Федеральное государственное бюджетное образовательное учреждение
высшего образования «Дипломатическая академия Министерства
иностранных дел Российской Федерации»

На правах рукописи

НИКИТИН Никита Алексеевич

СОВРЕМЕННАЯ СТРАТЕГИЯ НАТО В КИБЕРПРОСТРАНСТВЕ

Специальность 5.5.4. Международные отношения, глобальные
и региональные исследования

Диссертация на соискание ученой степени
кандидата политических наук

Научный руководитель:
Иванов Олег Петрович
Доктор политических наук, профессор

Москва – 2025

Содержание

Введение

Актуальность темы исследования

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[1]. Всё более широкое распространение стали получать термины, связанные с приставкой «кибер»: кибератака, киберспорт, киберкультура, кибербезопасность, киберпространство, что в большей степени напрямую связано с всеобъемлющей имплементацией информационно-коммуникационных технологий во все без исключения сферы общественной и государственной деятельности, современную жизнь и объективную реальность.

Прежде всего, проблема обеспечения глобальной кибербезопасности утвердилась в качестве одного из наиболее актуальных вызовов последнего десятилетия, что обусловлено её прямой связью с вопросами национальной и международной безопасности. Данная актуализация является прямым следствием тотальной цифровой трансформации, характеризующейся всеобъемлющей имплементацией информационно-коммуникационных технологий во все без исключения сферы общественной и государственной деятельности. Данный процесс привел к формированию принципиально новой гибридной реальности, центральным элементом которой стало киберпространство. Как следствие, киберпространство трансформировалось в

[1] 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.

новую стратегическую арену, где традиционное геополитическое соперничество государств закономерно приобретает форму интенсивного противоборства. Данная тенденция проявляется в эскалации конфликтного потенциала и требует выработки новых моделей сдерживания и регулирования. Одновременно с этими процессами наблюдается формирование и консолидация нового концептуального аппарата, о чем свидетельствует широкое распространение терминов с приставкой «кибер-». Подобное лингвистическое явление служит индикатором глубинных структурных изменений не только в технологической сфере, но и в общественном сознании и научном дискурсе, окончательно закрепляя киберпространство как неотъемлемый компонент современной объективной реальности. Таким образом, обозначенные тенденции формируют сложный комплекс проблем, требующий комплексного междисциплинарного осмысления и разработки адекватных политико-правовых механизмов реагирования.

Так, например, по словам президента России В.В. Путина, «вопрос с кибербезопасностью является одним из самых важных на сегодняшний день, потому что всякие отключения целых систем ведут к очень тяжелым последствиям, а это оказывается возможно»[2]. За последнее десятилетие резко возросла роль ИКТ в качестве одного из наиболее эффективных средств ведения военных действий специфическими методами (кибервойна), осуществления политической и экономической разведки.

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

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

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. Специальная военная операция (СВО), начатая 24 февраля 2022 года, стала феноменом истинно мирового значения. В течение десятилетий, последовавших за распадом социалистического блока, фактически существовал однополярный мир во главе с Соединёнными Штатами и их сателлитами в рамках Североатлантического альянса. 24 февраля обозначило начало конца однополярного мироустройства. Россия начала тернистый процесс утверждения себя в качестве отдельной цивилизации, реального полюса силы, в противовес западному либеральному глобализму. В широком смысле Специальную военную операцию следует определять в качестве противостояния однополярного и многополярного типов мироустройства. В течение последних лет мы были свидетелями того, как государства-члены НАТО осуществляли планомерную накачку Украины различными видами вооружений, которая, впрочем, не прекратилась, а в разы усилилась после начала СВО, что явно свидетельствует об уже случившемся существенном обострении противоречий между Россией и коллективным Западом, представленным прежде всего НАТО. Отметим, что хотя статус России как ключевого противника Североатлантического альянса был закреплён в Стратегической концепции НАТО 2022 г., в действительности он был приписан Москве ещё в 2010-х годах[3]. Таким образом, в настоящее время

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

НАТО не только укрепляет свою роль как оборонительного союза, но и выступает в качестве центрального институционального форума для координации западной политики в условиях острого противостояния с Россией, что делает его главным участником в процессе формирования новой, более конфронтационной и биполярной конфигурации системы европейской безопасности.

В данном контексте особого внимания заслуживают конкретные примеры злонамеренного использования государствами-членами Североатлантического альянса наступательных киберсредств, направленных против России.

Уже в первый срок президентства Д. Трампа на высшем уровне имели место подтверждения использования США киберсредств против ряда российских юридических лиц. Так в интервью изданию The Washington Post упоминалась санкционированная кибератака на российское агентство по исследованию интернета в 2018 году[4], в интервью информационному каналу Fox News в 2019 году Д. Трамп еще раз подтвердил упомянутую кибератаку[5].

В 2022 году с началом Специальной военной операции вновь актуализировалась тенденция использования коллективным Западом наступательного арсенала киберсредств. Так, но мнению специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности МИД России А.В. Крутских, в 2022 г. «ударам подвергались государственные учреждения, объекты критической и социальной инфраструктуры, хранилища

---

[4] Trump confirms, in an interview, a U.S. cyberattack on Russia URL: https://www.washingtonpost.com/opinions/2020/07/10/trump-confirms-an-interview-us-cyberattack-russia/ (дата обращения: 23.08.2024).

[5] Trump appears to confirm cyberattack against Russian entity during midterms URL: https://edition.cnn.com/2019/05/19/politics/trump-confirm-cyberattack-russia-midterms/index.html (дата обращения: 23.08.2024).

личных данных наших граждан и иностранцев, проживающих в России»[6]. Согласно данным, полученным в результате мониторинга и анализа специализированными структурами, организация масштабных DDoS-атак осуществлялась злоумышленниками с привлечением так называемых «кибердобровольцев». Для развертывания вредоносного программного обеспечения и координации действий активно эксплуатировалась инфраструктура международных IT-компаний, в частности, серверные мощности провайдеров Hetzner (Федеративная Республика Германия) и DigitalOcean (Соединенные Штаты Америки). Координация противоправной деятельности и управление ею реализовывались посредством зарубежных специализированных онлайн-платформ. По состоянию на май 2022 года было установлено, что в скоординированных атаках на объекты критической информационной инфраструктуры Российской Федерации, включая инциденты, направленные против видеохостинга Rutube, принимали постоянное участие более 65 000 физических лиц с территорий США, Турции, Грузии и ряда государств-членов Европейского союза[7].

В июне 2022 г. имело место официальное подтверждение прямого участия США в осуществлении кибератак, направленных на критическую инфраструктуру Российской Федерации. Так, согласно заявлению бывшего директора Агентства национальной безопасности США, главы Кибернетического командования США генерала армии США П. Накасоне,

---

[6] Ответ специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности МИД России А.В. Крутских на вопрос СМИ об атаках на объекты российской критической инфраструктуры URL: https://mid.ru/ru/foreign_policy/news/1817019/#sel=6:1:0Sj,6:70:Taj (дата обращения: 23.08.2024).

[7] Ответ специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности МИД России А.В. Крутских на вопрос СМИ об атаках на объекты российской критической инфраструктуры URL: https://mid.ru/ru/foreign_policy/news/1817019/#sel=6:1:0Sj,6:70:Taj (дата обращения: 23.08.2024).

«военные хакеры США провели наступательные кибероперации против России в поддержку Украины»[89].

Являясь одним из ключевых компонентов системы международных отношений и мировой политики, киберпространство становится принципиально новой ареной для межгосударственного взаимодействия и регулирования, а также ожесточённого противостояния. Исследователи активно работают над изучением концепции киберпространства, рассматривая его не только с перспективы теоретического осмысления, но и места и роли явления в практической плоскости. Понятие киберпространства, ставшее ключевым в эпоху цифровой трансформации, вызывает активный интерес у исследователей по всему миру. Киберпространство, как сложный и многогранный феномен, охватывает не только технологические аспекты, но и социальные, политические, экономические и правовые измерения. Согласно Стратегии национальной безопасности Российской Федерации, утверждённой указом президента Российской Федерации от 2 июля 2021 г. № 400: «Увеличивается количество компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств. Инициативы Российской Федерации в области обеспечения международной информационной безопасности встречают противодействие со стороны иностранных государств, стремящихся доминировать в глобальном информационном пространстве; активизируется деятельность специальных служб иностранных государств по проведению разведывательных и иных операций в российском информационном пространстве. Вооруженные силы таких государств отрабатывают действия по выведению из строя объектов критической

---

[8] US confirms cyberattacks on Russia in Ukraine war URL: https://www.techmonitor.ai/technology/cybersecurity/us-russia-cyberattacks-ukraine-war (дата обращения: 23.08.2024).

[9] Белый дом подтвердил проведение «кибероперaций» против России URL: https://www.rbc.ru/politics/02/06/2022/6297d5699a7947622ed04206 (дата обращения: 23.08.2024).

информационной инфраструктуры Российской Федерации»[10]. Соответственно, появляется неиллюзорная необходимость в организации эффективного обеспечения кибернетической безопасности государств.

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[11]. Киберпространство трансформируется в 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 данного исследования обуславливается необходимостью изучения современной стратегии НАТО в киберпространстве в условиях постоянно трансформирующейся международной обстановки и структуры глобальной безопасности.

---

[10] Стратегия национальной безопасности Российской Федерации, утверждённая указом президента Российской Федерации от 2 июля 2021 года № 400

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

Исследование данной проблематики позволяет дать объективную оценку современных приоритетов Североатлантического альянса в киберпространстве и идентифицировать основные тенденции стремительно развивающейся политики обеспечения кибербезопасности.

Все перечисленное определило актуальность выбранной темы диссертационной работы.

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: Стратегические концепции НАТО 1991, 1999, 2010, 2022 гг., Заявления 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[12], Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[13], Руководящие принципы оборонной политики ФРГ 2023 г.[14], Стратегия национальной безопасности Российской Федерации, утверждённая указом

[12] Проект Концепции стратегии кибербезопасности Российской Федерации URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf: (дата обращения: 01.08.2024).
[13] Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. - 2016. - № 50.- Ст. 7074.
[14] BMVg. (2023). German Cyber Security Strategy.

президента Российской Федерации от 2 июля 2021 года № 400[15], Стратегия кибербезопасности Великобритании на 2022-2030 годы[16], Национальная стратегия кибербезопасности США 2023 г.[17], бюджет Правительства США за 2023 фискальный год[18], План единой сети армии США, позволяющий проводить многодоменные операции[19], План реализации национальной стратегии кибербезопасности США 2023 г.[20], План реализации национальной стратегии кибербезопасности США 2024 г[21].

– Третья группа источников включает зарубежные аналитические материалы, посвящённые рассматриваемым в исследовании проблемам: аналитический доклад «10 лет мерам ОБСЕ по укреплению доверия в области кибербезопасности и ИКТ»[22], аналитический доклад Киберугрозы и НАТО-2030: обзор и анализ[23], аналитический отчёт Медиация и искусственный интеллект: заметки о будущем разрешения международных конфликтов[24].

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

---

[15] Стратегия национальной безопасности Российской Федерации, утверждённая указом президента Российской Федерации от 2 июля 2021 года № 400

[16] UK Government. (2022). National Cyber Strategy 2022–2030.

[17] US National Cybersecurity Strategy 2023.

[18] White House. (2023). Budget of the U.S. Government.

[19] 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).

[20] White House. (2023). National cybersecurity strategy implementation plan

[21] White House. (2024). National cybersecurity strategy implementation plan

[22] 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).

[23] 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).

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

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[25][26], М.В. Мишустина[27], С.В. Лаврова[28].

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»[29], «Мировая политика в фокусе современности»[30], «XXI век: Перекрестки мировой политики»[31], «Современный мир и геополитика»[32], «Новая эпоха международной безопасности»[33], «Международная политика и

---

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

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

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

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

[29]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.

[30] 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.

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

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

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

безопасность: новые контуры современного мира»[34], посвященные актуальным проблемам в современной системе международных отношений и внешней политике, исследования отечественного экспертного сообщества: Д.Ю. Базаркиной[3536], В.Г. Барановского[37], А.А Бартоша[38], И.В. Болговой[39], М.А. Везуиной[40], С.И. Грачева[41], Д.А. Данилова[424344], О.П. Иванова[454647], И.А.

---

[34] 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.

[35] 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.

[36] 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.

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

[38] 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).

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

[40] 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).

[41] 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.

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

[43] 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.

[44] 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.

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

[46] 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.

[47] 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.

Истомина[48], И.А. Кочина[49], Д.В. Луешкина[50], Е.А. Михалевича[51], Ю.И. Надточей[52535455], В.Н. Панина[5657], Е.Н. Пашенцева[58], О.И. Ребро[59], Н.Г.

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

[49] 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).

[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] 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.

[52] 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).

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

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

Самойлова[60], А.А. Синдеева[61], А.А. Сушенцова[62], В.С. Чикальдиной[63], А.Г. Шляхтунова[6465], Д. А. Ясковича[66], работы зарубежных учёных и экспертов: Р. Бёрнса[67], З. Бжезинского[68], Ф. Гейсбурга[69], Я.А. Зепоса[70], Д. Муравчика[71], доклад Картина нарождающегося мира: базовые черты и тенденции[72].

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[73], Э.Л.

---

[60] 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.

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

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

[63] 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.

[64] 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).

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

[66] Яскович Д.А. Эволюция стратегических концепций нато в постсоветский период: формирование стратегии продвижения на Восток // Манускрипт. 2017. №7 (81). URL: https://cyberleninka.ru/article/n/evolyutsiya-strategicheskih-kontseptsiy-nato-v-postsovetskiy-period-formirovanie-strategii-prodvizheniya-na-vostok (дата обращения: 22.01.2022).

[67] 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).

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

[69] 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.

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

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

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

[73] 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.

Ансельмо[74], Э. Араб-Оглы[75], Д. Арквиллы[76], Т.В. Барановой[77], И.Р. Бегишева[78], М.М. Безкоровайного[79], В.Е. Воскресенской[80], Д. Белла[8182], М. Бенедикта[8384], Т. Бёрнерса-Ли[8586], Д. Бетца, С.В. Бондаренко[87], С.С. Булгакова[88], А.Е.

[74] 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.

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

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

[77] 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.

[78] 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

[79] 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).

[80] 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.

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

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

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

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

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

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

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

[88] 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).

Войскунского[89], А.Г. Волова[90], У. Гибсона[9192], А.А. Данельяна[93], В.В. Денисовича[94], Д.Е. Добринской[95], П.В. Закалкина[9697], С.А. Иванова[9899], М. Кастельса[100], Л. Келло[101], Б. Коллина[102], В.В. Коровкина[103], А.В. Крутских[104],

[89] Войскунский А.Е. Метафоры интернета // Вопросы философии. 2001. № 11. С. 64–79.
[90] 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).
[91] Gibson W. Burning Chrome // Omni. 1982. July. URL: https://omni.media/omnimagazine-july-1982 (accessed: 15.07.2024).
[92] Gibson W. Neuromancer. N.Y., 1984.
[93] 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).
[94] 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
[95] Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского Университета. Сер. 18. Социология и политология. 2018. Т. 24. № 1. С. 52—70.
[96] 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).
[97] 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.
[98] 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.
[99] 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.
[100] Castells, M. (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford University Press.
[101] Kello, L. (2017). The Virtual Weapon and International Order.
[102] Collin B. The Future of Cyberterrorism // Crime & Justice International Journal. — 1997. — Vol. 13. — Вып. 2.
[103] 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).
[104] 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

П. Кузнецова[105], С.В. Куликова[106], В.И. Курбатова[107], С.И. Макаренко[108], Д. Липтона[109], С. Лэша[110], Д. Ная[111], Т. О'ОРайли[112], О.М. Папа[113], А.А. Пасса[114], Е.Н. Пашенцева[115], М.А. Петлина[116], А.Н. Позднякова[117], Т.В. Радченко[118], Х.

[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] 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.

[107] 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.

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

[109] Lipton J. Rethinking Cyberlaw: A New Vision for Internet Law.-Edward Elgar Publishing, 2015, 176 p.

[110] Lash S. Critique of information. L., 2002. P. 15.

[111] Nye, J. S. (2010). Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School.

[112] O'Reilly, T. (2005). "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software"

[113] 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.

[114] 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

[115] 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.

[116] 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).

[117] 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).

[118] 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).

Рейнгольда[119], Д. Ронфельда[120], М.И. Рыхтика[121122], Р.А. Сабитова[123], К. Сагана[124], П. Саймона[125], А.В. Скоробогатова[126], Е. Соджи[127], Ю.И. Стародубцева[128], Т. Стивенса[129], А.Л. Татузова[130], Л.В. Тереньевой[131], М.А. Федотова[132], В.А. Цвыка[133], К.В. Шевелевой[134], С.С. Ширина[135].

---

[119] Rheingold, H. (1993). The Virtual Community: Finding Connection in a Computerized World.

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

[121] 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.

[122] 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.

[123] 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

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

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

[126] 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

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

[128] 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).

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

[130] 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).

[131] 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).

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

[133] 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.

[134] 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).

[135] Ширин С.С. Всемирная паутина как объект исследования в политической науке // Вестник Санкт-Петербургского университета. Международные отношения. 2013. №2. URL:

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 безопасности: Е.А. Антюховой[136], Н.А. Баранова[137], Д. Блэка[138], Ю.В. Бородакия[139], Л. Брента[140], И.В. Бутусова[141], Л. Вихула[142][143], М. Галеотти[144], Ф. Гейди[145], Ю.Е. Горбачевой[146], Т.А. Гришаниной[147], А.Ю. Добродеева[148], П.В.

---

https://cyberleninka.ru/article/n/vsemirnaya-pautina-kak-obekt-issledovaniya-v-politicheskoy-nauke (дата обращения: 14.08.2024).

[136] 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).

[137] 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).

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

[139] 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.

[140] 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)

[141] 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.

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

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

[144] Galeotti, M. (2016). Hybrid War or Gibridnaya Voina? Small Wars Journal.

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

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

[147] 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).

[148] 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[149][150], С.А. Иванова[151][152], Л. Илвса[153], Н.В. Кардавы[154], О.Г. Карповича[155], Ф. Киллуфо[156], А. Климбурга[157], Н.П. Кобца[158], Ю.А. Кожанова[159], Е.С. Коренева[160], П. Котлера[161], А. Линча[162], Д. Лиона[163], Д.

[149] 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.

[150] 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.

[151] 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.

[152] 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.

[153] 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

[154] 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).

[155] 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.

[156] 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

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

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

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

[160] 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).

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

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

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

Маккарти[164], А.Н. Маловой[165], А.В. Манойло[166], М. Мински[167], А. Надау[168], И.Н. Панарина[169], С.А. Паршина[170], А.Ю. Поволотцкого[171], П.В. Попова[172], Т.А. Романовой[173], Н. Рочестера[174], М. Рустада[175], И.С. Семененко[176], П.

[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] 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).

[166] 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).

[167] 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

[168] 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

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

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

[171] 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).

[172] 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).

[173] 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).

[174] 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

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

[176] 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[177], М.В. Смекаловой[178], А.С. Соколова[179], Ю.И. Стародубцева[180][181], А. Стронелла[182], И.В. Сурмы[183], А.И. Ходанова[184], Н.А. Цвековой[185], В.А. Чебыкиной[186], Р.Н. Шангараева[187], М. Шмитта[188][189], Т. Эванса[190].

---

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

[178] 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).

[179] 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).

[180] 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.

[181] 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.

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

[183] 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.

[184] 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).

[185] 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.

[186] 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.

[187] 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.

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

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

[190] 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. Методологический аппарат исследования включает историко-хронологический подход, который позволил выделить три качественно различных этапа в эволюции киберстратегии НАТО: от первых фрагментарных мер в 1990-х годах через систематизацию подходов в 2000-х к полномасштабной милитаризации киберпространства в последнее десятилетие. Институциональный анализ помог проследить становление специализированных структур альянса, от первоначального Computer Incident Response Capability до современных Центров кибероперaций. Сравнительный метод выявил различия в подходах ключевых членов НАТО, особенно между централизованной американской и более децентрализованной европейской моделями кибербезопасности. Детальное изучение ключевых документов НАТО – от решений Пражского саммита 2002 года до Стратегической концепции 2022 года – позволило выявить эволюцию официальной позиции Североатлантического альянса по вопросам кибербезопасности. Междисциплинарный характер исследования проявляется в сочетании политического анализа с элементами международного права

(касательно вопросов легитимности применения статьи 5 Вашингтонского договора к кибератакам) и современных информационных технологий (касательно влияния искусственного интеллекта и квантовых вычислений на стратегию кибероборонны). Подобный комплексный подход не только позволил реконструировать процесс трансформации стратегии НАТО в киберпространстве, но и создал основу для прогнозирования её дальнейшего развития в условиях нарастающей технологической конкуренции и геополитической конфронтации.

При написании диссертационного исследования автор руководствовался принципами научности, системности, логической последовательности, достоверности, объективности и верифицируемости.

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.

Научные статьи в изданиях, включенных в перечень ВАК РФ для публикации диссертационных исследований по научной специальности 5.5.4 «Международные отношения, глобальные и региональные исследования»:

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).

Глава 1. Научные подходы к определению понятия «киберпространство»

1.1 Подходы отечественных исследователей к определению понятия «киберпространство»

Сегодня, в условиях стремительного развития технологий, которые всецело затрагивают все аспекты человеческой жизнедеятельности, всё большую важность приобретает понятие «киберпространство». Как отечественные, так и зарубежные исследователи активно работают над изучением концепции киберпространства, рассматривая его не только с перспективы теоретического осмысления, но и места и роли явления в практической плоскости.

В течение последнего десятилетия всё более широкое распространение стали получать термины, связанные с приставкой «кибер»: кибератака, киберспорт, киберкультура, кибербезопасность, киберпространство, что в большей степени напрямую связано со всеобъемлющей имплементацией информационно-коммуникационных технологий во все без исключения сферы общественной и государственной деятельности, современную жизнь и объективную реальность[191]. Практически ежедневно среднестатистический человек сталкивается с морфемой «кибер», чаще всего в негативном контексте ввиду экспоненциального роста злонамеренной деятельности в интернет-пространстве как в России, так и за рубежом. Говоря о растущей роли киберпространства в мировой политике, отметим, что тема международной информационной безопасности (МИБ) активизировалась относительно недавно. И ключевая роль в осмыслении новых реалий в мировой политике принадлежит именно России. По словам профессора А.В. Крутских: «Российская Федерация 2 сентября 1998 г. продемонстрировала характерный

[191] 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).

для её политического мышления стратегический подход к осмыслению процессов на мировой арене и первой призвала международное сообщество заблаговременно договориться и предпринять практические меры, чтобы не допустить превращения нарождающегося «киберджина в Армагеддон»»[192].

Говоря об истоках доктринального оформления определений к понятиям «киберпространство», «кибербезопасность», целесообразно опереться на определение термина «кибернетика». Сам термин «киберпространство» возможно рассматривать в качестве греко-латинской комбинации, согласно Оксфордскому словарю английского языка, морфема «cyber» происходит от греческого слова κυβερνήτες (дословно – правители)[193]. «Кибернетика» (от греч. «искусство управления») – наука об общих закономерностях процессов управления и передачи информации в машинах, живых организмах и обществе[194]. Отметим, что абстрактная кибернетическая система представляет собой совокупность взаимосвязанных объектов, именуемых элементами системы, которые способны воспринимать, сохранять и обрабатывать информацию, а также обмениваться ею. По мнению французского математика и физика А-М. Ампера, кибернетика является наукой об управлении государством, занимая положение между дипломатией и теорией власти[195]. В данном случае к области кибернетики можно отнести все современные информационно-коммуникационные технологии. Ключевым аспектом является то, что в рамках кибернетического подхода элементы системы рассматриваются как постоянно взаимодействующие между собой, а люди,

---

[192] 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

[193] Oxford dictionary of English. Oxford, 2010

[194] Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. – 4-е изд. – М., 1997.

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

как активные участники обмена информацией и использования информационных ресурсов, играют важную роль в киберпространстве[196].

Понятия «кибернетика» и «киберпространство» тесно связаны между собой, поскольку оба эти термина касаются взаимодействия и обработки информации, однако они охватывают различные аспекты этого взаимодействия. Кибернетика, как наука, изучает процессы управления и связи в сложных системах, акцентируя внимание на таких аспектах, как анализ информации, процессы обратной связи и моделирование. Основное внимание в кибернетике уделяется тому, как различные элементы системы взаимодействуют друг с другом для достижения определенных целей, будь то механизмы, организмы или социальные структуры. Кибернетика применима в самых разных областях, от инженерии до социологии, и предоставляет инструменты для понимания динамики и функционирования систем в целом. Киберпространство, в свою очередь, представляет собой виртуальную среду, образованную благодаря сети информационных технологий и коммуникаций. Это понятие чаще всего связано с интернетом и другими сетевыми ресурсами, где происходит обмен данными, взаимодействие пользователей и функционирование различных информационных платформ. Киберпространство охватывает различные аспекты цифровой жизни, включая социальные медиа, электронную коммерцию и онлайн-коммуникации. Связь между кибернетикой и киберпространством проявляется в том, что кибернетические принципы могут быть использованы для анализа и управления процессами, происходящими в киберпространстве. Например, кибернетические модели могут помочь в понимании динамики сетевых взаимодействий, алгоритмов, управляющих потоками информации, а также в разработке решений для обеспечения безопасности в цифровой среде. Таким образом, кибернетика предоставляет теоретическую и методологическую

[196] 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).

базу, необходимую для более глубокого понимания и эффективного управления многогранной и постоянно развивающейся структурой киберпространства.

В современном понимании кибернетика является наукой о процессах управления, передачи информации и коммуникациях в сложных динамических системах (технических, компьютерных, биологических, нейронных, социальных). Теоретической основой кибернетики являются достижения многих научных дисциплин, среди которых особое место занимают математические науки и логика, биологические науки, разработка автоматизированных средств управления и т.д.[197]. В парадигме стремительного развития информационно-коммуникационных технологий, компьютерных систем был дан новый толчок эволюции кибердискурса, который в свою очередь интенсифицировал процесс появления и имплементации принципиально новых понятий и терминов, обозначающих распространение компьютерно-опосредованной коммуникации. Сегодня префикс «cyber» (кибер), обозначающий связь с сетями электронных коммуникаций и виртуальной реальностью[198], определяется преимущественно как современная механическая технология[199]. Среди ключевых характеристик, применяемых к киберпространству целесообразно выделить следующие: наличие единого характера, неделимость, несводимость к границам физического пространства, их подвижность и изменчивость[200], отсутствие

---

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

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

[199] 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).

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

однозначной географической определенности[201], трансграничность, многомерность и отсутствие линейности, протяженности, физических параметров[202]. Необходимо отметить, что ввиду отсутствия законодательного оформления понятия «киберпространство» при определении его содержательных характеристик остаётся использовать научную доктрину.

Стремительная интенсификация имплементации современных технологий во все сферы человеческой жизнедеятельности подчёркивает необходимость методологического определения понятия ««киберпространство». Первостепенно необходимо определить общие подходы к пониманию терминов в сочетании с ключевыми точками зрения и подходами отечественных исследователей.

Представляя собой некую совокупность виртуальных систем, физических объектов, программного обеспечения и сервисов, а также аппаратных средств, киберпространство охватывает все без исключения глобальные и локальные компьютерные сети вне зависимости от их принадлежности, отдельных свойств и характеристик, включая информационно-коммуникационную сеть Интернет, которая будучи глобальной системой взаимосвязанных компьютерных сетей, использующей набор интернет-протоколов для связи между сетями и устройствами является наиболее известным, если не единственным примером такой сети, известной для обывателей. Однако чрезвычайно важно подчеркнуть, что киберпространство выходит далеко за рамки понятия Интернета, охватывая бесчисленное множество обособленных и взаимосвязанных структур, систем и сетей[203].

---

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

[202] 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.

[203] 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).

Научно-исследовательский анализ киберпространства позволяет установить его существенные критерии:

- единый характер: киберпространство невозможно разграничить или кластеризовать ввиду его природы, оно существует вне физического пространства и является неделимым[204];

- отсутствие однозначного географического определения: в отличие от физических объектов с четко определенными координатами и границами, киберпространство выходит за рамки этих величин, существуя трансгранично и многомерно;

- отрицание линейной структуры и иных физических параметров[205];

- глобальное распространение: сеть Интернет объединяет весь мир, существенно упрощает и способствует глобальному обмену информацией[206].

Для всецелого понимания теории и практики имплементации киберсредств как в парадигме современной системы международных отношений, так и в контексте международной безопасности, первостепенно необходимо идентифицировать ключевые подходы отечественных учёных к определению термина «киберпространство».

По мнению авторского коллетива Стародубцева Ю.И., Иванова С.А., Закалкина П.В, киберпространство – «искусственное неоднородное технологическое пространство с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, оно функционирует в интересах множества разнородных, в том числе антагонистических систем управления, при этом свойства

---

[204] 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

[205] 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).

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

киберпространства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей»[207][208].

Объединение элементов киберпространства позволяет определить его физическую структуру. С функциональной точки зрения, элементами киберпространства, образующими его физическую структуру, являются:

1. Искусственная и естественная среда распространения сигналов;

2. Средства каналообразования;

3. Средства распределения ресурсов киберпространства (маршрутизаторы, коммутаторы и т.д.);

4. Средства измерения и сбора первичных характеристик элементов киберпространства и обрабатываемого трафика;

5. Вычислительные средства хранения и комплексной обработки первичных данных;

6. Средства разграничения и защиты информационных ресурсов (в том числе: средства аутентификации и идентификации);

7. Средства управления фрагментами киберпространства и (или) их функциями;

8. Средства хранения и обработки информационных ресурсов;

9. Автоматизированные источники и потребители информационных ресурсов (IoT, АСУ ТП, роботы и т.д.);

10. Средства определения навигационных данных;

11. Устройства коммуникационного сопряжения информационных потребностей человека и возможностей киберпространства[209].

---

[207] 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.

[208] 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.

[209] Стародубцев Ю.И., Закалкин П.В., Иванов С.А. СТРУКТУРНО-ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ КИБЕРПРОСТРАНСТВА // Вопросы кибербезопасности. 2021. №4 (44). URL:

По мнению профессора Дипломатической академии МИД России А.А. Данельяна, ввиду отсутствия единого определения понятия, «в научной литературе киберпространство достаточно часто ошибочно ассоциируется с Интернетом»[210]. Интернет, будучи технической основой, не может полностью отражать сложность киберпространства как социального феномена, он служит инфраструктурной основой, но киберпространство выходит за её пределы, включая, например, виртуальную реальность и киберфизические системы. Данная ошибочная ассоциация зачастую связана с отсутствием единого определения понятия «киберпространство». Целесообразно отметить, что ошибочная ассоциация термина «киберпространство» исключительно с интернетом приводит к упрощённому пониманию его сущности.

Отсутствие единого понимания термина «киберпространство» и его смешение с понятием «Интернет» создают значительные сложности в сфере международных отношений и глобальной безопасности. Подобная неоднозначность влияет на формирование правовых норм, стратегий кибербезопасности и механизмов международного сотрудничества, что может привести к таким последствиям как ошибочная атрибуция атак. Если одни страны воспринимают киберпространство как синоним Интернета, а другие включают в него военные и инфраструктурные системы, это может привести к неверной интерпретации действий оппонентов. Например, хакерская атака на гражданскую инфраструктуру может быть расценена как акт кибервойны, даже если изначально не носила военного характера. Более того, различия в трактовках киберпространства могут существенно затруднить процесс разработки единых стандартов и имплементации глобальных инициатив[211].

---

https://cyberleninka.ru/article/n/strukturno-funktsionalnaya-model kiberprostranstva (дата обращения: 02.01.2025).

[210] 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).

[211] 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).

По мнению доктора социологических наук директора Центра прикладных исследований интеллектуальной собственности С.В. Бондаренко, киберпространство представляет собой сложную социотехническую систему, которая включает в себя не только информационные сети, но и социальные практики, культурные коды и виртуальные взаимодействия[212]. Автор подчёркивает, что интернет служит инфраструктурной основой, но киберпространство выходит за её пределы, включая, например, виртуальную реальность и киберфизические системы. Интернет, будучи технической основой, не может полностью отражать сложность киберпространства как социального феномена.

Существенный вклад в исследование феномена сетевых онлайн-сообществ, помимо С.В. Бондаренко, принадлежит исследователям В.И. Курбатову, Р.В. Кончаковскому, Л.Ш. Крупенниковой, С.В. Куликову и О.М. Папа.

Р.В. Кончаковсккий интерпретирует интернет не только в качестве социальной технологии, но и как автономную сферу жизнедеятельности, оказывающей трансформирующее воздействие на социальную реальность. В рамках социокультурного подхода автор исследует сетевое интернет-сообщество, концептуализируя его как логико-смысловое единство, продуцирующее специфический ценностно-нормативный контекст[213]. Исследователи В.И. Курбатов, С.В. Куликов и О.М. Папа в анализе онлайн-сообществ опираются на методологию социального конструктивизма, применяя методы структурного и функционального анализа. Согласно их выводам, данные сообщества репрезентируют принципиально новый тип социальности и участвуют в формировании информационного социума[214].

---

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

[213] Кончаковский, Р.В. (2010). Сетевое интернет-сообщество как социокультурный феномен. [Автореф. дис. … канд. социол. наук. Урал. гос. ун-т им. А.М. Горького]. Электронный научный архив УрФУ. https://elar.urfu.ru/ handle/10995/3102

[214] Курбатов, В.И., Куликов, С.В., Папа, О.М. (2018). Сетевые онлайн сообщества: факторы самоуправления в формировании цифрового гражданского общества. Гуманитарные,

Кроме того, зарубежные авторы, такие как М. Кастельс, подчёркивают, что киберпространство является «новой формой пространства, которая возникает в результате взаимодействия цифровых технологий и человеческой деятельности»[215]. Подобное мнение поддерживается в работах российских исследователей, которые рассматривают киберпространство как среду, где физическое и виртуальное переплетаются. Таким образом, ошибочная ассоциация термина «киберпространство» исключительно с интернетом приводит к упрощённому пониманию его сущности.

По мнению ведущего научного сотрудника кафедры общей психологии факультета психологии МГУ имени М.В. Ломоносова А.Е. Войскунского, киберпространство, или пространство Интернета, опирается одновременно на продукты информационных технологий и на социальные сервисы, являющиеся полем специфического поведения человека[216]. Исследователь сравнивает киберпространство с картой, причем весьма специфической. Ключевой особенностью этой «карты» является фрагментированность оной, её никогда не возможно увидеть целиком, напротив, для стороннего наблюдателя раскрывается лишь её определённая часть. При этом ключевой особенностью данного киберпространства в понимании А.Е. Войскунского является практическая возможность взаимодействовать с данной «картой» в любой произвольной точке, так как она располагает «множеством входов». По мнению ученого, «киберпространство подразумевает наличие некоего мира, обладающего протяженностью и метрикой, и представленного в сознании – вполне возможно, в сознании разных людей представленного по-разному»[217].

По мнению главного научного сотрудника Центра новых вызовов и угроз Института актуальных международных проблем Дипломатической

социально-экономические и общественные науки, 12. Взято 05 сентября 2020, с https://cyberleninka.ru/article/n/setevye-on-laynsoobschestva-faktory-samoupravleniya-v-formirovanii-tsifrovogo-grazhdanskogoobschestva

[215] Castells M. The Rise of the Network Society. — Wiley-Blackwell, 2010. — 656 p.

