита НАТО 2025 г.

- Вторая группа представлена отечественными и зарубежными концептуальными, доктринальными и законодательными источниками, такими как Проект Концепции стратегии кибербезопасности Российской Федерации[2], Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[3], Руководящие принципы оборонной политики ФРГ 2023 г.[4], Стратегия национальной безопасности Российской Федерации, утверждённая указом президента Российской Федерации от 2 июля 2021 года № 400[5], Стратегия кибербезопасности Великобритании на 2022-2030 годы[6], Национальная стратегия кибербезопасности США 2023 г.[7], бюджет Правительства США за 2023 фискальный год[8], План единой сети армии США, позволяющий проводить многодоменные операции[9], План реализации национальной стратегии кибербезопасности США 2023 г.[10], План реализации национальной стратегии кибербезопасности США 2024 г[11].
- Третья группа источников включает зарубежные аналитические материалы, посвящённые рассматриваемым в исследовании проблемам: аналитический доклад «10 лет мерам ОБСЕ по укреплению доверия в

---

[2] Проект Концепции стратегии кибербезопасности Российской Федерации URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf: (дата обращения: 01.08.2024).
[3] Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. - 2016. - № 50.- Ст. 7074.
[4] BMVg. (2023). German Cyber Security Strategy.
[5] Стратегия национальной безопасности Российской Федерации, утверждённая указом президента Российской Федерации от 2 июля 2021 года № 400
[6] UK Government. (2022). National Cyber Strategy 2022–2030.
[7] US National Cybersecurity Strategy 2023.
[8] White House. (2023). Budget of the U.S. Government.
[9] Unified Network Plan - U.S. Army URL: https:// api.army.mil/e2/c/downloads/2021/10/07/ d43180cc/army-unified-network-plan-2021. pdf (date of access: 18.02.2025).
[10] White House. (2023). National cybersecurity strategy implementation plan
[11] White House. (2024). National cybersecurity strategy implementation plan

области кибербезопасности и ИКТ»[12], аналитический доклад Киберугрозы и НАТО-2030: обзор и анализ[13], аналитический отчёт Медиация и искусственный интеллект: заметки о будущем разрешения международных конфликтов[14].

В основе исследования лежит анализ данных, полученных из открытых источников.

Степень разработанности проблемы:

Совокупность исследований, относящихся к проблематике современной стратегии Североатлантического альянса в киберпространстве, достаточно обширна и состоит из большого количества работ как отечественных, так и зарубежных авторов, статей, монографий и диссертаций. Значительное влияние на анализ изучаемой проблемы оказали разноплановые общетеоретические и практические исследования по международным отношениям и внешней политике, проведённые учёными Дипломатической академии МИД России. Весомый вклад в исследование эволюции стратегии НАТО в контексте международной безопасности также внесли и вносят МГИМО(У) МИД России, институты системы РАН.

Исследование опирается на выступления и заявления российских, официальных лиц. Среди них можно выделить заявления В.В. Путина[1516], М.В. Мишустина[17], С.В. Лаврова[18].

---

[12] 10 years of OSCE Cyber/ICT Security Confidence-Bulding Measures https://www.osce.org/files/f/documents/f/7/555999_1.pdf (accessed: 23.02.2025).

[13] Cyber Threats and NATO 2030: Horizon Scanning and Analysis URL: http://kclpure.kcl.ac.uk/portal/fi les/142284634/Cyber_Threats_ and_NATO_2030_Horizon_Scanning_and_ Analysis.pdf (accessed: 16.02.2025).

[14] Höne 2019 – Höne K.E. Mediation and Artificial Intelligence: Notes on the Future of International Conflict Resolution. Geneva: Diplofoundation, 2019. 24 p.

[15] Путин назвал кибербезопасность одной из важнейших тем современности URL: https://tass.ru/politika/11637535 (дата обращения: 23.11.2024).

[16] Конференция «Путешествие в мир искусственного интеллекта» URL: http://kremlin.ru/events/president/news/72811 (дата обращения: 01.08.2024).

[17] Мишустин назвал пять составляющих цифровой архитектуры будущего URL: https://ria.ru/20250131/mishustin-1996581876.html (дата обращения: 01.08.2024).

[18] Лавров: США препятствуют в ООН разработке правил поведения в киберпространстве URL: https://tass.ru/politika/5413659/amp (дата обращения: 01.08.2024).

Литературу по теме исследования можно условно разделить на несколько блоков. К первому блоку относятся работы, посвящённые эволюции стратегии Североатлантического альянса на современном этапе. Среди них коллективные монографии учёных ДА МИД России: «Россия и современный мир»[19], «Мировая политика в фокусе современности»[20], «XXI век: Перекрестки мировой политики»[21], «Современный мир и геополитика»[22], «Новая эпоха международной безопасности»[23], «Международная политика и безопасность: новые контуры современного мира»[24], посвященные актуальным проблемам в современной системе международных отношений и внешней политике, исследования отечественного экспертного сообщества: Д.Ю. Базаркиной[2526], В.Г. Барановского[27], А.А Бартоша[28], И.В. Болговой[29],

[19]Россия и современный мир: монография / Аникин В. И. [и др.]. Под ред. М. А. Неймарка. М.: «Канон+» РООИ «Реабилитация», Дипломатическая академия МИД России, 2016. 510 с.

[20] Мировая политика в фокусе современности: монография / В.И. Аникин [и др.]. Под ред. М.А. Неймарка. М.: «Дашков и К°», Дипломатическая академия МИД России, 2019. 516 с.

[21] XXI век: Перекрестки мировой политики / Отв. ред. М.А. Неймарк. – М.: «Канон+» РООИ «Реабилитация», 2014. – 424 с.

[22] Современный мир и геополитика / Отв. ред. М.А. Неймарк. – Москва: Издательство «Канон+» РООИ «Реабилитация», 2015. – 448 с.

[23] Новая эпоха международной безопасности. Россия и мир: монография / отв. ред. О.П. Иванов. – Москва: Проспект, 2020. – 416 с.

[24] Международная политика и безопасность: новые контуры современного мира: монография/ под науч. ред. О.П. Иванова; Дипломатическая академия МИД России. – Москва: Квант Медиа, 2021. -624 с.

[25] Базаркина, Д. Ю. Практика противодействия гибридным угрозам: опыт Европейского союза и его государств-членов / Д. Ю. Базаркина // Современная Европа. – 2022. – № 2(109). – С. 132-145. – DOI 10.31857/S0201708322020103. – EDN NBQEZR.

[26] Базаркина, Д. Ю. Регулирование рисков, связанных со злонамеренным использованием искусственного интеллекта в США, ЕС и Китае / Д. Ю. Базаркина, Е. Н. Пашенцев, Е. А. Михалевич // Современная Европа. – 2024. – № 6(127). – С. 156-167. – DOI 10.31857/S0201708324060147. – EDN EWWVII.

[27] Барановский В.Г. Новый миропорядок: преодоление старого или его трансформация? // МЭМО. 2019. No 5. С. 8, 10.

[28] Бартош А. Взгляд на Россию – в упор, на Китай – исподлобья. URL: https://nvo.ng.ru/gpolit/2021-02-11/10_1128_nato.html?print=Y (дата обращения: 14.02.2022).

[29] Европейский С., НАТО Р. П. Проблемы трансформации европейской безопасности в работах российских политологов. – 2020.

М.А. Везуиной[30], С.И. Грачева[31], Д.А. Данилова[323334], О.П. Иванова[353637], И.А. Истомина[38], И.А. Кочина[39], Д.В. Луешкина[40], Е.А. Михалевича[41], Ю.И.

[30] Везуина М.А. Эволюция европейской политики безопасности и обороны - новая архитектура европейской безопасности // Sciences of Europe. 2017. №14-3 (14). URL: https://cyberleninka.ru/article/n/evolyutsiya-evropeyskoy-politiki-bezopasnosti-i-oborony-novaya-arhitektura-evropeyskoy-bezopasnosti (дата обращения: 10.01.2022).

[31] Грачев, С. И. К вопросу о многогранности содержания военно-политической сферы: современный подход / С. И. Грачев, В. С. Чикальдина // KANT: Social Sciences & Humanities. – 2023. – № 2(14). – С. 20-24. – DOI 10.24923/2305-8757.2023-14.4. – EDN TJXCUU.

[32] Данилов Д.А. Россия-ЕС-НАТО: выбор рациональной стратегии // Научно-аналитический вестник ИЕ РАН. 2019. No 3. С. 70.

[33] Данилов, Д. А. Вильнюсский саммит НАТО в контексте украинского конфликта / Д. А. Данилов // Аналитические записки Института Европы РАН. – 2023. – № 3(35). – С. 41-48. – DOI 10.15211/analytics31920234148. – EDN VUSFMR.

[34] Данилов, Д. А. Глобальные горизонты атлантического альянса: "вакцина" Байдена / Д. А. Данилов // Современная Европа. – 2021. – № 5(105). – С. 19-31. – DOI 10.15211/soveurope520211931. – EDN DGNGXP.

