DOI: https://doi.org/10.24833/0869-0049-2025-1-125-137

Исследовательская статья
УДК: 341.6
Поступила в редакцию: 14.11.2024
Принята к публикации: 25.02.2025

Константин Константинович ЛАЗАРЬ
Дипломатическая академия МИД России
Остоженка ул., д. 53/2, стр. 1, г. Москва, 119021, Российская Федерация
lazariconstantin@yandex.ru
ORCID: 0009-0008-4763-1922

КИБЕРБЕЗОПАСНОСТЬ И СУВЕРЕНИТЕТ В КИБЕРПРОСТРАНСТВЕ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ МЕЖДУНАРОДНОГО ПРАВА

ВВЕДЕНИЕ. *Статья посвящена анализу концепции «киберсуверенитета» как совокупности юридических претензий и механизмов, посредством которых государства стремятся обеспечить контроль и защиту своих интересов в цифровой сфере. На фоне стремительного развития информационно-коммуникационных технологий, транснационального характера киберпространства и отсутствия единых международных норм усиливаются дискуссии о применимости классического понятия государственного суверенитета к цифровой среде. Рассматриваются различные подходы государств (Россия, Китай, США, страны Европейского союза (далее – ЕС) и др.) к регулированию киберпространства, подчеркивается рост значения кибербезопасности в международном праве, анализируется роль международных организаций (включая Организацию Объединенных Нация (далее – ООН)) и ключевых документов, таких как «Таллиннское руководство 2.0».*

МАТЕРИАЛЫ И МЕТОДЫ. *Исследование основано на качественном анализе научной литературы, международно-правовых актов (Устав ООН, решения Международного суда ООН, доктринальные документы), национальных стратегий в области кибербезопасности (России, США, Китая и др.), а также сравнительном изучении практик и позиций государств в сфере киберсуверенитета. Использовались общенаучные и частнонаучные методы познания: анализ и синтез, системный и сравнительно-правовой подход, позволяющие выявить правовые пробелы и противоречия в регулировании цифровой среды.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *Проведенный анализ показывает, что государства все более стремятся проецировать классический суверенитет на киберпространство, развивая национальное законодательство и формируя самостоятельные киберюрисдикции. Эта тенденция отражается в стратегиях и доктринах ряда стран (Китай, Россия), которые пытаются обеспечить контроль над своим сегментом интернета. Одновременно сохраняется противоречие между государствами, выступающими за открытость и свободное функционирование сети (США, страны ЕС), и теми, кто считает приоритетным укрепление национального контроля в цифровой сфере. Выявлено, что на практике государствам трудно достичь единого понимания границ допустимого вмешательства и масштабов правомерного применения принципа невмешательства и суверенитета в кибероперациях.*

ОБСУЖДЕНИЯ И ВЫВОДЫ. *Анализ свидетельствует о правовой неопределенности в определении кибероперациий, нарушающих суверенитет, а также в квалификации кибершпионажа и кибератак низкой интенсивности. В рамках ООН и специальных групп экспертов (GGE, OEWG) ведется работа по согласованию*

подходов, однако единый универсальный механизм пока не выработан. Наиболее острые противоречия касаются признания суверенитета в цифровой сфере как самостоятельной нормы международного права и установления четких критериев допустимости кибероперацій. Для преодоления правовых пробелов и снижения риска конфликтов необходимо формировать универсальные принципы, учитывающие специфику киберпространства, а также углублять международное сотрудничество, в том числе в области обмена информацией и выработки механизмов быстрого реагирования на киберугрозы.

КЛЮЧЕВЫЕ СЛОВА: *киберсуверенитет, международное право, кибербезопасность, киберпространство, кибершпионаж, суверенитет, информационная безопасность, ООН, национальные стратегии*

ДЛЯ ЦИТИРОВАНИЯ: Лазарь К.К. 2025. Кибербезопасность и суверенитет в киберпространстве: вызовы и перспективы международного права. – *Московский журнал международного права.* № 1. С. 125–137. DOI: https://doi.org/10.24833/0869-0049-2025-1-125-137

Автор заявляет об отсутствии конфликта интересов.

DOI: https://doi.org/10.24833/0869-0049-2025-1-125-137

Research article
UDC: 341.6
Received 11 November 2024
Approved 25 February 2025

Constantin C. LAZARI
Federal State Educational Public Institution of Higher Education
"Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation"
53/2, bld. 1, Ostozhenka St., Moscow, Russian Federation, 119021
lazariconstantin@yandex.ru
ORCID: 0009-0008-4763-1922