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

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

академии МИД России профессора Е.Н. Пашенцева, «новые технологии открывают и новые возможности для ведения информационно-психологического противоборства на национальном, региональном и глобальном уровнях. Тот, кто наиболее эффективно использует эти технологии, может получить решающее преимущество для победы над противником, обладающим равным или даже большим военно-экономическим потенциалом»[218]. Таким образом, становится очевидным усиление роли киберпространства и информационно-коммуникационных технологий в современной системе международных отношений и мировой политики.

Говоря о доктринальном оформлении понятия «киберпространство», первостепенно целесообразно обратиться к отечественным нормативно-правовым актам и их проектам. Так, в 2010 году был выпущен проект Концепции стратегии кибербезопасности Российской Федерации, который так и не был принят. В проекте Стратегии киберпространство рассматривается как «определенный, имеющий четкие границы элемент информационного пространства». Подобный подход согласуется с положениями международных стандартов, которые дают определения терминам из сферы информационной безопасности и устанавливают их соотношение». В качестве же определения термина даётся следующее объяснение: «киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации,

[218] Мировая политика в фокусе современности: к перспективам выхода из глобального кризиса: монография / отв. ред. М. А. Неймарк; Дипломатическая академия МИД России. — 4-е изд., перераб. и доп. — Москва: Издательско-торговая корпорация «Дашков и К°», 2023. — 509 с.

государства)»[219]. Несмотря на отсутствие в России действующих нормативно-правовых документов с названием «киберпространство», в Доктрине информационной безопасности Российской Федерации, утверждённой Указом Президента РФ от 5 декабря 2016 г. № 646, представлен термин «информационная сфера», который определяется в качестве «совокупности информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений»[220].

Целесообразно отметить, что российское законодательство предпочитает использовать более конкретные термины, такие как «информационная сфера», «информационная безопасность» или «информационно-телекоммуникационные сети». Это связано с тем, что термин «киберпространство» имеет философские и социотехнические корни, которые делают его слишком абстрактным для правового регулирования. Вместо этого отечественное законодательство фокусируется на конкретных объектах и процессах, таких как информация, сети связи и информационные системы. В свою очередь термин «информационная сфера» в российском законодательстве можно рассматривать как аналог «киберпространства», но с акцентом на регулируемость и безопасность. В то время как «киберпространство» часто ассоциируется с глобальными, трансграничными процессами и виртуальными средами, «информационная сфера» в отечественном понимании имеет более чёткие границы и привязку к национальным интересам, являясь более узким понятием, связанным с

---

[219] Проект Концепции стратегии кибербезопасности Российской Федерации URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf: (дата обращения: 01.08.2024).

[220] Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. - 2016. - № 50.- Ст. 7074.

законодательно контролируемыми объектами: сетями, данными и субъектами их обработки. В отечественной трактовке упор делается на защиту от внешнего вмешательства, что проявляется в законах о суверенном интернете и запрете иностранного контроля над критической инфраструктурой[221].

Таким образом, необходимо отметить, что научно-исследовательский анализ киберпространства позволяет установить следующие критерии, применимые к термину: единый характер, отсутствие однозначного географического определения, отрицание линейной структуры и иных физических параметров, глобальное распространение. Киберпространство представляет собой некую совокупность виртуальных систем, физических объектов, программного обеспечения и сервисов, а также аппаратных средств, киберпространство охватывает все без исключения глобальные и локальные компьютерные сети вне зависимости от их принадлежности, отдельных свойств и характеристик, включая интернет, который будучи глобальной системой взаимосвязанных компьютерных сетей, использующей набор интернет-протоколов для связи между сетями и устройствами, является наиболее известным примером такой сети.

1.2 Подходы зарубежных исследователей к определению понятия «киберпространство»

Говоря о первостепенных истоках определения понятия «киберпространство» в зарубежном научном дискурсе, стоит отметить, что впервые данный термин появился в научной фантастике 1980-х гг.[222], а в последствии был введён в научный оборот с целью описания усиления

[221] 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).
[222] Benedikt M. Cyberspace: Some Proposals // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press,1991 b. – P. 120–138.

тенденции глобального информационного обмена с помощью компьютерных сетей и устройств.

Учитывая необходимость идентификации ключевых подходов зарубежных исследований к определению понятия киберпространство, важно отметить отсутствие его единого универсального определения. Так, по мнению американского астронома, астрофизика и популяризатора науки К. Сагана, современное общество, всецело зависимое от развития науки и современных технологий, пронизывающих все без исключения сферы его деятельности, едва ли имеет целостное представление об этом понятии[223].

С началом стремительного развития интернет-технологий, повсеместного распространения компьютерного оборудования и его практической имплементации во все сферы общественной деятельности, термин «киберпространство» нашёл своё практическое применение. Сложно переоценить влияние на общество, которая оказала всемирная паутина (World Wide Web, WWW), являясь крупнейшим информационным объектом, созданным человеком за всю историю[224]. По мнению испанского социолога-постмарксиста М. Кастельса, появление всемирной паутины послужило толчком для возникновения некоего «коммуникационного гибрида», сводящего воедино места в физическом пространстве и киберпространстве[225].

Прежде всего следует подчеркнуть, что киберпростанство неразрывно связано с «сетью Интернет», являющейся не менее дискуссионным термином. Интернет определяется с точки зрения его технической характеристики как общемировая взаимосвязанная веб-сеть, глобальная паутина, объединяющая сети с использованием двух протоколов: Transmission Control Protocol (TCP), или «протокол управления передачей»; и Internet Protocol (IP), или «протокол

---

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

[224] 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).

[225] Кастельс М. Галактика Интернет. Екатеринбург, 2004.

интернета»[226]. Исходя из упомянутых характеристик необходимо более детально рассмотреть функцию данных протоколов. Так, TCP, являющийся первым уровнем доставления информации до конечного пользователя глобальной сети, обеспечивает сбор данных в меньшие по объёму группы, называемые «пакетами», а второй уровень – IP обеспечивает непосредственную доставку данных конкретному адресату[227].

За каждым пользователем всемирной паутины закрепляется уникальный IP адрес, который представляет собой цифровую комбинацию, являющуюся идентификатором устройства, и соответственно, пользователя Интернета. При этом необходимо сделать отступление, касающееся дифференциации IP на два типа: статический IP адрес и динамический IP адрес. Первый тип характеризуется присвоением пользователю постоянного IP-адреса в сети Интернет и закрепляется за MAC-адресом (от англ. Media Access Control – контроль доступа к среде, также Hardware Address, также физический адрес) – уникальный идентификатор, присваиваемый каждой единице сетевого оборудования или некоторым их интерфейсам в компьютерных сетях) оборудования. То есть IP при каждом переподключении к сети не меняется. Динамический IP-адрес постоянно изменяется, поэтому нельзя определить, что за устройство используется. Особенно активно он распространен в домашних сетях, когда не требуется четкая идентификация сервера.

Для управления и контроля различных IP адресов по всему миру в 1988 г. в США была создана некоммерческая организация Администрация адресного пространства Интернета (Internet Assigned Numbers Authority, IANA), благодаря которой произошло общемировое распространение употребления термина «Интернет»[228].

---

[226] Rustad M.L. Global Internet Law in a Nutshell//West Academic Publishing, 2013.-525p.-P.12
[227] Shacklett M.E., Novotny A., Gerwig K. TCP/IP//. [Электронный ресурс]: https://www.techtarget.com/searchnetworking/definition/TCP-IP (дата обращения: 03.01.2025).
[228] Internet Assigned Numbers Authority. [Электронный ресурс]: https://www.iana.org/ (дата обращения: 03.01.2025).

Резюмируя хронологический процесс возникновения и развития сети Интернет от момента его возникновения до сегодняшнего дня следует отразить 4 ключевых этапа: Web 1.0, Web 2.0, Web 3.0, Web 4.0.

Web 1.0, часто рассматриваемый как первая версия Интернета, охватывает период с конца 1980-х до начала 2000-х годов, когда веб-сайты в основном представляли собой статические страницы, содержащие текстовую и графическую информацию без возможности интерактивного взаимодействия. Пользователи в основном выступали в роли пассивных потребителей контента, а создание и размещение информации осуществлялось ограниченным числом разработчиков. Web 1.0 был ориентирован на публикацию информации, что способствовало формированию базовой структуры для дальнейшего развития интернета, но ограничивало возможности пользователей по взаимодействию с контентом[229].

Web 2.0 обозначает эволюцию интернета, в которой акцент смещается на интерактивность и пользовательский контент. В этой модели пользователи становятся активными участниками, создавая и делясь контентом через социальные медиа, блоги. Web 2.0 характеризуется такими принципами, как участие, сотрудничество и открытость, что значительно изменяет динамику взаимодействия между пользователями и платформами[230].

Web 3.0, также известный как «семантический веб», представляет собой следующую стадию развития Интернета, в которой акцент делается на автоматизацию обработки данных и улучшение взаимодействия между людьми и машинами с помощью технологий искусственного интеллекта и машинного обучения. Web 3.0 стремится сделать информацию более доступной и понятной для машин, что позволит создавать более интеллектуальные и персонализированные веб-приложения, способные обрабатывать и анализировать большие объемы данных[231].

---

[229] Berners-Lee, T. (1999). "The World Wide Web: A Very Short Personal History"
[230] O'Reilly, T. (2005). "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software"
[231] Berners-Lee, T. (2001). "The Semantic Web: A New Form of Web Architecture"

Web 4.0, концепция, находящаяся на стадии активного обсуждения, предполагает создание «интернета вещей» и интеграцию технологий, таких как виртуальная и дополненная реальность, что приведет к более глубокому взаимодействию между пользователями и цифровыми платформами. В этой модели акцент делается на создание адаптивных и контекстуально осведомленных систем, способных предугадывать потребности пользователей и обеспечивать более высокий уровень персонализации. Web 4.0 может кардинально изменить подходы к маркетингу и взаимодействию с клиентами, предоставляя новые возможности для бизнеса и пользователей[232].

Идентифицировав ключевые характеристики «сети Интернет», следует обратиться к истории возникновения термина «киберпространство» с перспективы зарубежного исследовательского сообщества.

Для полноценного определения и систематизации подходов зарубежных исследователей к определению понятия киберпространство целесообразно определить ключевые опорные точки в хронологии развития имплементации основных составных элементов киберпространства, включая сеть «Интернет».

Впервые тему киберпространства затронул американо-канадский писатель фантаст У. Гибсон в своём рассказе «Сожжение Хром», опубликованном в июльском номере журнала Omni в 1982 г[233]. В своих последующих литературных работах У. Гибсон активно использует термин «киберпространство», также планомерно внедряя передовые для эпохи понятия как «матрица», «виртуальная реальность», «искусственный интеллект». Особое внимание сыскал роман писателя «Нейромант», опубликованный в 1984 г. У. Гибсон описывает киберпространство как среду «чувственных галлюцинаций, испытываемых ежедневно миллиардами операторов всех наций, в том числе и детей, изучающих математические науки… Графическое отображение данных компьютеров, принадлежащих

[232] Kotler, P. (2019). "Marketing 4.0: Moving from Traditional to Digital"
[233] Gibson W. Burning Chrome // Omni. 1982. July. URL: https://omni.media/omnimagazine-july-1982 (accessed: 15.07.2017).

людям. Немыслимая сложность. Потоки света, упорядоченные человеческим разумом, скопления и созвездия информации»[234]. Таким образом, работы У. Гибсона оказали существенное влияние на формировании в общественном сознании тех годов базового представления понятия «киберпространство»[235][236].

Так как в 80-х годах XX века отсутствовала практическая возможность полноценного применения понятий «матрица», «виртуальная реальность», «искусственный интеллект» и ввиду обладания киберпространством таких специфических отличительных черт как виртуальность, представление о нем на данном этапе могло быть сформировано лишь в литературе.

В данной парадигме ключевым временным периодом в контексте развития киберпространства принято считать 90-е годы XX века, именно тогда возникла Всемирная «паутина» (World Wide Web, WWW) в современном её понимании. Первая веб-страница (web-page) была создана Т. Бёрнерсом-Ли в 1991 г. Для её полноценного функционирования автор ввёл три базовых понятия:

1) «язык гипертекстовой разметки» (HyperText Markup Language, HTML);

2) «унифицированный идентификатор ресурса» (Uniform Resource Identifier, URI);

3) «протокол прикладного уровня передачи данных» (Hypertext Transfer Protocol, HTTP)[237]. Не останавливаясь подробно на технической составляющей данных понятий, следует упомянуть, что они позволяют пользователю с помощью ссылки получить доступ к конкретному вебресурсу.

---

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

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

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

[237] World Wide Web Foundation. History of the Web. [Электронный ресурс]: https://webfoundation.org/about/vision/history-of-the-web/ (дата обращения: 03.01.2025).

Важно сделать оговорку, что киберпространство, будучи некой сущностью, характеризуемой уникальным режимом синергии виртуальных и физических объектов, средств «аппаратного обеспечения» (hardware) и «программного обслуживания» (software), всех локальных и глобальных компьютерных сетей по всему миру, намного шире понятия Интернет и не сводится лишь к его использованию.

В зарубежном научном дискурсе имеет место разграничение сети Интернет и киберпространства. Так, по мнению исследователей Д.Д. Бетца и Т. Стевенса, Интернет не может существовать и функционировать в отрыве от использования реального оборудования (Hardware), является глобальной сетью компьютеров, серверов и иного оборудования, использующей вышеупомянутые протоколы для связи друг с другом. В то же время киберпространство является некой метафорой, оно начало своё развитие задолго до возникновения Интернета и компьютеров в современном их понимании, оно уже стало развиваться благодаря появлению телефонной связи, телевизоров и другой техники. Интернет же представляет собой систему взаимосвязанных гипертекстовых документов, доступ к которым обеспечивается через протоколы[238].

Ж. Липтон обозначила основные черты, присущие киберпространству: 1) глобальное распространение Интернета; 2) отличительные нормы, регулирующие поведение в онлайн среде в отличие от норм, регулирующих поведение в обычном, «физическом» мире; 3) виды ущерба, понесённого в результате недобросовестного поведения в онлайн среде[239].

---

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

[239] Lipton J. Rethinking Cyberlaw: A New Vision for Internet Law.-Edward Elgar Publishing, 2015, 176 p.

В западном научном дискурсе по данным американского военного эксперта Ф. Крамера насчитывается порядка 28 определений «киберпространства»[240].

По мнению профессора социологии и культурологии Голдсмитского университета Лондона С. Лэша, ввиду крайне высокой степени технологизированности всех без исключения сфер общественной деятельности, человеку свойственно воспринимать окружающий мир через призму высокотехнологических систем. Таким образом, уместно говорить о некоем симбиотическом союзе между людьми и машинами, на основе которого сложился комплексный органико-технологический интерфейс[241]. Ключевой особенностью описанного С. Лэшем феномена становится доктринальное оформление принципиально нового измерения реальности – киберпространства[242].

В 1991 г. был выпущен сборник статей по итогам первой международной научной конференции по киберпространству, состоявшейся в 1990 г. в Университете Техаса, Остине, США, под редакцией архитектора-урбаниста и философа М. Бенедикта[243]. В своей программной статье М. Бенедикт дал следующую характеристику термину киберпространства: «киберпространство – это глобально связанная многомерная искусственная или «виртуальная» реальность, поддерживаемая компьютерами, доступная через компьютеры и создаваемая компьютерами… Киберпространство имеет географию, физику,

---

[240] Киберпространство как стратегический инструмент социальной инженерии URL: https://whatisgood.ru/theory/analytics/kiberprostranstvo-kak-strategicheskiy-instrument/ (дата обращения: 15.04.2023).

[241] Lash S. Critique of information. L., 2002. P. 15.

[242] 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).

[243] 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).

природу и верховенство человеческого закона»[244]. Действительно, оглядываясь на первоначальные этапы развития глобальных сетей, с перспективы сегодняшнего дня, когда человек уже не может представить свою жизнь без применения интернета, раскрывается пророческий смысл высказываний современников зарождения всемирной паутины. Киберпространство, которое по своей природе является одной из форм бытия, следует трактовать в качестве концептуального пространства, то есть как порядок сосуществования «предметов» в наших восприятиях, как порядок сосуществования идей[245]. Сложно переоценить влияние, которое развитие компьютерных технологий оказывает на формирование современного дискурса, формы общения. В этом случае мы сталкиваемся с усложнением конструирования моделей субъективности и усложнением процесса формирования идентичности, что влечёт за собой появление процессов, способствующих поглощению человеческой жизни киберпространством, оказывая существенное изменение самого образа мышления[246]. Говоря о роли киберпространства в современной системе международных отношений, региональной и глобальной безопасности необходимо отметить, что почти сразу же после своего возникновения киберпространство превратилось в пятое (после земли, моря, воздуха и космоса) поле битвы различных политических и военных сил и продолжает оставаться таковым. Сегодня киберпространство является неотъемлемой частью информационной, экономической, политической, военной деятельности отдельных людей, корпораций, государств и их союзов, наднациональных структур и образований[247].

---

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

[245] 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).

[246] 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).

[247] Кардава Н.В. Киберпространство как новая политическая реальность: вызовы и ответы // История и современность. 2018. №1-2 (27-28). URL:

Мо мнению американского социолога и культурного теоретика, профессора социологии в Университете Торонто Д. Белла, киберпространство является «виртуальной средой, созданной взаимодействием пользователей через компьютерные сети»[248]. Данное суждение подчеркивает важность сетевого взаимодействия и его влияние на современную культуру и общество[249]. Позднее Белл описывал киберпространство в качестве «многоуровневой и многогранной среды, в которой пересекаются технологии, культура и общество», акцентируя внимание на том, как цифровые технологии формируют новые формы взаимодействия и идентичности в современном мире[250], а также в качестве «сложной экосистемы, в которой взаимодействуют технологии, культура и экономика»[251].

Американский писатель, и один из первых исследователей виртуальных сообществ и влияния интернета на социальные связи Х. Рейнгольд в свою очередь определяет киберпространство в качестве новой формы пространства, где информация становится основным ресурсом, акцентируя внимание на экспоненциальном росте значения информационно-коммуникационных технологий и их влиянии на общество. По мнению Х. Рейнгольда киберпространство является «социальным пространством, созданным взаимодействием людей через цифровые технологии»[252].

Американский философ и исследователь, старший научный сотрудник Брукингского института, специализирующийся на исследовании влияния технологий на общество и военные конфликты П. Сингер, в своих работах рассматривает киберпространство в качестве «инфраструктуры, состоящей из компьютерных систем и сетей, влияющих на безопасность и стабильность», акцентирует внимание на становление киберпространства ареной

---

https://cyberleninka.ru/article/n/kiberprostranstvo-kak-novaya-politicheskaya-realnost-vyzovy-i-otvety (дата обращения: 22.08.2024).

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

[249] Bell, D. J. (2001). *Cyberculture: The Key Concepts*.

[250] The Cybercultures Reader (2010)

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

[252] Rheingold, H. (1993). The Virtual Community: Finding Connection in a Computerized World.

столкновения политических акторов в современных условиях, где практическая имплементация новых технологий и инноваций, включая использование кибератак и информационных войн приобретает ключевую роль[253]. В более поздних работах П. Сингер определяет киберпространство как «инфраструктуру, в которой происходят современные конфликты и кибератаки», подчеркивая витальную роль, отводимую кибербезопасности и защиты информационно-коммуникационных систем в условиях экспоненциального роста угроз[254].

Говоря о зарубежном опыте доктринального оформления понятия «киберпространство», целесообразно обратиться к западным нормативно-правовым актам на примере США.

Так, профессор Дипломатической академии МИД России О.П. Иванов подчёркивает, что наряду с воздухом, морем, сушей и космосом, киберпространство, которое входит в сферу противоборства, является одним из элементов пространства соперничества США. Более того, согласно американской официальной оценке, наряду с другими средствами, киберинструменты могут быть использованы для нанесения поражения условному противнику[255].

В своей статье «Международно-правовое регулирование киберпространства» профессор Дипломатической академии МИД России А.А. Данельян приводит основные подходы органов законодательной и исполнительной власти США к определению понятие «киберпространство»[256]. Исследовательской службой Конгресса США было предложено определение

---

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

[254] 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).

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

[256] Данельян А.А. Международно-правовое регулирование киберпространства [Электронный ресурс] // Образование и право. 2020. №1. URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie-kiberprostranstva/viewer (дата обращения: 01.08.2024)

киберпространства как «всеохватывающего множества связей между людьми, созданного на основе компьютеров и телекоммуникаций вне зависимости от физического и географического положения»[257]. В то же время Министерство обороны США полагает, что киберпространство – это «сфера (область), в которой применяются различные РЭС (связи, радиолокации, разведки, навигации, автоматизации, управления и наведения) для приема, передачи, обработки, хранения, видоизменения (трансформации) информации и связанная с ними информационная инфраструктура ВС»[258].

Таким образом, представляется возможным констатировать, что «разнообразие подходов к определению киберпространства, обусловленное различиями в политических, правовых и технологических приоритетах государств, а также теоретическими расхождениями в академической среде, оказывает существенное влияние на международные отношения. Отсутствие консенсуса в трактовке данного понятия приводит к фрагментации правового регулирования, усложняет формирование единых норм кибербезопасности и создает основу для конфликтов в цифровой сфере»[259].

Резюмируя вышесказанное, необходимо отметить, что в зарубежном научном дискурсе термин киберпространство впервые появился в научной фантастике, и лишь затем, следуя стремительному развитию информационно-коммуникационных технологий, программного и аппаратного обеспечения, локальных и глобальных сетей, и наконец, появлению и внедрению в широкие массы сети Интернет, получил своё доктринальное оформление в научном дискурсе. Отметим неразрывную связь киберпространства со всемирной паутиной, при этом чрезвычайно важным является осознание

---

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

[258] Air Force Doctrine Publication 3-13 - Information In Air Force Operations [Electronic Resource] // USAF. 2011. URL: https://nsarchive.gwu.edu/document/27351-united-states-air-force-air-force-doctrine-document-3-13-information-operations-11 (accessed: 15.12.2024)

[259] 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).

нетождественности данных понятий. В то время как глобальная паутина является всемирной информационной компьютерной сетью, связывающей между собой как пользователей компьютерных сетей, так и пользователей индивидуальных компьютеров для обмена информацией, определение понятия «киберпространство» в зарубежном научном дискурсе является более комплексным и неоднородным. Несмотря на множество описанных подходов к определению термина, киберпространство обладает следующими ключевыми уникальными характеристиками: являясь режимом синергии виртуальных и физических объектов, средств «аппаратного обеспечения» (hardware) и «программного обслуживания» (software), всех локальных и глобальных компьютерных сетей по всему миру, оно намного шире понятия Интернет и не сводится лишь к его использованию. Киберпространство является виртуальной средой, социальным пространством, многомерной искусственной и виртуальной реальностью.

1.3. Сравнительный анализ и классификация подходов отечественных и зарубежных исследователей к определению понятия «киберпространство»

Понятие киберпространства, ставшее ключевым в эпоху цифровой трансформации, вызывает активный интерес у исследователей по всему миру. Киберпространство, как сложный и многогранный феномен, охватывает не только технологические аспекты, но и социальные, политические, экономические и правовые измерения. Несмотря на широкое использование термина, его определение остается предметом дискуссий среди отечественных и зарубежных ученых, что обусловлено различиями в методологических подходах, культурных и исторических контекстах. Зарубежные исследователи, такие как М. Кастельс[260], рассматривают киберпространство

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

как глобальную сетевую структуру, которая трансформирует традиционные формы коммуникации и социальной организации. В свою очередь, британский социолог Д. Лайон акцентирует внимание на вопросах конфиденциальности и контроля в цифровой среде, подчеркивая её роль в формировании новых форм власти и управления[261]. Эти подходы отражают акцент на технологической и социальной динамике, характерной для западной научной традиции. Отечественные исследователи предлагают более детализированный анализ киберпространства с учетом специфики российской информационной среды. Они подчеркивают важность государственного регулирования и безопасности в условиях цифровой трансформации, что отражает особенности национального дискурса. Сравнительный анализ подходов отечественных и зарубежных исследователей к определению киберпространства позволяет выявить как общие тенденции, так и специфические особенности, обусловленные культурными, политическими и технологическими контекстами.

Киберпространство как концепция возникло в конце XX века и быстро стало объектом междисциплинарных исследований. И отечественные, и зарубежные исследователи сходятся в том, что киберпространство представляет собой виртуальную среду, созданную с помощью компьютерных технологий и сетей, где происходит взаимодействие между людьми, машинами и данными.

Киберпространство, привлекая внимание мультидисциплинарных исследователей различных дисциплин, может трактоваться в зависимости от методологических и культурно-политических контекстов.

Анализируя представленные в параграфе 1.1. подходы отечественных исследователей к определению понятия киберпространство, представляется возможным проследить общую парадигму, присущую рассмотренным определениям. Так, например, определению Стародубцева Ю.И., Иванова

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

С.А., Закалкина П.В («киберпространство – искусственное неоднородное технологическое пространство с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе антагонистических систем управления, при этом свойства киберпространства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей»[262][263]) присущи черты технологической парадигмы. Данное определение киберпространства раскрывает его как гибридный феномен, где пересекаются технологическое, социальное и политическое измерения. Философски оно требует переосмысления категорий пространства, власти и субъективности в контексте цифровой эпохи, предлагая новую оптику для анализа взаимодействия человека, технологии и общества.

Определение С.В. Бондаренко (киберпространство представляет собой сложную социотехническую систему, которая включает в себя не только информационные сети, но и социальные практики, культурные коды и виртуальные взаимодействия[264]) перекликается с идеями постмодернистской фрагментации и сетевого общества, где традиционные социальные структуры уступают место гибким, децентрализованным формам взаимодействия.

Данное определение киберпространства как сложной социотехнической системы раскрывает его многомерность и междисциплинарность. С философской точки зрения оно требует интеграции онтологического, эпистемологического, этического и культурологического подходов.

---

[262] 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.

[263] 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.

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

Киберпространство становится не просто технологическим феноменом, но новой формой социального и культурного бытия, которая трансформирует традиционные представления о реальности, субъективности и взаимодействии. Определение подчеркивает, что киберпространство – это не только техническая инфраструктура (информационные сети), но и социальные практики, культурные коды и виртуальные взаимодействия, что созвучно идеям социотехнических систем, где технология и общество взаимно влияют друг на друга. С философской точки зрения определение отражает диалектику материального и идеального: киберпространство становится пространством, где материальные технологии (серверы, алгоритмы) взаимодействуют с социальными и культурными процессами (коммуникация, идентичность, власть).

Описание А.Е. Войскунского («киберпространство опирается одновременно на продукты информационных технологий и на социальные сервисы, являющиеся полем специфического поведения человека»[265]) подчеркивает двойственную природу киберпространства: оно опирается как на продукты информационных технологий (материальная основа), так и на социальные сервисы (человеческое поведение и взаимодействие). Определение отражает философский спор между технологическим детерминизмом и социальным конструктивизмом. Киберпространство, таким образом, становится гибридным феноменом, где технология и общество взаимно влияют друг на друга.

Определение У. Гибсона (киберпространство – среда «чувственных галлюцинаций, испытываемых ежедневно миллиардами операторов всех наций, в том числе и детей, изучающих математические науки… Графическое отображение данных компьютеров, принадлежащих людям. Немыслимая сложность. Потоки света, упорядоченные человеческим разумом, скопления и созвездия информации»[266]) представляет собой попытку осмыслить феномен

[265] Войскунский А.Е. Метафоры интернета // Вопросы философии. 2001. № 11. С. 64–79.
[266] Gibson W. Neuromancer. N.Y., 1984.

цифровой реальности через призму философского и эстетического восприятия. Оно сочетает в себе элементы технологического детерминизма, феноменологии и постмодернистского взгляда на реальность. В данном контексте киберпространство воспринимается как субъективный опыт, создаваемый взаимодействием человека с технологиями, а упоминание «графического отображения данных компьютеров» и «потоков света, упорядоченных человеческим разумом» указывает на то, что киберпространство является продуктом технологического развития, формирующим новую реальность. Данное определение киберпространства представляет собой синтез технологического, эстетического и философского взглядов на цифровую реальность. Оно подчеркивает, что киберпространство – это не просто техническая среда, но и новая форма человеческого опыта, которая требует осмысления в контексте современной философии и культуры.

Определение М. Бенедикта («киберпространство – это глобально связанная многомерная искусственная или «виртуальная» реальность, поддерживаемая компьютерами, доступная через компьютеры и создаваемая компьютерами… Киберпространство имеет географию, физику, природу и верховенство человеческого закона»[267]) представляет собой попытку осмыслить цифровую реальность через призму её структуры, функциональности и взаимодействия с человеческим обществом. Определение подчеркивает, что киберпространство – это «искусственная или виртуальная реальность», указывая на его онтологический статус как созданной человеком среды, которая существует параллельно с физической реальностью. С философской точки зрения, это можно связать с идеями Ж. Бодрийяра о симулякрах и гиперреальности, где искусственное становится неотличимым от реального. Данное определение киберпространства представляет собой попытку осмыслить цифровую реальность как сложный, многомерный феномен, который существует на стыке технологий, общества и

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

человеческого опыта. Оно подчеркивает, что киберпространство – это не просто техническая среда, но и новая форма бытия.

Определения Д. Белла (киберпространство – виртуальная среда, созданная взаимодействием пользователей через компьютерные сети; многоуровневая и многогранная среда, в которой пересекаются технологии, культура и общество[268]; сложная экосистема, в которой взаимодействуют технологии, культура и экономика[269]) акцентирует техническую и функциональную природу киберпространства, рассматривая его как инфраструктуру, которая оказывает значительное влияние на безопасность и стабильность. Данное определение киберпространства представляет собой прагматичный и функциональный взгляд на цифровую реальность, акцентируя её роль как инфраструктуры, которая влияет на безопасность и стабильность. С философской точки зрения, оно поднимает важные вопросы о технологическом детерминизме, социальной ответственности, этике безопасности и политическом контроле. Данное определение отражает, что киберпространство – это не только техническая система, но и социальный феномен, который требует глубокого философского осмысления в контексте современного мира.

Определение П. Сингера (киберпространство – «инфраструктура, состоящая из компьютерных систем и сетей, влияющих на безопасность и стабильность»[270]) представляет собой прагматичный и функциональный взгляд на цифровую реальность, акцентируя её роль как инфраструктуры, которая влияет на безопасность и стабильность, поднимая важные вопросы о технологическом детерминизме, социальной ответственности, этике безопасности и политическом контроле. Данное определение отражает, что киберпространство – это не только техническая система, но и социальный

[268] Bell, D. J. (2001). Cyberculture: The Key Concepts.
[269] D. Bell, B. Kennedy The Cybercultures Reader (2010)
[270] P. Singer Wired for War: The Robotics Revolution and Conflict in the 21st Century (2009)

феномен, который требует глубокого философского осмысления в контексте современного мира.

Сходства и различия в подходах отечественных и зарубежных исследователей к определению киберпространства можно выделить на основе анализа приведенных определений. Оба подхода подчеркивают сложность и многогранность киберпространства, но акценты и формулировки различаются.

Сходства:

Киберпространство как сложная система.

И отечественные, и зарубежные исследователи описывают киберпространство как сложную систему, которая включает в себя множество элементов и процессов. Оба подхода подчеркивают, что это не статичная, а динамичная и развивающаяся среда.

Интеграция технологических и социальных аспектов.

И отечественные, и зарубежные исследователи признают, что киберпространство – это не только технологическая инфраструктура, но и среда, где пересекаются технологии, общество, культура и экономика. Отечественные исследователи говорят о «социотехнической системе», а зарубежные – о «сложной экосистеме» или «виртуальной среде взаимодействия».

Децентрализованность и глобальная связанность:

И отечественные, и зарубежные исследователи подчеркивают, что киберпространство не управляется единой системой и функционирует в интересах множества участников. Отечественные исследователи акцентируют внимание на разнородных и антагонистических системах управления, а зарубежные – на глобальной связанности и доступности через компьютеры.

Влияние на человека и общество:

И отечественные, и зарубежные исследователи отмечают, что киберпространство влияет на поведение человека, социальные практики и культурные коды. Отечественные исследователи говорят о «специфическом

поведении человека», а зарубежные – о «чувственных галлюцинациях» и «виртуальной реальности».

Различия:

Акцент на технологиях vs. виртуальной реальности:

Отечественные исследователи делают больший акцент на технологической составляющей, описывая киберпространство как «искусственное технологическое пространство» с множеством органов управления. Зарубежные исследователи чаще подчеркивают виртуальную природу киберпространства, описывая его как «виртуальную реальность» или «чувственные галлюцинации».

Социальные аспекты:

Определения отечественных исследователей более детально раскрывают социальные аспекты, описывая киберпространство как «социотехническую систему» с культурными кодами и социальными практиками. Зарубежные определения также включают социальные аспекты, но чаще акцентируют внимание на взаимодействии пользователей и создании новой реальности.

Практический vs. философский подход:

Определения отечественных исследователей имеют более практический и системный характер, описывая киберпространство с точки зрения управления, процессов и интересов потребителей. Зарубежные определения часто носят более философский и образный характер, используя метафоры («чувственные галлюцинации», «созвездия информации») для описания киберпространства.

Инфраструктурный аспект:

Определения отечественных исследователей меньше акцентируют внимание на инфраструктурной составляющей, в то время как зарубежные исследователи явно указывают на роль компьютерных систем и сетей как основы киберпространства. Например, одно из зарубежных определений

прямо говорит о киберпространстве как об «инфраструктуре, состоящей из компьютерных систем и сетей».

География и законы:

Зарубежные исследователи чаще упоминают, что киберпространство имеет свою «географию», «физику» и регулируется человеческими законами. Определения отечественных исследователей не акцентируют внимание на данных аспектах, делая упор на функциональные и управленческие характеристики.

Определив ключевые сходства и различия подходов отечественных и зарубежных исследователей к определению понятия «киберпространство» представляется возможным разработать классификацию определений, выделив следующие ключевые подходы.

1. Технологический подход – акцентирует внимание на технических и инфраструктурных аспектах киберпространства, рассматривая его как продукт развития информационных технологий и компьютерных сетей.
2. Социотехнический подход – рассматривает киберпространство как результат взаимодействия технологий и общества, подчеркивая взаимосвязь технических систем и социальных практик.
3. Философский и культурный подход – рассматривает киберпространство через призму восприятия, культуры и виртуальной реальности, акцентируя внимание на его символическом и ментальном измерении.

Анализируя представленные в параграфах 1.1., 1.2 подходы отечественных и зарубежных исследователей к определению понятия киберпространство, представляется возможным отнести к **технологическому подходу** следующие определения.

Определение Стародубцевой Ю.И., Иванова С.А., Закалкина П.В. подчёркивает сложность и неоднородность киберпространства как технологической среды, функционирующей в интересах множества систем управления. Акцент делается на зависимость свойств киберпространства от характеристик его элементов и реализуемых процессов.

В определении П. Сингера. киберпространство рассматривается в качестве технической основы, обеспечивающей функционирование современных систем. Упор делается на его роль в обеспечении безопасности и стабильности, что характерно для исследований в области кибербезопасности и информационных технологий.

Оба определения фокусируются на технологической составляющей, игнорируя или минимизируя социальные и культурные аспекты. Они отражают инженерный взгляд на киберпространство как на сложную систему, созданную для решения технических задач.

Социотехнический подход.

Определение С.В. Бондаренко подчеркивает интеграцию технологических и социальных элементов, что характерно для исследований в области социологии технологий.

Определение А.Е. Войскунского опирается на взаимодействие технологий и человеческого поведения, что отражает междисциплинарный подход к изучению киберпространства.

Определение Д. Белла расширяет рамки социотехнического подхода, включая культурные и экономические аспекты, что характерно для исследований в области цифровой антропологии и медиаисследований.

Социотехнический подход подчеркивает, что киберпространство не может быть сведено исключительно к технологическим компонентам. Оно формируется и развивается в результате взаимодействия людей, технологий и социальных институтов.