[35] Иванов О.П. Американский взгляд на стратегическое соперничество и роль военной силы // Обозреватель-Observer. 2024; (2). С 27–36.

[36] Иванов, О. П. Стратегия НАТО в условиях меняющейся среды международной безопасности в Европе / О. П. Иванов // Обозреватель. – 2024. – № 3(404). – С. 16-27. – DOI 10.48137/2074-2975_2024_3_16. – EDN PLHQDG.

[37] Иванов, О. П. Трансформация НАТО: от потепления климата до замерзания в политике / О. П. Иванов // Обозреватель. – 2022. – № 11-12(394–395). – С. 5-16. – DOI 10.48137/2074-2975_2022_11-12_5. – EDN TYCKOR.

[38] Истомин И.А. Военно-политическая трансформация НАТО в контексте противоборства России и Запада. МГИМО 2024 г.

[39] Кочин И. А. Эволюция модели общей внешней политики и политики безопасности Европейского Союза // Вестник РУДН. Серия: Юридические науки. 2006. №1. URL: https://cyberleninka.ru/article/n/evolyutsiya-modeli-obschey-vneshney-politiki-i-politiki-bezopasnosti-evropeyskogo-soyuza (дата обращения: 1.01.2022).

[40] Леушкин, Д. В. Эволюция НАТО как нормативной силы: от распада СССР до обострения украинского кризиса / Д. В. Леушкин, Н. Г. Самойлов // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2022. – № 2. – С. 7-15. – DOI 10.52452/19931778_2022_2_7. – EDN XSHWTL.

[41] Базаркина, Д. Ю. Регулирование рисков, связанных со злонамеренным использованием искусственного интеллекта в США, ЕС и Китае / Д. Ю. Базаркина, Е. Н. Пашенцев, Е. А. Михалевич // Современная Европа. – 2024. – № 6(127). – С. 156-167. – DOI 10.31857/S0201708324060147. – EDN EWWVII.

Надточея[42][43][44][45], В.Н. Панина[46][47], Е.Н. Пашенцева[48], О.И. Ребро[49], Н.Г. Самойлова[50], А.А. Синдеева[51], А.А. Сушенцова[52], В.С. Чикальдиной[53], А.Г. Шляхтунова[54][55], Д. А. Ясковича[56], работы зарубежных учёных и экспертов: Р.

---

[42] Надточей Ю. И. Российско-американский договор РСМД и проблема третьих стран // США & Канада: экономика – политика – культура. – 2019. – Выпуск № 3 С. 5-22 . URL: https://usacanada.jes.su/s032120680004152-1-1/ DOI: 10.31857/S032120680004152-1(дата обращения: 01.02.2022).

[43] Надточей, Ю. В преддверии «четвёртого возраста»: к итогам юбилейного саммита НАТО / Ю. Надточей // Европейская безопасность: события, оценки, прогнозы. – 2024. – № 74(90). – С. 4-17. – EDN IACVLT.

[44] Надточей, Ю. Мадридский саммит НАТО 2022: "старый" постмодерн против "нового" модерна / Ю. Надточей // Европейская безопасность: события, оценки, прогнозы. – 2022. – № 66(82). – С. 7-13. – EDN LWVPHO.

[45] Надточей, Ю. Повторение пройденного, или Послесловие к саммиту НАТО в Вильнюсе / Ю. Надточей // Европейская безопасность: события, оценки, прогнозы. – 2023. – № 70(86). – С. 13-26. – EDN CBPWZX.

[46] Панин, В. Н. Мировой порядок в XXI веке: теории и практики построения / В. Н. Панин, Г. В. Косов // Социально-политические и историко-культурные аспекты современной геополитической ситуации : материалы международной научно-практической конференции в рамках IX научно-образовательного форума, Сочи, 08–09 апреля 2016 года. – Сочи: Издательство "Перо", 2016. – С. 28-35. – EDN XWCQBZ.

[47] Panin, V. N. Geopolitical rivalry between Russia and NATO in the context of the crisis in Russian-Ukrainian relations / V. N. Panin, A. K. Botasheva, Yu. V. Usova // Modern Science and Innovations. – 2021. – No. 4(36). – P. 194-199. – DOI 10.37493/2307-910X.2021.4.23. – EDN VHCRBI.

[48] Базаркина, Д. Ю. Регулирование рисков, связанных со злонамеренным использованием искусственного интеллекта в США, ЕС и Китае / Д. Ю. Базаркина, Е. Н. Пашенцев, Е. А. Михалевич // Современная Европа. – 2024. – № 6(127). – С. 156-167. – DOI 10.31857/S0201708324060147. – EDN EWWVII.

[49] Европейский С., НАТО Р. П. Проблемы трансформации европейской безопасности в работах российских политологов. – 2020.

[50] Леушкин, Д. В. Эволюция НАТО как нормативной силы: от распада СССР до обострения украинского кризиса / Д. В. Леушкин, Н. Г. Самойлов // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2022. – № 2. – С. 7-15. – DOI 10.52452/19931778_2022_2_7. – EDN XSHWTL.

[51] Синдеев А.А. Проблемы трансформации европейской безопасности в работах российских политологов. М.: ИЕ РАН, 2020.

[52] Европейский С., НАТО Р. П. Проблемы трансформации европейской безопасности в работах российских политологов. – 2020.

[53] Грачев, С. И. К вопросу о многогранности содержания военно-политической сферы: современный подход / С. И. Грачев, В. С. Чикальдина // KANT: Social Sciences & Humanities. – 2023. – № 2(14). – С. 20-24. – DOI 10.24923/2305-8757.2023-14.4. – EDN TJXCUU.

[54] Шляхтунов А. Г. К вопросу о политике нато на ближайшую перспективу // Армия и общество. 2011. №1 (25). URL: https://cyberleninka.ru/article/n/k-voprosu-o-politike-nato-na-blizhayshuyu-perspektivu (дата обращения: 31.05.2022).

[55] Шляхтунов А. Г. Военная и экономическая политика США и НАТО: тенденции и перспективы развития //Вестник Екатерининского института. – 2019. – №. 2. – С. 80-86.

[56] Яскович Д.А. Эволюция стратегических концепций нато в постсоветский период: формирование стратегии продвижения на Восток // Манускрипт. 2017. №7 (81). URL:

Бёрнса[57], З. Бжезинского[58], Ф. Гейсбурга[59], Я.А. Зепоса[60], Д. Муравчика[61], доклад Картина нарождающегося мира: базовые черты и тенденции[62].

Второй блок составляют работы, в которых непосредственно исследуется феномен киберпространства, истоки его доктринального оформления. Среди них монографии и научные статьи ведущих отечественных и зарубежных исследователей: Р.А. Абдуллаева[63], Э.Л. Ансельмо[64], Э. Араб-Оглы[65], Д. Арквиллы[66], Т.В. Барановой[67], И.Р. Бегишева[68],

---

https://cyberleninka.ru/article/n/evolyutsiya-strategicheskih-kontseptsiy-nato-v-postsovetskiy-period-formirovanie-strategii-prodvizheniya-na-vostok (дата обращения: 22.01.2022).

[57] Burns R. New US European Command Leader will Take over amid NATO Worries and Tensions // Military Times. May 1, 2019. URL; https://www.militarytimes.com/news/ your-military/2019/05/01/new-useuropean-command-leader-will-take-over-amid-nato- worries-and-tensions/?utm_source=Sailthru&utm_medium=email&utm_campaign=ebb%20 05.02.19&utm term=Editorial%20-920Early%20Bird%20Brief (дата обращения: 01.02.2022).

[58] Brezinski Z. The Premature Partnership // Foreign Affairs. 1994. N 2. Vol. 73. P. 79.

[59] Heisbourg F. “The «European Security Strategy» is not a Security Strategy” / A European Way of War, St. Everts et al. (eds.). L.: Centre for European Reform, 2004. p. 27–39.

[60] Зепос Я. А. Оглянитесь назад, чтобы увидеть будущее //Международная жизнь. – 2012. – №. 1. – С. 21-35.

[61] Muravchik J. The Imperative of NATO’s Leadership. — Washington: American Enterprise Institute, 2010.

[62] Картина нарождающегося мира: базовые черты и тенденции: - Москва: Дипломатическая академия МИД России, 2024. – 68 с. с. 37.

[63] Абдуллаев, Р. А. Феномен "сетей поддержки" и влияние на него развития интернет-технологий / Р. А. Абдуллаев, М. И. Рыхтик // Власть. – 2014. – № 6. – С. 15-20. – EDN SHFMMF.

[64] Ансельмо Э. Л. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? // Экономические стратегии. 2006. Т. 8. № 2. С. 24—31.

[65] Араб-Оглы Э. Кибернетика и моделирование социальных процессов // Кибернетика ожидаемая и кибернетика неожиданная / Сост. В.Д. Пекелис. М., 1968. С. 152–153.