CYBERSECURITY AND SOVEREIGNTY IN CYBERSPACE: CHALLENGES AND PROSPECTS OF INTERNATIONAL LAW

INTRODUCTION. *This article explores the concept of "cyber sovereignty", understood as the set of legal claims and mechanisms through which states seek to control and protect their interests in the digital domain. Amid the rapid development of information and communication technologies, the transnational nature of cyberspace, and the lack of unified international norms, debates on the applicability of classical state sovereignty to the digital realm are intensifying. The paper examines various approaches taken by different countries (Russia, China, the United States, EU member states, etc.) in regulating cyberspace, highlighting the growing importance of cybersecurity in international law, and analyzing the role of international organizations (including the UN) and key documents such as the Tallinn Manual 2.0.*

MATERIALS AND METHODS. *The study is based on a qualitative analysis of academic literature, international legal instruments (UN Charter, International Court of Justice rulings, doctrinal documents), national cybersecurity strategies (Russia, the USA, China, among others), and a comparative examination of state practices and positions regarding cyber sovereignty. General and specific scientific methods – analysis and synthesis, systematic and comparative-legal approaches – were employed to identify legal gaps and contradictions in the regulation of the digital environment.*

RESULTS. *The analysis shows that states increasingly aim to extend the concept of classical sovereignty to cyberspace by developing national legislation and creating independent cyber jurisdictions. This trend is reflected in the strategies and doctrines of several countries (China, Russia), which seek to control their segment of the internet. At the same time, a rift remains between states that advocate for an open and free internet (the USA, EU states) and those that prioritize strengthening national control over the digital sphere. In practice, it is difficult for states to reach consensus on the permissible scope of intervention and the application of the principles of non-intervention and sovereignty in cyber operations.*

DISCUSSION AND CONCLUSIONS. *The analysis reveals legal uncertainty in defining what kinds of cyber operations violate sovereignty, as well as in the categorization of cyber espionage and low intensity cyberattacks. The UN and its specialized expert groups (GGE, OEWG) are working on harmonizing approaches; however, no single universal mechanism has yet been established. The most acute controversies concern recognizing sovereignty in the digital sphere as a distinct norm of international law and establishing clear criteria for legitimate cyber operations. Overcoming legal gaps and reducing the risk of conflict require the development of universal principles that account for the unique characteristics of cyberspace, as well as the deepening of international cooperation, including the exchange of information and the creation of rapid response mechanisms to cyber threats.*

KEYWORDS: *cyber sovereignty, international law, cybersecurity, cyberspace, cyber espionage, sovereignty, information security, United Nations, national strategies*

FOR CITATION: Lazari C.C. Cybersecurity and Sovereignty in Cyberspace: Challenges and Prospects of International Law. – *Moscow Journal of International Law.* 2025. No. 1. P. 125–137. DOI: https://doi.org/10.24833/0869-0049-2025-1-125-137

The author declares the absence of conflict of interest.

Введение

Стремительное развитие информационно-коммуникационных технологий за последние десятилетия привело к возникновению нового пространства взаимодействия – киберпространства. Эта виртуальная среда стала неотъемлемой частью современной жизни, оказывая значительное влияние на экономику, политику, культуру и повседневное общение. В российской научной традиции ему нередко соответствует более широкое понятие «информационное пространство», включающее не только технологическую инфраструктуру, но и социально-правовые отношения. В настоящей статье мы будем использовать термин «киберпространство», поскольку он закреплен в ключевых международных источниках, таких как «Таллиннское руководство 2.0»[1] и доклады ООН[2]. Однако это не означает, что мы ограничиваем его исключительно технологическим аспектом. Напротив, мы признаем, что киберпространство включает в себя и социальные компоненты, связанные с обменом информацией и взаимодействием людей, но, следуя принятой международной терминологии, придерживаемся данного обозначения.

Различия в терминологии могут влиять на дискуссии о том, в какой мере государство способно (и должно ли) осуществлять свою власть и защиту национальных интересов в цифровой среде. В то же время цифровая эра несет не только преимущества, но и серьезные вызовы, связанные с обеспечением безопасности и регулированием отношений в киберпространстве.

Один из центральных вопросов, стоящих перед международным сообществом, – применимость традиционного понятия государственного суверенитета к киберпространству. В классическом понимании суверенитет государства основан на территориальных границах и контроле над населением и ресурсами. Однако

[1] Руководство Таллинн 2.0 по международному праву, применимому к кибероперациям. Cambridge University Press, 2017. 562 с.

[2] ООН: Имеется в виду Доклад группы правительственных экспертов ООН **A/68/98 (2013)**, Доклад группы правительственных экспертов ООН **A/70/174 (2015)**, а также Итоговый доклад Рабочей группы открытого состава ООН **(2021)**.

киберпространство по своей природе транснационально, не ограничено физическими рубежами, что затрудняет применение существующих норм международного права к его регулированию и требует новых подходов.

В данной работе под «киберсуверенитетом» понимается совокупность юридических претензий и механизмов, посредством которых государство стремится обеспечить контроль и защиту своих интересов в цифровой сфере. Такие механизмы включают национальное регулирование интернет-инфраструктуры, законы об обработке данных и кибербезопасности. Некоторые исследователи, в том числе российские и китайские, используют термин «информационный суверенитет», акцентируя внимание на более широком понимании информационного пространства [Данельян 2020*a*][3]. Однако, учитывая специфику международных дискуссий, в статье сохраняется термин «киберсуверенитет», так как он чаще фигурирует в глобальном контексте (ООН, Таллиннское руководство, западная научная литература).