Философский и культурный подход.

Определение У. Гибсона отражает философский взгляд на киберпространство как на виртуальную реальность, созданную человеческим восприятием и технологиями. Оно близко к концепциям, разработанным в рамках философии технологий и постмодернистской мысли.

Определение М. Бенедикта описывает киберпространство в качестве альтернативной реальности, обладающей собственной структурой и законами,

что характерно для исследований в области виртуальной реальности и цифровой философии.

Философский и культурный подход акцентирует внимание на символическом и ментальном измерении киберпространства, рассматривая его как пространство, созданное человеческим разумом и культурой.

В данном контексте является целесообразным отметить, что в настоящий момент имеет место смешение формулировок, представленных в различных концептуальных и нормативных документах как государственных, так и негосударственных акторов международных отношений, неправительственных организаций.

Согласно определению международного стандарта Международной организации по стандартизации (ISO) от 2012 года, киберпространство – это «сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и сервисов в Интернете с помощью подключенных к нему технологических устройств и сетей, которая не существует ни в какой физической форме»[271].

Определение ISO представляет собой технолого-социальный конструкт, его ключевыми атрибутами являются:

- Примат взаимодействия над субстанцией: киберпространство не является статичным объектом, а возникает как динамический процесс из взаимодействия агентов (людей) посредством технологий, что лишает его жесткой привязки к юрисдикции конкретного государства по принципу территориальности.
- Имматериальность: утверждение, что киберпространство «не существует ни в какой физической форме», подчеркивает его виртуальную, сетевую природу, что ставит сложные вопросы

[271] ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en обращения: 24.08.2024).

о применимости традиционных правовых режимов, основанных на контроле над физической территорией и инфраструктурой.

– Глобальность и открытость: определение предполагает глобальный и универсальный характер среды, где технологические стандарты и протоколы (как те, что разрабатывает ISO) имеют приоритет над национальным регулированием.

Данное определение, будучи продуктом международного экспертного консенсуса в рамках ISO, служит отправной точкой для анализа фундаментальной дихотомии между отечественными и западными подходами к концептуализации киберпространства. Целесообразно отметить, что данное расхождение коренится не в технической сфере, а в сферах политологии, международных отношений и государственного суверенитета. Анализируя ключевые атрибуты определения, представляется возможным отразить дихотомию отечественного и западного (на примере НАТО и США) подходов к определению понятия «киберпространство».

Определение киберпространства, сформулированное Международной организацией по стандартизации (ISO) в 2012 году, выступает в качестве репрезентативной модели социотехнического и децентрализованного понимания данной среды, преимущественно характерного для западной научной и политической традиции. Согласно этому подходу, киберпространство интерпретируется как сложная и динамическая система, возникающая из процесса взаимодействия между людьми, программными сервисами и технологическими устройствами, лишенная единого центра управления и не существующая в физической форме. Подобная онтологическая установка – восприятие киберпространства в качестве процесса и деятельности, а не как статичного объекта – является фундаментом для последующих политико-правовых импликаций, которые радикально расходятся с официальной отечественной позицией.

В западной парадигме, созвучной определению ISO, имматериальная и глобальная природа киберпространства закономерно ведет к развитию концепций транснационального управления. В рамках данной модели государство является лишь одним из многих равноправных акторов наряду с гражданским обществом, техническим сообществом и частным сектором. Ключевая роль отводится не суверенному контролю, а выработке общих технических стандартов и «мягкого права», призванных обеспечивать устойчивость и безопасность глобальной сети. Угрозы в этой системе координат носят прежде всего технико-криминальный характер (киберпреступность, нарушение конфиденциальности, целостности и доступности данных), а безопасность понимается в качестве защищённости интересов всех пользователей, а не исключительно государственных институтов.

Напротив, официальный российский подход основывается на стремлении реифицировать, то есть овеществить, киберпространство, придав ему атрибуты территории, подконтрольной национальному суверенитету, что выражается использованием терминов «информационная сфера» и «пятая сфера противоборства», которые имплицитно содержат пространственную метафору, аналогичную сухопутной, морской или воздушной территории. Подобный взгляд закономерно приводит к этатистской и геополитической трактовке: киберпространство становится новым театром межгосударственной конкуренции, где действуют законы силовой политики.

Следствием подобного подхода является концепция «суверенного интернета» и «государственного управления» национальным сегментом сети, что прямо противоречит децентрализованной модели ISO. В рамках отечественной парадигмы ключевым понятием становится «информационная безопасность», которая трактуется значительно шире, чем кибербезопасность. Она включает не только защиту от технических угроз, но и обеспечение информационно-психологической стабильности, защиту от дезинформации и идеологического вмешательства извне, что рассматривается как гарантия

сохранения политического строя и конституционного порядка. Таким образом, угрозы носят преимущественно внешний и идеологический характер, а государство выступает как верховный суверен и главный гарант безопасности.

Таким образом, определение ISO, будучи технологически нейтральным, объективно высвечивает глубинный цивилизационный раскол. Этот раскол проходит между либерально-космополитической моделью, видящей в киберпространстве глобальное общественное благо, управляемое совместными усилиями всех заинтересованных сторон, и реалистической этатистской моделью, рассматривающей его как продолжение традиционного межгосударственного противоборства, требующее жесткого национального контроля и суверенизации. Именно это фундаментальное расхождение в понимании самой сути объекта делает столь сложным достижение международного консенсуса по нормам ответственного поведения в киберпространстве. Представляется возможным отметить, что подобное различие подходов осложняет международное регулирование: например, российские инициативы в ООН по кибербезопасности часто противоречат американской модели «открытого киберпространства». В условиях гибридного противостояния России и НАТО эти концептуальные расхождения становятся инструментом политики. Кибератаки на критическую инфраструктуру, кампании дезинформации и борьба за технологический суверенитет (например, через отказ от западных IT-платформ) показывают, что киберпространство превратилось в арену «войн смыслов». Если США видят в нем поле для проекции силы, то РФ – зону уязвимости, требующую жесткого контроля. Это противоречие будет лишь углубляться по мере развития ИИ и квантовых технологий, делая киберпространство главным полем битвы XXI века[272].

[272] 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).

Резюмируя вышесказанное необходимо отметить, что проведённый анализ определений киберпространства позволяет сделать вывод о многогранности и междисциплинарности этого феномена. 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. Каждый из рассмотренных подходов – технологический, социотехнический, философский и культурный – выделяет определенные аспекты киберпространства, что подчеркивает его сложность и многоуровневость. Технологический подход акцентирует внимание на технической основе киберпространства, рассматривая его как продукт развития компьютерных сетей и информационных технологий. Социотехнический подход расширяет это понимание, включая в анализ социальные практики, культурные коды и взаимодействия, что отражает взаимосвязь технологий и общества. Философский и культурный подходы обращаются к символическому и ментальному измерению киберпространства, рассматривая его как виртуальную реальность, созданную человеческим восприятием и культурой. Таким образом, можем констатировать, что киберпространство представляет собой уникальный объект исследования, который требует междисциплинарного подхода для своего полного понимания. Его изучение должно учитывать как технические аспекты, так и социальные, культурные и философские контексты, что делает его одной из ключевых тем современных научных исследований в области политологии, информационных технологий, социологии, философии и культурологии.

Проведенный анализ также выявляет фундаментальную дихотомию в концептуализации киберпространства. Определение Международной организации по стандартизации (ISO), трактующее киберпространство как имматериальный, глобальный и возникающий из взаимодействия социотехнический процесс, служит основой для западной (либерально-космополитической) модели управления. Данная модель предполагает

децентрализованное, многополярное управление с приоритетом технических стандартов и «мягкого права», где государство является одним из многих акторов. Напротив, отечественный подход основан на реификации киберпространства, рассматривая его как новую сферу государственного суверенитета и межгосударственного противоборства, что приводит к этатистской парадигме, требующей жесткого национального контроля, суверенизации и где ключевым понятием выступает расширительно трактуемая «информационная безопасность». Указанное расхождение, коренящееся в различных онтологических и политико-правовых установках, представляет собой глубинный цивилизационный раскол. Это противоречие между глобальным и национально-суверенным подходами существенно затрудняет выработку международных норм ответственного поведения и трансформирует киберпространство в арену стратегической конкуренции, что, вероятно, будет лишь усугубляться с развитием новых технологий.

Основываясь на рассматриваемых в исследовании трактовках, представляется возможным предложить авторское определение понятия «киберпространство». Таким образом, 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). Данное пространство характеризуется архитектурной многоуровневостью и наличием множества разнородных, зачастую антагонистических, систем оперативного и стратегического управления, процесс создания и эксплуатации которых не детерминирован единой управляющей инстанцией.

Ключевые свойства киберпространства являются производными как от имманентных характеристик его элементов (аппаратно-программных комплексов, сетевых протоколов, интерфейсов), так и от объема,

направленности и свойств реализуемых в нем процессов, обслуживающих интересы внутренних и внешних акторов (индивидуальных, корпоративных, государственных). Будучи новой формой пространства, где информация выступает основным ресурсом, оно представляет собой не только среду для осуществления экономической, политической и культурной активности, но и арену современных конфликтов, что обусловливает его критическую значимость для обеспечения безопасности и стабильности.

Глава 2. Ключевые особенности стратегии НАТО в киберпространстве на современном этапе

2.1. Основные этапы трансформации стратегии НАТО в киберпространстве в период 1999 – 2022 гг.

Современная система международных отношений рассматривается многими исследователями в парадигме усиления турбулентности, нестабильности и гетерогенности. Технологический прорыв позволяет говорить о повсеместном применении интернет-технологий во всех без исключения сферах международных отношений, включая международную безопасность.

Трансформация стратегии НАТО в киберпространстве отражает эволюцию подходов Североатлантического альянса к новым вызовам и угрозам, связанным с цифровизацией и ростом зависимости от информационных технологий. Начиная с первых шагов в конце XX века и заканчивая современными стратегиями, стратегия НАТО в киберпространстве прошла несколько ключевых этапов, каждый из которых был обусловлен изменениями в технологической и геополитической среде[273].

Для всестороннего понимания проблемы первостепенно следует обратиться к трансформации современной системы кибербезопасности в Европе. Говоря о понятиях киберпространство, информационная безопасность, ИКТ следует учитывать, что начало их практического применения в мировой политике датируется концом XX, началом XXI веков. Истоки появления вышеперечисленных понятий прослеживаются вплоть до возникновения интернета в его современном понимании и являются неразрывно связанными с научно-технологическим прогрессом. По мере развития современных технологий, киберпространство существенно

[273] 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.

расширялось, включая в себя принципиально новые элементы, такие как социальные сети, виртуальные сообщества и онлайн платформы. Постепенное внедрение широкого инструментария практического применения кибервозможностей в сферу международной безопасности следует рассматривать в качестве комплексного и постоянно эволюционирующего явления. По мере планомерного роста зависимости акторов международных отношений от цифровой инфраструктуры, киберпространство перешло в парадигму источника потенциальных, в том числе витальных угроз и уязвимостей.

Североатлантический альянс признает растущую важность киберпространства в сфере безопасности и активно занимается противодействием киберугрозам. Подход НАТО к киберпространству основан на понимании того, что оно является областью операций наряду с сушей, морем, воздухом и космическим пространством. Важно понимать, что краеугольная 5 статья Североатлантического договора предусматривает коллективный ответ в том числе при кибератаке на одно из государств-членов альянса. Так, по словам бывшего генерального секретаря НАТО Йенса Столтенберга, «серьёзная кибератака может привести к срабатыванию статьи 5, согласно которой нападение на одного союзника рассматривается как нападение на всех»[274]. При этом главной опасностью практического применения такого подхода является несовершенство алгоритма идентификации источника злонамеренного акта кибер-воздействия.

В качестве первого этапа трансформации стратегии Североатлантического альянса в киберпространстве возможно выделить период 1990-х – начала 2000-х годов.

Первые упоминания о киберугрозах в документах НАТО появились в конце 1990-х годов, когда Североатлантический альянс начал осознавать потенциальные риски, связанные с развитием информационных технологий. В

[274] NATO will defend itself URL: https://www.nato.int/cps/en/natohq/news_168435.htm (дата обращения: 12.03.2024)

этот период киберпространство рассматривалось преимущественно как сфера гражданской инфраструктуры, а не как область военных операций. Однако уже в 1999 году, во время операции «Союзная сила», Североатлантический альянс столкнулся с кибератаками на свои системы, что стало первым сигналом о необходимости уделять больше внимания кибербезопасности[275]. Исследователи Д. Аркилла и Д. Ронфельдт, отмечают, что уже в этот период началось формирование концепции «кибервойны» как новой формы конфликта, где информационные технологии играют ключевую роль[276]. Однако на данном этапе НАТО еще не имело чёткой стратегии в киберпространстве, а меры по защите носили фрагментарный характер.

Рассматривая процесс эволюции подходов европейских государств-членов НАТО, необходимо констатировать об изменении объектно-субъектных отношений понятия кибербезопасности (от традиционных интерпретаций киберпространства к экосистемным терминам и концепциям)[277]. Более того, при изучении темы особенностей региональной кибербезопасности НАТО на европейском континенте необходимо учитывать принципиальное различие американского и европейского подходов. Европейские государства-члены Североатлантического альянса сталкивались с теми же проблемами и вызовами в киберпространстве, что и их американские партнёры, однако в данной парадигме наблюдается фундаментальное различие институциональных структур США и европейских стран. В то время как в случае с США имели место единая внешняя политика, централизированные вооружённые силы и единый бюджет, европейским государствам-членам Североатлантического альянса приходилось затрачивать

[275] Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation.
[276] Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation.
[277] 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).

усилия на разработку и внедрение собственных программ по имплементации политики в сфере кибербезопасности на национальных уровнях, при этом осуществляя координацию в рамках наднациональной структуры в лице Европейского Союза и военно-политического блока в лице НАТО[278].

Хотя стратегия Североатлантического альянса всегда в той или иной мере затрагивала проблемы обеспечения собственных систем связи и обмена информацией, защита от кибернетических угроз в качестве доктринально оформленного компонента стратегии впервые была включена в политическую повестку организации в ходе саммита НАТО в Праге в 2002 году[279], а в последствии вновь актуализирована по итогам саммита в Риге в 2006 году[280]. Так, согласно итоговому коммюнике Пражского саммита НАТО, государства-члены Североатлантического альянса договорились «укреплять свои возможности по защите от кибератак»[281].

Говоря о важнейшей вехе формирования современной стратегии кибербезопасности НАТО как на глобальном, так и региональном уровнях (на Европейском континенте) следует обратиться к итогам Пражского саммита 2002 года. Одним из наиболее важных последствий данного саммита стало заложение фундамента к созданию программы киберзащиты «NCIRC» (NATO Computer Incident Response Capability) (Возможность реагирования на компьютерные инциденты НАТО) в 2002 году.

Программа изначально задумывалась как централизованный механизм для:

---

[278] 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

[279] Cyber defence.URL: https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en#defence (дата обращения: 05.11.2024)

[280] Riga Summit Declaration. URL: https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en (дата обращения: 17.10.2024).

[281] Cyber defence.URL: https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en#defence (дата обращения: 05.11.2024)

1. мониторинга компьютерных инцидентов;
2. координации реагирования на кибератаки;
3. разработки стандартов защиты информационной инфраструктуры;
4. обеспечения оперативного обмена информацией между странами-членами.

Особое значение имело то, что NCIRC стала первым наднациональным механизмом киберзащиты в военно-политической организации такого масштаба. Её создание ознаменовало переход от разрозненных национальных мер к системному подходу в обеспечении коллективной кибербезопасности[282].

Значение NCIRC для развития киберстратегии Североатлантического альянса трудно переоценить. Программа не только обеспечила практический инструментарий защиты, но и:

1. заложила основы для последующего признания киберпространства областью операций;
2. способствовала выработке общих стандартов и процедур;
3. создала прецедент наднационального управления кибербезопасностью.

Таким образом, создание NCIRC стало поворотным моментом в трансформации подходов НАТО к вопросам кибербезопасности, ознаменовав переход от концептуальных дискуссий к практической реализации принципов коллективной кибероборонь[283].

Представляется возможным констатировать, что в период 1990-2006 гг. киберпространство превратилось в ключевую сферу обеспечения международной безопасности, требующую комплексного и адаптивного регулирования. Изначально воспринимаемое как второстепенная область гражданской инфраструктуры, киберпространство постепенно

---

[282] NATO Cyber Defence URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf (дата обращения: 12.03.2025)

[283] 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.

трансформировалось в полноценный театр военных и стратегических операций, что потребовало от Североатлантического альянса разработки специализированных механизмов противодействия угрозам.

Особое значение в этом процессе сыграли Пражский и Рижский саммиты НАТО, на которых были заложены основы современной киберстратегии альянса, включая создание системы реагирования на киберинциденты (NCIRC).

В качестве второго этапа трансформации стратегии Североатлантического альянса в киберпространстве возможно выделить период 2007-2014 годов, характеризуемый прежде всего началом формирования основ киберстратегии военно-политического блока.

По словам западных исследователей в области кибербезопасности, «тремя наиболее яркими примерами киберагрессии между национальными государствами являются события в Эстонии (2007 г.), Грузии (2008 г.) и Украине (2014, 2015 гг.), совершенные Россией и её прокси»[284]. По мнению ряда исследователей, «в 2007 году с российской стороны имели место непрерывные DDoS атаки, направленные на нарушение стабильной работы веб-сервисов эстонского правительства. В 2008 году, за три недели до начала операцию по принуждению к миру Грузии, российской стороной вновь была применена стратегия использования DDoS-атак с целью блокировки веб-ресурсов (что позже стало частью российской общей стратегии ведения боевых действий). В 2014 году в ходе воссоединения Крыма с Россией также имели место многочисленные кибератаки, направленные на государственные и частные медиа сервисы украинской стороны»[285].

[284] 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

[285] 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

Одним из запоминающихся событий в области формирования современной стратегии Североатлантического альянса в сфере кибербезопасности в Европе стало открытие Киберцентра НАТО в г. Таллине (Эстония) в 2008 году[286]. Ключевой предпосылкой к данному событию стала серия массированных кибератак сайтов газет, основных банков и правительственных учреждений Эстонии[287]. Подчеркнем, что ответственность за упомянутые действия была возложена на Россию при отсутствии каких-либо исчерпывающих доказательств. Тем самым уже в конце 2010-х годов стал явно прослеживаться более чем однозначный вектор антироссийской риторики в политике как отдельных государств Североатлантического альянса, так и самого военно-политического блока[288].

Рассматривая итоговое коммюнике саммита НАТО в Лиссабоне (2010 г.), следует отметить существенный рост внимания государств-членов Североатлантического альянса к киберпространству. Согласно Стратегической концепции 2010 года «Активное участие, современная оборона», принятой на встрече в верхах в Лиссабоне в ноябре 2010 года, государства-члены Североатлантического альянса согласились, что произошел качественный скачок в интенсификации кибератак, а также усилился их негативный эффект, напрямую воздействующий на государственные органы, коммерческие предприятия, транспортные системы и логистику, тем самым комплексно подрывая национальные экономики. Исходя из вышесказанного, было принято принципиальное решение «совершенствовать способность НАТО по предотвращению и обнаружению

---

[286] 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.

[287] В Таллине начал работу центр киберзащиты НАТО. URL: https://www.securitylab.ru/news/353773.php (дата обращения: 17.10.2022).

[288] 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.

кибератак, защите и нивелированию причиненного ими ущерба, в частности, используя процесс планирования с целью укрепления и координации национальных средств киберзащиты, путем связывания всех органов альянса централизированной сетью киберзащиты и интеграции механизмов Североатлантического альянса и государств-членов по осведомлению, предупреждению и реагированию на киберугрозы»[289].

Анализ трансформации стратегии НАТО в киберпространстве в период 2007–2014 годов позволяет сделать вывод о качественном изменении подхода Североатлантического альянса к кибербезопасности. Данный этап характеризовался переходом от фрагментарных мер к формированию системной стратегии, что было обусловлено серией масштабных кибератак в Эстонии (2007), Грузии (2008) и Украине (2014) приписываемых России. Эти инциденты продемонстрировали, что киберпространство стало неотъемлемой частью современных конфликтов, а его использование в гибридных войнах потребовало от НАТО разработки новых механизмов коллективной обороны. Важным шагом в этом направлении стало создание Киберцентра НАТО в Таллине (2008), что подчеркнуло растущую роль кибербезопасности в стратегии альянса. Примечательно, что обвинения в адрес России носили преимущественно политизированный характер, что отражало усиление антироссийской риторики в политике НАТО. Дальнейшее институциональное развитие киберстратегии военно-политического блока было закреплено в Стратегической концепции НАТО 2010 года, где киберугрозы были официально признаны вызовом коллективной безопасности, требующим скоординированных мер защиты. Таким образом, рассматриваемый период стал ключевым этапом в трансформации подходов НАТО к киберпространству, когда Североатлантический альянс перешел от

[289] Активное участие, современная оборона "Стратегическая Концепция Обороны и Обеспечения Безопасности Членов Организации Североатлантического Договора" Утверждена Главами Государств и Правительств в Лиссабоне URL: https://www.nato.int/cps/en/natohq/official_texts_68580.htm?selectedLocale=ru (дата обращения: 17.10.2022).

реагирования на отдельные инциденты к формированию комплексной системы кибероборонь.

В качестве третьего этапа трансформации стратегии Североатлантического альянса в киберпространстве возможно выделить период с 2014 года по настоящее время, характеризуемый прежде всего признанием киберпространства областью операций[290].

Первостепенно целесообразно упомянуть прошедший в 2016 г. саммит НАТО в Варшаве, где киберпространство было официально признано сферой операций военно-политического блока. Саммит в Варшаве проходил в ключевой для Североатлантического альянса момент, связанный с кардинальными изменениями в Европейском регионе и на мировой арене в целом. С точки зрения Коллективного Запада с Соединёнными Штатами в главной роли, НАТО столкнулась с существенными угрозами безопасности евроатлантического региона. Так, согласно 70 статье итогового коммюнике Варшавского саммита, «кибернетические нападения представляют явную угрозу безопасности Североатлантического союза и могут оказать столь же вредное воздействие на современные общества, что и обычные нападения. В Уэльсе мы пришли к соглашению о том, что киберзащита является частью основной задачи НАТО по обеспечению коллективной обороны. Теперь, в Варшаве мы вновь подтверждаем оборонительный мандат НАТО и признаем кибернетическое пространство как сферу операций, где НАТО должна так же эффективно обороняться, как и в воздухе, на суше и на море»[291]. По мнению профессора А.В. Крутских, именно Варшавский саммит НАТО стал поворотным моментом в плане милитаризации киберпространства. С 2018

---

[290] 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.

[291] Заявление по итогам встречи на высшем уровне в Варшаве обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Варшаве 8-9 июля 2016 URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=ru (дата обращения: 08.08.2022).

года Североатлантический альянс приступил к интеграции киберсил государств-участников НАТО в командную структуру военно-политического блока. В планах было создание в 2023 г. объединённого киберпотенциала альянса, который в случае необходимости был бы задействован Союзным командованием операций, в том числе при проведении наступательных кибероперацій[292].

Говоря о современной стратегии НАТО в киберпространстве на европейском континенте нельзя не упомянуть трансформацию подхода к так называемым «многодоменным операциям» (Multi-Domain Operations, MDO). Концепцию MDO, впервые имплементированную в 2016 г. в результате осознания рисков недостаточной защиты компьютерных систем, можно охарактеризовать в качестве некоего результата осмысления киберпространства в качестве витального компонента активного противоборства акторов международных отношений и неотъемлемого компонента глобальной и региональной системы безопасности. Таким образом, уже в 2016 году киберпространство рассматривали в качестве не только связующего звена и платформы для взаимодействия систем ведения боевых действий, но и как обособленную оружейную платформу[293]. Развитие вооруженными силами США концепта MDO шло параллельно с эволюцией подхода Североатлантического альянса к кибероперациям. В то время как вышеупомянутый Киберцентр НАТО в г. Таллине (Эстония) продолжал свою работу, руководством альянса было объявлено открытие Интегрированного центра НАТО по киберзащите (NICC) и заявлено продолжение разработки доктрины для кибероперацій[294].

---

[292] 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

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

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

После начала Специальной военной операции России на Украине (СВО) в период с 2022 по 2023 гг. концепция MDO стала рассматриваться Североатлантическим альянсом в качестве одного из ключевых стратегических приоритетов. Концепция альянса по многодоменным операциям, представленная в марте 2023 года, характеризовала MDO в качестве «организации военных действий во всех областях и средах, синхронизированных с невоенными действиями, чтобы позволить альянсу создавать конвергентные эффекты»[295].

Анализ первого года СВО показал необходимость развития концепта MDO с целью практической имплементации военных и коммерческих возможностей для разведки, обеспечения устойчивости связи, киберзащиты, координации, управления огнем и беспилотными авиационными системами.

Целесообразно отметить, что на современном этапе стал очевиден экспоненциальный рост значимости киберпространства в деятельности Североатлантического альянса. С течением времени международное сообщество свидетельствовало эволюцию доктринального оформления подходов альянса к проблемам обеспечения кибербезопасности, а также стратегии деятельности в киберпространстве. Киберпространство имеет огромное значение для организации и ее членов, поскольку современные военные операции и общая безопасность все более зависят от цифровых технологий.

Важнейшим этапов в формировании современной стратегии Североатлантического альянса в киберпространстве является состоявшийся в июне 2022 г. Мадридский саммит НАТО, где была утверждена новая стратегическая концепция военно-политического блока[296]. Особое внимание в данной концепции уделяется аспектам деятельности в киберпространстве, в

---

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

[296] Стратегическая концепция НАТО 2022 года https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf (дата обращения: 01.03.2024).

ней отмечается, что возможности НАТО в цифровом пространстве являются социальным элементов его оборонного и сдерживающего потенциала: «потенциал НАТО в области сдерживания и обороны основан на надлежащем сочетании ядерных и обычных сил и средств, а также сил и средств противоракетной обороны, дополненных космическими и кибернетическими средствами. Этот потенциал является оборонительным, соразмерным и полностью соответствует нашим международным обязательствам. Мы будем использовать военные и невоенные средства пропорциональным, согласованным и комплексным образом для реагирования на все угрозы нашей безопасности выбранным нами способом, в сроки и в областях по нашему усмотрению»[297]. Декларируется приверженность государств-членов военно-политического блока принципам так называемого «порядка, основанного на правилах». Фиксируется позиция стран-участниц НАТО о применимости к киберпространству действующего международного права, акцентируется что потенциальные акты злонамеренного кибервоздействия «могут привести к задействованию Североатлантическим советом положений статьи 5 Вашингтонского договора». Более того, Россия была определена в качестве наиболее существенной и непосредственной угрозой безопасности стран-участниц военно-политического блока, а также миру и стабильности на Евроатлантическом пространстве. Москве вменяется использование гибридных и киберсредств наряду с конвенциональными против участников и партнёров организации[298]: «Российская Федерация является наиболее значительной и прямой угрозой безопасности государств-членов НАТО, а также миру и стабильности в евроатлантическом регионе. Она стремится

[297] Стратегическая концепция НАТО 2022 года https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf (дата обращения: 01.03.2024).

[298] 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

установить сферы влияния и прямой контроль посредством принуждения, подрывной деятельности, агрессии и аннексии. Она использует обычные, кибер- и гибридные средства против нас и наших партнеров. Её направленные на принуждение военный потенциал, риторика и доказанная готовность использовать силу для достижения своих политических целей подрывают основанный на правилах международный порядок. Российская Федерация модернизирует свои ядерные силы и расширяет свои новые и разрушительные системы доставки двойного назначения, используя при этом в целях принуждения угрозу ядерного оружия. Ее целью является дестабилизация стран к востоку и югу от нас. На Крайнем Севере ее способность нарушить усиление стран НАТО и свободу судоходства через Северную Атлантику является стратегическим вызовом Североатлантическому союзу. Наращивание Москвой военной мощи, в том числе в регионах Балтийского, Черного и Средиземного морей, наряду с ее военной интеграцией с Беларусью, бросает вызов нашей безопасности и интересам»[299].

Мадридский саммит НАТО 2022 года и утверждённая на нём Стратегическая концепция ознаменовали собой критически важный этап в эволюции подходов Североатлантического альянса к безопасности в киберпространстве. Проведённый анализ позволяет заключить, что киберпотенциал был официально интегрирован в ядро стратегии сдерживания и обороны военно-политического блока, будучи определённым в качестве социально значимого элемента наравне с ядерными, обычными и космическими силами. Это свидетельствует о переходе от восприятия киберугроз как второстепенных к их признанию фундаментальным вызовом коллективной безопасности. Ключевым аспектом новой концепции стала чёткая легитимизация применения коллективных оборонительных мер, включая возможность активизации Статьи 5 Вашингтонского договора в ответ

[299] Стратегическая концепция НАТО 2022 года https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf (дата обращения: 01.03.2024).

на масштабные злонамеренные кибервоздействия. Данная позиция, подкреплённая заявлением о применимости международного права к киберпространству, формирует правовую и операционную основу для ответных действий Североатлантического альянса, повышая порог сдерживания. Существенным фактором, обусловившим данную трансформацию, была прямая идентификация Российской Федерации в качестве наиболее значительной и непосредственной угрозы. В официальной риторике НАТО акцентируется комплексный и гибридный характер этой угрозы, где киберсредства используются Москвой наряду с обычными вооружёнными силами, подрывной деятельностью и ядерной риторикой для принуждения и установления сфер влияния. Таким образом, киберпространство окончательно утвердилось в качестве одной из ключевых арен геополитического противостояния между НАТО и Россией, что детерминирует дальнейшую милитаризацию цифровой сферы и делает кибербезопасность неотъемлемым компонентом оборонного планирования Североатлантического альянса.

Проведенный анализ позволяет констатировать, что период с 2014 года по настоящее время представляет собой третий этап трансформации стратегии НАТО в киберпространстве, ключевой характеристикой которого стало официальное признание киберпространства в качестве полноценной области операций. Варшавский саммит 2016 года стал поворотным моментом в этом процессе, закрепив кибербезопасность в рамках коллективной обороны и обозначив необходимость эффективного противодействия угрозам в цифровой среде наравне с традиционными доменами. Последующая интеграция киберсил стран-членов НАТО в командную структуру военно-политического блока, а также разработка объединенного киберпотенциала свидетельствуют о последовательной милитаризации киберпространства. Особое значение в этом контексте приобрела концепция многодоменных операций (MDO), предполагающая комплексное использование военных и невоенных инструментов для достижения стратегических целей. Развитие

данной концепции, особенно после начала Специальной военной операции России на Украине, подчеркивает растущую роль киберпространства в современных конфликтах и необходимость его интеграции в общую систему безопасности НАТО. Стратегическая концепция Североатлантического альянса, принятая на Мадридском саммите 2022 года, подтвердила ключевые тенденции в политике НАТО, включая усиление киберкомпоненты в механизмах сдерживания и обороны, а также акцентирование гибридных угроз, исходящих от России. В документе Москва прямо обозначена как наиболее значительная угроза евроатлантической безопасности, что обуславливает дальнейшее наращивание альянсом киберпотенциала и разработку новых доктринальных подходов к противодействию цифровым вызовам. Таким образом, современный этап стратегии НАТО в киберпространстве характеризуется углубленной институционализацией кибероперaций, их интеграцией в оборонительную и наступательную доктрины, а также активным развитием многофакторных подходов к обеспечению безопасности в условиях цифровой эпохи. Эскалация киберугроз и их тесная взаимосвязь с гибридными формами конфликтов предопределяют дальнейшую эволюцию стратегии Североатлантического альянса в данном направлении.

Важнейшими характеристиками данного периода стали:

1. институционализация киберпотенциала через интеграцию национальных киберсил в структуру альянса;
2. разработка концепции многодоменных операций (MDO), рассматривающей киберпространство как самостоятельную платформу ведения боевых действий;
3. создание новых структурных элементов для координации оборонительных и наступательных возможностей.

Трансформация подходов НАТО демонстрирует переход от оборонительной парадигмы к комплексному восприятию киберпространства как:

1. среды для ведения гибридных конфликтов;
2. самостоятельного театра военных действий;
3. критически важного элемента системы коллективной безопасности.

Однако подобная милитаризация киберпространства вызывает ряд вопросов, касающихся: критериев применения статьи 5 Вашингтонского договора; правовых рамок наступательных кибероперациий; баланса между национальными и наднациональными элементами кибербезопасности[300].

Таким образом, рассматриваемый период заложил основы для дальнейшего развития киберстратегии НАТО, определив киберпространство как ключевой элемент современной системы международной безопасности, требующий постоянной адаптации подходов военно-политического блока к новым вызовам и угрозам.

Рассматривая трансформацию стратегии Североатлантического альянса на современном этапе, нельзя не упомянуть превалирующую роль США в деятельности НАТО. США одними из первых стали прорабатывать законодательные основы киберстратегии, нацеленной прежде всего на обеспечение безопасности страны после терактов 2001 г. С течением времени был принят не один десяток законодательных актов, создан ряд комитетов и агентств, ответственных за обеспечение информационной безопасности страны.

Активное участие США в киберстратегии НАТО подчеркивает их лидерство в этой области и демонстрирует необходимость коллективного подхода к преодолению киберугроз. Эффективная киберзащита требует не только технических решений, но и политической воли, международного сотрудничества и соблюдения этических норм.

На правах пионера интернет-технологий США регулярно обновляют государственные документы, прямо или косвенно связанные с обеспечением

[300] 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.

кибербезопасности страны. Частая смена декларируемых приоритетов происходит не только ввиду прихода к власти новых администраций, но и в первую очередь в связи с беспрецедентным распространением ИКТ и постоянным технологическим развитием, стремительно опережающим действия государств[301].

Старт формулированию официальных подходов в киберпространстве был дан еще в 2003 г., в годы администрации Дж. Буша-мл., когда появилась Национальная стратегия кибербезопасности[302].

В начале 2000-х годов НАТО начала осознавать важность кибербезопасности. Первые шаги в этом направлении были предприняты на саммите НАТО в Праге в 2002 году, где было решено создать новые возможности в области киберзащиты. Это решение стало первым шагом к формулированию киберстратегии, в которой подчеркивалась необходимость защиты информационных систем союзников и обеспечения их устойчивости к потенциальным кибератакам. США играли ключевую роль в этом процессе, подчеркивая важность интеграции киберзащиты в общую стратегию безопасности НАТО. В этот период внимание сосредоточивалось на создании базовых механизмов для обмена информацией о киберугрозах и разработке стандартов киберзащиты[303].

К 2007 году киберугрозы стали более очевидными для государств Североатлантического альянса, особенно после ранее упомянутых кибератак на Эстонию, которые продемонстрировали уязвимость государств к киберугрозам. Это событие стало катализатором для НАТО, чтобы более активно развивать свою киберстратегию. В 2008 году по итогам саммита

---

[301] 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).

[302] The National Strategy to Secure Cyberspace. February 2003 // The White House. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy. pdf (accessed: 16.05.2023).

[303] NATO (2002). "Prague Summit Declaration". Prague Summit Declaration.

НАТО в Бухаресте (Румыния) была принята Политика киберзащиты НАТО («Cyber Defence Policy»), в которой подчеркивалась необходимость защиты информационных систем союзников и обмена информацией о киберугрозах[304]. США, как ведущая держава в области технологий, начали активно продвигать идеи о совместной киберзащите и необходимости создания специальных структур для реагирования на кибератаки. Это время стало важным для формирования совместных механизмов реагирования на киберугрозы и повышения уровня осведомленности среди союзников о потенциальных рисках[305].