[66] Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation.

[67] Воскресенская, Н. Г. Цифровизация в восприятии студентов поколений Y и Z / Н. Г. Воскресенская, М. И. Рыхтик, Т. В. Баранова // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. – 2020. – № 4(60). – С. 137-148. – EDN XZLLGP.

[68] Бегишев, И.Р., Денисович, В.В., Сабитов, Р.А., Пасс, А.А., Скоробогатов, А.В. Уголовно-правовое значение метавселенных: коллизии в праве // Правопорядок: история, теория, практика. 2023. № 4(39). С. 58-62. DOI: 10.47475/2311-696X-2023-39-4-58-62

М.М. Безкоровайного[69], В.Е. Воскресенской[70], Д. Белла[7172], М. Бенедикта[7374], Т. Бёрнерса-Ли[7576], Д. Бетца, С.В. Бондаренко[77], С.С. Булгакова[78], А.Е. Войскунского[79], А.Г. Волова[80], У. Гибсона[8182], А.А. Данельяна[83], В.В.

[69] Безкоровайный, М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. №1 (2). URL: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (дата обращения: 01.08.2024).

[70] Воскресенская, Н. Г. Цифровизация в восприятии студентов поколений Y и Z / Н. Г. Воскресенская, М. И. Рыхтик, Т. В. Баранова // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. – 2020. – № 4(60). – С. 137-148. – EDN XZLLGP.

[71] Bell D.J. // Cyberculture: The Key Concepts. 2001

[72] D. Bell, B. Kennedy The Cybercultures Reader (2010)

[73] Benedikt M. Cyberspace: Some Proposals // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press,1991 b. – P. 120–138.

[74] Benedikt M. Introduction // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press, 1991 a. – P. 1–25.

[75] Berners-Lee, T. (1999). "The World Wide Web: A Very Short Personal History"

[76] Berners-Lee, T. (2001). "The Semantic Web: A New Form of Web Architecture"

[77] Бондаренко, С.В. (2002). Социальная система киберпространства 210 Парадигмы и процессы как новая социальная общность. Научная мысль Кавказа. Приложение, 12(38).

[78] Булгаков С.С., Поздняков А.Н. О новых терминах в сфере отечественной правоохранительной деятельности: «киберпреступность» // Труды Академии управления МВД России. 2022. №4 (64). URL: https://cyberleninka.ru/article/n/o-novyh-terminah-v-sfere-otechestvennoy-pravoohranitelnoy-deyatelnosti-kiberprestupnost (дата обращения: 01.08.2024).

[79] Войскунский А.Е. Метафоры интернета // Вопросы философии. 2001. № 11. С. 64–79.

[80] Волов А.Г. Философский анализ понятия «Киберпространство» // Философские проблемы информационных технологий и киберпространства. 2011. №2. URL: https://cyberleninka.ru/article/n/filosofskiy-analiz-ponyatiya-kiberprostranstvo (дата обращения: 20.08.2024).

[81] Gibson W. Burning Chrome // Omni. 1982. July. URL: https://omni.media/omnimagazine-july-1982 (accessed: 15.07.2024).

[82] Gibson W. Neuromancer. N.Y., 1984.

[83] Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. 2020. №1. URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie-kiberprostranstva (дата обращения: 27.08.2024).

Денисовича[84], Д.Е. Добринской[85], П.В. Закалкина[8687], С.А. Иванова[8889], М. Кастельса[90], Л. Келло[91], Б. Коллина[92], В.В. Коровкина[93], А.В. Крутских[94], П. Кузнецова[95], С.В. Куликова[96], В.И. Курбатова[97], С.И. Макаренко[98], Д.

---

[84] Бегишев, И.Р., Денисович, В.В., Сабитов, Р.А., Пасс, А.А., Скоробогатов, А.В. Уголовно-правовое значение метавселенных: коллизии в праве // Правопорядок: история, теория, практика. 2023. № 4(39). С. 58-62. DOI: 10.47475/2311-696X-2023-39-4-58-62

[85] Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского Университета. Сер. 18. Социология и политология. 2018. Т. 24. № 1. С. 52—70.

[86] Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Структурно-функциональная модель киберпространства // Вопросы кибербезопасности. 2021. №4 (44). URL: https://cyberleninka.ru/article/n/strukturno-funktsionalnaya-model-kiberprostranstva (дата обращения: 02.01.2025).

[87] Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С.16–21.

[88] Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С.16–21.

[89] Стародубцев Ю.И., Иванов С.А., Закалкин П.В. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации // Военная мысль. 2021. № 4. С. 39–49.

[90] Castells, M. (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford University Press.

[91] Kello, L. (2017). The Virtual Weapon and International Order.

[92] Collin B. The Future of Cyberterrorism // Crime & Justice International Journal. — 1997. — Vol. 13. — Вып. 2.

[93] Коровкин В.В. Международное регулирование киберпространства: возможно ли эффективное взаимопонимание? // Социальные новации и социальные науки. 2020. №1 (1). URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-regulirovanie-kiberprostranstva-vozmozhno-li-effektivnoe-vzaimoponimanie (дата обращения: 07.08.2024).

[94] Крутских А.В. Угрозы безопасности в цифровой среде и международное сотрудничество в области цифровой безопасности // Международные отношения: грани настоящего и будущего / [под ред. И.С. Иванова, И.Н. Тимофеева, Е.О. Карпинской, Е.А. Солодухиной, С.М. Гавриловой]; Российский совет по международным делам (РСМД). – М.: НП РСМД, 2023. – 472с. С. 197

[95] Пашенцев, Е. Н. Злонамеренное использование искусственного интеллекта и угрозы информационно-психологической безопасности для Ирана: многоуровневая реальность / Е. Н. Пашенцев, П. Кузнецов, В. А. Чебыкина // Восток. Афро-азиатские общества: история и современность. – 2025. – № 3. – С. 125-136. – DOI 10.31696/S086919080033177-1. – EDN ZMIMPA.

[96] Курбатов, В.И., Куликов, С.В., Папа, О.М. (2018). Сетевые онлайн сообщества: факторы самоуправления в формировании цифрового гражданского общества. Гуманитарные, социально-экономические и общественные науки.

[97] Курбатов, В.И., Куликов, С.В., Папа, О.М. (2018). Сетевые онлайн сообщества: факторы самоуправления в формировании цифрового гражданского общества. Гуманитарные, социально-экономические и общественные науки.

[98] Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. / СПб.: Наукоемкие технологии, 2017. 237 с.

Липтона[99], С. Лэша[100], Д. Ная[101], Т. О'Райли[102], О.М. Папа[103], А.А. Пасса[104], Е.Н. Пашенцева[105], М.А. Петлина[106], А.Н. Позднякова[107], Т.В. Радченко[108], Х. Рейнгольда[109], Д. Ронфельда[110], М.И. Рыхтика[111112], Р.А. Сабитова[113], К.

[99] Lipton J. Rethinking Cyberlaw: A New Vision for Internet Law.-Edward Elgar Publishing, 2015, 176 p.
[100] Lash S. Critique of information. L., 2002. P. 15.
[101] Nye, J. S. (2010). Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School.
[102] O'Reilly, T. (2005). "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software"
[103] Курбатов, В.И., Куликов, С.В., Папа, О.М. (2018). Сетевые онлайн сообщества: факторы самоуправления в формировании цифрового гражданского общества. Гуманитарные, социально-экономические и общественные науки.
[104] Бегишев, И.Р., Денисович, В.В., Сабитов, Р.А., Пасс, А.А., Скоробогатов, А.В. Уголовно-правовое значение метавселенных: коллизии в праве // Правопорядок: история, теория, практика. 2023. № 4(39). С. 58-62. DOI: 10.47475/2311-696X-2023-39-4-58-62
[105] Пашенцев, Е. Н. Злонамеренное использование искусственного интеллекта и угрозы информационно-психологической безопасности для Ирана: многоуровневая реальность / Е. Н. Пашенцев, П. Кузнецов, В. А. Чебыкина // Восток. Афро-азиатские общества: история и современность. – 2025. – № 3. – С. 125-136. – DOI 10.31696/S086919080033177-1. – EDN ZMIMPA.
[106] Петлин М. А. Социально-философские аспекты киберпространства // Вестник ОмГУ. 2014. №3 (73). URL: https://cyberleninka.ru/article/n/sotsialno-filosofskie-aspekty-kiberprostranstva (дата обращения: 20.08.2024).
[107] Булгаков С.С., Поздняков А.Н. О новых терминах в сфере отечественной правоохранительной деятельности: «киберпреступность» // Труды Академии управления МВД России. 2022. №4 (64). URL: https://cyberleninka.ru/article/n/o-novyh-terminah-v-sfere-otechestvennoy-pravoohranitelnoy-deyatelnosti-kiberprestupnost (дата обращения: 01.08.2024).
[108] Радченко Т. В., Шевелева К. В. Правовые аспекты определения границ киберпространства // Вестник экономики, управления и права. 2024. №3. URL: https://cyberleninka.ru/article/n/pravovye-aspekty-opredeleniya-granits-kiberprostranstva (дата обращения: 02.01.2025).
[109] Rheingold, H. (1993). The Virtual Community: Finding Connection in a Computerized World.
[110] Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation.
[111] Абдуллаев, Р. А. Феномен "сетей поддержки" и влияние на него развития интернет-технологий / Р. А. Абдуллаев, М. И. Рыхтик // Власть. – 2014. – № 6. – С. 15-20. – EDN SHFMMF.
[112] Воскресенская, Н. Г. Цифровизация в восприятии студентов поколений Y и Z / Н. Г. Воскресенская, М. И. Рыхтик, Т. В. Баранова // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. – 2020. – № 4(60). – С. 137-148. – EDN XZLLGP.
[113] Бегишев, И.Р., Денисович, В.В., Сабитов, Р.А., Пасс, А.А., Скоробогатов, А.В. Уголовно-правовое значение метавселенных: коллизии в праве // Правопорядок: история, теория, практика. 2023. № 4(39). С. 58-62. DOI: 10.47475/2311-696X-2023-39-4-58-62