США активно продвигают идею киберзащиты как важного элемента коллективной безопасности в НАТО. В 2016 году на саммите в Варшаве НАТО признало киберпространство новым полем боя, что стало значительным шагом в направлении интеграции киберзащиты в стратегию Североатлантического альянса.

Это решение открывало новые возможности для сотрудничества между союзниками в области кибербезопасности. США сыграли ключевую роль в этом процессе, подчеркивая важность киберзащиты как элемента коллективной безопасности. На этом этапе НАТО начала проводить регулярные учения по киберзащите, такие как Cyber Coalition, которые позволили улучшить взаимодействие между союзниками и повысить готовность к возможным кибератакам, что также способствовало созданию новых механизмов для обмена информацией и совместного реагирования на киберугрозы[306].

Программа учений включала в себя:

- создание киберкоманд: НАТО создало специальные киберкоманды, которые отвечают за защиту информационных систем стран-членов.

---

[304] NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf

[305] NATO (2008). "Cyber Defence Policy". Cyber Defence Policy.

[306] NATO (2016). "Warsaw Summit Communiqué". Warsaw Summit Communiqué.

- совместные операции: разработка совместных операций и учений в киберпространстве с целью улучшения взаимодействия между союзниками.

Саммит в Варшаве проходил в ключевой для альянса момент, связанный с кардинальными изменениями в Европейском регионе и на мировой арене в целом. С точки зрения Коллективного Запада с Соединёнными Штатами в главной роли, НАТО столкнулась с существенными угрозами безопасности евроатлантического региона. Целью саммита стала идентификация основных направлений действий, необходимых для адаптации организации к принципиально новым вызовам в области обеспечения коллективной безопасности[307].

Анализ трансформации стратегии Североатлантического альянса в киберпространстве на современном этапе позволяет сделать вывод о ключевой роли США в формировании и реализации киберстратегии НАТО. Соединённые Штаты, обладая значительным технологическим и стратегическим потенциалом, с начала 2000-х годов выступали основным драйвером развития кибербезопасности как на национальном, так и на наднациональном уровне. Принятие Национальной стратегии кибербезопасности в 2003 году заложило основу для последующей интеграции киберугроз в систему коллективной обороны НАТО. Первые шаги в этом направлении были предприняты на Пражском саммите НАТО 2002 года, где была обозначена необходимость создания механизмов киберзащиты. Однако решающим фактором, ускорившим разработку единой стратегии альянса в киберпространстве, стали масштабные кибератаки на Эстонию в 2007 году, продемонстрировавшие уязвимость государств-членов перед цифровыми угрозами. В ответ на эти вызовы в 2008 году была принята Политика киберзащиты НАТО («Cyber Defence Policy»), закрепившая принципы совместного реагирования и обмена информацией. Дальнейшее развитие

---

[307] NATO: The Enduring Alliance 2016 URL: http://www.krzysztofmiszczak.pl/files/262649006/lib/FWPN_publication_on_NATO.pdf (дата обращения: 03.02.2022).

стратегии НАТО в киберпространстве, особенно после признания киберпространства областью операций на Варшавском саммите Североатлантического альянса в 2016 году, во многом определялось лидерством США, которые активно продвигали идею кибербезопасности как неотъемлемого элемента коллективной обороны. Создание специализированных киберкоманд, проведение регулярных учений (таких как Cyber Coalition) и разработка доктринальных основ многофакторного противодействия угрозам подчеркивают стремление альянса к комплексной милитаризации киберпространства. Таким образом, представляется возможным констатировать, что современная киберстратегия НАТО формируется под значительным влиянием США, чей опыт в области информационной безопасности и технологического доминирования задает вектор развития Североатлантического альянса. Однако динамичный характер киберугроз и необходимость адаптации к новым вызовам требуют дальнейшего укрепления международного сотрудничества, выработки единых стандартов реагирования и балансирования между оборонительными и наступательными возможностями в цифровой сфере.

Резюмируя вышесказанное, отметим, что технологический прогресс трансформирует традиционные подходы к международной безопасности, делая киберпространство новым театром военных и стратегических операций. В этом контексте эволюция стратегии НАТО в киберпространстве отражает адаптацию альянса к вызовам цифровой эпохи, включая гибридные угрозы и киберконфликты.

Анализ трансформации киберстратегии НАТО позволяет выделить три ключевых этапа. Первый этап (1990-е – 2006 гг.) ознаменовался осознанием киберугроз в качестве потенциального риска для коллективной безопасности. Изначально киберпространство воспринималось как сфера гражданской инфраструктуры, однако серия инцидентов, включая кибератаки во время операции «Союзная сила» (1999), продемонстрировала его военно-стратегическое значение. Важнейшими вехами этого периода стали Пражский

(2002) и Рижский (2006) саммиты, на которых были заложены основы системной киберстратегии НАТО, включая создание программы NCIRC (NATO Computer Incident Response Capability).

Второй этап (2007–2014 гг.) характеризовался переходом от фрагментарных мер к формированию комплексной стратегии кибербезопасности. Ключевым катализатором стали масштабные кибератаки на Эстонию (2007), Грузию (2008) и Украину (2014), которые подчеркнули роль киберпространства в гибридных конфликтах. В ответ Североатлантическим альянсом был учрежден Киберцентр в Таллине (2008) и была принята обновленная Стратегическая концепции (2010), которая закрепила кибербезопасность в рамках коллективной обороны.

Третий этап (2014 г. – настоящее время) связан с признанием киберпространства полноценной областью операций. Варшавский саммит (2016) стал поворотным моментом, официально включив киберугрозы в механизм коллективной безопасности (статья 5 Вашингтонского договора). Дальнейшая милитаризация киберпространства проявилась в развитии концепции многодоменных операций (MDO), интеграции национальных киберсил в структуру альянса и создании новых координационных центров, таких как NICC (NATO Integrated Cyber Defence Centre). Мадридская стратегическая концепция НАТО (2022) подтвердила приоритет кибербезопасности, обозначив Россию как основную угрозу и акцентировав необходимость противодействия гибридным и киберугрозам.

Особую роль в формировании киберстратегии НАТО играют США, выступающие технологическим и стратегическим лидером альянса. С 2003 года американские администрации последовательно развивают национальные и наднациональные механизмы кибербезопасности, что отражается в стратегии НАТО, включая проведение учений Cyber Coalition и создание специализированных киберкоманд. Таким образом, трансформация стратегии НАТО в киберпространстве демонстрирует переход от оборонительных мер к комплексному восприятию цифровой среды как ключевого элемента

современной безопасности. Однако остаются нерешенными вопросы, связанные с критериями применения коллективной обороны, правовыми рамками кибероперaций и балансом между национальными и наднациональными подходами. Дальнейшее развитие киберстратегии Североатлантического альянса будет определяться способностью адаптироваться к динамичным угрозам, сохраняя при этом международно-правовую легитимность.

2.2. Концептуальные основы реализации стратегии НАТО в киберпространстве на современном этапе

На сегодняшний день вопросы обеспечения кибербезопасности выходят на глобальный уровень, на уровень создания единой системы кибербезопасности как государственных акторов, так и международных организаций, включая НАТО. Пока что не существует однозначного определения киберпространства. В докладе исследовательской службы конгресса США в 2001 году впервые прозвучало общегосударственное определение киберпространства, где оно было определено в качестве «всеохватывающего множества связей между людьми, созданного на основе компьютеров и телекоммуникаций вне зависимости от физической географии»[308].

Можно констатировать, что на сегодняшний день одной из ключевых характеристик научно-технологического развития вооружённых сил национальных государств является процесс повсеместной и всеобъемлющей цифровизации, подразумевающей «насыщение войск на всех уровнях, и прежде всего штабов различного уровня, «умными устройствами», в том числе средствами связи, управления, навигации»[309]. С одной стороны,

[308] Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны. – URSS, 2010.
[309] Манойло А.В. Современные стратегии кибербезопасности и кибероборoны НАТО // АПЕ. 2020. №3. URL: https://cyberleninka.ru/article/n/sovremennye-strategii-kiberbezopasnosti-i-kiberoborony-nato (дата обращения: 23.01.2025).

интенсификация процесса стремительного развития технологий предоставляет военным штабам возможность значительно расширить свои оперативные возможности за счет оптимизации использования войск. С другой стороны, приводит к существенному увеличению уязвимости вооруженных сил перед кибератаками и другими методами, способными нарушить функционирование систем управления и связи. В условиях, когда такие системы начинают давать сбои или полностью выходят из строя, современные военные формирования становятся значительно более уязвимыми по сравнению с предыдущими эпохами, когда уровень информатизации был ниже. Таким образом, исследование кризиса контроля над вооружениями не может быть проведено в полной мере без учета вопросов, связанных с обеспечением деятельности в киберпространстве[310].

Проведенный анализ позволяет констатировать, что динамика развития киберпространства формирует комплексный вызов международной безопасности, характеризующийся глубокой противоречивостью. Ключевая парадоксальность заключается в том, что технологический прогресс, выступающий основным драйвером повышения оперативных возможностей современных вооруженных сил, одновременно является источником их фундаментальной уязвимости. Всеобъемлющая цифровизация, подразумевающая интеграцию «умных» устройств в системы управления и связи, создает принципиально новую, высоко централизованную архитектуру ведения боевых действий, критически зависимую от бесперебойного функционирования кибернетической инфраструктуры. Подобная зависимость порождает стратегическую дилемму: усиление военной мощи неминуемо сопряжено с расширением поверхности для потенциальных атак, способных парализовать командный потенциал, что делает современные армии в ситуации сбоя уязвимее, чем менее технологичные формирования прошлого.

---

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

Данная реальность актуализирует необходимость перехода к глобальным моделям регулирования, о чем свидетельствует тенденция к формированию единых систем кибербезопасности на уровне государств и международных организаций, таких как НАТО. Однако процесс выработки эффективных механизмов кооперации наталкивается на системное препятствие – отсутствие консенсусного онтологического определения самого киберпространства. Несмотря на попытки его концептуализации, подобные предложенной исследовательской службой Конгресса США в 2001 году, эта категория продолжает оставаться предметом интерпретаций, что блокирует разработку универсальных правовых норм и режимов контроля. Следовательно, исследование проблем стратегической стабильности, контроля над вооружениями и управления кризисами в современную эпоху теряет аналитическую ценность без интеграции кибернетического измерения. Киберпространство утвердилось в качестве пятой операционной среды, а киберугрозы – в качестве неотъемлемого компонента гибридных конфликтов. Таким образом, преодоление концептуальной неопределенности и разработка моделей, способных учесть двойственную природу цифровизации, становятся императивом для обеспечения международной безопасности в XXI веке.

Говоря о роли и месте Североатлантического альянса в глобальных процессах, связанных с имплементацией возможностей киберпространства в практической плоскости, можем констатировать что в течение последнего десятилетия кибернетические угрозы приобретают все более регулярный, сложный, разрушительный и силовой характер. На современном этапе киберпространство стало ключевой сферой геополитической конкуренции, что подтверждает необходимость адаптации стратегий международных организаций к новым вызовам и угрозам. НАТО является частью системы европейской и глобальной безопасности и одним из наиболее значимых международных институтов во всём мире. Будучи ведущим военно-политическим блоком, Североатлантический альянс активно трансформирует свою стратегию в киберпространстве, стремясь обеспечить коллективную

кибербезопасность и противодействовать угрозам гибридного характера. 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.

Так, например, в рассматриваемый в исследовании период государствами-членами Североатлантического альянса был предпринят перечень витальных мер в сфере кибернетической защиты. Согласно публикации сотрудника Управления новых вызовов безопасности НАТО Л. Брент, «впервые руководители Североатлантического союза признали необходимость укреплять силы и средства в целях защиты от кибернетических нападений на встрече на высшем уровне в 2002 году в Праге. С тех пор кибернетической проблематике стало уделяться все большее внимание в повестках дня встреч НАТО на высшем уровне»[311].

В настоящее время НАТО предпринимает значительные усилия в сфере организации киберзащиты: так, в 2014 г. государства-члены НАТО «определили киберзащиту как одну из основных составляющих коллективной обороны», заявив, что «в результате кибернетического нападения может быть приведено в действие положение о коллективной обороне»; в 2016 г. государства-члены НАТО «обозначили кибернетическое пространство в качестве одной из сфер проведения военных операций» (как в военное, так и в мирное время) и обязались в дальнейшем «в приоритетном порядке укреплять киберзащиту своих национальных сетей и инфраструктуры»[312]. В 2018 г.

---

[311] Роль НАТО в кибернетическом пространстве URL: https://www.nato.int/docu/review/ru/articles/2019/02/12/rol-nato-v-kiberneticheskom-prostranstve/index.html (дата обращения: 17.03.2024).

[312] Brent L. (2019). The role of NATO in cyber space [Rol' NATO v kiberneticheskom prostranstve] // NATO Review. – Brussels. – 12.02. – Mode of access: https://www.nato.int/docu/review/ru/articles/2019/02/12/rol-nato-v-kiber neticheskom-prostranstve/index.html (Date of access – 28.01.2020)

страны-участницы НАТО отдельно договорились о том, как именно интегрировать деятельность по обеспечению кибербезопасности на уровне отдельных национальных государств-членов НАТО «в контексте операций и миссий Североатлантического альянса», а также приняли решение о создании «Центра кибероперацій» военно-политического блока[313].

Поскольку киберугрозы присутствуют постоянно, хотя их характер меняется, Североатлантическому альянсу необходимо все время проверять, адаптируется ли он и реагирует ли он надлежащим образом.

Эволюция подходов НАТО к вопросам кибербезопасности демонстрирует последовательный и поступательный процесс институционализации киберпространства в качестве ключевой операционной среды. Анализ решений, принятых в период с 2014 по 2018 годы, позволяет выявить четкую стратегическую траекторию, характеризующуюся тремя взаимосвязанными тенденциями. Во-первых, наблюдается переход от восприятия киберугроз как потенциального фактора риска к их официальному признанию в качестве непосредственного повода для применения статьи 5 Вашингтонского договора о коллективной обороне. Это принципиальное решение 2014 года легитимизировало кибератаку как акт агрессии, приравниваемый к вооруженному нападению, что подняло кибербезопасность с технического до стратегического уровня и заложило правовую основу для коллективного ответа. Во-вторых, последующее объявление киберпространства в 2016 году полноправной сферой ведения военных операций ознаменовало завершение концептуального переформатирования. Данный шаг не только поставил кибероперации в один ряд с действиями на суше, на море и в воздухе, но и создал предпосылки для разработки соответствующих доктрин, стандартов и наступательных возможностей, интегрируемых в общие планы Североатлантического альянса как в мирное,

[313] Brussels Summit declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels / NATO. – Brussels, 2018. – 11.07. – Mode of access: https://www. nato.int/cps/en/natohq/official_texts_156624.htm (Date of access – 28.01.2020).

так и в военное время. В-третьих, решения 2018 года свидетельствуют о переходе к фазе практической имплементации и углубленной интеграции. Создание Центра кибероперациий и выработка механизмов координации национальных усилий в рамках операций и миссий НАТО указывают на стремление преодолеть фрагментарность и создать единый, скоординированный и оперативно управляемый командный потенциал. Это отражает понимание того, что кибербезопасность не может обеспечиваться исключительно на национальном уровне и требует централизованного управления для эффективного сдерживания и ответа. Однако данный процесс является не завершенным, а перманентным. Постоянно эволюционирующий характер киберугроз формирует императив для НАТО находиться в состоянии непрерывной адаптации. Североатлантический альянс вынужден проводить постоянный мониторинг и критическую оценку адекватности своих политик, структур и возможностей, чтобы сохранять стратегическую устойчивость и выполнять обязательства по коллективной обороне в условиях быстро меняющейся цифровой реальности. Таким образом, киберполитика НАТО представляет собой динамически развивающуюся систему, находящуюся в диалектической взаимосвязи с внешними вызовами.

Говоря о целях и трудностях Североатлантического альянса в контексте своей деятельности в киберпространстве, первостепенно целесообразно обратиться к итогам и результатам саммитов НАТО, прошедших в г. Варшава, Польша в 2016 г. и в г. Брюсселе, Бельгии в 2018 г. Впервые наиболее чёткое заявление о цели НАТО в киберпространстве было сделано в ходе Варшавского саммита 2016 г. и затем в ходе саммита 2018 г. в Брюсселе. Так, согласно заявлению по итогам встречи на высшем уровне в Брюсселе, государства-члены Североатлантического альянса «должны уметь действовать в кибернетическом пространстве так же эффективно, как и в воздухе, на суше и на море, чтобы укрепить потенциал сдерживания и обороны

НАТО»[314]. В связи с вышесказанным стало очевидным стремление стран-участниц военно-политического блока:

- интенсифицировать процесс трансформации киберпространства в сферу операций;

- достигнуть консенсуса в сфере интеграции внутренних действий государств-членов Североатлантического альянса в киберпространстве и в контекст операций и миссий НАТО в рамках строгого политического надзора;

- рассматривать возможность выявления злонамеренных действий в кибернетической сфере и принятия согласованных действий, признавая это суверенной прерогативой государств[315].

Можем констатировать, что по состоянию на сегодняшний день Североатлантический альянс работает на двух основных направлениях:

1) над тем, чтобы киберпространство стало сферой операций,

1) над выполнением обязательства по киберзащите.

Рассматривая роль киберпространства в качестве сферы операций военно-политического блока, первостепенно целесообразно отметить, что хотя в общетеоретическом плане подходы Североатлантического альянса к обеспечению информационной и кибербезопасности не отличаются существенно от подходов США и РФ (ряд положений концептуальных документов РФ перекликается с пунктами военных доктрин США и практических руководств в данной области). Все члены НАТО используют в своих руководящих документах сходные понятия и целевые установки, а также руководствуются схожей (по своему организационному и техническому

---

[314] Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 11-12 июля 2018 года URL: https://www.nato.int/cps/cn/natohq/official_texts_156624.htm?selectedLocale=ru (дата обращения: 17.03.2024).

[315] Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 11-12 июля 2018 года URL: https://www.nato.int/cps/cn/natohq/official_texts_156624.htm?selectedLocale=ru (дата обращения: 17.03.2024).

исполнению) тактикой действий. Заметные различия в подходах стран-участниц НАТО к обеспечению информационной и кибербезопасности возникают лишь на уровне практической реализации задач по обеспечению информационной и кибербезопасности государства (на уровне стратегии, тактики, форм и методов)[316].

С момента, когда в 2016 году по итогам Варшавского саммита Североатлантического альянса государства-члены НАТО определили киберпространство как область операций, военно-политический блок прошел через несколько значительных этапов развития. В частности, стоит отметить, что в октябре 2018 года НАТО объявило о создании на начальном этапе Центра кибероперaций, который функционирует как компонент военно-политического блока, занимающийся вопросами киберпространства в рамках операций.

В 2016 году Североатлантический альянс принял Комплексную политику в области киберзащиты (Comprehensive Cyber Defence Policy), которая стала основой для всех последующих инициатив в этой области. CCDP направлена на достижение следующих целей:

1. Защита собственных сетей и инфраструктуры НАТО, включает обеспечение безопасности информационных систем, используемых для управления войсками, разведки и связи.
2. Укрепление киберустойчивости государств-членов. НАТО стремится помочь своим членам развить национальные возможности для защиты от кибератак.
3. Интеграция киберпространства в стратегию коллективной обороны. Документ подчёркивает, что киберпространство является областью операций, где применяются принципы статьи 5 Вашингтонского договора.

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

4. Сотрудничество с партнёрами. НАТО активно взаимодействует с частным сектором, академическими учреждениями и международными организациями для обмена знаниями и технологиями.

CCDP основана на нескольких ключевых принципах:

- Проактивная защита. НАТО стремится не только реагировать на кибератаки, но и предотвращать их, используя передовые технологии и методы.
- Международное сотрудничество. Североатлантический альянс активно сотрудничает с другими международными организациями, такими как ООН и ЕС, для разработки норм и стандартов в области кибербезопасности.
- Гибкость и адаптивность. Политика предусматривает регулярное обновление стратегий и подходов в ответ на новые угрозы.

Для реализации CCDP НАТО использует ряд механизмов и инструментов:

a. Создание специализированных структур

В рамках CCDP был создан Центр оперативного командования в киберпространстве (Cyberspace Operations Centre, CyOC), который отвечает за координацию действий в случае кибератак. Кроме того, был учреждён Киберпространственный командный центр (Cyberspace Command Centre), который занимается разработкой стратегий и оперативных планов.

b. Укрепление киберустойчивости стран-членов

НАТО оказывает поддержку своим членам в развитии национальных возможностей кибербезопасности. Это включает:

- Обучение и подготовку специалистов. НАТО проводит регулярные тренинги и учения, такие как Cyber Coalition, которые позволяют странам-участницам отработать совместные действия в случае кибератак.

- Техническую помощь. Североатлантический альянс предоставляет странам-членам технологии и оборудование для защиты критической инфраструктуры.
- Разработку национальных стратегий кибербезопасности. НАТО помогает странам разрабатывать и внедрять стратегии, соответствующие международным стандартам.

c. Сотрудничество с частным сектором и академическими учреждениями

НАТО активно сотрудничает с частным сектором и академическими учреждениями для укрепления своих кибервозможностей. В 2020 году был создан Инновационный фонд НАТО (NATO Innovation Fund), который финансирует проекты в области кибербезопасности, искусственного интеллекта и других передовых технологий.

d. Учения и симуляции кибератак.

НАТО регулярно проводит учения и симуляции кибератак, чтобы проверить готовность своих членов к реальным инцидентам. Одним из ключевых мероприятий является Cyber Coalition, крупнейшие киберучения Североатлантического альянса, в которых участвуют более 30 стран.

Помимо этой критически важной организационной адаптации на встрече на высшем уровне в Брюсселе страны НАТО договорились о том, как интегрировать внутренние действия государств, осуществляемые странами НАТО на добровольной основе, в операции и миссии Североатлантического союза. Вместе с тем приобретают более четкие очертания стратегия и руководящие указания. В июне 2018 года страны НАТО утвердили «Видение и стратегию относительно кибернетического пространства как сферы операций»[317]. В 2019 г. была завершена работа над первой доктриной кибероперациий НАТО, которую «предстоит утвердить странам НАТО и

[317] NATO in the Cyber Age: Strengthening security and defence, stabilising detterence. (2019) / NATO. – Brussels. – 18.04. – 16 p. – Mode of access: https://nato-pa.int/download-file?filename=sites/default/files/2019-04/087_ STC_19_E%20-%20NATO.pdf (Date of access – 28.01.2020).

которая в таком случае станет руководством для командующих (командиров) НАТО»[318][319][320].

Обучением специалистов НАТО по кибербезопасности и кибероборонe занимается Центр передового опыта НАТО по совместной киберзащите, отвечающий также за выработку «учебно-образовательных решений» в сфере операций по кибербезопасности и кибероборонe в интересах всех государств-членов Североатлантического альянса. Закрепление знаний, умений и навыков происходит в форме регулярно проводимых учений: примером могут служить учения «Cyber Coalition» (в 2018 г. более 700 участников)[321], посвященные интеграции в военные операции НАТО национальных сил и средств, добровольно предоставляемых государствами-участниками, а также крупнейшие после окончания холодной войны учения «Trident Juncture 2018», в ходе которых отрабатывалось кризисное управление в условиях кибератак высокой степени интенсивности[322][323].

Представляется возможным констатировать, что подходы Североатлантического альянса к обеспечению кибербезопасности в целом соответствуют общемировым тенденциям, включая концепции, разрабатываемые США и РФ. На доктринальном уровне наблюдается значительное сходство в терминологии, целевых установках и базовых принципах организации кибероборонe. Однако на практике реализация этих принципов государствами-членами НАТО имеет существенные различия,

---

[318] Брент Л. Роль НАТО в кибернетическом пространстве // Вестник НАТО. – Брюссель, 2019. – 12.02. – URL: https://www. nato.int/ docu/review/ru/articles/2019/02/12/rol-nato-v-kiberneticheskom-prostranst ve/index.html (дата обращения – 28.01.2024).

[319] NATO. (2018). Cyberspace Operations Centre. Retrieved from https://www.nato.int

[320] NATO. (2020). Defence Capacity Building Initiative. Retrieved from https://www.nato.int

[321] Cyber Coalition helps prepare NATO for today's threats. (2018) / NATO. – Brussels. – 27.11. – Mode of access: https://www.nato.int/cps/ru/natohq/ news_160898.htm?selectedLocale=en (Date of access – 28.01.2020).

[322] Trident Juncture 18: Media resources. (2018) / NATO. – Brussels. – 31.10. – Mode of access: https://www.nato.int/cps/en/natohq/news_158620.htm? selectedLocale=en (Date of access – 28.01.2020).

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

обусловленные национальными особенностями, уровнем технологического развития и степенью интеграции в структуры альянса.

С момента официального признания киберпространства сферой операций на Варшавском саммите (2016 г.) НАТО предприняла ряд ключевых шагов по институционализации своей киберстратегии. Принятие Комплексной политики в области киберзащиты (CCDP) заложило основу для системного подхода, включающего защиту инфраструктуры альянса, укрепление киберустойчивости стран-членов, интеграцию киберпространства в коллективную оборону и развитие международного сотрудничества. Создание специализированных структур свидетельствует о стремлении НАТО к централизованному управлению кибероперациями. Важным элементом стратегии Североатлантического альянса является развитие киберпотенциала стран-участниц посредством обучения профильных специалистов, технической поддержки и проведения масштабных учений. Более того, сотрудничество с частным сектором и академическими институтами подчеркивает стремление военно-политического блока к адаптации передовых технологий в сфере кибербезопасности. Тем не менее, несмотря на формальное единство подходов, реализация стратегии НАТО в киберпространстве остается неоднородной. Различия в возможностях и приоритетах стран-членов приводят к асимметрии в уровне киберзащиты, что может создавать уязвимости в системе коллективной безопасности. Кроме того, сохраняются вопросы, связанные с критериями применения статьи 5 Вашингтонского договора, правовыми рамками наступательных кибероперациий и балансом между национальным суверенитетом и наднациональным управлением. Таким образом, стратегия НАТО в киберпространстве продолжает эволюционировать, сочетая унифицированные доктринальные принципы с гибкой адаптацией к новым вызовам. Однако её эффективность будет зависеть от способности военно-политического блока преодолеть фрагментацию в реализации киберстратегии,

усилить координацию между членами и выработать чёткие механизмы реагирования на быстро меняющиеся киберугрозы.

Рассматривая второе ключевое для Североатлантического альянса направление деятельности в киберпространстве, касающееся выполнения обязательств по киберзащите, целесообразно отметить, что в условиях растущей значимости киберпространства и увеличения числа кибератак, вопрос о том, как квалифицировать злонамеренные действия в киберпространстве в контексте международных норм, становится особенно актуальным. Кибератаки могут наносить значительный ущерб критической инфраструктуре, вызывать экономические потери и подрывать доверие к государственным институтам. Однако сложность идентификации и атрибуции подобных атак создает дополнительные сложности для государств, международных организаций и военно-политических блоков, включая Североатлантический альянс, стремящихся адекватно ответить на них. В настоящий момент можно констатировать, что НАТО адаптирует свою стратегию коллективной безопасности, включая кибератаки в свои планы и обязательства перед членами. Это подчеркивает важность кибербезопасности как составной части общей безопасности Североатлантического альянса. Однако отсутствие ясных механизмов для определения источника атаки затрудняет принятие решений о правомерности применения силы, что в свою очередь создает правовые и политические дилеммы для государств, которые могут оказаться под давлением необходимости реагировать на кибератаки, не имея достаточных доказательств их происхождения[324]. Хотя статья 5 Североатлантического договора гласит, что если одно государство-член НАТО становится жертвой вооруженного нападения, все остальные страны-участницы Североатлантического союза будут считать этот акт насилия вооруженным нападением на все страны НАТО и предпримут действия,

[324] 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).

которые сочтут необходимыми, чтобы помочь стране НАТО, подвергшейся нападению[325], вопрос о её активизации в случае кибератаки на одно из государств-членов военно-политического блока остаётся открытым.

Одной из основных проблем, связанных с применением статьи 5 в контексте кибератак, является сложность атрибуции. Кибератаки часто осуществляются анонимно, и идентификация их источника может быть затруднена, неопределенность в атрибуции кибератак создает правовые и политические дилеммы для государств, что затрудняет принятие решений о правомерности применения силы. Это в свою очередь затрудняет возможность единогласного решения среди членов НАТО о необходимости применения коллективной обороны. Кроме того, необходимо учитывать, что кибератаки могут варьироваться по своему масштабу и последствиям. Некоторые атаки могут быть достаточно разрушительными, чтобы вызвать серьезные последствия для национальной безопасности, тогда как другие могут быть менее значительными и не требовать активных ответных действий. В этом контексте, необходимость чёткой классификации и определения уровня угрозы, исходящей от кибератак, становится критически важной для применения статьи 5, что усугубляется недостатком ясности в правовых нормативах. Современные международные нормы не всегда учитывают специфику киберугроз, что может привести к правовым коллизиям, а необходимость пересмотра международного права в свете киберугроз становится очевидной, чтобы обеспечить адекватные механизмы реагирования на такие вызовы. Согласно заявлению главы Военного комитета НАТО Р. Бауэра в июне 2024 г., страны НАТО договорились, что кибератака

---

[325] Коллективная оборона и статья 5 https://www.nato.int/cps/ru/natohq/topics_110496.htm#:~:text=%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F%205%20%D0%B3%D0%BB%D0%B0%D0%B2%D0%B0%D1%81%D0%B8%D1%82%2C%20%D1%87%D1%82%D0%BE%2C%20%D0%B5%D1%81%D0%BB%D0%B8,%D1%87%D1%82%D0%BE%D0%B1%D1%8B%20%D0%BF%D0%BE%D0%BC%D0%BE%D1%87%D1%8C%20%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%20%D0%9D%D0%90%D0%A2%D0%9E%2C%20%D0%BF%D0%BE%D0%B4%D0%B2%D0%B5%D1%80%D0%B3%D1%88%D0%B5%D0%B9%D1%81%D1%8F

против одной из них может стать причиной применения пятой статьи устава Североатлантического альянса. По его словам, это было общим решением всех государств-членов НАТО. Кибератака, по словам Р. Бауэра, может стать основанием для начала дебатов о применении пятой статьи и «выполнения последующих процедур». При этом, для того чтобы признать кибератаку на важную цифровую инфраструктуру актом войны, нужно «удостовериться, что атака совершена государством, а не неизвестным частным актором»[326].

Необходимо отметить, что в НАТО по линии обязательства о киберзащите поощряется общегосударственная работа по адаптации в каждой отдельной стране НАТО. Обязательство было взято в контексте статьи 3 Вашингтонского договора, которая гласит, что страны Североатлантического союза «будут поддерживать и наращивать свой индивидуальный и коллективный потенциал борьбы с вооруженным нападением»[327]. Поскольку невозможно полностью отделить военные, гражданские и промышленные вопросы в данной сфере, НАТО в большой мере заинтересована в совершенствовании потенциала киберзащиты организаций, не относящихся к оборонным органам.

В обязательстве подчеркивается ход работы в таких областях, как обеспечение киберзащиты должными ресурсами во всей государственной сфере; обмен информацией и передовым опытом; использование новаторских методов, применяемых в научных кругах и частном секторе. Ежегодно страны-участницы НАТО дают оценку своей работе с помощью общего свода контрольных показателей. В своем докладе, представленном на встрече на высшем уровне в Брюсселе, государства-члены Североатлантического альянса подчеркнули дальнейшую целесообразность обязательства: благодаря ему

---

[326] В НАТО допустили применение пятой статьи договора в случае кибератаки URL: https://lenta.ru/news/2024/06/01/v-nato-dopustili-primenenie-pyatoy-stati-dogovora-v-sluchae-kiberataki/ (дата обращения: 05.07.2024).

[327] Североатлантический договор Вашингтон, Федеральный округ Колумбия, 4 апреля 1949 г. URL: https://www.nato.int/cps/ru/natolive/official_texts_17120.htm (дата обращения: 23.01.2024).

удалось привлечь внимание политического руководства к вопросам киберзащиты, а также поощрить внутригосударственное взаимодействие в странах-участницах НАТО[328].

Вместе с тем члены НАТО предпринимают шаги, с тем чтобы рассмотреть вопрос о более систематическом реагировании на злонамеренную кибернетическую деятельность, не достигающую порога вооруженного конфликта. На встрече на высшем уровне в Брюсселе государства-члены Североатлантического альянса выразили свою решимость «использовать весь свой потенциал, в том числе в кибернетической сфере, чтобы обеспечивать сдерживание и оборону и противодействовать всему спектру кибернетических угроз, в частности осуществляемых в рамках гибридной кампании».[329]

Более того, члены военно-политического блока решили «продолжить дальнейшую совместную работу по разработке мер, которые позволили бы заставить пойти на затраты тех, кто причинил вред». Данный полный спектр мер реагирования, осуществляемых всегда в соответствии с международным правом и принципами сдержанности и соразмерности, имеет критическое значение для эффективного решения часто встречающейся проблемы кибернетической деятельности ниже порога вооруженного конфликта[330].

Наконец, чтобы успешно адаптироваться к быстро меняющейся обстановке, НАТО работает в более тесной увязке с постоянно растущим

---

[328] Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 11-12 июля 2018 года URL: https://www.nato.int/cps/cn/natohq/official_texts_156624.htm?selectedLocale=ru (дата обращения: 17.03.2024).

[329] Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 11-12 июля 2018 года URL: https://www.nato.int/cps/cn/natohq/official_texts_156624.htm?selectedLocale=ru (дата обращения: 17.03.2024).

[330] Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 11-12 июля 2018 года URL: https://www.nato.int/cps/cn/natohq/official_texts_156624.htm?selectedLocale=ru (дата обращения: 17.03.2024).

числом партнеров. В 2016 году генеральный секретарь Североатлантического альянса, председатель Европейского совета и председатель Европейской комиссии выступили с совместным заявлением о сотрудничестве НАТО и ЕС. В соответствии с этим заявлением, а также техническим соглашением, которое было заключено между группами по реагированию на инциденты НАТО и ЕС, расширилось сотрудничество между организациями, в частности в таких областях, как обмен информацией, учебная подготовка, научно-исследовательская работа и учения[331].

Благодаря партнёрству между НАТО и промышленностью углубляются их связи в кибернетической сфере. По линии данной всеобъемлющей программы создаются многочисленные площадки для обмена информацией, изучения тенденций угроз и передового опыта. Данное взаимодействие способствует укреплению доверия в отношениях Североатлантического альянса с промышленным сектором и помогает всем сторонам лучше предотвращать кибернападения и реагировать на них.

Таким образом, резюмируя вышесказанное, отметим, что на современном этапе киберпространство приобретает ключевое значение в контексте глобальной безопасности, становясь не только средой технологического взаимодействия, но и ареной геополитической конкуренции. Несмотря на отсутствие единого общепризнанного определения киберпространства, его роль в военно-политической стратегии государств и международных организаций неуклонно возрастает.

Процесс цифровизации вооружённых сил, с одной стороны, расширяет оперативные возможности государств, а с другой – увеличивает их уязвимость перед киберугрозами. В условиях, когда сбои в системах управления и связи могут парализовать военные формирования, вопросы кибербезопасности становятся неотъемлемой частью стратегий национальной и коллективной

[331] Сотрудничество ЕС–НАТО: Совет ЕС принял выводы по реализации Совместной декларации URL: https://www.eeas.europa.eu/node/16866_en (дата обращения: 29.01.2024).

обороны. В этой связи исследование кризисов контроля над вооружениями требует обязательного учёта кибернетического измерения.