Сагана[114], П. Саймона[115], А.В. Скоробогатова[116], Е. Соджи[117], Ю.И. Стародубцева[118], Т. Стивенса[119], А.Л. Татузова[120], Л.В. Тереньевой[121], М.А. Федотова[122], В.А. Цвыка[123], К.В. Шевелевой[124], С.С. Ширина[125].

К третьему блоку относятся монографии и научные статьи ведущих отечественных и зарубежных исследователей, посвящённые проблематике изучения ключевых особенностей стратегии НАТО в киберпространстве на современном этапе, а также её реализации в условиях постоянно трансформирующейся международной обстановки и структуры глобальной

---

[114] Sagan C. Conversations with Carl Sagan//University Press of Mississippi, 2006.-P.99.

[115] Simon P. The Age of the Platform (2015)

[116] Бегишев, И.Р., Денисович, В.В., Сабитов, Р.А., Пасс, А.А., Скоробогатов, А.В. Уголовно-правовое значение метавселенных: коллизии в праве // Правопорядок: история, теория, практика. 2023. № 4(39). С. 58-62. DOI: 10.47475/2311-696X-2023-39-4-58-62

[117] Soja E. Postmetropolis. Critical studies of cities and regions. Malden, 2000. P. 333.

[118] Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Структурно-функциональная модель киберпространства // Вопросы кибербезопасности. 2021. №4 (44). URL: https://cyberleninka.ru/article/n/strukturno-funktsionalnaya-model-kiberprostranstva (дата обращения: 02.01.2025).

[119] Betz D.J., Stevens T. Cyberspace and the State: Toward a Strategy for Cyber- Power.- Taylor & Francis Ltd, 2011, 162p.- P.13.

[120] Безкоровайный, М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. №1 (2). URL: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (дата обращения: 01.08.2024).

[121] Терентьева Л.В. Понятие киберпространства и очерчивание его территориальных контуров // Правовая информатика. 2018. №4. URL: https://cyberleninka.ru/article/n/ponyatie-kiberprostranstva-i-ocherchivanie-ego-territorialnyh-konturov (дата обращения: 01.08.2024).

[122] Федотов М.А. Конституционные ответы на вызовы киберпространства // Lex Russica. 2016. № 3. С. 164—182.

[123] Цвык, В. А. Искусственный интеллект в современном обществе: шаги, вызовы, стратегии / В. А. Цвык, И. В. Цвык, Г. И. Цвык // Вестник Российского университета дружбы народов. Серия: Философия. – 2024. – Т. 28, № 2. – С. 589-600. – DOI 10.22363/2313-2302-2024-28-2-589-600. – EDN UBJZTG.

[124] Радченко Т. В., Шевелева К. В. Правовые аспекты определения границ киберпространства // Вестник экономики, управления и права. 2024. №3. URL: https://cyberleninka.ru/article/n/pravovye-aspekty-opredeleniya-granits-kiberprostranstva (дата обращения: 02.01.2025).

[125] Ширин С.С. Всемирная паутина как объект исследования в политической науке // Вестник Санкт-Петербургского университета. Международные отношения. 2013. №2. URL: https://cyberleninka.ru/article/n/vsemirnaya-pautina-kak-obekt-issledovaniya-v-politicheskoy-nauke (дата обращения: 14.08.2024).

безопасности: Е.А. Антюховой[126], Н.А. Баранова[127], Д. Блэка[128], Ю.В. Бородакия[129], Л. Брента[130], И.В. Бутусова[131], Л. Вихула[132][133], М. Галеотти[134], Ф. Гейди[135], Ю.Е. Горбачевой[136], Т.А. Гришаниной[137], А.Ю. Добродеева[138], П.В.

[126] Антюхова Е.А. Система планирования деятельности НАТО в контексте положений Повестки «НАТО-2030» и Стратегической концепции НАТО 2022 г. // Вестник международных организаций. 2024. Т. 19. № 3. С. 31-47 (на русском и английском языках).
[127] Баранов Н. А., Попов П. В. Стратегии гибридных войн стран НАТО как вызов российской Федерации // Евразийская интеграция: экономика, право, политика. 2019. №2 (28). URL: https://cyberleninka.ru/article/n/strategii-gibridnyh-voyn-stran-nato-kak-vyzov-rossiyskoy-federatsii (дата обращения: 03.03.2025).
[128] Black and Lynch, “Cyber Threats to NATO from a Multi-Domain Perspective,” 126–30.
[129] Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) //Вопросы кибербезопасности. – 2013. – №. 1. – С. 2-9.
[130] Brent L. (2019). The role of NATO in cyber space [Rol’ NATO v kiberneticheskom prostranstve] // NATO Review. – Brussels. – 12.02. – URL: https://www.nato.int/docu/review/ru/articles/2019/02/12/rol-nato-v-kiber neticheskom-prostranstve/index.html (date of access – 28.01.2024)
[131] Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) //Вопросы кибербезопасности. – 2013. – №. 1. – С. 2-9.
[132] Schmitt, M. N., & Vihul, L. (2017). The Nature of International Law Cyber Norms.
[133] Schmitt, M. N., & Vihul, L. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
[134] Galeotti, M. (2016). Hybrid War or Gibridnaya Voina? Small Wars Journal.
[135] Gady and Stronell, “Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030,” 152
[136] Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны. – URSS, 2010.
[137] Гришанина Т.А. Искусственный интеллект в международных отношениях: роль и направления исследования // Вестник РГГУ. Серия: Политология. История. Международные отношения. 2021. №4. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-mezhdunarodnyh-otnosheniyah-rol-i-napravleniya-issledovaniya (дата обращения: 13.01.2025).
[138] Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) //Вопросы кибербезопасности. – 2013. – №. 1. – С. 2-9.

Закалкина[139][140], С.А. Иванова[141][142], Л. Илвса[143], Н.В. Кардавы[144], О.Г. Карповича[145], Ф. Киллуфо[146], А. Климбурга[147], Н.П. Кобца[148], Ю.А. Кожанова[149], Е.С. Коренева[150], П. Котлера[151], А. Линча[152], Д. Лиона[153], Д.

[139] Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С.16–21.

[140] Стародубцев Ю.И., Иванов С.А., Закалкин П.В. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации // Военная мысль. 2021. № 4. С. 39–49.

[141] Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С.16–21.

[142] Стародубцев Ю.И., Иванов С.А., Закалкин П.В. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации // Военная мысль. 2021. № 4. С. 39–49.

[143] Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. PRISM, 6(2), 126–141. http://www.jstor.org/stable/26470452

[144] Кардава Н.В. Киберпространство как новая политическая реальность: вызовы и ответы // История и современность. 2018. №1-2 (27-28). URL: https://cyberleninka.ru/article/n/kiberprostranstvo-kak-novaya-politicheskaya-realnost-vyzovy-i-otvety (дата обращения: 22.08.2024).

[145] Карпович, О. Г. Новые цифровые военные технологии Запада на Украине против России / О. Г. Карпович, Р. Н. Шангараев // Вестник Дипломатической академии МИД России. Россия и мир. – 2024. – № 3(41). – С. 6-21. – EDN QTGWPW.

[146] Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. PRISM, 6(2), 126–141. http://www.jstor.org/stable/26470452

[147] Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. Penguin Press.

[148] Кобец П.Н. Характеристика современных особенностей противоправных проявлений, совершаемых в киберпространстве // Современная наука. 2022. № 3. С. 18-20

[149] Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны. – URSS, 2010.

[150] Коренев Е.С. НАТО 2030 И Россия: Трансформация военно-политической стратегии альянса в контексте российских национальных интересов Материалы Молодежной секции «Примаковских чтений» «Глобальные проблемы постковидного мироустройства: новые вызовы и лидеры» URL: https://www.imemo.ru/files/File/ru/publ/2022/SMU-sbornik-PR2021-1.pdf (дата обращения: 08.09.2024).