НАТО, как ведущий военно-политический блок, активно адаптируется к новым вызовам, трансформируя свою стратегию в киберпространстве. Начиная с 2002 года, когда кибербезопасность впервые была включена в повестку НАТО, Североатлантический альянс последовательно усиливает свою киберзащиту, интегрируя её в стратегию коллективной обороны. Важными вехами стали:

- признание киберпространства сферой операций (2016);

- создание Центра кибероперациий (2018);

- разработка Комплексной политики киберзащиты (CCDP) и доктрины кибероперациий.

Ключевыми направлениями деятельности НАТО в киберпространстве являются:

1. Трансформация киберпространства в сферу операций, что подразумевает развитие наступательных и оборонительных возможностей, проведение учений (например, Cyber Coalition) и координацию с союзниками.

2. Выполнение обязательств по киберзащите, включая укрепление национальных потенциалов государств-членов, обмен информацией и взаимодействие с частным сектором.

Однако остаются нерешённые проблемы, такие как:

- Сложность атрибуции кибератак, затрудняющая применение статьи 5 Вашингтонского договора;

- Отсутствие чётких международных норм, регулирующих ответные меры на киберугрозы;

- Необходимость баланса между коллективной безопасностью и национальным суверенитетом при реагировании на гибридные угрозы.

В перспективе НАТО предстоит углублять сотрудничество с ЕС, частным сектором и научными кругами, а также совершенствовать механизмы

реагирования на кибератаки, включая те, что не достигают порога вооружённого конфликта. Успех Североатлантического альянса в этой сфере будет зависеть от его способности адаптироваться к динамично меняющемуся ландшафту киберугроз, сохраняя при этом единство среди членов организации.

Отметим, что первостепенная цель НАТО в киберпространстве – обеспечение безопасности и устойчивости своих членов в условиях растущих киберугроз. Это достигается через защиту собственных сетей, укрепление коллективной обороны, повышение киберустойчивости стран-членов, противодействие гибридным угрозам, развитие международного сотрудничества и интеграцию инновационных технологий. Эти усилия направлены на то, чтобы Североатлантический альянс оставался лидером в области кибербезопасности и мог эффективно противостоять вызовам цифровой эпохи.

Несмотря на значительные усилия и достижения в области кибербезопасности, НАТО сталкивается с рядом серьёзных трудностей, которые осложняют реализацию стратегических целей в киберпространстве. Эти вызовы носят как технический, так и политический, организационный и правовой характер.

Одной из главных трудностей является высокая скорость технологических изменений. Киберпространство постоянно эволюционирует, появляются новые технологии, такие как искусственный интеллект, квантовые вычисления и интернет вещей, которые создают как новые возможности, так и новые уязвимости. Североатлантический альянс вынужден постоянно адаптировать свои стратегии и инструменты, чтобы оставаться на передовой технологического развития. Можем констатировать, что по состоянию на сегодняшний день в киберпространстве НАТО сталкивается с рядом вызовов и проблем.

Необходимо отметить, что на сегодняшний день вопросы обеспечения кибербезопасности выходят на глобальный уровень, на уровень создания

единой системы кибербезопасности как государственных акторов, так и международных организаций, включая НАТО. Можно констатировать, что на сегодняшний день одной из ключевых характеристик научно-технологического развития вооружённых сил национальных государств является процесс повсеместной и всеобъемлющей цифровизации, подразумевающей «насыщение войск на всех уровнях, и прежде всего штабов различного уровня, «умными устройствами», в том числе средствами связи, управления, навигации». Говоря о роли и месте Североатлантического альянса в глобальных процессах, связанных с имплементацией возможностей киберпространства в практической плоскости, можем констатировать что в течение последнего десятилетия кибернетические угрозы безопасности НАТО приобретают все более регулярный, сложный, разрушительный и силовой характер.

2.3. Прогнозный сценарий дальнейшего развития современной стратегии НАТО в киберпространстве

Современная система международных отношений и система глобальной международной безопасности характеризуются стремительной трансформацией вызовов и угроз, связанных с развитием цифровых технологий и их интеграцией в различные сферы общественной жизни. Киберпространство, как новая сфера стратегического соперничества, становится ключевым элементом международной безопасности, что обусловливает необходимость пересмотра подходов к формированию стратегии в данной области. Североатлантический альянс, как одна из ведущих международных организаций в сфере безопасности, активно адаптирует свои стратегии к вызовам в киберпространстве, что делает исследование перспектив стратегии НАТО в данной области особенно актуальным. Киберпространство, по мнению ряда исследователей становится пятой областью ведения войны наряду с сушей, морем, воздухом и

космосом[332]. В то же время киберпространство создаёт новые возможности для асимметричных действий негосударственных акторов, что усложняет традиционные подходы к обеспечению безопасности. Подобные изменения требуют от НАТО разработки новых стратегических документов и механизмов координации действий государств-членов. Официальные документы Североатлантического альянса, такие как «Стратегическая концепция 2022 года» и «Политика киберзащиты НАТО», подчёркивают важность укрепления киберзащиты и развития коллективных мер противодействия киберугрозам[333][334]. Однако, эффективность стратегии НАТО в киберпространстве зависит от способности военно-политического блока адаптироваться к быстро меняющимся технологическим условиям и координировать действия с частным сектором. В эпоху глобализации и цифровизации киберпространство кристаллизовалось как важный аспект международных отношений, существенно влияющий на характер взаимодействия между государственными и негосударственными субъектами. В данном контексте исследование перспектив развития стратегии НАТО в киберпространстве приобретает особую значимость. С целью идентификации наиболее вероятных перспектив развития стратегии НАТО в киберпространстве целесообразно провести комплексный анализ современных тенденций и вызовов, с которыми сталкивается Североатлантический альянс, а также оценку возможных направлений эволюции его стратегий в условиях растущей киберугрозы.

Основываясь на решениях состоявшегося в декабре 2019 г. Лондонского саммита Североатлантического альянса, государствами-членами НАТО «был инициирован процесс активных внутриблоковых консультаций и перспективного анализа различных сфер деятельности альянса, получивший

[332] Nye, J. S. (2010). Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School.
[333] NATO (2022). Strategic Concept 2022. Brussels: NATO Headquarters.
[334] NATO (2022). NATO Cyber Defence Policy. Brussels: NATO Headquarters.

название «Повестка «НАТО-2030»»[335]. Ключевой задачей данной инициативы было обозначено стремление стран-участниц Североатлантического альянса интенсифицировать процесс трансформации деятельности НАТО и содействовать адаптации к стремительно меняющейся системе международных отношений, мировой политики и международной безопасности. Необходимость совершенствования стратегических целей и ориентиров военно-политического блока с целью идентификации ключевых векторов его развития продиктована как влиянием состояния международной стабильности в целом, так и внутренними противоречиями, связанными прежде всего с «принципами коалиционной солидарности и национальными интересами стран-участниц»[336]. Особого внимания заслуживает рост гетерогенности и конфликтогенности в современной системе международных отношений, что в свою очередь напрямую отражается на стратегическом видении и идентификации ключевых векторов Североатлантического альянса. Так, по мнению профессора Дипломатической академии МИД России О.П. Иванова, «на современном этапе стратегическое соперничество отличается нарастающим конфликтным потенциалом, который сопровождается расширением разлома между коллективным Западом во главе с США и незападным миром с такими ведущими странами, как Россия и КНР»[337].

---

[335] 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).

[336] 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).

[337] Иванов О.П. ТРАНСФОРМАЦИЯ НАТО: ОТ ПОТЕПЛЕНИЯ КЛИМАТА ДО ЗАМЕРЗАНИЯ В ПОЛИТИКЕ // Обозреватель - Observer. 2022. №11-12 (394–395). URL: https://cyberleninka.ru/article/n/transformatsiya-nato-ot-potepleniya-klimata-do-zamerzaniya-v-politike (дата обращения: 29.01.2025).

Анализируя представленные в параграфах 2.1, 2.2 положения, перспективы развития стратегии НАТО в киберпространстве можно классифицировать по следующим категориям.

1) укрепление киберзащиты;
2) киберпространство как область военных действий;
3) сотрудничество с частным сектором и международными партнёрами.

Говоря о перспективных направлениях эволюции деятельности Североатлантического альянса в области укрепления киберзащиты, первостепенно целесообразно обратиться к наиболее «свежей» стратегической концепции организации. Стратегическая концепция НАТО, принятая главами государств и правительств на встрече в верхах военно-политического блока в Мадриде 29 июня 2022 г., прямо указывает на одно их ключевых значений киберпространства в контексте коллективной обороны государств-членов Североатлантического альянса. Так, согласно статье 24, страны-участницы НАТО «ускорят цифровую трансформацию, адаптируют структуру органов военного управления НАТО к информационному веку и укрепят киберзащиту, сети и инфраструктуру, будут поощрять инновации и увеличивать инвестиции в новые и прорывные технологии, чтобы сохранить оперативную совместимость и военное превосходство, будут работать вместе над внедрением и интеграцией новых технологий, сотрудничать с частным сектором, защищать наши инновационные экосистемы, формировать стандарты и придерживаться принципов ответственного использования, которые отражают наши демократические ценности и права человека»[338].

Основываясь на текущем состоянии системы международных отношений и мировой политики, а также анализируя ключевые тренды глобального научно-технологического развития, представляется возможным

[338] Стратегическая концепция НАТО 2022 года https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf (дата обращения: 01.03.2024).

констатировать интенсификацию внедрения искусственного интеллекта (ИИ) в инструментарий Североатлантического альянса с целью анализа потенциальных и реальных кибернетических угроз и прогнозирования кибератак, что в свою очередь позволит быстрее выявлять уязвимости и реагировать на инциденты. Растущая сложность кибератак требует автоматизации процессов защиты. ИИ уже используется в некоторых странах-членах НАТО, таких как США и Великобритания, для анализа больших объемов данных.

Анализируя тему имплементации искусственного интеллекта в современную систему международных отношений и мировую политику, можем констатировать, что технологии ИИ являются одним из наиболее характерных примеров подтверждения тенденции содействия национальными государствами трансфера высоких информационно-коммуникационных технологий из гражданской в оборонную сферу. Так, анализ источников из зарубежных стран (США, КНР, Индия, Республика Корея, Франция и др.) даёт возможность идентифицировать некоторые направления применения технологий искусственного интеллекта в военной сфере:

- прогнозирование здоровья военнослужащих;
- обеспечение разведки и целеуказания;
- качественное повышение боевых возможностей БПЛА;
- наращивание эффективности ударной пилотируемой авиации;
- обеспечение более эффективного противоборства в киберпространстве;
- использование технологий искусственного интеллекта для задач противоракетной обороны, для систем предупреждения о ракетном нападении и систем контроля космического пространства.

При этом отметим, что ставка по применению искусственного интеллекта в оборонной сфере вышеперечисленных стран делается в первую очередь, на заимствование данных технологий из гражданской сферы[339].

Именно данные вышеуказанные направления применения технологий ИИ с высокой долей вероятности станут ключевыми направлениями деятельности Североатлантического альянса в области укрепления собственной киберзащиты.

Увеличение инвестиций в кибероборону военно-политического блока является необходимым условием для обеспечения коллективной безопасности стран-членов НАТО. Рост киберугроз, технологическая гонка и эскалация киберконфликтов требуют значительных финансовых вложений. Рост числа кибератак, их сложности и масштабов вынуждает государств-членов Североатлантического альянса пересматривать свои подходы к кибероборонe. Одним из ключевых аспектов данной трансформации является увеличение инвестиций в кибербезопасность.

Обосновывая необходимость увеличения инвестиций в кибероборону в качестве элемента потенциальной стратегии укрепления киберзащиты Североатлантического альянса, целесообразно опереться на следующие факторы.

Во-первых, необходимо выделить как экспоненциальный рост суммарного количества кибератак, так и комплексный качественный рост угроз, которые они в себе несут.

Согласно данным из аналитического отчёта Федерального бюро расследований США о преступлениях в интернете за 2023 г., ущерб от злонамеренной киберактивности в США составил 12,5 миллиардов долларов США[340]. По данным Cybersecurity Ventures, в 2023 году киберпреступность

---

[339] О мегатрендах мирового развития на период до 2035 года и их геополитическое значение: - Москва: Институт перспективных стратегических исследований Национального исследовательского университета «Высшая школа экономики», 2023. – 28 с. с. 23

[340] Federal Bureau of Investigation Internet Crime Report 2023 URL: https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf (accessed: 12.08.2025).

обошлась миру в 8 триллионов долларов США. Cybersecurity Ventures прогнозирует, что глобальные затраты на ущерб от киберпреступности будут расти на 15 процентов в год в течение следующих трех лет, достигнув 10,5 триллионов долларов США в год к 2025 году, по сравнению с 3 триллионами долларов США в 2015 году[341].

Во-вторых, развитие высоких технологий, таких как искусственный интеллект (ИИ), квантовые вычисления и интернет вещей (IoT), создает новые уязвимости. Для противодействия этим угрозам требуются значительные финансовые вложения в исследования и разработки.

Ещё 10 лет назад в экспертной среде имели место дискуссии об исчерпании возможностей пятого технологического уклада («пятый технологический уклад зародился примерно в 1980–1990-е гг., опирался на достижения в областях микроэлектроники, информатики, биотехнологии, генной инженерии, новых видов энергии и материалов, освоения космического пространства, спутниковой связи и т.д., характеризуется переходом от разрозненных фирм к единой сети крупных и мелких компаний, соединённых электронной сетью на основе Интернета, тесно взаимодействующих в области технологий, контроля качества продукции, планирования инноваций»[342]), возникновения «инновационной паузы». Сегодня абсолютное большинство позиций в перечнях критических эмерджентных технологий, составляемых ведущими акторами международных отношений, занимают направления, напрямую связанные с информационно-коммуникационными технологиями.

В качестве наиболее частно упоминаемых в научном дискурсе и СМИ технологий целесообразно выделить следующие:

---

[341] Cybercrime Damages To Cost The World $8 Trillion USD in 2023 URL: https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023 (accessed: 01.02.2024).

[342] Технологический уклад // Большая российская энциклопедия: научно-образовательный портал – URL: https://bigenc.ru/c/tekhnologicheskii-uklad-f21f29/?v=6124666. – (дата обращения: 27.01.2025).

- искусственный интеллект;
- «Интернет вещей»;
- связь пятого и шестого поколений (5G и 6G);
- аналитика на основе «больших данных»[343].

На саммите НАТО в Мадриде в 2022 году страны-члены подтвердили обязательство выделять 2% ВВП на оборону, при этом значительная часть этих средств должна быть направлена на кибербезопасность[344]. Говоря же об увеличении инвестиций в кибероборону отдельными государствами-членами Североатлантического альянса, следует принять во внимание следующие статистические данные.

- США увеличили бюджет на кибербезопасность до $18,8 млрд в 2023 году, включая финансирование Киберкомандования США (USCYBERCOM)[345].
- Великобритания выделила £2,6 млрд на кибербезопасность в рамках своей Национальной киберстратегии на 2022–2030 годы[346].
- Федеративная Республика Германия планирует инвестировать €3 млрд в кибербезопасность до 2025 года, включая создание нового агентства по киберзащите[347].

НАТО также увеличивает финансирование кибероборонны через свои структуры и программы:

1. Фонд киберзащиты НАТО (NATO Cyber Defence Fund). Фонд был создан для поддержки совместных проектов в области кибербезопасности, включая разработку новых технологий и

[343] О мегатрендах мирового развития на период до 2035 года и их геополитическое значение: - Москва: Институт перспективных стратегических исследований Национального исследовательского университета «Высшая школа экономики», 2023. – 28 с. с. 23
[344] NATO. (2022). Madrid Summit Declaration.
[345] White House. (2023). Budget of the U.S. Government: Cybersecurity.
[346] UK Government. (2022). National Cyber Strategy 2022–2030.
[347] BMVg. (2023). German Cyber Security Strategy.

обучение специалистов. В 2023 году объем фонда составил €1 млрд[348].

2. Программа НАТО по киберзащите (NATO Cyber Defence Programme). Программа включает финансирование исследований, разработку стандартов и проведение учений. В 2022 году на программу было выделено €500 млн[349].
3. Центр операций киберзащиты (Cybersecurity Operations Centre). Центр получил дополнительное финансирование в размере €200 млн для модернизации своих возможностей по мониторингу и реагированию на кибератаки[350].

Рассматривая перспективы увеличения инвестиций в кибероборону Североатлантического альянса, на ближайшую историческую перспективу ожидается:

1. Рост расходов до 2030 года. Ожидается, что к 2030 году общие расходы стран-членов НАТО на кибербезопасность превысят $100 млрд в год. Это связано с необходимостью защиты критической инфраструктуры, развития технологий и подготовки специалистов[351].
2. Инвестиции в ИИ и квантовые технологии. НАТО планирует выделить €2 млрд на разработку технологий искусственного интеллекта и квантовых вычислений для киберзащиты. Эти технологии позволят быстрее выявлять угрозы и повысить устойчивость систем[352].
3. Создание новых фондов и инициатив. На саммите НАТО в Вильнюсе в 2023 году было объявлено о создании нового Фонда кибербезопасности для Украины с бюджетом €500 млн. Это

[348] NATO. (2023). Vilnius Summit Communiqué
[349] NATO. (2022). Madrid Summit Declaration.
[350] NATO. (2023). Vilnius Summit Communiqué
[351] Rand Corporation. (2023). Future of NATO Cyber Defence.
[352] NATO Review. (2023). AI and Quantum Technologies in Cyber Defence.

подчеркивает важность кибербезопасности в контексте современных конфликтов[353].

Анализ современных тенденций в сфере кибероборонысевероатлантического альянса позволяет сделать ряд выводов, отражающих стратегические приоритеты НАТО в условиях эскалации цифровых угроз.

Рост инвестиций стран-членов Североатлантического альянса свидетельствует о переходе от периферийного финансирования к системной интеграции кибербезопасности в оборонные бюджеты. Подобный тренд обусловлен:

- ростом гибридных угроз, включая атаки на критическую инфраструктуру (энергосети, транспорт, системы управления);

- необходимостью стандартизации киберзащиты в рамках коллективной обороны (Статья 5 Вашингтонского договора);

- расширением международного сотрудничества, в частности, посредством программ («NATO CCDCOE») и совместных учений («Locked Shields», «Cyber Coalition»).

Выделение €2 млрд на разработку искусственного интеллекта и квантовых вычислений подчеркивает стремление Североатлантического альянса к технологическому доминированию. Ожидаемые эффекты включают в себя:

- автоматизации киберзащиты: алгоритмы машинного обучения ускорят обнаружение аномалий и снизят нагрузку на операторов;

- квантовую криптографию: внедрение постквантовых алгоритмов минимизирует риски взлома шифрованных каналов связи;

- углубление взаимодействия с частным сектором: партнерство с корпорациями (Microsoft, Google, IBM) ускорит трансфер технологий в военную сферу.

[353] NATO. (2023). Vilnius Summit Communiqué

Создание новых фондов и инициатив демонстрирует эволюцию подходов НАТО к:

- адаптации к современным конфликтам: киберпространство становится ключевым театром военных действий, что подтверждается опытом Специальной военной операции на Украине.

- децентрализации финансирования: переход от общих бюджетов к целевым фондам повышает гибкость распределения ресурсов;

- глобализации киберсоюзов: расширение сотрудничества с ЕС, Японией и Республикой Корея формирует многоуровневую систему сдерживания.

Инвестиционная политика НАТО в сфере кибероборонs отражает парадигматический сдвиг от традиционных военных расходов к комплексной цифровой безопасности. В ближайшее десятилетие ключевыми факторами успеха станут скорость принятия решений, гибкость институциональных механизмов и глобальная координация с целью противодействия транснациональным киберугрозам.

Рассматривая основные перспективы развития стратегии НАТО в киберпространстве как области военных действий, первостепенно следует обратить внимание на следующие аспекты.

НАТО активно развивает как оборонительные, так и наступательные кибервозможности, что включает создание Центра операций киберзащиты (Cybersecurity Operations Centre) и проведение регулярных учений, таких как Cyber Coalition и Locked Shields[354].

НАТО будет развивать способности проводить кибератаки для сдерживания противников и нейтрализации угроз. Это включает разработку инструментов для деактивации вражеских систем и защиты собственной инфраструктуры[355].

НАТО активно участвует в разработке международных норм и правил поведения в киберпространстве. Это включает сотрудничество с ООН, ЕС и

[354] NATO. (2023). Cybersecurity Operations Centre.
[355] Kello, L. (2017). The Virtual Weapon and International Order.

другими организациями для создания глобальных стандартов кибербезопасности.

Перспектива:

- Разработка международных кибернорм. НАТО будет способствовать созданию норм, регулирующих использование кибероперацій в военных целях. Это включает запрет на атаки на гражданскую инфраструктуру и использование кибероружия[356].
- Расширение сотрудничества с частным сектором. НАТО будет укреплять партнерства с технологическими компаниями для разработки инновационных решений в области киберзащиты[357].

Перспективы развития стратегии НАТО в киберпространстве как области военных действий характеризуются комплексной трансформацией, сочетающей институциональное развитие, наращивание оперативных возможностей и формирование нормативной базы. НАТО активно развивает наступательный киберпотенциал, включая инструменты для нейтрализации вражеских систем, что подтверждается регулярными учениями (Cyber Coalition, Locked Shields) и интеграцией киберкомпонента в стратегию сдерживания. Одновременно Североатлантический альянс участвует в разработке международных норм поведения в киберпространстве через сотрудничество с ООН и ЕС, фокусируясь на запрете атак на гражданскую инфраструктуру и регулировании кибероружия. Важным элементом стратегии становится углубление партнёрства с технологическими компаниями для развития инновационных решений в области ИИ и квантовых технологий. Эти процессы отражают двойственный подход НАТО: с одной стороны – милитаризация киберпространства как инструмента сдерживания, с другой – формирование глобальных стандартов кибербезопасности. Подобная стратегия, сформированная под влиянием гибридных конфликтов (в частности, украинского кризиса), указывает на превращение

[356] Schmitt, M. N., & Vihul, L. (2017). The Nature of International Law Cyber Norms.
[357] NATO. (2023). NATO Industry Forum

киберпространства в полноценный театр военных действий, где технологическое превосходство будет определять баланс сил. Дальнейшие исследования могли бы сосредоточиться на сравнительной эффективности киберстратегий различных акторов и этических аспектах применения автономных киберсистем.

Сохранение информационно-коммуникационных технологий в качестве ядра технологического уклада даст преимущество тем странам, которые на протяжении нескольких десятилетий осуществляли наибольшие инвестиции в соответствующие области и побудит их к максимальному ограничению доступа конкурентов, что будет вести к усилению технонационализма. Прорывы стран-конкурентов – в особенности в области развития искусственного интеллекта, а также квантовых вычислений, могут восприниматься в качестве чуть ли не экзистенциальных угроз национальной конкурентоспособности и национальной безопасности – в том числе в военном её измерении[358].

За последнее десятилетие стала очевидной тенденция заметного усиления роли национальных государств в мировой политике и современной системе международных отношений. Несмотря на сохранение глобализационных тенденций и развитие транснациональных акторов, таких как международные организации, неправительственные организации и мультинациональные корпорации, национальные государства продолжают оставаться центральными субъектами международной политики. Пандемия COVID-19 оказала значительное влияние на современную мировую политику и международные отношения и лишь усилила роль национальных государств. Целесообразно отметить утрату государством роли главного инвестора в инновационное развитие. В большинстве технологически развитых государств доля инвестиций частных корпораций в информационно-коммуникационные

[358] О мегатрендах мирового развития на период до 2035 года и их геополитическое значение: - Москва: Институт перспективных стратегических исследований Национального исследовательского университета «Высшая школа экономики», 2023. – 28 с. с. 23

технологии колеблется от половины до трети всех трат на разработки и исследования. Ввиду таких объективных факторов как отсутствие принципиальных ограничений, частный сектор добивается существенного сокращение цикла производства востребованных высокотехнологических инноваций. Таким образом, одним из ключевых ориентиров для национальных государств становится трансфер высоких информационно-коммуникационных технологий из гражданского в военный или оборонный сектор. На протяжении последнего десятилетия очень многие государства занимались активным выстраиванием механизмов гражданско-военного взаимодействия при реализации своей военно-технологической политики.

Частный сектор играет ключевую роль в разработке инновационных решений для противодействия киберугрозам. Компании, специализирующиеся на кибербезопасности, обладают уникальными знаниями и ресурсами, которые могут быть использованы для укрепления обороноспособности альянса. Например, партнёрство с такими технологическими гигантами, как Microsoft, Google и IBM, позволяет НАТО получать доступ к передовым технологиям искусственного интеллекта и машинного обучения для анализа кибератак и прогнозирования угроз. Кроме того, частный сектор активно участвует в создании механизмов обмена информацией о киберугрозах. Такие инициативы как Cybersecurity Information Sharing Partnership (CISP), демонстрируют эффективность сотрудничества между государственными и частными структурами в борьбе с киберпреступностью[359]. НАТО также активно развивает подобные механизмы, что позволяет оперативно реагировать на возникающие угрозы.

Сотрудничество с международными партнёрами является ещё одним важным аспектом киберстратегии НАТО.

---

[359] ENISA. (2021). Cybersecurity Information Sharing Partnerships. Retrieved from https://www.enisa.europa.eu

Например, в рамках инициативы «Партнёрство ради мира» НАТО предоставляет странам-партнёрам доступ к своим кибертехнологиям и обучающим программам[360].

Особое внимание уделяется сотрудничеству с негосударственными акторами, такими как неправительственные организации и академические институты. Их участие в разработке стратегий кибербезопасности позволяет учитывать различные точки зрения и создавать более устойчивые системы защиты[361].

В ближайшие годы можно ожидать дальнейшего углубления сотрудничества НАТО с частным сектором и международными партнёрами. Одним из ключевых направлений станет развитие технологий искусственного интеллекта и квантовых вычислений, которые могут значительно повысить эффективность киберзащиты. Кроме того, Североатлантичсекий альянс будет стремиться к созданию более гибких механизмов реагирования на киберугрозы, включая возможность применения статьи 5 Вашингтонского договора в случае масштабных кибератак[362].

Важным шагом в этом направлении станет укрепление нормативной базы, регулирующей взаимодействие между государственными и частными структурами, что позволит обеспечить более эффективный обмен информацией и координацию усилий в борьбе с киберугрозами.

Резюмируя вышесказанное, отметим, что современная система международных отношений претерпевает глубокую трансформацию под влиянием стремительного развития цифровых технологий, которые не только создают новые возможности, но и формируют принципиально иные вызовы в сфере безопасности. Киберпространство, ставшее пятой областью ведения войны наряду с традиционными сферами (суша, море, воздух и космос), превратилось в ключевой элемент стратегического соперничества. В этих

---

[360] NATO. (2020). NATO 2030: United for a New Era. Retrieved from https://www.nato.int
[361] Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. Penguin Press.
[362] Schmitt, M. N., & Vihul, L. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

условиях Североатлантический альянс, как ведущий военно-политический блок, вынужден адаптировать свои подходы к обеспечению коллективной безопасности, что делает исследование его киберстратегии особенно актуальным. Проведённый анализ позволяет выделить три ключевых направления развития стратегии НАТО в киберпространстве. Североатлантический альянс активно инвестирует в развитие технологий искусственного интеллекта, квантовых вычислений и автоматизированных систем кибероборонны. 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 млрд, что отражает переход от периферийного финансирования к системной интеграции киберугроз в стратегию коллективной обороны. НАТО постепенно милитаризирует киберпространство, развивая как оборонительные, так и наступательные возможности. Создание централизованного киберкомандования по модели USCYBERCOM, регулярные учения (Cyber Coalition, Locked Shields) и разработка норм применения кибероружия свидетельствуют о формировании полноценного кибертеатра военных действий. Однако этот процесс сопровождается этическими и правовыми вызовами, включая вопросы регулирования атак на гражданскую инфраструктуру. Поскольку частные корпорации (Microsoft, IBM, Google) играют ключевую роль в технологических инновациях, НАТО расширяет механизмы гражданско-военного взаимодействия. Партнерство с ЕС, ООН и странами Азиатско-Тихоокеанского региона направлено на создание глобальных стандартов кибербезопасности и противодействие асимметричным угрозам со стороны негосударственных акторов.

Стратегия НАТО в киберпространстве эволюционирует в ответ на усложнение угроз, включая гибридные атаки и технологическую гонку с Россией и Китаем. Приоритетами остаются технологическое превосходство (ИИ, квантовые технологии), нормотворчество и гибкие альянсы с частным

сектором. Ключевым риском является дестабилизация международных норм из-за противоречий между милитаризацией киберпространства и необходимостью его регулирования. Перспективы дальнейших исследований связаны с анализом эффективности киберстратегий НАТО в условиях конфликтов (например, украинского кризиса), а также с оценкой влияния автономных киберсистем на стабильность международной безопасности. В долгосрочной перспективе Североатлантическому альянсу предстоит балансировать между сдерживанием, сотрудничеством и инновациями, чтобы сохранить свою роль в формировании архитектуры кибербезопасности.

Глава 3. Реализация стратегии НАТО в киберпространстве в контексте современной международной безопасности

3.1. Развитие информационно-коммуникационных технологий НАТО в военно-политических целях в контексте международной безопасности

Сегодня, в условиях бурного развития информационно-коммуникационных технологий и стремительно трансформирующейся системы международных отношений киберпространство «становится принципиально новой ареной для межгосударственного взаимодействия и регулирования, а также ожесточённого противостояния, учитывая стремление ядерных держав избегать прямого военного столкновения». Более того, практическая имплементация широкого инструментария прокси-войн в киберпространстве существенно нивелирует риск для государства или военного блока быть обвинённым в агрессии[363].

В контексте глобальной цифровой трансформации и эскалации киберугроз информационно-коммуникационные технологии (ИКТ) приобретают стратегическое значение для модернизации военно-политического курса и оперативной деятельности ведущих международных институтов, в частности НАТО. Данные технологии эволюционировали из вспомогательного инструментария, нацеленного на повышение эффективности операций, в фундаментальный компонент системы стратегического сдерживания и поддержания глобальной безопасности. Таким образом, активная интеграция Североатлантическим альянсом ИКТ в военно-политическую сферу демонстрирует его системный ответ на вызовы современности, к числу которых относятся кибертерроризм, гибридные войны и целенаправленная дестабилизация информационной среды.

В современную эпоху киберпространство, будучи принципиально трансграничным по своей природе, приобретает статус ключевой арены для

[363] Картина нарождающегося мира: базовые черты и тенденции: - Москва: Дипломатическая академия МИД России, 2024. – 68 с. с. 36.

соперничества в политической, экономической, информационной и культурной сферах. Стремительная эволюция цифровых технологий привела к формированию принципиально нового типа политического поля – виртуального, где происходит столкновение интересов многообразных акторов мировой политики: национальных государств и иных центров силы. Исторически, практически с момента своего возникновения, данная сфера была милитаризирована и институционализирована в качестве пятого театра военных действий (после суши, моря, воздушного и космического пространства), сохраняя за собой эту стратегическую роль и в настоящее время [364].

На сегодняшний день вопросы обеспечения кибербезопасности выходят на глобальный уровень, на уровень создания единой системы кибербезопасности как государственных акторов, так и международных организаций, включая Североатлантический альянс.

Наблюдается переход от продолжительной эпохи либерализации трансфера высоких технологий и ноу-хау, выступавшей одним из ключевых драйверов глобализации, к противоположной тенденции – преднамеренному ограничению их распространения. Данный сдвиг инициирован целенаправленными действиями национальных государств, нацеленными на защиту технологического суверенитета от внешних угроз. Наиболее выраженно эта динамика проявляется в области информационно-коммуникационных технологий (ИКТ). Согласно экспертным оценкам, замедление темпов технологической диффузии способно спровоцировать значительные экономические издержки, прежде всего для стран с развивающейся экономикой, выражающиеся в падении производительности труда, росте производственных затрат и инфляции. Наиболее критичными последствия технологической фрагментации окажутся для отраслей,

[364] 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).

зависящих от функционирования глобальных платформ, таких как сфера трансграничных финансовых расчетов[365].

Сокращение темпов технологической диффузии порождает ряд значимых геополитических последствий. Данный тренд способствует усугублению цифрового неравенства и усиливает социальную стратификацию в государствах Глобального Юга, что, в свою очередь, ведет к замедлению экономического развития. Эта совокупность факторов формирует потенциальный источник социальной напряженности, чреватой дестабилизацией и возникновением конфликтов. В то же время, хотя ограничение трансфера технологий и выступает инструментом защиты технологического суверенитета национальных государств, оно же может провоцировать акторов международной арены на поиск обходных путей для доступа к инновациям, в том числе посредством незаконных методов, таких как кибершпионаж[366].

Одной из наиболее характерных тенденций научно-технологического прогресса последних лет является нарастающий институциональный разрыв между скоростью технологических изменений и способностью управленческих структур – как на национальном, так и на глобальном уровне – вырабатывать адекватные нормативно-правовые ответы в форме стандартов и регламентов. Наиболее остро данный дисбаланс проявляется в таких прорывных областях, как искусственный интеллект, генная инженерия и освоение космоса. В условиях усиления геополитической конкуренции перспективы формирования единых международных стандартов в этих сферах в обозримом будущем оцениваются как маловероятные. Ярким подтверждением этой тенденции служит растущее число стран,

---

[365] 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.

[366] О мегатрендах мирового развития на период до 2035 года и их геополитическое значение: - Москва: Институт перспективных стратегических исследований Национального исследовательского университета «Высшая школа экономики», 2023. – 28 с. с. 23

законодательно требующих локализации критически важных массивов данных в пределах своей юрисдикции.

Исследование воздействия информационно-коммуникационных технологий на эволюцию военно-политической стратегии НАТО и их влияния на расстановку сил в мировой политике дает возможность идентифицировать ключевые последствия для архитектуры глобальной и региональной безопасности. Интеграция инновационных технологических решений, включая искусственный интеллект, обработку больших данных и квантовые вычисления, формирует принципиально новые перспективы для усиления оборонного потенциала.

Совершенствование потенциала применения информационно-коммуникационных технологий (ИКТ) в военно-политической сфере представляет собой ключевой компонент стратегического курса НАТО, обусловленного текущим геополитическим контекстом. Приоритетными направлениями развития данного потенциала выступают:

1) использование искусственного интеллекта (ИИ) и больших данных;
2) интеграция информационно-коммуникационных технологий (ИКТ) в гибридные войны[367].

Цифровая трансформация обуславливает интеграцию технологий искусственного интеллекта и больших данных в военно-политическую стратегию Североатлантического альянса в качестве её неотъемлемого элемента. Данные инструменты создают принципиально новые перспективы для аналитической обработки информации, прогнозирования рисков и повышения эффективности операций. При этом их применение в сфере международной безопасности является неоднозначным: обладая потенциалом для укрепления стабильности, они одновременно генерируют новые виды

[367] 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.

угроз. В этой связи комплексное исследование исторического опыта и текущих практик эксплуатации ИИ государствами-членами НАТО позволяет проанализировать его значение в структуре современных международных отношений и оценить степень воздействия на архитектуру глобальной безопасности.

Качественный скачок в развитии искусственного интеллекта, наблюдаемый в последнее десятилетие, детерминирует его растущее влияние на современную систему международных отношений. Уникальная природа данной технологии позволяет прогнозировать, что её дальнейшая эволюция станет катализатором беспрецедентного прорыва во всех сферах научного знания и технологического развития, масштабы которого не имеют аналогов в истории. Данная трансформация сопряжена с серьёзными геополитическими последствиями[368]. Являясь частью процесса цифровизации международных отношений, ИИ влияет на восприятие меняющейся системы самими акторами.

Отправной точкой для исследований в области ИИ является «Дартмутский летний исследовательский проект по вопросам искусственного интеллекта», проведенный в 1956 г[369]. Гипотеза заключалась в том, что «любой аспект интеллектуальной деятельности человека можно описать так, что машина будет способна его воспроизвести»[370].

Понятие ИИ следует рассматривать прежде всего в качестве совокупности принципов компьютерной обработки мышления и интеллектуального поведения человека.

С перспективы теории международных отношений, в изучении ИИ существуют парадигмальные различия. Так, неореализм рассматривает ИИ в

---

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

[369] 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).

[370] McCarthy, Minsky, Rochester, Shannon 2006, p. 12

качестве одного из факторов потенциального изменения баланса сил в международной системе. В данном случае речь прежде всего идет о цифровых войнах, войнах данных, информационной безопасности, новых вызовах для международной безопасности (например, по части разработки боевых роботов – LAWS), создании суверенного ИИ. Неолиберализм в свою очередь рассматривает ИИ в качестве технологии, направленной на достижение всеобщего блага, тем не менее, несущей в себе не только перспективные возможности, но и потенциальные риски. Значимость приобретают правовые и этические аспекты ИИ, права и свободы человека в мире ИИ, большая роль в принятии ключевых решений отводится негосударственным акторам (IT-гигантам)[371].

Необходимо отметить роль развития и распространения технологий имплементации ИИ в систему международных отношений. Так, повсеместная цифровизация международных отношений породила всеобъемлющую тенденцию цифровой трансформации дипломатических ведомств и практик, а применение больших данных и алгоритмов на основе ИИ в цифровой дипломатии привело к появлению дипломатии данных[372].

В цифровой дипломатии и дипломатии данных ИИ используется непосредственно в качестве инструмента для прогнозирования цифрового поведения пользователей социальных сетей на основе анализа мнений, предпочтений и цифрового следа. Исследователи выделяют три основных аспекта использования ИИ в дипломатии:

1) ИИ как тема для переговоров;

2) ИИ как дипломатический инструмент;

---

[371] 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).

[372] 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.

3) ИИ как фактор изменения переговорного контекста[373].

Сегодня можно констатировать качественное изменение технологий ИИ. Запущенный в 2022 г. чат-бот с генеративным искусственным интеллектом, разработанный компанией OpenAI ChatGPT (Generative Pre-trained Transformer «генеративный предварительно обученный трансформер») стал значительным прорывом в области искусственного интеллекта, особенно в сфере обработки естественного языка. Эта модель, основанная на архитектуре GPT-3, продемонстрировала впечатляющие способности в генерации текста, ведении диалогов и выполнении различных задач, что привлекло внимание как широкой общественности, так и научных кругов. Реакция на ChatGPT была разнообразной: с одной стороны, многие пользователи отметили его способность генерировать осмысленные и контекстуально уместные ответы, что открыло новые горизонты для применения ИИ в образовании, бизнесе и творчестве. С другой стороны, среди ученых и экспертов возникли обеспокоенности по поводу этических аспектов использования таких технологий, включая вопросы о дезинформации, безопасности и возможном влиянии на рынок труда. Некоторые исследователи подчеркивали необходимость разработки четких регуляторных рамок для контроля за использованием подобных ИИ-систем, чтобы минимизировать риски и негативные последствия. Обсуждения о ChatGPT также затронули философские и социокультурные аспекты, включая вопросы о том, как взаимодействие с ИИ может изменить наше понимание общения и творчества. В итоге запуск ChatGPT стал не только технологическим достижением, но и поводом для широкой дискуссии о будущем искусственного интеллекта и его роли в обществе. Свидетельством уникальности предложенной OpenAI технологии является факт, что данный абзац всецело был сгенерирован упомянутым чат-ботом.

---

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

Тем не менее, необходимо отметить потенциальную возможность использования ИИ в злонамеренных целях, как на межличностном, так и межгосударственном уровнях. Автор настоящей диссертации неоднократно сталкивался с попытками мошенничества, в ходе которых злоумышленники использовали искусственно сгенерированные аудиосообщения на основе голосовых данных абонентов. Как подчёркивал президент России В.В. Путин в своём выступлении на конференции «Путешествие в мир искусственного интеллекта» 24 ноября 2023 г., «нужно обязательно использовать российские решения в сфере создания надёжных, прозрачных и безопасных для человека систем искусственного интеллекта, а также подключать к общей работе специалистов гуманитарных дисциплин»[374]. Таким образом, можно констатировать, что интеграция усилий профильных специалистов является необходимым условием для устойчивого развития ИИ на современном этапе.

Говоря об использовании Североатлантическим альянсом ИИ в военно-политических целях в контексте международной безопасности, первостепенно целесообразно рассмотреть некоторые ключевые вехи.

В 2019 г. экспертами Оборонного колледжа НАТО был представлен доклад, в котором была обоснована необходимость интенсифицировать программы искусственного интеллекта. В докладе утверждалось, что усовершенствование технологий на базе ИИ, машинного обучения и больших данных сможет помочь государствам-членам Североатлантического альянса значительно усилить «военное превосходство». В докладе подчёркивалось, что «доработка и совершенствование существующего технологического и промышленного потенциала позволит НАТО сохранить и нарастить военное превосходство, тем самым на долгие годы обеспечив его вклад в поддержание глобальной безопасности»[375].

---

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

[375] В НАТО выступили за активное развитие программ искусственного интеллекта https://russian.rt.com/world/news/610689-nato-razvitie-programm-intellekt (дата обращения: 05.01.2025).

В этом же году на полях промышленного форума НАТО бывший генеральный секретарь Североатлантического альянса Й. Столтенберг заявил о намерениях военно-политического блока активизировать внедрение технологий искусственного интеллекта в ряд военных систем. По его словам, в течение 15 лет планируется заменить флот авиационных комплексов радиолокационного обнаружения управления AWACS на системы с использованием искусственного интеллекта[376].

Принятие Североатлантическим альянсом в 2021 году специализированной Стратегии в области искусственного интеллекта ознаменовало формирование нормативных основ для ответственного и этически обоснованного применения ИИ в оборонной сфере[377]. Этот документ подчёркивает важность разработки стандартов и принципов, которые бы минимизировали риски, связанные с автономными системами. Ключевые фокусы документа концентрируются на трёх прикладных областях: анализе массивов данных, обработке изображений и обеспечении кибербезопасности. В нём киберпространство идентифицируется в качестве критически важной среды, в которой формируются современные вызовы безопасности, а кибератаки признаются способными нанести существенный ущерб политической, экономической и военной стабильности государств-членов. Североатлантический альянс официально закрепляет статус киберпространства как полноправного операционного домена, наряду с традиционными сферами – сухопутной, морской, воздушной и космической. В рамках Стратегии подтверждается курс на усиление оборонительного потенциала, включая развитие возможностей в сфере предотвращения, детекции, реагирования и восстановления после инцидентов. Особый статус получает принцип коллективной обороны, являющийся краеугольным камнем

---

[376] Искусственный интеллект в НАТО: динамичное внедрение, ответственное использование URL: https://www.nato.int/docu/review/ru/articles/2020/11/24/iskusstvennyj-intellekt-v-nato-dinamichnoe-vnedrenie-otvetstvennoe-ispol-zovanie/index.html (дата обращения: 20.03.2024).

[377] NATO. (2021). NATO’s Artificial Intelligence Strategy. Retrieved from https://www.nato.int

Вашингтонского договора (Статья 5). Подчеркивается, что масштабное кибервоздействие может быть классифицировано как акт вооруженной агрессии, что потенциально инициирует применение соответствующих механизмов коллективного реагирования. Кроме того, документ апеллирует к значимости международной кооперации в сфере кибербезопасности и призывает к имплементации норм международного права в киберпространстве, в частности принципов суверенитета, неприменения силы и мирного разрешения конфликтов. Североатлантический альянс также намерен развивать многоплановое взаимодействие с партнёрами из частного сектора, академической среды и гражданского общества для повышения общего уровня киберустойчивости. В перспективе НАТО планирует продолжить адаптацию своих стратегических подходов и операционных возможностей к эволюционирующему ландшафту киберугроз[378].

В Стратегии обозначены 4 ключевые цели:

1) обеспечение основы для того, чтобы НАТО и союзники могли подавать пример и поощрять разработку и использование ИИ ответственным образом в целях обороны и безопасности;
2) ускорение внедрения ИИ в разработку и предоставление новых возможностей, повышение функциональной совместимости в рамках Североатлантического альянса, в том числе за счёт предложений по сценариям использования ИИ, структур и программ;
3) защита и мониторинг технологий ИИ в НАТО и обеспечение внедрения новшеств, учитывая соображения политики безопасности;
4) выявление и защита от угроз злонамеренного использования ИИ государственными и негосударственными субъектами[379].

---

[378] Summary of the NATO Artificial Intelligence Strategy URL: https://www.nato.int/cps/em/natohq/official_texts_187617.htm (accessed: 03.02.2024).

[379] Summary of the NATO Artificial Intelligence Strategy URL: https://www.nato.int/cps/em/natohq/official_texts_187617.htm (accessed: 03.02.2024).

Использование искусственного интеллекта (ИИ) и больших данных в военно-политических целях становится ключевым элементом стратегии Североатлантического альянса в условиях цифровой трансформации. Подобные технологии открывают новые возможности для анализа угроз, прогнозирования рисков и оптимизации военных операций, что способствует укреплению обороноспособности военно-политического блока. Однако их применение сопряжено с серьезными вызовами, включая этические, правовые и стратегические аспекты, которые требуют комплексного регулирования.

Развитие ИИ в контексте международных отношений демонстрирует качественный скачок за последнее десятилетие, оказывая влияние на баланс сил, дипломатические практики и глобальную безопасность. Особое значение приобретает цифровая дипломатия, где ИИ используется в качестве инструмента анализа данных, прогнозирования поведения акторов международный отношений и оптимизации переговорных процессов. Однако наряду с преимуществами возникают новые угрозы, такие как злонамеренное использование ИИ в киберпространстве, распространение дезинформации и автономных систем вооружений (LAWS).

Стратегия НАТО по искусственному интеллекту 2021 года отражает стремление Североатлантического альянса к ответственному внедрению технологий, сочетающему инновации с мерами безопасности. Документ подчеркивает важность международного сотрудничества, соблюдения норм международного права и развития киберустойчивости. Тем не менее, гонка технологий в сфере ИИ между ведущими державами создает риски эскалации, что требует выработки многосторонних механизмов контроля.

Таким образом, можем констатировать, что интеграция ИИ в военно-политическую сферу представляет собой двойственный процесс: с одной стороны, она усиливает потенциал обороны и безопасности, с другой – порождает новые вызовы, требующие скоординированных действий на глобальном уровне. Дальнейшее развитие этой области должно основываться

на балансе между технологическим прогрессом, этическими стандартами и международной стабильностью.

Применение современных технологий изменяет привычную картину мира, восприятия реальности, что сказывается на всех сферах жизнедеятельности общества. По мнению российского политолога И.С. Семененко, «революция в информационных технологиях придала новые качества социокультурной динамике современного мира, отличительная черта которого – это углубляющиеся разрывы социальной ткани современных обществ в условиях уплотнения информационных потоков и поистине драматического роста их воздействия на сознание и поведение людей»[380].

Концепция гибридных войн базируется на комплексном применении широкого спектра инструментария, интегрирующего методы пропаганды, кампании дезинформации и кибервоздействия для реализации стратегических интересов. Информационно-коммуникационные технологии (ИКТ) выступают ключевым катализатором, обеспечивающим высокую эффективность и масштабируемость данных операций. Как отмечается в работах зарубежных экспертов, доминирующим трендом современных конфликтов становится имплементация информационных кампаний, нацеленных на деструкцию доверия к институтам государственной власти и эскалацию социальной дестабилизации. В ответ на эти вызовы Североатлантический альянс осуществляет планомерное наращивание операционного потенциала в сферах кибербезопасности и ведения информационного противоборства [381].

В предисловии ежегодного издания Лондонского международного института стратегических исследований «Military Balance 2015» приводится следующее определение гибридной войны: «использование военных и

---

[380] 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

[381] Galeotti, M. (2016). Hybrid War or Gibridnaya Voina? Small Wars Journal.

невоенных инструментов в интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических преимуществ, используемых в дипломатических действиях; масштабные и стремительные информационные, электронные и кибероперации; прикрытие и сокрытие военных и разведывательных действий; в сочетании с экономическим давлением»[382]. Гибридная война охватывает широкий спектр различных форм военных действий. Как правило, этот термин применяется для описания комбинации военных и невоенных методов, а также скрытых и открытых операций. С перспективы Североатлантического альянса примерами гибридной войны считаются действия России, приведшие к воссоединению Крыма с Россией, а также её роль в конфликте в Донбассе. Гибридные войны увеличивают непредсказуемость мировой политики, поскольку они разрабатываются втайне и направлены на дестабилизацию государств, кардинальное изменение их внутренней и внешней политики, установление внешнего, прежде всего финансово-экономического контроля над страной, что в конечном итоге ведёт к хаотизации международных отношений[383].

Технология гибридных войн настолько стала широко распространенной, что на встрече Совета министров иностранных дел НАТО, состоявшейся 1 декабря 2015 г., была принята «Стратегия гибридных войн». Под гибридными войнами страны-участницы Североатлантического альянса понимают тактику, которая не использует открытое применение обычных военных средств, а включает в себя пропаганду и дезинформацию, методы

---

[382] Military Balance 2015. International Institute for Strategic Studies [Электронный ресурс]. URL: https://www.iiss.org/publications/the-militarybalance/the-military-balance-2015 (дата обращения: 03.03.2025).

[383] 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).

экономического давления, а также тайное использование сил специального назначения[384].

По словам бывшего генерального секретаря НАТО Йенса Столтенберга, суть стратегии базировалась на «трёх китах: подготовка, сдерживание и оборона». Среди ответов на гибридные угрозы, кроме улучшения в работе разведывательных служб и обмене развединформацией, значится также возможность применения специальных сил быстрого реагирования[385].

По мнению российского политолога И.Н. Панарина, стратегия ведения гибридной войны Североатлантического альянса предполагает доминирование инструментов «мягкой силы» и нацелена на дезинтеграцию евразийского пространства, создание хаоса и нестабильности в соседних с Россией государствах с использованием технологий цветных революций, информационной войны, терроризма и экстремизма, финансово-экономического давления, военно-силового принуждения[386].

Институционализация гибридной войны в качестве новой парадигмы межгосударственного противоборства актуализирует задачи по оперативному обнаружению признаков подготовки подобных действий, их своевременной диагностике и организации комплексного нейтрализации. Важнейшим элементом стратегического успеха в данном контексте остается фактор внезапности, традиционно занимающий центральное место в военной теории. Его реализация позволяет достичь тактического превосходства за счет осуществления действий, непредвиденных для противоположной стороны. Следует отметить, что внезапность агрессии создает экстремально сжатые временные рамки для парирования угроз и восстановления нарушенного

---

[384] НАТО приняла стратегию против гибридных войн. 02.12.2015 [Электронный ресурс]. URL: https://newsland.com/user/4296735949/content/ nato-priniala-strategiiu-protiv-quotgibridnykh-voinquot/4854888 (дата обращения: 03.03.2025)

[385] НАТО приняла стратегию против гибридных войн. 02.12.2015 [Электронный ресурс]. URL: https://newsland.com/user/4296735949/content/ nato-priniala-strategiiu-protiv-quotgibridnykh-voinquot/4854888 (дата обращения: 14.01.2019)

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

баланса. Применение современных технологических решений в таких сферах, как киберпространство, информационно-коммуникационная область, космические системы и финансовые операции, многократно усиливает значимость достижения эффекта неожиданности, превращая его в критический фактор успеха гибридных операций [387].

Резюмируя вышесказанное, отметим, что анализ роли ИКТ в контексте эволюции военно-политической доктрины Североатлантического альянса, а также его влияния на баланс сил в современной системе международных отношений позволяет выявить последствия для глобальной и региональной безопасности. Внедрение передовых технологий, таких как искусственный интеллект, большие данные и квантовые вычисления, открывает новые возможности для укрепления обороноспособности.

Динамичное внедрение ИИ в НАТО обусловлено необходимостью адаптации к быстро меняющимся условиям глобальной безопасности, что требует постоянного обновления подходов и технологий. Особое внимание уделяется принципам ответственного использования ИИ, включая соблюдение этических норм, международного права и требований прозрачности. Разработка стандартов и руководящих принципов, направленных на обеспечение безопасного и эффективного применения ИИ, является приоритетом для организации. Это включает минимизацию рисков, связанных с потенциальными ошибками или злоупотреблениями, а также обеспечение совместимости систем ИИ между странами-участницами Североатлантического альянса. Международное сотрудничество в области ИИ также играет важную роль. НАТО активно взаимодействует с партнерами, научными учреждениями и частным сектором для обмена знаниями и опытом. Подобное сотрудничество позволяет военно-политическому блоку оставаться на передовой технологического прогресса, одновременно укрепляя

[387] 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).

коллективную безопасность и способствуя развитию инноваций. Подчеркивается необходимость баланса между инновациями и ответственностью. Внедрение ИИ в военные и стратегические процессы требует тщательного анализа и контроля, чтобы обеспечить его использование в интересах мира и стабильности. НАТО продолжает развивать свои подходы к ИИ, стремясь к тому, чтобы технологии служили инструментом укрепления безопасности, а не источником новых угроз.

Гибридные войны предполагают использование широкого спектра инструментов, включая пропаганду, дезинформацию и кибератаки, для достижения стратегических целей. ИКТ позволяют осуществлять эти действия с высокой эффективностью. НАТО признает важность ИКТ в современных конфликтах и активно инвестирует в развитие соответствующих технологий. Североатлантический альянс разрабатывает системы киберзащиты, которые могут использоваться как для обороны, так и для наступательных операций. Кроме того, НАТО активно сотрудничает с частным сектором и академическими учреждениями для разработки передовых технологий, таких как искусственный интеллект и большие данные, которые могут быть использованы для анализа и прогнозирования действий противника. НАТО использует ИКТ для создания информационных платформ, которые позволяют координировать действия между государствами-членами Североатлантического альянса и их союзниками. Это особенно важно в условиях гибридных войн, где скорость реакции и точность информации являются критическими факторами[388].

Анализ эволюции гибридных войн демонстрирует, что их отличительной чертой является комбинация открытых и скрытых методов воздействия, направленных на дестабилизацию государств, подрыв доверия к институтам власти и формирование социально-политической нестабильности.

---

[388] 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.

Как отмечают исследователи, гибридные угрозы усложняют традиционные модели конфликтов, поскольку включают элементы информационной войны, экономического давления и кибероперaций, что затрудняет их своевременное выявление и нейтрализацию. В этом контексте Стратегия гибридных войн НАТО, сформулированная в 2015 году, основывается на принципах подготовки, сдерживания и обороны, предполагая усиление разведывательных возможностей, развитие кибербезопасности и создание сил быстрого реагирования.

Особую значимость приобретает использование искусственного интеллекта и больших данных, позволяющих анализировать массивы информации, прогнозировать действия противника и оптимизировать процессы принятия решений. Однако внедрение этих технологий сопряжено с этическими и правовыми вызовами, включая риски автономизации военных систем и злонамеренного использования ИКТ. Североатлантический альянс стремится минимизировать подобные угрозы через разработку нормативных рамок, международное сотрудничество и взаимодействие с частным сектором.

Таким образом, гибридные войны, усиленные цифровыми технологиями, становятся доминирующей формой современного межгосударственного противостояния. Их главная опасность заключается в размывании границ между войной и миром, а также в сложности атрибуции атак. В ответ на эти вызовы Североатлантический альянс продолжает совершенствовать свои оборонительные и наступательные возможности в киберпространстве, делая акцент на превентивном сдерживании и укреплении коллективной безопасности. Дальнейшее развитие гибридных угроз требует не только технологической адаптации, но и выработки международных стандартов, направленных на предотвращение эскалации и сохранение стратегической стабильности.

Проведенное исследование позволяет констатировать, что современные военно-политические стратегии переживают период фундаментальной трансформации, обусловленной стремительным развитием цифровых

технологий. Анализ двух взаимосвязанных аспектов этой трансформации – внедрения искусственного интеллекта и больших данных в деятельность НАТО, а также эволюции гибридных войн в цифровую эпоху – выявляет системные изменения в природе международных конфликтов и парадигмах обеспечения безопасности.

Центральное значение в данном контексте приобретает технологизация военно-стратегического планирования. Как показывает исследование, искусственный интеллект и технологии работы с большими массивами данных перешли из разряда вспомогательных инструментов в категорию стратегических факторов, определяющих баланс сил на международной арене. Их применение позволяет военно-политическим акторам:

- осуществлять комплексный мониторинг угроз в режиме реального времени;

- моделировать сценарии развития кризисных ситуаций;

- оптимизировать процессы принятия решений;

- повышать эффективность оперативного реагирования.

Однако технологический прогресс в военной сфере носит принципиально двойственный характер. С одной стороны, он способствует укреплению обороноспособности и повышению точности военного планирования. С другой – создаёт новые уязвимости и риски, связанные с возможностью несанкционированного доступа к критически важным системам, ошибками алгоритмов или их целенаправленным злонамеренным использованием. Это обуславливает необходимость разработки комплексных регуляторных механизмов, сочетающих технологическое развитие с мерами контроля и безопасности.

Параллельно с технологической трансформацией происходит качественное изменение природы современных конфликтов. Гибридные войны, сочетающие традиционные военные методы с инструментами информационно-психологического воздействия, кибератаками и экономическим давлением, становятся доминирующей формой

межгосударственного противостояния. Их ключевыми характеристиками являются:

- размывание границ между военными и невоенными методами воздействия;

- возрастающая роль информационных операций в достижении стратегических целей;

- усложнение процедур атрибуции атак и определения агрессора;

- необходимость разработки новых подходов к сдерживанию и противодействию.

В ответ на эти вызовы НАТО демонстрирует системный подход к цифровой трансформации, включающий не только технологическую модернизацию, но и институциональные изменения. Стратегии Североатлантического альянса в области искусственного интеллекта и противодействия гибридным угрозам предусматривают:

- создание специализированных структурных подразделений;

- углубление сотрудничества с технологическими компаниями и академическими институтами;

- значительные инвестиции в исследовательские программы;

- разработку нормативных рамок для ответственного использования новых технологий.

Особого внимания заслуживает вопрос международного регулирования цифровых технологий военного назначения. Проведенное исследование выявляет острую потребность в:

- разработке универсальных международно-правовых норм применения новых технологий в военных целях;

- создании механизмов предотвращения технологических конфликтов;

- установлении чётких правил ответственности за злонамеренные кибероперации;

- развитии многосторонних диалоговых площадок по вопросам цифровой безопасности.

Перспективы дальнейших исследований в данной области видятся в углубленном изучении нескольких ключевых направлений:

- влияния квантовых технологий на военно-стратегический баланс;

- этических аспектов разработки и применения автономных систем вооружений;

- возможностей искусственного интеллекта в области кризисного прогнозирования и предотвращения конфликтов;

- сравнительного анализа национальных подходов к обеспечению цифровой безопасности.

В заключение следует подчеркнуть, что цифровая трансформация военно-политических стратегий представляет собой сложный, многомерный процесс, требующий постоянного научного осмысления и адаптации институциональных механизмов международной безопасности. Развитие технологий искусственного интеллекта и совершенствование методов противодействия гибридным угрозам будут оставаться ключевыми факторами, определяющими эволюцию системы международных отношений в обозримой перспективе. При этом особую значимость приобретает поиск баланса между технологическим прогрессом и поддержанием стратегической стабильности, что требует скоординированных усилий как на национальном, так и на международном уровне.

3.2 Место и роль России в современной политике НАТО в киберпространстве

В условиях стремительной цифровизации и роста зависимости государств от информационных технологий киберпространство стало одной из ключевых сфер геополитического соперничества. Россия, обладающая значительным потенциалом в области кибербезопасности и кибероперациий, занимает важное место в стратегических расчетах НАТО. Взаимодействие России и Североатлантического альянса в киберпространстве характеризуется

сложным сочетанием конфронтации, конкуренции и поиска механизмов сдерживания.

Важно отметить, что Российская Федерации неоднократно сталкивалась с ложными обвинениями со стороны США и их сателлитов в контексте злонамеренного использования киберсредств для достижения политических целей. Начиная с 2014 года, было зафиксировано множество фактов обвинения России в масштабном кибершпионаже, заражении мейнфреймов и компьютеров американских компаний и государственных учреждений и т.д.

Так, например, в 2016 году глава Кибернетического командования США, директор Агентства национальной безопасности и руководитель Центральной службы безопасности адмирал М. Роджерс включил Россию в список основных угроз в киберпространстве[389]. Особый резонанс вызвали обвинения России во вмешательство в президентские выборы в США в 2016 году. 8 июля 2021 года пресс-секретарь президента США Д. Байдена Д. Псаки заявляла, что Вашингтон считает, что Москва несет ответственность за действия всех хакеров в России вне зависимости от причастности правительства[390]. Несмотря на всецелую готовность российской стороны к сотрудничеству в расследовании актов киберпреступности, позиция Соединенных Штатов не претерпевала изменений. 2 августа 2021 года Чрезвычайный и Полномочный Посол Российской Федерации в США А.И. Антонов сообщил о 35 запросах относительно происхождения кибератак в 2021 году. В свою очередь с 2020 года Российская сторона ответила на 12 запросов США по кибератакам, в то время как 80 российских запросов

[389] Глава АНБ назвал Россию самой опасной страной в киберпространстве URL: https://www.cnews.ru/news/top/2016-04-07_glava_anb_nazval_rossiyu_glavnoj_ugrozoj_v_kiberprostranstve (дата обращения: 14.02.2025).

[390] White House: U.S. engaged in ongoing talks with Russia about ransomware, other cyberattacks URL: https://www.ny1.com/nyc/all-boroughs/politics/2021/07/06/white-house--u-s--engaged-in-ongoing-talks-with-russia-about-ransomware--other-cyberattacks (accessed: 08.03.2025).

остались без ответа[391]. Вышеуказанные факты дают ясное понимание о фактическом нежелании США вести плодотворное сотрудничество в области международной кибербезопасности и реальной борьбы с транснациональной киберпреступностью. Напротив, столь явная антироссийская риторика ярко свидетельствовала о том, что действительным приоритетом правительства США является не противодействие киберугрозам, а выставление России в негативном свете, в качестве страны-покровителя хакеров и рассадника киберпреступности, которой не чуждо использование запретных методов для реализации своей внешней политики. Впрочем, столь агрессивная, и что важно подчеркнуть, безосновательная политика уже давно стала отличительной чертой Российско-Американских отношений. Однако, прошедшая в Женеве 16 июня 2021 года встреча на высшем уровне между Президентом России В.В. Путиным и Президентом США Д. Байденом дала некую надежду на продолжение поиска точек соприкосновения и даже заключения договоренностей в сфере кибербезопасности между Россией и США. Профессор политической географии Рэдфордского университета Г. Иоффе заявил в беседе с корреспондентами ТАСС, что обеспокоенность администрации президента Байдена из-за угрозы кибератак стала одной из основных причин проведения саммита. По итогам встречи впервые за долгий период появилась определенная перспектива в развитии российско-американского сотрудничества в области кибербезопасности и совместного противодействия международной киберпреступности. В ходе состоявшейся по итогам переговоров конференции, президент США Д. Байден заявил, что обе стороны дадут поручение группам экспертов рассмотреть конкретные случаи

[391] РФ с начала года сделала 35 запросов США о происхождении кибератак URL: https://iz.ru/1201625/2021-08-02/rf-s-nachala-goda-sdelala-35-zaprosov-ssha-o-proiskhozhdenii-kiberatak (дата обращения: 03.07.2023).

кибератак, которые имели место в обеих странах, и разработать четкие принципы неприемлемого поведения в киберпространстве[392].

Особого внимания заслуживают киберугрозы, направленные на критическую инфраструктуру Российской Федерации. По мнению многих экспертов, политически ангажированные хакеры могут получить возможность выводить из строя при помощи кибератак крупные объекты критической инфраструктуры – системы связи, энергетические объекты и т.д. Так, в 2018 году было выявлено 4,3 млрд кибератак на критическую информационную структуру РФ. Объектами атак стали компания «Роснефть» и два десятка других крупных российских организаций, в том числе относящихся к таким стратегическим отраслям, как нефтепереработка, газовая и химическая промышленность, сельское хозяйство и т.д. Злоумышленники также пытались атаковать несколько крупных российских бирж.

В 2020 году были зафиксированы DDoS-атаки из США, Великобритании и Украины при голосовании по поправкам в Конституцию Российской Федерации. «Например, в период проведения голосования по поправкам в Конституцию Российской Федерации (25 июня – 1 июля 2020 г.) имели место масштабные нападения на инфраструктуру ЦИК и другие государственные органы России. Источники DDoS-атак мощностью до 240 тыс. запросов в секунду фиксировались с территории США, Великобритании, Украины и ряда стран СНГ», – сообщал спецпредставитель президента РФ по вопросам международного сотрудничества в сфере информационной безопасности А.В. Крутских[393].

В ходе выборов в Государственную думу Федерального собрания Российской Федерации VIII созыва, проходивших 17-19 сентября 2021 года

---

[392] Эксперт: саммит в Женеве дает надежду на заключение США и РФ договоренностей в киберсфере URL: https://tass.ru/mezhdunarodnaya-panorama/11672185 (дата обращения: 07.02.2025).

[393] При голосовании по конституции в РФ фиксировали DDoS-атаки из США, Великобритании, Украины URL: https://tass.ru/politika/9391631 (дата обращения: 07.02.2025).

было зафиксировано беспрецедентное количество хакерских атак. Глава Минцифры М.И. Шадаев сообщал, что кибератаки на системы электронного голосования на выборах в России велись с IP-адресов, зарегистрированных в США, Германии, при этом половина пришлась на Соединенные Штаты. «Ростелеком» заявлял, что на связанные с выборами порталы совершили 19 атак. По данным оператора, в атаках также участвовали зараженные устройства из ряда стран. Минцифры утверждало, что кибератаки не оказали значимого эффекта[394].

Вторым рассматриваемым аспектом использования информационно-коммуникационной сети Интернет в целях, направленных против безопасности Российской Федерации и стран постсоветского пространства, является террористическая и экстремистская деятельность в киберпространстве. Как известно, термин «Кибертерроризм», обозначающий использование компьютерных и телекоммуникационных технологий в террористических целях, был предложен в 1980-х годах старшим научным сотрудником Института безопасности и разведки Б. Коллином[395]. За последнее десятилетие, ввиду повсеместного использования технологий «информационных войн», данный термин стал как никогда актуальным. На сегодняшний день в России и на постсоветском пространстве гипотетические кибератаки могут преследовать определённые цели. Среди них следует рассматривать пассивный сбор закрытых данных, захват контроля над военными объектами, ядерными электростанциями, космическими объектами и т.д[396].

---

[394] Матвиенко назвала беспрецедентным вмешательство в выборы в Госдуму URL: https://www.kommersant.ru/doc/4995745 (дата обращения: 13.02.2025).

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

[396] 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).

Рассматривая место и роль России в политике Североатлантического альянса в киберпространстве на современном этапе первостепенно необходимо выделить компоненту гибридных войн. Так, особенности гибридной войны, применяемой НАТО, заключаются в использовании широкого спектра невоенных и военных средств воздействия на противника без официального объявления войны. Данная стратегия в отношении Российской Федерации демонстрирует свою эффективность, поскольку позволяет избежать значительных потерь, которые страны-участницы Североатлантического альянса могли бы понести в условиях полномасштабного вооруженного конфликта. В связи с этим, осуществление гибридной войны с целью потенциального достижения политических целей рассматривается НАТО в качестве ключевого приоритета и стратегической задачи[397].

Говоря о доктринальном оформлении места и роли России в политике Североатлантического альянса в киберпространстве на современном этапе, первостепенно целесообразно рассмотреть основные положения Стратегической концепции НАТО, принятой главами государств и правительств на встрече в верхах НАТО в Мадриде 29 июня 2022 г. Стратегия прямо указывает на одно их ключевых значений киберпространства в контексте коллективной обороны государств-членов Североатлантического альянса. Так, согласно статье 24, страны-участницы НАТО «ускорят цифровую трансформацию, адаптируют структуру органов военного управления НАТО к информационному веку и укрепят киберзащиту, сети и инфраструктуру, будут поощрять инновации и увеличивать инвестиции в новые и прорывные технологии, чтобы сохранить оперативную совместимость и военное превосходство, будут работать вместе над внедрением и интеграцией новых технологий, сотрудничать с частным

[397] Countering Hybrid Warfare Project: Understanding Hybrid Warfare.28.09.2017. [Электронный ресурс]. URL: https://www.gov.uk/government/ publications/countering-hybrid-warfare-project-understanding-hybrid-warfare#history (дата обращения: 05.03.2025).

сектором, защищать наши инновационные экосистемы, формировать стандарты и придерживаться принципов ответственного использования, которые отражают наши демократические ценности и права человека»[398].

В Стратегической концепции Североатлантического альянса 2022 года Россия занимает центральное место как один из ключевых вызовов безопасности военно-политического блока. Документ отражает существенное изменение восприятия России по сравнению с предыдущими концепциями, где акцент делался на диалог и сотрудничество. В новой концепции Россия характеризуется как прямая и существенная угроза безопасности, стабильности и миропорядку, основанному на правилах, что прежде всего связно с проведением Специальной военной операции на Украине. Специальная военная операция России, начатая 24 февраля 2022 года, стала феноменом истинно мирового значения. В течение десятилетий, последовавших за распадом социалистического блока, фактически, существовал однополярный мир во главе с Соединёнными Штатами и их сателлитами в рамках Североатлантического альянса. 24 февраля обозначило начало конца однополярного мироустройства. Россия начала тернистый процесс утверждения себя в качестве отдельной цивилизации, реального полюса силы, в противовес западному либеральному глобализму. В широком смысле Специальную военную операцию следует определять в качестве противостояния однополярного и многополярного типов мироустройства. В течение последних лет мы были свидетелями того, как государства-члены НАТО осуществляли планомерную накачку Украины различными видами вооружения, которая, впрочем, не прекратилась, а в разы усилилась после начала Специальной Операции, что явно свидетельствует об уже случившихся существенной интенсификации и обострении противоречий между Россией и

---

[398] Стратегическая концепция НАТО 2022 года https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf (дата обращения: 01.03.2024).

всем Коллективным Западом, прежде всего в лице Североатлантического альянса.

Возвращаясь к доктринальному оформлению места и роли России в современной политике НАТО в киберпространстве в Стратегической концепции военно-политического блока 2022 г., отметим, что Россия рассматривается как государство, которое использует широкий спектр инструментов гибридной войны, включая кибератаки, дезинформацию, экономическое давление и военную силу, для достижения своих стратегических целей. В концепции подчеркивается, что действия России подрывают международное право, суверенитет и территориальную целостность других государств, что представляет угрозу для евроатлантической безопасности. Так, согласно статье 8 Стратегической концепции, «Российская Федерация является наиболее значительной и прямой угрозой безопасности государств-членов НАТО, а также миру и стабильности в евроатлантическом регионе. Она стремится установить сферы влияния и прямой контроль посредством принуждения, подрывной деятельности, агрессии и аннексии. Она использует обычные, кибер- и гибридные средства против нас и наших партнеров. Её направленные на принуждение военный потенциал, риторика и доказанная готовность использовать силу для достижения своих политических целей подрывают основанный на правилах международный порядок. Российская Федерация модернизирует свои ядерные силы и расширяет свои новые и разрушительные системы доставки двойного назначения, используя при этом в целях принуждения угрозу ядерного оружия. Её целью является дестабилизация стран к востоку и югу от нас. На Крайнем Севере её способность нарушить усиление стран НАТО и свободу судоходства через Северную Атлантику является стратегическим вызовом Североатлантическому союзу. Наращивание Москвой военной мощи, в том числе в регионах Балтийского, Черного и Средиземного морей, наряду с её

военной интеграцией с Беларусью, бросает вызов нашей безопасности и интересам»[399].