[151] Kotler, P. (2019). "Marketing 4.0: Moving from Traditional to Digital"

[152] Black and Lynch, “Cyber Threats to NATO from a Multi-Domain Perspective,” 126–30.

[153] Lyon, D. (2015). Surveillance after Snowden. Polity Press.

Маккарти[154], А.Н. Маловой[155], А.В. Манойло[156], М. Мински[157], А. Надау[158], И.Н. Панарина[159], С.А. Паршина[160], А.Ю. Поволотцкого[161], П.В. Попова[162], Т.А. Романовой[163], Н. Рочестера[164], М. Рустада[165], И.С. Семененко[166], П.

[154] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. AI Magazine, 27(4), 12. https://doi.org/10.1609/aimag.v27i4.1904

[155] Романова Т.А., Малова А.Н. Проблема применения категории "стрессоустойчивость" в политике кибербезопасности Евросоюза // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2019. №1. URL: https://cyberleninka.ru/article/n/problema-primeneniya-kategorii-stressoustoychivost-v-politike-kiberbezopasnosti-evrosoyuza (дата обращения: 08.08.2023).

[156] Манойло А.В. Современные стратегии кибербезопасности и кибероборонь НАТО // АПЕ. 2020. №3. URL: https://cyberleninka.ru/article/n/sovremennye-strategii-kiberbezopasnosti-i-kiberoborony-nato (дата обращения: 23.01.2025).

[157] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. AI Magazine, 27(4), 12. https://doi.org/10.1609/aimag.v27i4.1904

[158] Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. PRISM, 6(2), 126–141. http://www.jstor.org/stable/26470452

[159] Панарин И. Н. Гладиаторы гибридной войны // Экономические стратегии. 2016. № 2. С. 60–65.

[160] Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны. – URSS, 2010.

[161] Соколов А. С., Поволотцкий А. Ю. Кибертерроризм в России и странах Центральной Азии // Российско-азиатский правовой журнал. 2020. №2. URL: https://cyberleninka.ru/article/n/kiberterrorizm-v-rossii-i-stranah-tsentralnoy-azii (дата обращения: 22.07.2025).

[162] Баранов Н. А., Попов П. В. Стратегии гибридных войн стран НАТО как вызов российской Федерации // Евразийская интеграция: экономика, право, политика. 2019. №2 (28). URL: https://cyberleninka.ru/article/n/strategii-gibridnyh-voyn-stran-nato-kak-vyzov-rossiyskoy-federatsii (дата обращения: 03.03.2025).

[163] Романова Т.А., Малова А.Н. Проблема применения категории "стрессоустойчивость" в политике кибербезопасности Евросоюза // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2019. №1. URL: https://cyberleninka.ru/article/n/problema-primeneniya-kategorii-stressoustoychivost-v-politike-kiberbezopasnosti-evrosoyuza (дата обращения: 08.08.2023).

[164] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. AI Magazine, 27(4), 12. https://doi.org/10.1609/aimag.v27i4.1904

[165] Rustad M.L. Global Internet Law in a Nutshell//West Academic Publishing, 2013.-525p.-P.12

[166] Семененко И.С. Политические изменения в современном мире: новые контуры исследовательского поля // Политическая наука перед вызовами глобального и регионального развития / под ред. О. В. ГаманГолутвиной. М. : Аспект Пресс, 2016. С. 20–37

Сингера[167], М.В. Смекаловой[168], А.С. Соколова[169], Ю.И. Стародубцева[170171], А. Стронелла[172], И.В. Сурмы[173], А.И. Ходанова[174], Н.А. Цвековой[175], В.А. Чебыкиной[176], Р.Н. Шангараева[177], М. Шмитта[178179], Т. Эванса[180].

---

[167] P. Singer Wired for War: The Robotics Revolution and Conflict in the 21st Century (2009)

[168] Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2019. №1. URL: https://cyberleninka.ru/article/n/evolyutsiya-doktrinalnyh-podhodov-ssha-k-obespecheniyu-kiberbezopasnosti-i-zaschite-kriticheskoy-infrastruktury (дата обращения: 20.01.2025).

[169] Соколов А. С., Поволотцкий А. Ю. Кибертерроризм в России и странах Центральной Азии // Российско-азиатский правовой журнал. 2020. №2. URL: https://cyberleninka.ru/article/n/kiberterrorizm-v-rossii-i-stranah-tsentralnoy-azii (дата обращения: 22.07.2025).

[170] Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С.16–21.

[171] Стародубцев Ю.И., Иванов С.А., Закалкин П.В. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации // Военная мысль. 2021. № 4. С. 39–49.

[172] Gady and Stronell, “Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030,” 152

[173] Сурма И. В. Межгосударственное киберпротивоборство и вмешательство во внутренние дела суверенных государств (НАТО и его инструменты) / И. В. Сурма // Мировой политический процесс: информационные войны и «цветные революции» : Сборник материалов Международной научно-практической конференции, Москва, 27–29 октября 2021 года. – Москва: Московский государственный лингвистический университет, 2022. – С. 141-149. – EDN GXOCYF.

[174] Ходанов А.И. Проблемы придания статуса casus belli кибератаке на государство – члена НАТО // Правовое государство: теория и практика. 2024. №3 (77). URL: https://cyberleninka.ru/article/n/problemy-pridaniya-statusa-casus-belli-kiberatake-na-gosudarstvo-chlena-nato (дата обращения: 27.01.2025).

[175] Цветкова Н.А. Феномен цифровой дипломатии в международных отношениях и методология его изучения // Вестник РГГУ. Серия «Политология. История. Международные отношения». 2020. № 2. С. 37–47.

[176] Пашенцев, Е. Н. Злонамеренное использование искусственного интеллекта и угрозы информационно-психологической безопасности для Ирана: многоуровневая реальность / Е. Н. Пашенцев, П. Кузнецов, В. А. Чебыкина // Восток. Афро-азиатские общества: история и современность. – 2025. – № 3. – С. 125-136. – DOI 10.31696/S086919080033177-1. – EDN ZMIMPA.

[177] Карпович, О. Г. Новые цифровые военные технологии Запада на Украине против России / О. Г. Карпович, Р. Н. Шангараев // Вестник Дипломатической академии МИД России. Россия и мир. – 2024. – № 3(41). – С. 6-21. – EDN QTGWPW.

[178] Schmitt, M. N., & Vihul, L. (2017). The Nature of International Law Cyber Norms.

[179] Schmitt, M. N., & Vihul, L. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

[180] Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. PRISM, 6(2), 126–141. http://www.jstor.org/stable/26470452

Четвёртый блок включает материалы печатных и электронных СМИ, в первую очередь российских и международных информационных агентств.

Цель исследования: идентифицировать и раскрыть ключевые особенности современной стратегии НАТО в киберпространстве.

Для достижения этой цели необходимо решить ряд следующих **задач:**

1. Определить ключевые подходы отечественных и зарубежных исследователей к определению понятия киберпространство.
2. Провести сравнительный анализ и классификацию подходов отечественных и зарубежных исследователей к определению понятия киберпространство.
3. Идентифицировать особенности ключевых этапов трансформации стратегии НАТО в киберпространстве в период 1999 – 2022 гг., а также концептуальные основы реализации стратегии НАТО в киберпространстве на современном этапе, установить перспективы дальнейшего развития современной стратегии НАТО в киберпространстве.
4. Сформулировать особенности развития возможностей использования информационно-коммуникационных технологий НАТО в военно-политических целях в контексте международной безопасности.
5. Идентифицировать место и роль России в современной стратегии НАТО в киберпространстве.

Теоретико-методологическая основа исследования.

Теоретико-методологическая основа исследования стратегии НАТО в киберпространстве представляет собой комплексный синтез современных теорий международных отношений и специализированных методов анализа, позволяющий всесторонне рассмотреть эволюцию подходов альянса к цифровым вызовам. В основе работы лежит сочетание классических парадигм международных отношений с инновационными подходами к изучению кибербезопасности, что отражает междисциплинарный характер современной науки о международной безопасности. Исследование опирается на фундаментальные положения политического реализма, рассматривающего

киберпространство как новую арену геополитического соперничества, где Североатлантический альянс стремится сохранить стратегическое превосходство. Неореалистический подход помогает объяснить логику милитаризации киберпространства военно-политическим блоком как естественное продолжение традиционной борьбы за влияние в условиях анархичной международной системы. При этом либеральный институционализм позволяет анализировать механизмы многостороннего сотрудничества в рамках НАТО, включая развитие специализированных структур киберзащиты и взаимодействие с частным сектором. Конструктивистская перспектива дает возможность понять, как через дискурсивные практики формируются представления о киберугрозах и каким образом антироссийская риторика стала важным элементом стратегического нарратива Североатлантического альянса.