По мнению профессора А.В. Крутских, в стратегии отмечается, что возможности Североатлантического альянса в киберпространстве являются составным элементом его оборонного и сдерживающего потенциала. Декларируется приверженность государств-членов военно-политического блока принципам так называемого «порядка, основанного на правилах». Фиксируется их позиция о применимости к киберпространству действующего международного права. Акцентируется, что одно или несколько злонамеренных воздействий в киберпространстве «могут привести к задействованию Советом НАТО положений статьи 5 Вашингтонского договора». Более того, Российская Федерация названа «самой существенной и прямой угрозой безопасности государств-членов Североатлантического альянса, а также миру и стабильности на Евроатлантическом пространстве». России вменяется «использование гибридных и киберсредств» наряду с конвенциональными против участников и партнёров военно-политического блока[400].

В целом, статья 8 Стратегической концепции НАТО 2022 года представляет собой системный анализ угроз, исходящих от России, и отражает решимость Североатлантического альянса адаптироваться к новым вызовам. Документ подчеркивает необходимость укрепления сдерживания и обороны, а также развития новых стратегических возможностей для противодействия гибридным, кибер- и ядерным угрозам. Это свидетельствует о том, что Россия остается центральным элементом в стратегическом планировании НАТО, а её

---

[399] Стратегическая концепция НАТО 2022 года https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf (дата обращения: 01.03.2024).

[400] 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

действия продолжают оказывать значительное влияние на безопасность и стабильность в евроатлантическом регионе.

Особую значимость в глобальном и прикладном контексте представляет доклад Центра передового опыта НАТО в области киберзащиты под названием «Киберугрозы и НАТО 2030». В данном документе подробно анализируются меры реагирования Североатлантического альянса на действия противников в киберпространстве, включая применение новых технологий, ведение боевых действий в киберсфере, необходимость обмена информацией, анализа киберугроз и проведения специализированных учений. Кроме того, в докладе рассматриваются нормативные и политические механизмы, направленные на противодействие вызовам в сфере кибербезопасности. Примечательно, что отдельный раздел, посвященный обзору потенциальных противников НАТО, полностью сфокусирован на роли и действиях России[401].

Конкретизируя место и роль России в современной политике НАТО в киберпространстве, целесообразно рассмотреть категоризацию приписываемых Российской Федерации злонамеренных действий в киберпространстве в контексте проведения Специальной военной операции на Украине.

Важно отметить, что еще в июне 2021 года Североатлантический альянс признал существенные изменения в структуре угроз, что потребовало учёта трансформации киберпространства в рамках своей деятельности. Это привело к разработке и принятию новой комплексной политики в области киберзащиты, направленной на решение трёх ключевых задач НАТО: обеспечения коллективной обороны, управления кризисами и укрепления безопасности на основе международного сотрудничества. Согласно данной политике, киберпотенциал Североатлантического альянса призван обеспечить сдерживание, защиту и противодействие широкому спектру киберугроз как в

[401] 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).

условиях мирного времени, так и в период военных конфликтов, а также в процессе урегулирования кризисных ситуаций в политической, военной и технической сферах[402].

Рассматривая статью американского исследователя в области международных отношений Д. Хейли «Понимание киберэффектов в современной войне», представляется возможным идентифицировать видение ключевых компонентов современной политики России в киберпространстве с перспективы Североатлантического альянса.

В современной оборонной доктрине операции, осуществляемые до начала активных боевых действий, не классифицируются как военные операции в традиционном понимании, однако их роль заключается в создании условий, способствующих успеху в будущих вооруженных конфликтах или в рамках стратегического соперничества ниже порога открытого военного противостояния. Подобные действия, как правило, проводятся на нулевой или первой фазах конфликта, которые включают этапы формирования стратегической обстановки и сдерживания. Государства активно используют уникальные возможности наступательных кибероперациий, которые позволяют им достигать стратегических целей без применения традиционных форм военной силы[403].

Ярким примером подобной стратегии по мнению Д. Хейли являются действия России перед началом Специальной военной операции на Украине в 2022 году. Согласно данным Microsoft, российские кибероперации были направлены на получение первоначального доступа к критически важным объектам инфраструктуры, что могло быть использовано для их последующего уничтожения. Эти действия демонстрируют использование

---

[402] Cyber defence NATO. URL: https:// www.nato.int/cps /en/natohq/topics_78170. htm (дата обращения: 23.02.2022).

[403] Understanding Cyber Effects in Modern Warfare URL: https://warontherocks.com/2025/01/understanding-cyber-effects-in-modern-warfare/?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru (accessed: 08.03.2025).

информационных операций для подготовки будущих военных операций. Кроме того, в статье американского политолога заявлено, что Россия осуществляла атаки на информационные сети и IT-системы, а также проводила кампании по подрыву доверия к государственным институтам и снижению морального духа населения. Д. Хейли утверждает, что российская военная разведка провела масштабные атаки на сотни систем украинского правительства, а также на организации энергетического и финансового секторов. В результате этих атак были повреждены правительственные сайты, а также распространены заявления об удалении данных с серверов и их возможной публикации. Подобные операции не только подготавливают почву для будущих военных действий, но и могут оказывать кумулятивное воздействие на стратегическом уровне, подрывая источники национальной власти[404].

Констатируя вышесказанное, отметим, что в контексте современных реалий и с учетом стремительно меняющейся системы международных отношений и архитектуры глобальной и региональной безопасности, место и роль России в современной политике НАТО в киберпространстве на сегодняшний день определяется в качестве одного из ключевых источников угроз, что стимулирует развитие коллективной обороны, укрепление киберзащиты и сотрудничество между странами-членами. Занимая значимое место в современной политике НАТО в киберпространстве, выступая как один из ключевых акторов, формирующих вызовы и угрозы в этой сфере, Россия является ключевым «антагонистом» в современной политике Североатлантического альянса в киберпространстве.

Проведенный анализ позволяет констатировать, что место и роль России в современной политике НАТО в киберпространстве определяются сложным сочетанием стратегического противостояния, взаимных обвинений и поиска

---

[404] Understanding Cyber Effects in Modern Warfare URL: https://warontherocks.com/2025/01/understanding-cyber-effects-in-modern-warfare/?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru (accessed: 08.03.2025).

механизмов сдерживания. В условиях цифровой трансформации и возрастающей зависимости государств от информационных технологий киберпространство стало ключевой ареной геополитического соперничества, в котором Россия рассматривается Североатлантическим альянсом как один из основных источников угроз.

Во-первых, российско-американские отношения в киберпространстве характеризуются высокой степенью конфронтации, что проявляется в регулярных обвинениях России в проведении кибератак на критическую инфраструктуру и государственные учреждения западных стран. Несмотря на отсутствие неопровержимых доказательств, США и их союзники по НАТО последовательно включают Россию в число главных угроз кибербезопасности, что свидетельствует о политизированности данного вопроса. При этом диалог по вопросам противодействия киберпреступности остается односторонним: российские запросы о расследовании атак на свою инфраструктуру систематически игнорируются, тогда как Москва демонстрирует готовность к сотрудничеству.

Во-вторых, в рамках стратегических документов НАТО Россия определяется в качестве наиболее значительной и прямой угрозы безопасности организации. Подчеркивается, что Москва использует гибридные методы, включая кибератаки, дезинформацию и экономическое давление, для достижения своих внешнеполитических целей. Это отражает радикальное изменение восприятия России по сравнению с предыдущими доктринами, где акцент делался на диалог и партнёрство.

В-третьих, в контексте Специальной военной операции киберпространство стало важным элементом гибридного противостояния. Западные аналитики и эксперты НАТО обвиняют Россию в использовании кибероперaций для дестабилизации Украины, атаках на критическую инфраструктуру и подготовке информационных кампаний, направленных на подрыв доверия к государственным институтам. В то же время сама Россия сталкивается с масштабными DDoS-атаками на свои информационные

системы, включая выборы и государственные порталы, что свидетельствует о взаимном характере киберконфликта.

Таким образом, в современной политике НАТО Россия занимает место ключевого антагониста в киберпространстве, что стимулирует развитие альянсом новых механизмов киберзащиты, коллективного сдерживания и стратегического противодействия. В долгосрочной перспективе данная конфронтация будет определять динамику международной кибербезопасности, усиливая риски дальнейшей фрагментации глобального цифрового пространства.

3.3. Киберпространство как фактор отношений России и НАТО в условиях новой геополитической напряженности

В условиях стремительной цифровизации и роста киберугроз взаимодействие между государствами в сфере кибербезопасности становится важным элементом обеспечения международной стабильности. Российская Федерация и Североатлантический альянс, несмотря на сложные политические отношения, имеют потенциальные возможности для сотрудничества в этой области, что могло бы способствовать снижению рисков и укреплению доверия между сторонами.

Киберпространство, являясь глобальной средой, не признаёт национальных границ, что делает киберугрозы транснациональными по своей природе. Кибератаки на критическую инфраструктуру, использование киберпространства для вмешательства во внутренние дела государств, а также распространение вредоносного программного обеспечения представляют собой вызовы, требующие совместного реагирования. В этом контексте сотрудничество России и НАТО могло бы стать важным шагом в создании механизмов предотвращения и урегулирования киберконфликтов.

Противоборство между Российской Федерацией и Североатлантическим альянсом в киберпространстве представляет собой комплексное и многогранное измерение стратегического соперничества.

Данная конфронтация характеризуется применением широкого спектра кибероперaций, включая шпионаж, дезинформационные кампании, дестабилизацию критической инфраструктуры и тестирование систем обороны, что осуществляется в гибридном формате, часто ниже условного порога открытого вооруженного конфликта. Подобная динамическая конфронтация непрерывно эволюционирует, определяя новые вызовы международной стабильности и безопасности.

Ранее описанные действия и элементы стратегии Североатлантического альянса указывают на его дестабилизирующую роль в международной киберсреде. Действия НАТО, под предлогом укрепления обороноспособности, ведут к наращиванию конфронтационного потенциала в цифровой сфере. Активное развёртывание Североатлантическим альянсом наступательных киберподразделений и интеграция искусственного интеллекта в системы управления рассматриваются как подготовка к силовому доминированию в будущих конфликтах. Политика киберсдерживания, продвигаемая военно-политическим блоком, по сути, легитимизирует превентивные удары по критической инфраструктуре суверенных государств, что грубо нарушает базовые принципы международного права. Расширение сферы коллективной обороны на киберпространство создает опасный прецедент, позволяющий Североатлантическому альянсу интерпретировать любые инциденты как casus belli. Подобные действия, осуществляемые без мандата ООН, подрывают архитектуру глобальной безопасности и провоцируют новую гонку кибервооружений, вынуждая другие государства принимать асимметричные меры для защиты своего цифрового суверенитета.

Российская Федерация занимает принципиальную и последовательную позицию в вопросах обеспечения международной информационной безопасности, выступая в роли гаранта стратегической стабильности и архитектора справедливой многополярной системы в цифровом пространстве. В условиях наращивания наступательного киберпотенциала

Североатлантическим альянсом и агрессивной экспансии военно-политического блока вблизи российских границ, Россия вынужденно принимает асимметричные и превентивные меры для защиты своего национального суверенитета и обеспечения безопасности критической информационной инфраструктуры. Российская инициатива по установлению международно-правовых норм поведения в киберпространстве, основанных на принципах уважения государственного суверенитета и невмешательства во внутренние дела, демонстрирует её конструктивную роль. Эти предложения, однако, систематически блокируются западными странами. Таким образом, действия России носят сугубо оборонительный и вынужденный характер, являясь ответом на дестабилизирующую деятельность Североатлантического альянса, и направлены на создание сбалансированной и равноправной системы международной кибербезопасности, свободной от диктата одной группы государств.

Несмотря на сложные политические отношения между Россией и НАТО, обусловленные геополитическими противоречиями и кризисами доверия, сотрудничество в области кибербезопасности может стать важным инструментом снижения напряжённости. В контексте современной системы международных отношений, где многополярность сочетается с усилением конкуренции между государствами, киберпространство становится ареной как конфронтации, так и потенциального диалога. Учитывая транснациональный характер киберугроз, ни одна страна или альянс не способны в одиночку обеспечить эффективную защиту от них. Данный фактор создаёт объективную основу для поиска точек соприкосновения между Россией и НАТО.

Кибербезопасность становится ключевым элементом глобальной стабильности, однако взаимодействие между Россией и Североатлантическим альянсом в этой области характеризуется отсутствием доверия и взаимными обвинениями. Россия неоднократно заявляла о своей готовности к диалогу по вопросам кибербезопасности, подчёркивая необходимость выработки международных норм и правил, которые бы регулировали деятельность

государств в цифровой сфере. Москва выступает за создание многосторонних механизмов, способных предотвратить эскалацию киберконфликтов и обеспечить прозрачность действий всех сторон. Однако, как отмечают эксперты, отсутствие единого понимания угроз и целей между Россией и НАТО существенно затрудняет достижение договорённостей. Со своей стороны, Североатлантический альянс активно развивает стратегии кибероборонs, рассматривая киберпространство как новое поле для потенциальных конфликтов.

НАТО неоднократно обвиняло Россию в причастности к кибератакам на критически важную инфраструктуру стран-членов военно-политического блока, что Москва категорически отрицает. Россия, в свою очередь, указывает на двойные стандарты в подходе Североатлантического альянса, подчёркивая, что подобные обвинения часто используются для оправдания наращивания собственного киберпотенциала и усиления военного присутствия вблизи российских границ.

Так, по словам бывшего заместителя Министра иностранных дел Российской Федерации О.В. Сыромолотова, Вашингтон оказывает поддержку ИТ-армии Украины, в том числе для осуществления атак на критическую информационную инфраструктуру. В настоящее время наибольшее количество кибератак на территорию России совершается с территории США, стран НАТО и Украины[405].

Рассматривая перспективы взаимодействия России и Североатлантического альянса в области кибербезопасности на современном этапе первостепенно необходимо учитывать роль Специальной военной операции на Украине. Так, по словам заместителя директора РУНЦ «Безопасность» МГТУ им. Н.Э. Баумана С. Короткова, «число кибератак на Россию в 2022 году увеличилось на 80%. А с начала специальной военной операции возросла мощность DDoS-атак на российские ресурсы,

[405] Замглавы МИД РФ: США тренируют украинскую "IT-армию" URL: https://tass.ru/interviews/16906301 (дата обращения: 05.01.2025).

продолжительность каждой из кибератак в мае 2022 года достигала 57 часов»[406].

Опираясь на современные политические реалии, со вступлением в должность Президента США Д. Трампа 20 января 2025 года и с учётом взятого текущей администрацией США курса на деэскалацию, представляется возможным говорить о некоторых подвижках в контексте взаимодействия России и НАТО в области кибербезопасности.

Так, в статье The Washington Post от 1 марта 2025 г. указывается, что США прекращаются наступательные кибероперации против России. По словам действующего и бывшего чиновников Министерства обороны США, пауза продлится до тех пор, пока продолжаются переговоры по урегулированию украинского кризиса. По словам бывшего дипломата в администрации президента США Б. Клинтона Д. Льюиса, Россия по-прежнему остается одной из главных киберугроз США, но прекращение кибероперaций может стать разумным тактическим шагом с целью содействия переговорному процессу[407].

Вопросы обеспечения кибербезопасности всё чаще становятся неотъемлемой частью международной политики и дипломатии. Прекращение наступательных кибероперaций со стороны США может рассматриваться как попытка снижения напряжённости и создания условий для диалога, что соответствует общим тенденциям к поиску мирных решений в условиях глобальных вызовов. Однако сохраняющаяся оценка России как одной из главных киберугроз подчёркивает сложность и противоречивость данного процесса.

---

[406] Злонамеренные дезинформационные кампании - дестабилизирующий фактор поддержания международной информационной безопасности URL: https://interaffairs.ru/jauthor/material/2745 (дата обращения: 05.09.2024).

[407] As Trump warms to Putin, U.S. halts offensive cyber operations against Moscow URL: https://www.washingtonpost.com/national-security/2025/03/01/trump-putin-russia-cyber-offense-cisa/ (accessed: 01.04.2025).

Говоря о перспективах взаимодействия России и Североатлантического альянса в области кибербезопасности на современном этапе первостепенно целесообразно отметить, что и Россия, и государства-члены Североатлантического альянса имеют общие интересы в области кибербезопасности. Во-первых, обе стороны заинтересованы в предотвращении эскалации конфликтов в киберпространстве. Во-вторых, существует необходимость в разработке международных норм и правил поведения в киберпространстве, которые могли бы снизить риски непреднамеренных конфликтов.

Потенциальные векторы взаимодействия России и Североатлантического альянса в области кибербезопасности возможно категоризировать следующим образом:

1) восстановление диалога посредством многосторонних диалоговых площадок;
2) восстановление взаимного доверия и создание механизмов взаимодействия;
3) разработка международных норм деятельности государственных и негосударственных акторов в киберпространстве;
4) совместные усилия по борьбе с киберпреступностью и злонамеренными актами кибервоздействия;
5) участие в международных инициативах по кибербезопасности;
6) содействие осуществлению образовательных и научных обменов.

Восстановление диалога посредством многосторонних диалоговых площадок.

Одной из ключевых перспектив взаимодействия России и НАТО в области кибербезопасности является восстановление диалога через многосторонние международные площадки. Организация Объединенных Наций (ООН) и Организация по безопасности и сотрудничеству в Европе (ОБСЕ) могли бы стать основными платформами для обсуждения вопросов

кибербезопасности. В рамках ООН уже существуют инициативы, направленные на разработку международных норм поведения в киберпространстве. Например, Рабочая группа ООН по вопросам киберпространства (OEWG) в 2021 году предложила рекомендации, включая создание механизмов доверия, обмен информацией о киберугрозах и предотвращение эскалации конфликтов в киберпространстве[408]. Россия и НАТО могли бы совместно поддержать эти инициативы, что позволило бы снизить уровень недоверия и создать основу для дальнейшего сотрудничества.

Восстановление взаимного доверия и создание механизмов взаимодействия.

Одним из наиболее перспективных направлений сотрудничества является создание механизмов доверия и прозрачности (Confidence-Building Measures, CBMs). Такие механизмы могут включать:

- Обмен информацией о киберугрозах: Россия и НАТО могли бы договориться о регулярном обмене данными о кибератаках, их источниках и методах предотвращения, что позволило бы снизить риски непреднамеренных конфликтов и улучшить понимание намерений сторон.
- Уведомление о крупных киберучениях: стороны могли бы договориться о предварительном уведомлении о проведении крупных киберучений, что снизило бы риск неправильной интерпретации действий друг друга.
- Создание «горячих линий» для экстренной связи: подобно так называемым «красным телефонам» времен холодной войны, такие линии связи могли бы использоваться для предотвращения эскалации в случае киберинцидентов.

[408] Open-ended Working Group URL: https://disarmament.unoda.org/open-ended-working-group/ (дата обращения: 05.08.2024).

Еще одной перспективой сотрудничества является разработка и принятие международных норм поведения в киберпространстве. Такие нормы могли бы включать:

- Мораторий на кибератаки на критическую инфраструктуру: Россия и НАТО могли бы договориться о неприкосновенности объектов критической инфраструктуры, таких как энергетические сети, системы водоснабжения и медицинские учреждения.
- Ограничение использования кибероружия: стороны могли бы согласовать ограничения на использование кибероружия, направленного на нарушение работы государственных систем или причинение вреда гражданскому населению.
- Создание международного органа по расследованию киберинцидентов: такой орган мог бы заниматься расследованием крупных кибератак и выявлением их источников, что способствовало бы повышению прозрачности и доверия.

Совместные усилия по борьбе с киберпреступностью и злонамеренными актами кибервоздействия.

Россия и Североатлантический альянс могли бы активизировать сотрудничество в борьбе с транснациональной киберпреступностью. Киберпреступники часто действуют вне юрисдикции отдельных государств, что требует координации усилий на международном уровне.

- Создание совместных оперативных групп: Россия и НАТО могли бы создать совместные оперативные группы для расследования и пресечения деятельности киберпреступных группировок.
- Обмен опытом и технологиями: стороны могли бы обмениваться опытом и технологиями в области киберзащиты, что позволило бы повысить эффективность борьбы с киберугрозами.

Россия и НАТО могли бы совместно участвовать в международных инициативах, направленных на укрепление кибербезопасности. Например, инициатива Парижского призыва за доверие и безопасность в киберпространстве (Paris Call for Trust and Security in Cyberspace) уже объединяет более 1000 участников, включая государства, компании и неправительственные организации[409]. Участие России и НАТО в подобных инициативах могло бы способствовать выработке общих подходов к кибербезопасности.

Таким образом целесообразно отметить, что перспективы взаимодействия России и Североатлантического альянса в области обеспечения кибербезопасности, несмотря на существующие политические разногласия, остаются значительными. Восстановление диалога посредством взаимодействия через многосторонние площадки, создание механизмов доверия и прозрачности, разработка международных норм поведения, совместная борьба с киберпреступностью и участие в международных инициативах – всё это может способствовать укреплению стабильности в киберпространстве. Однако для реализации этих перспектив необходимо преодоление политических барьеров и восстановление доверия между сторонами. Взаимодействие России и Североатлантического альянса в области кибербезопасности остается одной из наиболее сложных и противоречивых задач современной международной политики. Несмотря на очевидные общие интересы в обеспечении стабильности и безопасности киберпространства, сотрудничество между сторонами затруднено глубокими политическими разногласиями, отсутствием доверия и взаимными обвинениями в причастности к кибератакам. Тем не менее, в условиях растущей сложности киберугроз и их транснационального характера, игнорирование необходимости диалога становится всё менее допустимым. Основным препятствием для сотрудничества между Россией и НАТО в

[409] Paris Call for Trust and Security in Cyberspace. (2018). Retrieved from https://pariscall.international

области кибербезопасности остается отсутствие политического доверия. Фактическое положение дел свидетельствует о том, что Россия и НАТО находятся в состоянии киберпротивостояния, которое периодически перерастает в открытые конфликты в виртуальном пространстве.

Проведённый анализ перспектив взаимодействия России и НАТО в области кибербезопасности позволяет сделать ряд ключевых выводов, отражающих как существующие вызовы, так и потенциальные направления сотрудничества. В условиях глобальной цифровизации и роста транснациональных киберугроз необходимость диалога между основными акторами международных отношений становится всё более очевидной, несмотря на сохраняющиеся геополитические противоречия.

В среднесрочной перспективе сотрудничество России и НАТО в киберпространстве останется ограниченным и фрагментарным. Однако даже минимальные меры (например, возобновление диалога в ОБСЕ или создание каналов экстренной связи) могут снизить риски непреднамеренной эскалации. В долгосрочном плане конвергенция позиций возможна лишь в рамках пересмотра архитектуры глобальной кибербезопасности с учетом принципа многополярности.

Заключение

В соответствии с поставленной целью в ходе диссертационного исследования был решен комплекс взаимосвязанных задач: от концептуализации базового терминологического аппарата и анализа трансформации стратегии НАТО в киберпространстве за период с 1999 г. по настоящее время до идентификации места и роли России в киберполитике Североатлантического альянса. Теоретико-методологическая основа, синтезирующая парадигмы политического реализма, либерального институционализма и конструктивизма в сочетании с историко-хронологическим и сравнительным методами, позволила обеспечить комплексность и междисциплинарность анализа.

Настоящая диссертационная работа, посвящённая исследованию деятельности Североатлантического альянса в киберпространстве, включая политические, военно-стратегические и технологические аспекты, была инициирована в ответ на системные вызовы, сформировавшиеся в современной системе международных отношений и глобальной безопасности в течение последнего десятилетия. Исходной точкой послужил констатируемый факт тотальной цифровой трансформации, которая привела к имплементации информационно-коммуникационных технологий во все без исключения сферы общественной и государственной деятельности, породив принципиально новую гибридную реальность. В данном контексте киберпространство утвердилось не только как технологическая среда, но и как новая стратегическая арена, на которой традиционное геополитическое соперничество, в частности, между Россией и коллективным Западом в лице Североатлантического альянса, обретает форму интенсивного противоборства.

В контексте современной геополитической конфронтации, инициированной коллективным Западом во главе с США, деятельность Североатлантического альянса в киберпространстве представляет собой не

просто один из множества вызовов, а системную и многомерную угрозу национальной безопасности Российской Федерации. Данная угроза носит комплексный характер и проявляется в нескольких взаимосвязанных аспектах, включающих прямую военно-стратегическую угрозу, угрозу дестабилизации государственного и общественного строя, угрозу технологического доминирования и нарушения технологического суверенитета, подрыв основ международной безопасности и деструктивная роль в формировании режима регулирования.

Исходной точкой исследования послужила констатация фундаментального парадокса: киберпространство, возникшее как децентрализованная глобальная среда для свободного обмена информацией, трансформировалось в новую стратегическую арену ожесточенного межгосударственного противоборства, где военно-политические блоки, и в первую очередь НАТО, активно наращивают свой наступательный потенциал.

Идентификация ключевых подходов отечественных и зарубежных учёных к определению понятия «киберпространство» создала необходимый теоретико-методологический фундамент для всего последующего диссертационного исследования, позволив анализировать киберпространство как сложный многогранный феномен, требующий междисциплинарного подхода.

Следует отметить, что на современном этапе, принимая во внимание эволюцию подходов отечественных исследователей, киберпространство рассматривается в качестве принципиально нового (в исторических рамках) измерения человеческой жизнедеятельности. Уже не эфемерное, а вполне реальное значение приобретает геополитическое противоборство в киберпространстве и чрезвычайно важным является доктринальное оформление термина «киберпространство» в официальных нормативно-правовых документах.

Отечественные исследователи предлагают детализированный анализ киберпространства с учётом специфики российской информационной среды.

Они подчеркивают важность государственного регулирования и безопасности в условиях цифровой трансформации, что отражает особенности национального дискурса.

Необходимо отметить, что научно-исследовательский анализ киберпространства позволяет установить следующие критерии, применимые к термину: единый характер, отсутствие однозначного географического определения, отрицание линейной структуры и иных физических параметров, глобальное распространение. Киберпространство представляет собой некую совокупность виртуальных систем, физических объектов, программного обеспечения и сервисов, а также аппаратных средств, оно охватывает все без исключения глобальные и локальные компьютерные сети вне зависимости от их принадлежности, отдельных свойств и характеристик, включая Интернет. Отметим неразрывную связь киберпространства со всемирной паутиной, при этом чрезвычайно важным является осознание нетождественности данных понятий. В то время как глобальная паутина является всемирной информационной компьютерной сетью, связывающей между собой как пользователей компьютерных сетей, так и пользователей персональных компьютеров для обмена информацией, определение понятия «киберпространство» в отечественном и зарубежном научном дискурсе является более комплексным и неоднородным.

При этом представляется возможным констатировать, что разнообразие подходов к определению киберпространства, обусловленное теоретическими расхождениями в академической среде, оказывает существенное влияние на международные отношения. Отсутствие консенсуса в трактовке данного понятия приводит к фрагментации правового регулирования, усложняет формирование единых норм кибербезопасности и создает основу для конфликтов в цифровой сфере.

Зарубежные исследователи рассматривают киберпространство как глобальную сетевую структуру, которая трансформирует традиционные формы коммуникации и социальной организации. Эти подходы, характерные

для западной научной традиции, отражают акцент на технологической и социальной динамике.

Разнообразие подходов к определению киберпространства, обусловленное различиями в политических, правовых и технологических приоритетах государств, а также теоретическими расхождениями в академической среде, оказывает существенное влияние на международные отношения. Государства, руководствуясь национальными интересами, по-разному интерпретируют вопросы суверенитета, контроля и применения силы в киберпространстве, что затрудняет достижение международных договоренностей. В свою очередь, международные организации, предлагая альтернативные концепции (от военизированных до гуманитарных), сталкиваются с проблемой согласования позиций, что снижает эффективность глобального управления интернетом. В этих условиях ключевым направлением международного сотрудничества должна стать выработка универсальных, но гибких определений, учитывающих как технологическую специфику киберпространства, так и многообразие политических подходов. Только на основе многостороннего диалога и компромиссных решений возможно минимизировать риски эскалации, обеспечить устойчивость цифровой среды и сформировать инклюзивную систему международной кибербезопасности.

Основываясь на рассматриваемых в исследовании трактовках, представляется возможным предложить авторское определение понятия «киберпространство». Таким образом, 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). Данное пространство характеризуется архитектурной многоуровневостью и наличием множества

разнородных, зачастую антагонистических, систем оперативного и стратегического управления, процесс создания и эксплуатации которых не детерминирован единой управляющей инстанцией.

Проведенное исследование современной стратегии НАТО в киберпространстве позволило сформулировать ряд основополагающих выводов, раскрывающих сущность, эволюцию и специфику подходов Североатлантического альянса в цифровой сфере.

На современном этапе стал очевиден экспоненциальный рост значимости киберпространства в деятельности Североатлантического альянса. С течением времени международное сообщество свидетельствовало эволюцию доктринального оформления подходов военно-политического блока к проблемам обеспечения кибербезопасности, а также стратегии деятельности в киберпространстве. Киберпространство имеет огромное значение для организации и её членов, поскольку современные военные операции и общая безопасность всё более зависят от цифровых технологий. В то же время следует выделить роль ключевого для Североатлантического альянса европейского региона, государства Европейского союза остаются уникальными и важнейшими партнёрами НАТО. В контексте современных геополитических реалий именно Европа является ареной для обкатки нововведений альянса в киберпространстве. Начав своё зарождение в начале 2000-х годов, политика государств-членов НАТО в киберпространстве эволюционировала, планомерно отвечая на новые вызовы и угрозы.

Проведённое исследование эволюции политики НАТО в киберпространстве с конца XX века по настоящее время позволяет выделить три ключевых этапа трансформации подходов военно-политического блока, каждый из которых характеризовался качественным изменением восприятия киберугроз и методов противодействия им.

На первом этапе (конец 1990-х - 2006 гг.) происходило осознание потенциальных рисков киберпространства, что нашло отражение в первых концептуальных документах и создании базовых структур защиты (NCIRC).

Пражский (2002 г.) и Рижский (2006 г.) саммиты Североатлантического альянса заложили институциональные основы киберполитики НАТО, хотя меры носили преимущественно оборонительный и фрагментарный характер.

Второй этап (2007-2014 гг.) был ознаменован реакцией на серию масштабных кибератак, что привело к созданию Киберцентра НАТО в Таллине (2008 г.) и принятию Стратегической концепции НАТО 2010 года. В этот период происходит переход от технического восприятия киберугроз к их осмыслению как элемента гибридных войн и инструмента геополитического противостояния.

Третий этап (2014 г. - н.в.) характеризовался окончательной милитаризацией киберпространства, официально признанного на Варшавском саммите (2016 г.) полноценной областью операций. Разработка концепции многодоменных операций (MDO) и создание Интегрированного центра по киберзащите свидетельствовали о переходе к комплексному восприятию киберпространства как: самостоятельного театра военных действий; критического элемента системы коллективной безопасности; платформы для наступательных операций.

Анализ эволюции подходов НАТО позволяет сделать следующие выводы.

1. Произошла трансформация от технико-оборонительных мер к комплексной военно-политической стратегии;
2. Киберпространство стало неотъемлемым элементом концепции коллективной обороны;
3. Сформировался институциональный каркас кибербезопасности альянса;
4. Сохраняются проблемы атрибуции атак и правового регулирования наступательных операций.

Перспективы дальнейшего развития киберполитики НАТО связаны с необходимостью:

1. совершенствования механизмов коллективного реагирования;

2. разработки чётких критериев применения 5 статьи Североатлантического договора;
3. балансирования между наступательными и оборонительными возможностями;
4. гармонизации национальных и наднациональных подходов.

Таким образом, трансформация стратегии Североатлантического альянса в киберпространстве отражает общую тенденцию милитаризации цифровой среды, что требует постоянной адаптации международно-правовых норм и механизмов поддержания стратегической стабильности в условиях новых технологических вызовов.

Вместе с тем стратегия НАТО сталкивается с системными вызовами, ограничивающими её эффективность. К ним относятся технологические (необходимость постоянной адаптации к скорости появления новых технологий (ИИ, квантовые вычисления)), операционные (проблемы оперативной атрибуции атак, технологическое и ресурсное неравенство между странами-участницами, дефицит квалифицированных кадров) и политико-правовые вызовы (отсутствие универсальных международно-правовых норм, регулирующих применение кибероружия, и противоречия между наднациональным управлением и национальным суверенитетом).

Не менее важным вызовом, с которым сталкивается Североатлантический альянс в контексте формирования коллективной киберполитики – внутренние противоречия государств-членов военно-политического блока. Основной раскол проходит между сторонниками жесткого и сдержанного подходов. Первые, в основном восточноевропейские члены, настаивают на низком пороге применения Статьи 5 к кибератакам, требуя решительного ответа, включая возможности активной кибероборонs и сдерживания. Вторые, преимущественно ряд западноевропейских стран, выступают за более осторожный подход, ссылаясь на трудности атрибуции и риски эскалации, и предпочитая дипломатические и экономические меры. Углубляет разногласия технологическая асимметрия. Несколько государств

(США, Великобритания, Франция) обладают передовыми кибервозможностями, в то время как остальные обладают несопоставимо меньшим потенциалом в данной области, что порождает недоверие в обмене разведданными и вопросах совместного использования инструментов. Таким образом, внутренняя несогласованность в интерпретации правовых норм, уровней эскалации и бремени ответственности продолжает оставаться ключевым вызовом для эффективности коллективной обороны НАТО в киберпространстве.

Центральное место в стратегии НАТО занимает образ России как основного источника угроз, что определяет конфронтационный и оборонительно-сдерживающий характер мер Североатлантического альянса. Российско-натовское киберпротивостояние приобрело системный и взаимный характер, став одним из ключевых дестабилизирующих факторов глобальной кибербезопасности. Перспективы полноформатного сотрудничества в обозримой перспективе остаются минимальными на фоне глубоких геополитических противоречий и взаимного отсутствия доверия, хотя ограниченный диалог в многосторонних форматах (ОБСЕ, ООН) по вопросам нормотворчества и снижения рисков остается возможным.

На основании проведённого анализа места и роли Российской Федерации в современной политике Североатлантического альянса в киберпространстве, а также киберпространства в качестве фактора отношений России и НАТО в условиях новой геополитической напряженности представляется возможным сформулировать ряд ключевых тезисов и рекомендаций для выработки сбалансированного и прагматичного курса России в данной сфере.

В Стратегической концепции НАТО 2022 года Россия обозначена как «наиболее значительная и прямая угроза», что знаменует отказ от риторики диалога и сотрудничества в пользу конфронтационной логики сдерживания. Киберпространство стало центральным театром этого стратегического противоборства, характеризующегося взаимными обвинениями в гибридных

атаках, целенаправленными кампаниями по дискредитации и активным наращиванием наступательного и оборонительного потенциала.

В данных условиях ключевой вызов для российской политики в киберпространстве заключается в необходимости адекватного ответа на наступательную стратегию Североатлантического альянса при одновременном поиске возможностей для деэскалации и создания механизмов управления рисками, что соответствует долгосрочным интересам международной стабильности.

Наиболее перспективными стратегическими приоритетами Российской Федерации в данном контексте могли бы стать следующие элементы.

Во-первых, это безусловное укрепление национального киберсуверенитета и обороноспособности. Целесообразным является продолжение масштабной работы по изоляции и усилению защиты объектов критической информационной инфраструктуры (КИИ). Сдерживание в киберпространстве является составным элементом оборонного потенциала Североатлантического альянса. В связи с чем необходимо продолжать развитие собственных надёжных потенциалов сдерживания, способных гарантировать неприемлемый ущерб любому агрессору. Ускорение импортозамещения в сфере критических информационных технологий, программного обеспечения и микроэлектроники является императивом национальной безопасности в условиях использования Западом технологического доминирования как инструмента давления.