Научная новизна диссертационного исследования:

Основные обладающие научной новизной результаты исследования заключаются в следующем:

1. В исследовании предложена авторская периодизация трансформации стратегии НАТО в киберпространстве, включающая три ключевых этапа, выявлены и систематизированы ключевые решения Североатлантического альянса, повлиявшие на развитие стратегии военно-политического блока в киберпространстве.
2. Автором исследования предложен прогнозный сценарий дальнейшего развития киберстратегии НАТО в контексте глобальных вызовов и угроз, обозначены сценарии развития киберконфликтов, используя междисциплинарный подход, сочетающий анализ первичных документов НАТО (стратегий, коммюнике), кейс-стади (кибератаки 2016–2024 гг.), экспертных интервью (позиции отечественных и западных специалистов).
3. Выявлены роль и место России в киберполитике НАТО: от образа угрозы к практикам противодействия, определена дихотомия восприятия России в документах Североатлантического альянса.

4. Предложено собственное определение понятия «киберпространство». Киберпространство – это глобальный, искусственно сконструированный, неоднородный и динамичный социотехнический континуум, возникающий в результате симбиоза технологической инфраструктуры (включая компьютерные системы, сети передачи данных и обеспечивающие их функционирование технологические платформы) и человеческой деятельности (социальных практик, культурных кодов и коммуникативных взаимодействий).
5. Проведена комплексная систематизация и классификация отечественных и зарубежных подходов к определению понятия «киберпространство». Выделено три ключевых методологических подхода (технологический, социотехнический, философско-культурный), что позволяет структурировать существующее концептуальное многообразие в данной области.

Хронологические рамки: начало 1990-х гг. – Н.В. обуславливаются поставленными целями и задачами.

Теоретическая и практическая значимость работы:

Теоретическая значимость исследования заключается в комплексном анализе этапов трансформации концепции киберпространства и его роли в современной системе международных отношений и системе международной безопасности. Исследовательская работа вносит вклад в теорию международных отношений, систематизируя подходы к пониманию киберпространства – от технической инфраструктуры до сложной социотехнической системы, трансформирующей политические и социальные практики. Исследование раскрывает парадигмальные изменения в стратегии Североатлантического альянса, прослеживая её эволюцию от первых шагов в 1990-х годах до признания киберпространства областью операций и последующей милитаризации. Особую ценность представляет анализ интеграции информационно-коммуникационных технологий в военное планирование, включая роль искусственного интеллекта и больших данных в

трансформации доктрин коллективной обороны. Разработанные концептуальные рамки для анализа взаимодействия России и НАТО в киберпространстве расширяют научные представления о гибридных конфликтах и международном регулировании цифровой среды.

Практическая значимость исследования проявляется в его прикладном потенциале для укрепления российской политики в сфере кибербезопасности. Результаты работы могут быть использованы для совершенствования защиты критической инфраструктуры, разработки асимметричных мер противодействия наращиванию киберпотенциала Североатлантического альянса и формирования стратегий международного сотрудничества. Материалы исследования представляют ценность для дипломатической работы, обеспечивая аналитическую базу для аргументации российской позиции на площадках ООН и ОБСЕ. Выводы диссертации также могут быть применены в образовательном процессе при подготовке специалистов в области международной безопасности и киберполитики, а также для разработки перспективных технологий в условиях технологических санкций. Таким образом, исследование сочетает фундаментальный анализ с практическими решениями, направленными на укрепление национальной безопасности в условиях цифровых вызовов.

Основные положения, выносимые на защиту:

1. Авторское определение киберпространства. Под ним понимается «глобальный, искусственно сконструированный, неоднородный и динамичный социотехнический континуум, возникающий в результате симбиоза технологической инфраструктуры (включая компьютерные системы, сети передачи данных и обеспечивающие их функционирование технологические платформы) и человеческой деятельности (социальных практик, культурных кодов и коммуникативных взаимодействий).»
2. Авторская классификация отечественных и зарубежных подходов к определению понятия «киберпространство». Киберпространство не может

быть сведено к единому определению, так как оно одновременно является технологической инфраструктурой, социотехнической системой, культурным и философским конструктом, а также сложной экосистемой.

3. Комплексный анализ трансформации киберстратегии НАТО в контексте глобальных вызовов и угроз позволяет констатировать, что первый этап трансформации (1990-е – 2006 гг.) ознаменовался осознанием киберугроз в качестве потенциального риска для коллективной безопасности, второй этап (2007–2014 гг.) характеризовался переходом от фрагментарных мер к формированию комплексной стратегии кибербезопасности, третий этап (2014 г. – настоящее время) связан с признанием киберпространства полноценной областью операций.
4. Идентификация концептуальных основ реализации стратегии НАТО в киберпространстве на современном этапе позволила сделать выводы, что сегодня киберпространство приобретает ключевое значение в контексте глобальной безопасности, становясь не только средой технологического взаимодействия, но и ареной геополитической конкуренции, Североатлантический альянс сталкивается с множеством трудностей в достижении своих целей в киберпространстве, включая быстрое развитие технологий, сложность атрибуции атак, гибридные угрозы, различия в возможностях стран-членов, правовые и этические вопросы, угрозы критической инфраструктуре и недостаток квалифицированных кадров.

Апробация результатов исследования:

Основные положения и результаты диссертационного исследования были представлены и апробированы в ходе ряда научно-практических мероприятий. Автор участвовал и выступал с докладами по теме исследования на следующих научных конференциях: Международная научно-практическая онлайн-конференция молодых учёных «Трансформация международной безопасности в современных условиях: как избежать глобальной конфронтации» (18 апреля 2023 года), X Ежегодная международная научная конференция молодых учёных «Актуальные проблемы мировой политики» (8

декабря 2023 года), Международная научно-практическая онлайн-конференция молодых учёных «Трансформация международной безопасности в современных условиях: конфронтация и сотрудничество» (4 апреля 2024 года), Международная научно-практическая онлайн-конференция молодых учёных «Трансформация международной безопасности в современных условиях: новые вызовы и новые возможности» (3 апреля 2025 года).

Структура диссертации соответствует поставленным целям и задачам, представлена введением, основной частью, включающей три главы, заключением, списком источников и литературы, а также приложениями.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность диссертационного исследования, определяются его объект, предмет, цели и задачи, анализируется методологическая основа исследования, оценивается источниковая база исследования и степень научной проработанности проблемы, теоретическая и практическая значимость.

Первая глава «Научные подходы к определению понятия «киберпространство»» закладывает теоретическую основу для более глубокого изучения ключевых подходов отечественных и зарубежных исследователей к определению понятия киберпространство.

В первом параграфе «Подходы отечественных исследователей к определению понятия «киберпространство»» осуществляется комплексный теоретический анализ концепции киберпространства с перспективы отечественного экспертного сообщества. Центральной задачей является концептуализация и четкое определение самого понятия «киберпространство». Для этого проводится этимологический анализ, восходящий к кибернетике как науке об управлении, и устанавливается разграничение между кибернетикой (теоретической основой) и киберпространством (практической средой применения её принципов). На основе синтеза различных научных подходов формулируются сущностные

характеристики киберпространства: его единый и неделимый характер, трансграничность, отсутствие четкой географической привязки и отрицание физических параметров. Особое внимание уделяется критике распространенной ассоциации киберпространства исключительно с интернетом, подчеркивается, что интернет является лишь его важнейшей технологической основой, в то время как киберпространство охватывает более широкий спектр явлений, включая социальные практики и киберфизические системы. Терминологический анализ завершается сопоставлением понятия «киберпространство» с используемым в российском законодательстве термином «информационная сфера», что демонстрирует более узкий и нормативно ориентированный характер последнего.

Во втором параграфе «Подходы зарубежных исследователей к определению понятия «киберпространство»» исследуются генезис и эволюция понятия «киберпространство» в зарубежном научном дискурсе. Автор устанавливает, что термин первоначально возник в научно-фантастической литературе 1980-х годов. Центральным для параграфа является тезис о фундаментальном различии между «Интернетом» как технической инфраструктурой, и «киберпространством» как более широкой социотехнической реальностью. Несмотря на терминологический плюрализм, параграф демонстрирует консенсус в зарубежной литературе относительно ключевых атрибутов киберпространства: его виртуальности, глобальности, трансграничности и роли в качестве принципиально новой среды для социальной, экономической и политической деятельности, выходящей далеко за рамки технической инфраструктуры Интернета.