Во-вторых, это последовательная и наступательная работа на дипломатическом фронте. Продвижение Российской Федерацией инициатив по выработке универсальных правовых норм, запрещающих атаки на гражданскую и критическую инфраструктуру, окажет содействие в формировании образа России как ответственного и конструктивного актора. Целесообразным в данном контексте также является более активная инициация процессов по правовой квалификации кибератак на российские

объекты КИИ в качестве преступных и террористических актов, привлечение внимания международных организаций и широкой общественности.

В-третьих, несмотря на то, что взаимодействие России и НАТО в киберпространстве в настоящее время достигло своей нижайшей точки, смена президентской администрации в США в 2025 г. может создать условия для ограниченного диалога в области кибербезопасности. Россия должна быть готова к точечному, прагматичному диалогу по таким вопросам, как: восстановление каналов экстренной связи для предотвращения эскалации на фоне киберинцидентов (аналог «красных телефонов»); обсуждение мер доверия (например, уведомление о крупных киберучениях); координация в борьбе с транснациональной киберпреступностью (неполитизированные угрозы).

Таким образом, политика Российской Федерации в отношении взаимодействия с НАТО в киберпространстве должна базироваться на трезвом понимании текущей конфронтационной реальности и отсутствии иллюзий относительно подлинных целей Североатлантического альянса. Основной путь – это курс на укрепление собственной обороноспособности и суверенитета, сочетаемый с активной наступательной дипломатией, направленной на разоблачение двойных стандартов и продвижение альтернативной, справедливой модели регулирования киберпространства.

Диалог с НАТО не является самоцелью и возможен лишь в строго ограниченных, прагматичных рамках, исключительно по вопросам, представляющим взаимный интерес (снижение рисков прямой конфронтации, борьба с аполитичной преступностью), и только тогда, когда это не наносит ущерба национальной безопасности и международному имиджу Российской Федерации. Сила и независимость остаются главными гарантами безопасности в условиях, когда киберпространство стало новым фронтом гибридного противоборства.

Проведённое исследование позволяет сделать вывод о том, что сложившаяся международная военно-политическая обстановка,

характеризующаяся качественной трансформацией характера угроз и средств противоборства, в особенности в киберпространстве, обуславливает необходимость разработки и принятия новой Военной доктрины Российской Федерации.

Новая Военная доктрина Российской Федерации требуется не как механическая актуализация предыдущих редакций, а как фундаментальный стратегический документ, адекватный вызовам XXI века. Она должна отразить парадигмальный сдвиг в понимании современной войны, где киберпространство является одним из ключевых театров военных действий, а гибридные методы – основной формой противоборства. Её принятие будет означать переход от реагирования на угрозы к их активному прогнозированию и сдерживанию через создание чёткой, легитимной и понятной для всех государственных институтов системы обеспечения национальной безопасности в новых условиях. Это является неотъемлемым условием для сохранения суверенитета и обеспечения стратегической стабильности в условиях формирующегося многополярного мирового порядка.

Таким образом, резюмируя вышесказанное, отметим, что киберпространство представляет собой глобальный, искусственно сконструированный и динамичный социотехнический континуум, возникающий в результате симбиоза технологической инфраструктуры и человеческой деятельности. Его сущность выходит далеко за рамки простой технологической инфраструктуры, превращаясь в принципиально новое измерение человеческой жизнедеятельности, где информация выступает ключевым ресурсом. Это пространство характеризуется архитектурной многоуровневостью, отсутствием однозначных географических и физических параметров, а также наличием множества разнородных и зачастую антагонистических систем управления. Свойства киберпространства производны как от имманентных характеристик его элементов, так и от объема и направленности социальных практик, что обуславливает его двойственную

природу: оно является одновременно средой для экономической, политической и культурной активности и ареной современных конфликтов.

Эволюция подходов Североатлантического альянса к киберпространству демонстрирует отчетливую трансформацию от осознания потенциальных рисков и фрагментарных оборонительных мер к комплексной военно-политической стратегии, где киберпространство окончательно милитаризировано и признано полноправной областью операций. Этот путь, пройденный с конца 1990-х годов по настоящее время, включил три ключевых этапа: институционального становления, стратегического переосмысления в ответ на масштабные кибератаки и окончательной интеграции в концепцию коллективной обороны и многодоменных операций. Данная эволюция отражает общую тенденцию милитаризации цифровой среды, что подчёркивает критическую значимость киберпространства для современной системы международной безопасности. Однако стратегия Североатлантического альянса сталкивается с системными вызовами, ограничивающими ее эффективность. Технологические трудности, связанные с необходимостью адаптации к скорости появления новых технологий, операционные проблемы атрибуции атак и ресурсного неравенства между государствами-членами, а также политико-правовые противоречия, вызванные отсутствием универсальных международных норм и коллизией между наднациональным управлением и национальным суверенитетом, создают значительные барьеры. Центральное место в стратегии НАТО занимает образ России как основного источника угроз, что детерминирует её конфронтационный и оборонительно-сдерживающий характер. Российско-натовское киберпротивостояние приобрело системный и взаимный характер, став ключевым дестабилизирующим фактором глобальной кибербезопасности, что минимизирует перспективы полноформатного сотрудничества в обозримой перспективе.

В более широком контексте разнообразие подходов к определению и регулированию киберпространства, обусловленное теоретическими

расхождениями в академической среде и различиями в политических и правовых приоритетах государств, оказывает глубокое влияние на международные отношения. Отсутствие консенсуса приводит к фрагментации правового регулирования, усложняет формирование единых норм кибербезопасности и создает основу для конфликтов. Таким образом, выработка универсальных, но гибких определений, учитывающих как технологическую специфику, так и многообразие политических подходов, представляется необходимым условием для минимизации рисков эскалации и обеспечения устойчивости цифровой среды. Дальнейшие исследования должны быть направлены на поиск баланса между государственным суверенитетом и глобальной стабильностью, что является основой для гармоничного развития киберпространства в XXI веке.

Список источников и литературы

Список источников

Нормативные правовые акты, официальные документы, доклады

1. 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).
2. Активное участие, современная оборона "Стратегическая Концепция Обороны и Обеспечения Безопасности Членов Организации Североатлантического Договора" Утверждена Главами Государств и Правительств в Лиссабоне URL: https://www.nato.int/cps/en/natohq/official_texts_68580.htm?selectedLocale=ru (дата обращения: 17.10.2022).
3. Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 11-12 июля 2018 года URL: https://www.nato.int/cps/cn/natohq/official_texts_156624.htm?selectedLocale=ru (дата обращения: 17.03.2024).
4. Заявление по итогам встречи на высшем уровне в Варшаве. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Варшаве 8-9 июля 2016 URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=ru (дата обращения: 08.08.2022).
5. Коллективная оборона и статья 5 URL: https://www.nato.int/cps/ru/natohq/topics_110496.htm#:~:text=%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F%205%20%D0%B3%D0%BB%D0%B0%D1%81%D0%B8%D1%82%2C%20%D1%87%D1%82%D0%BE%2C%20%D0%B5%D1%81%D0%BB%D0%B8,%D1%87%D1%82%D0%BE%D0%B1%D1%8B%20%D0%BF%D0%BE%D0%BC%D0%BE%D1%87%D1%

8C%20%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%20%D0%9D%D0%90%D0%A2%D0%9E%2C%20%D0%BF%D0%BE%D0%B4%D0%B2%D0%B5%D1%80%D0%B3%D1%88%D0%B5%D0%B9%D1%81%D1%8F (дата обращения: 08.09.2024).

6. Проект Концепции стратегии кибербезопасности Российской Федерации URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf: (дата обращения: 01.08.2024).
7. Североатлантический договор Вашингтон, Федеральный округ Колумбия, 4 апреля 1949 г. URL: https://www.nato.int/cps/ru/natolive/official_texts_17120.htm (дата обращения: 23.01.2024).
8. Стратегическая концепция НАТО 2022 года https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf (дата обращения: 01.03.2024).
9. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. - 2016. - № 50.- Ст. 7074.
10. Air Force Doctrine Publication 3-13 - Information In Air Force Operations [Electronic Resource] // USAF. 2011. URL: https://nsarchive.gwu.edu/document/27351-united-states-air-force-air-force-doctrine-document-3-13-information-operations-11 (accessed: 15.12.2024)
11. BMVg. (2023). German Cyber Security Strategy.
12. 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).
13. Federal Bureau of Investigation Internet Crime Report 2023 URL: https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf (accessed: 12.08.2025).

14. Höne 2019 – Höne K.E. Mediation and Artificial Intelligence: Notes on the Future of International Conflict Resolution. Geneva: Diplofoundation, 2019. 24 p.
15. ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en обращения: 24.08.2024).
16. NATO (2002). "Prague Summit Declaration". Prague Summit Declaration.
17. NATO (2008). "Cyber Defence Policy". Cyber Defence Policy.
18. NATO (2016). "Warsaw Summit Communiqué". Warsaw Summit Communiqué.
19. NATO (2022). NATO Cyber Defence Policy. Brussels: NATO Headquarters.
20. NATO (2022). Strategic Concept 2022. Brussels: NATO Headquarters.
21. NATO Cyber Defence URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf (дата обращения: 12.03.2025)
22. NATO in the Cyber Age: Strengthening security and defence, stabilising detterence. (2019) / NATO. – Brussels. – 18.04. – 16 p. – Mode of access: https://nato-pa.int/download-file?filename=sites/default/files/2019-04/087_STC_19_E%20-%20NATO.pdf (accessed: 28.01.2020).
23. NATO Review. (2023). AI and Quantum Technologies in Cyber Defence.
24. NATO Review. (2023). The Future of NATO Cyber Defence.
25. NATO will defend itself URL: https://www.nato.int/cps/en/natohq/news_168435.htm (accessed: 12.03.2024)
26. NATO: The Enduring Alliance 2016 URL: http://www.krzysztofmiszczak.pl/files/262649006/lib/FWPN_publication_on_NATO.pdf (дата обращения: 03.02.2022).
27. NATO. (2018). Cyberspace Operations Centre. Retrieved from https://www.nato.int
28. NATO. (2020). NATO 2030: United for a New Era. Retrieved from https://www.nato.int

29. NATO. (2021). NATO's Artificial Intelligence Strategy. Retrieved from https://www.nato.int
30. NATO. (2022). Madrid Summit Declaration.
31. NATO. (2023). Cybersecurity Operations Centre.
32. NATO. (2023). NATO Industry Forum
33. NATO. (2023). Vilnius Summit Communiqué
34. NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf
35. Summary of the NATO Artificial Intelligence Strategy URL: https://www.nato.int/cps/em/natohq/official_texts_187617.htm (accessed: 03.02.2024).
36. The National Strategy to Secure Cyberspace. February 2003 // The White House. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy. pdf (accessed: 16.05.2023).
37. UK Government. (2022). National Cyber Strategy 2022–2030.
38. 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).
39. US National Cybersecurity Strategy 2023.
40. White House. (2023). Budget of the U.S. Government.
41. White House. (2024). National cybersecurity strategy implementation plan

Выступления официальных лиц

42. Конференция «Путешествие в мир искусственного интеллекта» URL: http://kremlin.ru/events/president/news/72811 (дата обращения: 01.08.2024).
43. Матвиенко назвала беспрецедентным вмешательство в выборы в Госдуму URL: https://www.kommersant.ru/doc/4995745 (дата обращения: 13.02.2025).

44. Лавров: США препятствуют в ООН разработке правил поведения в киберпространстве URL: https://tass.ru/politika/5413659/amp (дата обращения: 01.08.2024).
45. Мишустин назвал пять составляющих цифровой архитектуры будущего URL: https://ria.ru/20250131/mishustin-1996581876.html (дата обращения: 01.08.2024).
46. Riga Summit Declaration. URL: https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en (дата обращения: 17.10.2024).

Список литературы

Монографии и материалы конференций на русском и английском языках

47. Араб-Оглы Э. Кибернетика и моделирование социальных процессов // Кибернетика ожидаемая и кибернетика неожиданная / Сост. В.Д. Пекелис. М., 1968. С. 152–153.
48. Картина нарождающегося мира: базовые черты и тенденции: - Москва: Дипломатическая академия МИД России, 2024. – 68 с. с. 37.
49. Кастельс М. Галактика Интернет. Екатеринбург, 2004.
50. 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).
51. 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

52. 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.
53. Мировая политика в фокусе современности: к перспективам выхода из глобального кризиса: монография / отв. ред. М. А. Неймарк; Дипломатическая академия МИД России. — 4-е изд., перераб. и доп. — Москва: Издательско-торговая корпорация «Дашков и К°», 2023. — 509 с.
54. О мегатрендах мирового развития на период до 2035 года и их геополитическое значение: - Москва: Институт перспективных стратегических исследований Национального исследовательского университета «Высшая школа экономики», 2023. – 28 с. с. 23
55. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. – 4-е изд. – М., 1997.
56. Семененко И.С. Политические изменения в современном мире: новые контуры исследовательского поля // Политическая наука перед вызовами глобального и регионального развития / под ред. О. В. Гаман-Голутвиной. М. : Аспект Пресс, 2016. С. 20–37
57. Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation.
58. Bell D.J. // Cyberculture: The Key Concepts. 2001
59. Berners-Lee, T. (1999). "The World Wide Web: A Very Short Personal History"
60. Berners-Lee, T. (2001). "The Semantic Web: A New Form of Web Architecture"
61. Betz D.J., Stevens T. Cyberspace and the State: Toward a Strategy for Cyber-Power.- Taylor & Francis Ltd, 2011, 162p.- P.13.
62. Black and Lynch, “Cyber Threats to NATO from a Multi-Domain Perspective,” 126–30.

63. Castells M. The Rise of the Network Society. — Wiley-Blackwell, 2010. — 656 p.
64. D. Bell, B. Kennedy The Cybercultures Reader (2010)
65. Gady and Stronell, “Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030,” 152
66. Kello, L. (2017). The Virtual Weapon and International Order.
67. Kotler, P. (2019). "Marketing 4.0: Moving from Traditional to Digital"
68. Lash S. Critique of information. L., 2002. P. 15.
69. Lipton J. Rethinking Cyberlaw: A New Vision for Internet Law.-Edward Elgar Publishing, 2015, 176 p.
70. Nye, J. S. (2010). Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School.
71. O'Reilly, T. (2005). "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software"
72. Rheingold, H. (1993). The Virtual Community: Finding Connection in a Computerized World.
73. Schmitt, M. N., & Vihul, L. (2017). The Nature of International Law Cyber Norms.
74. Simon P. The Age of the Platform (2015)
75. Singer P. Wired for War: The Robotics Revolution and Conflict in the 21st Century (2009)
76. Soja E. Postmetropolis. Critical studies of cities and regions. Malden, 2000. P. 333.

Статьи на русском и английском языках

77. 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.
78. 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.

79. 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).
80. 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.
81. 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.
82. 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).
83. 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
84. 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).

85. Бондаренко, С.В. (2002). Социальная система киберпространства. Парадигмы и процессы как новая социальная общность. Научная мысль Кавказа. Приложение, 12(38).
86. 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.
87. Брент Л. Роль НАТО в кибернетическом пространстве // Вестник НАТО. – Брюссель, 2019. – 12.02. – URL: https://www. nato.int/ docu/review/ru/articles/2019/02/12/rol-nato-v-kiberneticheskom-prostranstve/index.html (дата обращения – 28.01.2024).
88. 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).
89. Войскунский А.Е. Метафоры интернета // Вопросы философии. 2001. № 11. С. 64–79.
90. 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).
91. 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.
92. 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.

93. 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).
94. 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).
95. 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.
96. 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.
97. Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского Университета. Сер. 18. Социология и политология. 2018. Т. 24. № 1. С. 52—70.
98. Иванов О.П. Американский взгляд на стратегическое соперничество и роль военной силы // Обозреватель-Observer. 2024; (2). С 27–36.
99. 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.
100. 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.

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

102. 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).

103. 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.

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

105. 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).

106. 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.

107. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сете-центрических войнах начала XXI века. / СПб.: Наукоемкие технологии, 2017. 237 с.

108. 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).

109. 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.
110. 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.
111. 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.
112. 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).
113. 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).
114. 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.
115. 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.
116. Панарин И. Н. Гладиаторы гибридной войны // Экономические стратегии. 2016. № 2. С. 60–65.

117. 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.

118. Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны. – URSS, 2010.

119. 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.

120. 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).

121. 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).

122. 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).

123. 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).

124. 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).

125. 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).

126. 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.

127. 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.

128. 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.

129. 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).

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

131. 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).

132. 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.

133. 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.

134. 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).

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

136. 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 – 28.01.2020)

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

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

139. Galeotti, M. (2016). Hybrid War or Gibridnaya Voina? Small Wars Journal.

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

141. Gibson W. Neuromancer. N.Y., 1984.

142. 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

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

144. Lyon, D. (2015). Surveillance after Snowden. Polity Press.

145. 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

146. Oxford dictionary of English. Oxford, 2010

147. 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.

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

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

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

Диссертации на русском и английском языках

151. Кончаковский, Р.В. (2010). Сетевое интернет-сообщество как социокультурный феномен. [Автореф. дис. … канд. социол. наук. Урал. гос. ун-т им. А.М. Горького]. Электронный научный архив УрФУ. https://elar.urfu.ru/ handle/10995/3102

Электронные ресурсы на русском и английском языках

152. В НАТО выступили за активное развитие программ искусственного интеллекта https://russian.rt.com/world/news/610689-nato-razvitie-programm-intellekt (дата обращения: 05.01.2025).

153. В НАТО допустили применение пятой статьи договора в случае кибератаки URL: https://lenta.ru/news/2024/06/01/v-nato-dopustili-primenenie-pyatoy-stati-dogovora-v-sluchae-kiberataki/ (дата обращения: 05.07.2024).

154. В Таллине начал работу центр киберзащиты НАТО. URL: https://www.securitylab.ru/news/353773.php (дата обращения: 17.10.2022).

155. Глава АНБ назвал Россию самой опасной страной в киберпространстве URL: https://www.cnews.ru/news/top/2016-04-07_glava_anb_nazval_rossiyu_glavnoj_ugrozoj_v_kiberprostranstve (дата обращения: 14.02.2025).

156. Замглавы МИД РФ: США тренируют украинскую "IT-армию" URL: https://tass.ru/interviews/16906301 (дата обращения: 05.01.2025).

157. Злонамеренные дезинформационные кампании - дестабилизирующий фактор поддержания международной информационной безопасности URL: https://interaffairs.ru/jauthor/material/2745 (дата обращения: 05.09.2024).

158. Искусственный интеллект в НАТО: динамичное внедрение, ответственное использование URL:

https://www.nato.int/docu/review/ru/articles/2020/11/24/iskusstvennyj-intellekt-v-nato-dinamichnoe-vnedrenie-otvetstvennoe-ispol-zovanie/index.html (дата обращения: 20.03.2024).

159. Киберпространство как стратегический инструмент социальной инженерии URL: https://whatisgood.ru/theory/analytics/kiberprostranstvo-kak-strategicheskiy-instrument/ (дата обращения: 15.04.2023).

160. НАТО приняла стратегию против гибридных войн. 02.12.2015 [Электронный ресурс]. URL: https://newsland.com/user/4296735949/content/nato-priniala-strategiiu-protiv-quotgibridnykh-voinquot/4854888 (дата обращения: 03.03.2025)

161. Ответ специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности МИД России А.В. Крутских на вопрос СМИ об атаках на объекты российской критической инфраструктуры URL: https://mid.ru/ru/foreign_policy/news/1817019/#sel=6:1:0Sj,6:70:Taj (дата обращения: 23.08.2024).

162. При голосовании по конституции в РФ фиксировали DDoS-атаки из США, Великобритании, Украины URL: https://tass.ru/politika/9391631 (дата обращения: 07.02.2025).

163. Роль НАТО в кибернетическом пространстве URL: https://www.nato.int/docu/review/ru/articles/2019/02/12/rol-nato-v-kiberneticheskom-prostranstve/index.html (дата обращения: 17.03.2024).

164. РФ с начала года сделала 35 запросов США о происхождении кибератак URL: https://iz.ru/1201625/2021-08-02/rf-s-nachala-goda-sdelala-35-zaprosov-ssha-o-proiskhozhdenii-kiberatak (дата обращения: 03.07.2023).

165. Сотрудничество ЕС–НАТО: Совет ЕС принял выводы по реализации Совместной декларации URL: https://www.eeas.europa.eu/node/16866_en (дата обращения: 29.01.2024).

166. Технологический уклад // Большая российская энциклопедия: научно-образовательный портал – URL: https://bigenc.ru/c/tekhnologicheskii-uklad-f21f29/?v=6124666. – (дата обращения: 27.01.2025).

167. Эксперт: саммит в Женеве дает надежду на заключение США и РФ договоренностей в киберсфере URL: https://tass.ru/mezhdunarodnaya-panorama/11672185 (дата обращения: 07.02.2025).

168. As Trump warms to Putin, U.S. halts offensive cyber operations against Moscow URL: https://www.washingtonpost.com/national-security/2025/03/01/trump-putin-russia-cyber-offense-cisa/ (accessed: 01.04.2025).

169. Countering Hybrid Warfare Project: Understanding Hybrid Warfare.28.09.2017. [Электронный ресурс]. URL: https://www.gov.uk/government/ publications/countering-hybrid-warfare-project-understanding-hybrid-warfare#history (дата обращения: 05.03.2025).

170. Cyber Coalition helps prepare NATO for today's threats. (2018) / NATO. – Brussels. – 27.11. – URL: https://www.nato.int/cps/ru/natohq/ news_160898.htm?selectedLocale=en (accessed: – 28.01.2023).

171. Cyber defence NATO. URL: https:// www.nato.int/cps /en/natohq/topics_78170. htm (дата обращения: 23.02.2022).

172. Cybercrime Damages To Cost The World $8 Trillion USD in 2023 URL: https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023 (accessed: 01.02.2024).

173. ENISA. (2021). Cybersecurity Information Sharing Partnerships. Retrieved from https://www.enisa.europa.eu

174. Internet Assigned Numbers Authority. [Электронный ресурс]: https://www.iana.org/ (accessed:: 03.01.2025).

175. Military Balance 2015. International Institute for Strategic Studies [Электронный ресурс]. URL: https://www.iiss.org/publications/the-militarybalance/the-military-balance-2015 (accessed: 03.03.2025).

176. Open-ended Working Group URL: https://disarmament.unoda.org/open-ended-working-group/ (дата обращения: 05.08.2024).

177. Paris Call for Trust and Security in Cyberspace. (2018). Retrieved from https://pariscall.international

178. Rand Corporation. (2023). Future of NATO Cyber Defence.

179. Shacklett M.E., Novotny A., Gerwig K. TCP/IP//. [Электронный ресурс]: https://www.techtarget.com/searchnetworking/definition/TCP-IP (accessed: 03.01.2025).

180. Trident Juncture 18: Media resources. (2018) / NATO. – Brussels. – 31.10. – Mode of access: https://www.nato.int/cps/en/natohq/news_158620.htm?selectedLocale=en (accessed: – 28.01.2020).

181. Trump appears to confirm cyberattack against Russian entity during midterms URL: https://edition.cnn.com/2019/05/19/politics/trump-confirm-cyberattack-russia-midterms/index.html (дата обращения: 23.08.2024).

182. Trump confirms, in an interview, a U.S. cyberattack on Russia URL: https://www.washingtonpost.com/opinions/2020/07/10/trump-confirms-an-interview-us-cyberattack-russia/ (дата обращения: 23.08.2024).

183. Understanding Cyber Effects in Modern Warfare URL: https://warontherocks.com/2025/01/understanding-cyber-effects-in-modern-warfare/?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru (accessed: 08.03.2025).

184. White House: U.S. engaged in ongoing talks with Russia about ransomware, other cyberattacks URL: https://www.ny1.com/nyc/all-boroughs/politics/2021/07/06/white-house--u-s--engaged-in-ongoing-talks-with-russia-about-ransomware--other-cyberattacks (accessed: 08.03.2025).

185. World Wide Web Foundation. History of the Web. [Электронный ресурс]: https://webfoundation.org/about/vision/history-of-the-web/ (accessed: 03.01.2025).

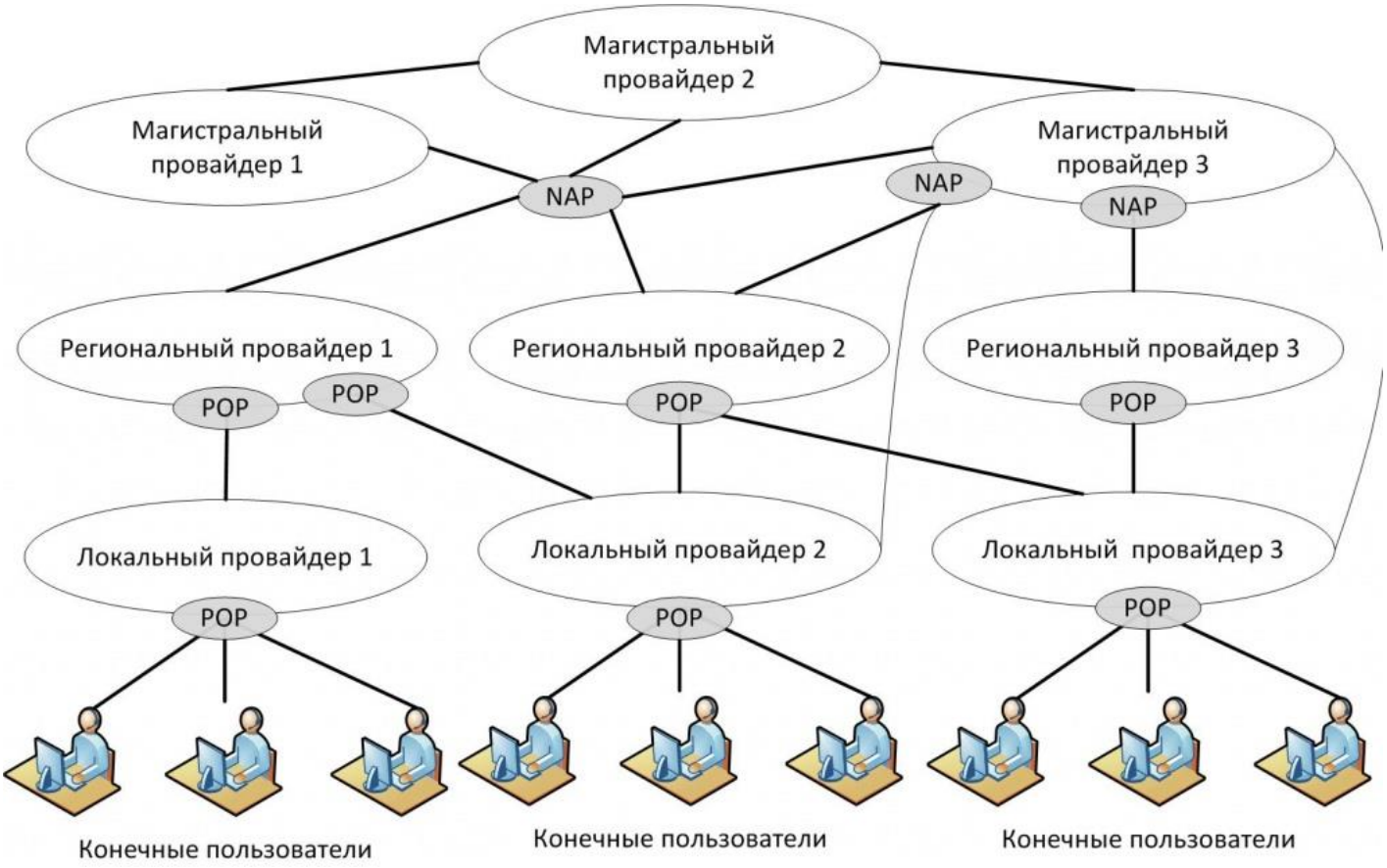
Приложения

Приложение А

Государства-члены НАТО

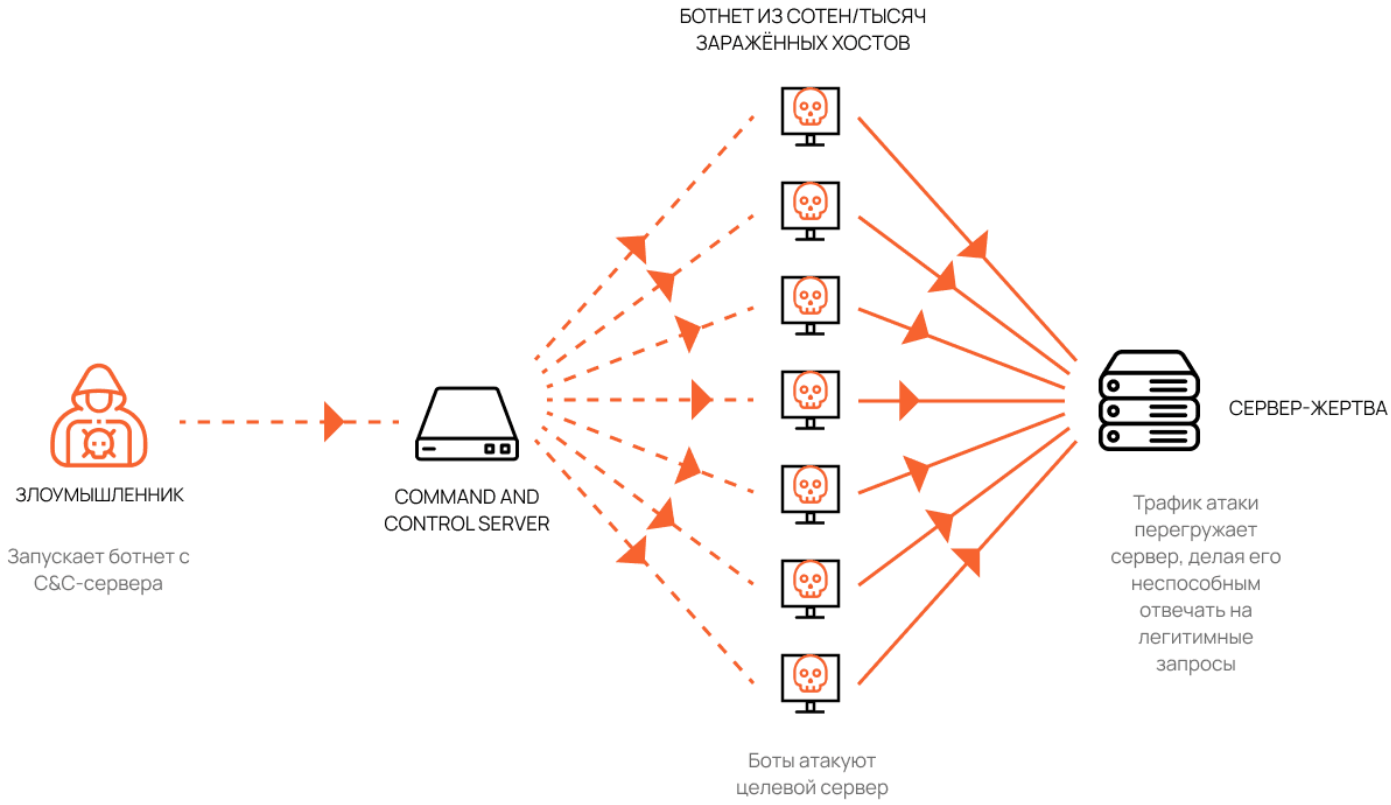
Приложение Б

Адресация в сети Интернет



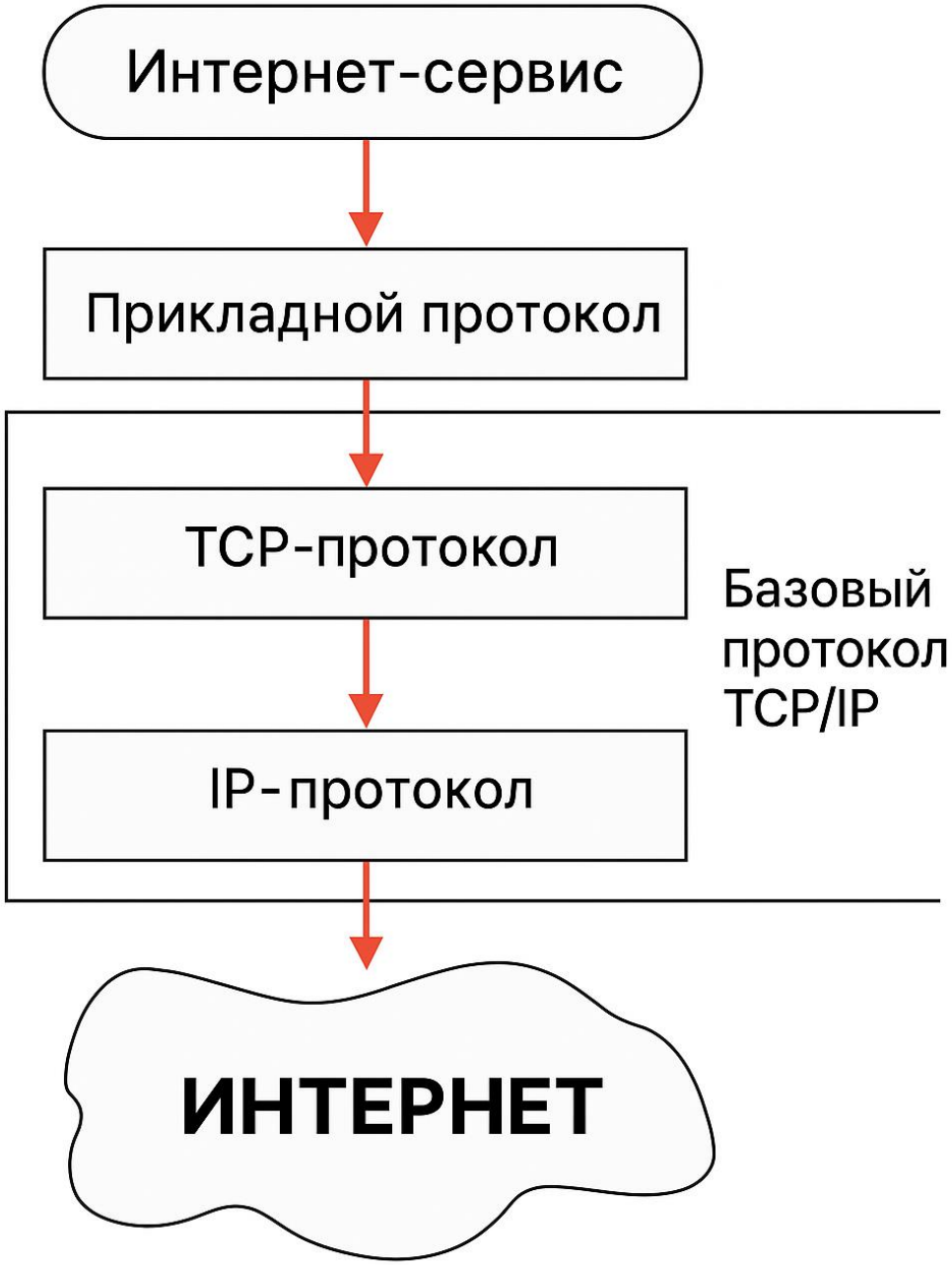
Приложение В

DDoS-атака



Приложение Г

Система протоколов Интернета



Приложение Д

Web 1.0, Web 2.0, Web 3.0