В третьем параграфе «Сравнительный анализ и классификация подходов отечественных и зарубежных исследователей к определению понятия «киберпространство»» осуществляется комплексный анализ концепции киберпространства через призму сравнительного изучения отечественных и зарубежных исследовательских подходов. Автор последовательно решает несколько ключевых задач. Во-первых, проводится

систематизация многообразия существующих определений киберпространства, выявляются их общие черты и принципиальные различия. На основе проведенного сравнительного анализа автор разрабатывает и предлагает оригинальную классификацию подходов к определению киберпространства, выделяя три основных парадигмы: технологическую, социотехническую и философско-культурную, что позволяет структурировать все многообразие концепций и выявить их специфические черты. Кульминацией становится формулировка авторского интегративного определения, синтезирующего ключевые элементы проанализированных подходов. Киберпространство определяется как глобальный, искусственно сконструированный, неоднородный и динамичный социотехнический континуум, возникающий в результате симбиоза технологической инфраструктуры и человеческой деятельности. Подчеркиваются его ключевые свойства: архитектурная многоуровневость, наличие множества, зачастую антагонистических систем управления, а также производный характер его свойств от характеристик элементов и реализуемых процессов. В определении также фиксируется двойственная роль киберпространства как среды для экономической, политической, культурной активности и одновременно как арены современных конфликтов, что обуславливает его критическую значимость для безопасности и стабильности.

Во второй главе «Ключевые особенности стратегии НАТО в киберпространстве на современном этапе» рассматриваются особенности ключевых этапов трансформации стратегии НАТО в киберпространстве в период 1999 – 2022 гг., а также концептуальные основы реализации стратегии НАТО в киберпространстве на современном этапе, устанавливаются перспективы дальнейшего развития современной стратегии НАТО в киберпространстве.

В первом параграфе «Основные этапы трансформации стратегии НАТО в киберпространстве в период 1999 – 2022 гг.» проводится комплексный анализ трансформации стратегии НАТО в киберпространстве,

выделяются три ключевых этапа её эволюции в контексте меняющихся технологических и геополитических реалий. На первом этапе (1990-е – 2006 гг.) происходило первоначальное осознание киберугроз. Киберпространство изначально воспринималось как сфера гражданской инфраструктуры, однако такие инциденты, как кибератаки во время операции «Союзная сила» (1999 г.), продемонстрировали его стратегический потенциал. Второй этап (2007–2014 гг.) был охарактеризован серией масштабных кибератак на Эстонию (2007 г.), Грузию (2008 г.) и Украину (2014 г.), которые обозначили роль киберпространства в гибридных конфликтах, что потребовало от Североатлантического альянса разработки более комплексной стратегии. Ключевыми шагами стало создание Киберцентра НАТО в Таллине (2008 г.) и закрепление кибербезопасности в качестве элемента коллективной обороны в обновлённой Стратегической концепции (2010 г.). Третий, современный этап (с 2014 г. по настоящее время), характеризуется окончательной милитаризацией киберпространства. Автором делается вывод о том, что эволюция подходов НАТО демонстрирует переход от реактивных оборонительных мер к проактивному и комплексному восприятию киберпространства как полноценного театра военных действий и неотъемлемого компонента системы коллективной безопасности. В заключение отмечается, что дальнейшее развитие стратегии будет определяться способностью Североатлантического альянса адаптироваться к динамичным угрозам, одновременно решая вопросы правового регулирования и баланса между национальным суверенитетом и наднациональными механизмами реагирования.

Во втором параграфе «Концептуальные основы реализации стратегии НАТО в киберпространстве на современном этапе» анализируется трансформация стратегии НАТО в киберпространстве и фундаментальные вызовы, связанные с цифровизацией вооруженных сил. Деятельность альянса развивается по двум основным направлениям: трансформация киберпространства в сферу операций через развитие

наступательных и оборонительных возможностей и выполнение обязательств по киберзащите через укрепление национальных потенциалов стран-членов. Однако реализация стратегии сталкивается с серьезными вызовами, включая сложность атрибуции кибератак, отсутствие четких международно-правовых норм, неоднородность возможностей стран-членов и необходимость баланса между национальным суверенитетом и наднациональным управлением. Эффективность стратегии НАТО будет зависеть от способности альянса преодолеть эти вызовы и выработать адекватные механизмы реагирования на быстро эволюционирующие угрозы.

Проведённый в третьем параграфе «Прогнозный сценарий дальнейшего развития современной стратегии НАТО в киберпространстве» анализ позволяет выделить три ключевых направления развития стратегии НАТО в киберпространстве. Во-первых, Североатлантический альянс активно инвестирует в развитие технологий искусственного интеллекта, квантовых вычислений и автоматизированных систем кибероборонь. Принятие Стратегической концепции 2022 года и обновление стратегии киберзащиты подчеркивают стремление НАТО к технологическому лидерству. Ожидается, что к 2030 году совокупные расходы стран-членов на кибербезопасность превысят 100 миллиардов долларов США, что отражает переход к системной интеграции киберугроз в стратегию коллективной обороны. Во-вторых, НАТО последовательно милитаризирует киберпространство, развивая как оборонительные, так и наступательные возможности. Создание централизованного киберкомандования, проведение регулярных учений и разработка норм применения кибероружия свидетельствуют о формировании полноценного кибертеатра военных действий. Однако данный процесс сопровождается существенными этическими и правовыми вызовами, включая вопросы регулирования атак на гражданскую инфраструктуру. В-третьих, альянс расширяет сотрудничество с частным сектором и международными партнерами. Поскольку частные корпорации играют ключевую роль в технологических инновациях, НАТО

развивает механизмы гражданско-военного взаимодействия. Стратегия НАТО в киберпространстве эволюционирует в ответ на усложнение угроз, включая гибридные атаки и технологическую гонку. Приоритетами остаются технологическое превосходство, нормотворчество и гибкие альянсы с частным сектором. Ключевым вызовом является необходимость балансирования между милитаризацией киберпространства и разработкой международных норм его регулирования. В долгосрочной перспективе альянсу предстоит найти равновесие между сдерживанием, сотрудничеством и инновациями для сохранения своей роли в формировании архитектуры глобальной кибербезопасности.

В третьей главе «Реализация стратегии НАТО в киберпространстве в контексте современной международной безопасности» анализируются особенности развития возможностей использования информационно-коммуникационных технологий НАТО в военно-политических целях в контексте международной безопасности, идентифицируется место и роль России в современной стратегии НАТО в киберпространстве, а также выделяются особенности взаимодействия России и НАТО в области кибербезопасности в контексте современных геополитических реалий.

В первом параграфе «Развитие информационно-коммуникационных технологий НАТО в военно-политических целях в контексте международной безопасности» осуществляется комплексный синтез и теоретическое обобщение ключевых результатов исследования, посвященного трансформации военно-политической стратегии НАТО под влиянием информационно-коммуникационных технологий. Анализ сосредоточен на двух взаимосвязанных процессах: интеграции искусственного интеллекта и больших данных в операционную деятельность Североатлантического альянса, а также эволюции гибридных войн в условиях цифровизации международных отношений. Центральным тезисом является утверждение о переходе технологий из вспомогательного инструментария в категорию стратегических факторов, определяющих баланс сил на глобальной

арене. Подчеркивается дуальная природа технологического прогресса, который, с одной стороны, усиливает обороноспособность за счет повышения точности планирования, оптимизации процессов принятия решений и реализации превентивного сдерживания, а с другой порождает принципиально новые уязвимости, связанные с рисками кибернетических атак, ошибками алгоритмов и сложностями атрибуции воздействий. Детализируется специфика гибридных войн как доминирующей формы современного межгосударственного противостояния, характеризующейся размыванием границ между военными и невоенными методами воздействия, комбинацией открытых и скрытых операций, а также активным использованием инструментов информационно-психологического влияния и экономического давления.

Второй параграф «Место и роль России в современной политике НАТО в киберпространстве» посвящён комплексному анализу места и роли Российской Федерации в политике Североатлантического альянса в киберпространстве на современном этапе. Автор аргументирует тезис о том, что киберпространство стало ключевой ареной геополитического соперничества, в рамках которого Россия позиционируется альянсом в качестве основного источника угроз. Автором констатируется возрастающая значимость киберпространства для международной безопасности и стратегических расчетов НАТО. Далее подробно исследуется конфронтационный характер российско-американских отношений в данной сфере. Приводятся конкретные примеры обвинений в адрес России со стороны США и их союзников в проведении масштабного кибершпионажа и вмешательстве в избирательные процессы, начиная с 2016 года. Критически оценивается асимметричный характер диалога, выражающийся, по мнению автора, в игнорировании многочисленных запросов российской стороны при тщательном рассмотрении запросов, исходящих от США. Центральное место в анализе занимает исследование эволюции стратегических документов НАТО, в частности, обновленной Стратегической концепции 2022 года.

Подчеркивается радикальное изменение восприятия России Североатлантическим альянсом: от потенциального партнера к наиболее значительной и прямой угрозе безопасности, использующей широкий спектр гибридных инструментов, включая кибератаки и дезинформацию. Отмечается, что действия России, согласно данной доктрине, подрывают основанный на правилах международный порядок. Отдельно рассматривается применение кибернетических инструментов в контексте Специальной военной операции на Украине. Со ссылкой на западных экспертов описываются обвинения в адрес России относительно использования кибероперацій для подготовки будущих военных действий, атак на критическую инфраструктуру и подрыва доверия к государственным институтам. Параллельно освещается позиция российской стороны о масштабных кибератаках, исходящих с территорий стран-членов НАТО и направленных на объекты критической информационной инфраструктуры и избирательные процессы в Российской Федерации. В заключительной части параграфа делается вывод о том, что место России в киберполитике НАТО определяется как роль ключевого антагониста. Это, по мнению автора, стимулирует развитие альянсом механизмов коллективной кибероборонь, сдерживания и стратегического противодействия, что в долгосрочной перспективе способно привести к дальнейшей фрагментации глобального цифрового пространства и усилению конфронтации.

Третий параграф «Киберпространство как фактор отношений России и НАТО в условиях новой геополитической напряженности» посвящён текущему состоянию взаимоотношений Российской Федерации и Североатлантического альянса, характеризующимся отсутствием доверия, взаимными обвинениями в причастности к кибератакам на критическую инфраструктуру и двойными стандартами. При этом отмечается, что Россия последовательно выступает с инициативами по выработке многосторонних международных норм, регулирующих деятельность в цифровой сфере. Отдельное внимание уделяется влиянию Специальной военной операции на

Украине на киберпространство, выражающемуся в значительном росте количества и мощности кибератак на российские ресурсы. Основной вклад работы заключается в систематизации и детальной проработке потенциальных векторов сотрудничества. Автором предложена и всесторонне обоснована следующая категоризация таких направлений: восстановление диалога через многосторонние площадки (ООН, ОБСЕ); создание механизмов доверия и прозрачности (СВМ), включая обмен информацией об угрозах, уведомление об учениях и «горячие линии»; разработка международных норм, запрещающих атаки на критическую инфраструктуру; совместная борьба с транснациональной киберпреступностью через создание оперативных групп; участие в международных инициативах; осуществление образовательных и научных обменов. В заключение делается вывод, что, несмотря на значительный потенциал сотрудничества, в среднесрочной перспективе оно останется ограниченным вследствие фундаментального отсутствия политического доверия. Перспективы реализации предложенных векторов увязываются с необходимостью преодоления политических барьеров и общим процессом пересмотра архитектуры глобальной кибербезопасности с учетом принципа многополярности. Таким образом, работа вносит существенный вклад в понимание диалектики конфронтации и кооперации между Россией и НАТО в киберпространстве.

III. ЗАКЛЮЧЕНИЕ

В диссертационном исследовании решена научная задача и достигнута цель исследования. Научные результаты работы представлены теоретическими выводами и практическими рекомендациями. К теоретическим выводам следует отнести следующие положения.

1. Были получены фундаментальные теоретические выводы, раскрывающие сущность киберпространства и динамику международных отношений в этой сфере. Прежде всего, киберпространство – это глобальный, искусственно сконструированный, неоднородный и динамичный социотехнический континуум, возникающий в результате симбиоза

технологической инфраструктуры и человеческой деятельности. Этот феномен, характеризующийся архитектурной многоуровневостью и отсутствием четких физических границ, трансформировался из децентрализованной среды обмена информацией в принципиально новое измерение человеческой жизнедеятельности и стратегическую арену межгосударственного противоборства. При этом установлено, что отсутствие консенсуса в его определении, обусловленное теоретическими расхождениями и различиями в национальных приоритетах, оказывает дестабилизирующее воздействие на международные отношения, приводя к фрагментации правового регулирования и создавая почву для конфликтов.

2. Анализ эволюции подходов Североатлантического альянса к цифровым вызовам выявил четкую трехэтапную траекторию движения от осознания потенциальных рисков и фрагментарных оборонительных мер к комплексной военно-политической стратегии, в рамках которой киберпространство было окончательно милитаризировано и признано полноправной областью операций. Подобная трансформация, отражающая общую тенденцию милитаризации цифровой среды, однако, сталкивается с системными вызовами. К их числу относятся технологические трудности, операционные проблемы атрибуции атак и ресурсного неравенства между союзниками, а также политико-правовые противоречия, вызванные коллизией между наднациональным управлением и национальным суверенитетом. Центральное место в стратегии НАТО занимает образ России как основного источника угроз, что детерминирует конфронтационный характер мер Альянса и придает российско-натовскому киберпротивостоянию системный и взаимный характер, минимизируя перспективы полноформатного сотрудничества.

3. В этих условиях для Российской Федерации императивной необходимостью становится выработка сбалансированного и прагматичного курса. Ключевыми направлениями являются безусловное укрепление национального киберсуверенитета и обороноспособности, включая ускорение

импортозамещения в сфере критических технологий, а также последовательная и наступательная работа на дипломатическом фронте по продвижению универсальных правовых норм. В более широком теоретическом плане исследование подтверждает, что гармоничное развитие киберпространства в XXI веке требует выработки универсальных, но гибких определений и поиска баланса между государственным суверенитетом и глобальной стабильностью, что выступает необходимым условием для минимизации рисков эскалации и обеспечения устойчивости цифровой среды.

На основании представленных теоретических выводов можно сформулировать **следующие практические рекомендации и предложения,** направленные на укрепление национальной безопасности и усиление позиций Российской Федерации в киберпространстве.

В сфере обороны и безопасности первостепенной задачей является ускоренное развитие национального киберсуверенитета, что предполагает продолжение системной работы по изоляции и усилению защиты критической информационной инфраструктуры, а также наращивание собственных надежных потенциалов сдерживания, способных гарантировать неприемлемый ущерб любому потенциальному агрессору. Императивом является ускорение импортозамещения в сфере критических информационных технологий, программного обеспечения и микроэлектроники с целью нейтрализации использования Западом технологического доминирования как инструмента давления.

В связи с качественной трансформацией характера угроз представляется необходимым инициировать разработку новой Военной доктрины Российской Федерации. Этот документ должен стать не механической актуализацией, а фундаментальной стратегией, адекватной вызовам XXI века, где киберпространство официально признается одним из ключевых театров военных действий, а гибридные методы – основной формой противоборства.

На дипломатическом фронте необходима последовательная и наступательная работа по продвижению российской повестки. Целесообразно

активно продвигать инициативы по выработке универсальных правовых норм, запрещающих атаки на гражданскую и критическую инфраструктуру, что будет способствовать формированию образа России как ответственного и конструктивного актора. Параллельно следует инициировать процессы по правовой квалификации кибератак на российские объекты в качестве преступных и террористических актов, активно привлекая внимание международных организаций и широкой общественности к данным фактам для разоблачения двойных стандартов.

Что касается взаимодействия с Североатлантическим альянсом, диалог не должен рассматриваться как самоцель, но его возможные формы следует просчитывать. Россия должна быть готова к ограниченному, прагматичному взаимодействию, которое возможно лишь в строго очерченных рамках и исключительно по вопросам, представляющим взаимный интерес. К таким вопросам относятся восстановление каналов экстренной связи для предотвращения эскалации на фоне киберинцидентов, обсуждение мер доверия, таких как уведомление о крупных киберучениях, а также координация в борьбе с транснациональной киберпреступностью, не носящей политизированного характера. Любой такой диалог должен основываться на принципах прагматизма и не наносить ущерба национальной безопасности и международному имиджу страны.

Таким образом, резюмируя вышесказанное, основной путь обеспечения национальных интересов в киберпространстве лежит в сочетании курса на безусловное укрепление собственной обороноспособности и суверенитета с активной наступательной дипломатией, направленной на продвижение альтернативной, справедливой модели регулирования киберпространства. Сила и независимость остаются главными гарантами безопасности в условиях, когда цифровая сфера превратилась в новый фронт гибридного противоборства.

IV. НАУЧНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ИССЛЕДОВАНИЯ

Основные положения диссертационного исследования отражены в следующих **публикациях в изданиях, которые включены в перечень рецензируемых научных журналов Высшей аттестационной комиссии:**

1. Никитин, Н. А. Развитие возможностей использования информационно-коммуникационных технологий НАТО в военно-политических целях в контексте международной безопасности / Н. А. Никитин // Вопросы политологии. – 2025. – Т. 15, № 4(116). – С. 1467-1477. – DOI 10.35775/PSI.2025.116.4.034. – EDN DNHGZH.
2. Никитин, Н. А. Трансформация современной политики НАТО в киберпространстве / Н. А. Никитин // Евразийский Союз: вопросы международных отношений. – 2025. – Т. 14, № 4(69). – С. 970-980. – DOI 10.35775/PSI.2025.69.4.021. – EDN QVHDAN.
3. Никитин, Н. А. Основные подходы к определению понятия «киберпространство» в контексте международных отношений – отечественный опыт / Н. А. Никитин // Евразийский Союз: вопросы международных отношений. – 2025. – Т. 14, № 5(70).
4. Никитин, Н. А. Основные подходы к определению понятия «киберпространство» в контексте международных отношений – зарубежный опыт/ Н. А. Никитин // Вопросы политологии. – 2025. – Т. 15, № 6(118).