Отсутствие единых международных норм и различие подходов к киберсуверенитету среди государств создают правовые пробелы, осложняющие эффективное регулирование киберпространства. Одни страны (Россия, Китай) настаивают на расширении понятия суверенитета на цифровую сферу, стремясь установить контроль над национальными сегментами интернета и защитить критически важные информационные ресурсы. Другие (США, страны ЕС) выступают за сохранение открытого и свободного киберпространства, опасаясь, что усиление государственного контроля приведет к ограничению свобод и нарушению прав человека.

Актуальность темы обусловлена не только теоретическими противоречиями, но и практическими вызовами. Киберугрозы все чаще затрагивают критическую инфраструктуру, финансовые системы и национальную безопасность [Горелик 2021*a*:32]. Отсутствие единых подходов порождает неопределенность:

– что считать нарушением суверенитета в случае кибератаки?

– где проходит грань между легитимным сбором разведданных и недопустимым кибершпионажем?

– каковы критерии допустимого государственного вмешательства в цифровую сферу других стран?

Пробелы в правовом регулировании становятся причиной конфликтов и взаимных обвинений, особенно если одно государство не признает за другим права на вмешательство в его сети.

Цель данной статьи – анализ современных подходов к киберсуверенитету, изучение позиций государств и международных организаций, а также оценка перспектив международно-правового регулирования киберпространства. Особое внимание уделяется адаптации классических принципов суверенитета к цифровой реальности и выявлению шагов, необходимых для формирования эффективных механизмов регулирования.

Методологически исследование основано на качественном анализе, включающем доктринальный подход и сравнительное изучение международных практик. В работе рассматриваются:

– ключевые международно-правовые документы (включая Устав ООН и решения Международного суда ООН[4]);

– стратегии ведущих государств (Россия, США, Китай) в сфере кибербезопасности[5];

– роль международных организаций в преодолении правовых пробелов и формировании новых норм.

Таким образом, данная статья стремится проанализировать существующие концепции киберсуверенитета, выявить ключевые противоречия и предложить возможные пути адаптации международного права к вызовам цифровой эпохи.

[3] Министерство иностранных дел Китайской Народной Республики: Международная стратегия сотрудничества в киберпространстве (март 2017 г.)

[4] МС ООН: Решения по делам «Военные и паравоенные действия в Никарагуа и против нее (1986)», «Дело пролива Корфу (1949)», «С.С. Лотус (Франция против Турции) (1927)», «Дело о ядерных испытаниях (1974)» и др.

[5] См., напр., Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 5 декабря 2016 г. № 646; Международная стратегия сотрудничества в киберпространстве (март 2017 г.); Международная стратегия киберпространства. Белый дом США (май 2011 г.); Закон CLOUD (Clarifying Lawful Overseas Use of Data Act, 2018 г.); Руководство по ведению войны (июнь 2015 г.).

1. Кибербезопасность и рост значения киберсуверенитета

В научной литературе существует множество определений киберпространства. Например, Д.Е. Добринская отмечает, что «киберпространство – это особый тип пространства, возникающий в результате развития информационно-коммуникационных технологий» [Добринская 2018:59]. В другом исследовании М.В. Мигулева киберпространство определяется как «всемирная система в информационной среде, состоящая из взаимозависимой сети информационно-коммуникационных инфраструктур, включая интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры» [Мигулева 2018:43].

В рамках данного исследования под киберпространством понимается глобальная система взаимосвязанных информационных технологий, обеспечивающих обмен данными и коммуникацию между людьми по всему миру. Однако ключевой вопрос, связанный с его правовым статусом и регулированием в международном праве, остается открытым, что порождает многочисленные дискуссии среди ученых и практиков [Mueller 2010:100]. При этом некоторые исследователи отмечают, что неоднородность киберпространства осложняет формирование универсальных норм, поскольку оно выходит за классические государственные границы [Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, Spiegel 2012:820].

Первоначально киберпространство рассматривалось как общее достояние человечества (*res communis omnium*), аналогично открытому морю или космосу. Такой подход исключал возможность его присвоения отдельными государствами и предполагал, что управление киберпространством должно осуществляться на основе международных соглашений и коллективного регулирования [Данельян 2020б:263].

В частности, Д.Р. Джонсон и Д.Г. Пост утверждали, что киберпространство выходит за рамки территориальных границ и должно регулироваться через многосторонние механизмы, а не отдельными государствами [Johnson, Post 1996:1390]. Эта концепция основывалась на децентрализованной природе киберпространства, технологической архитектуре интернета и сложности применения к нему традиционных механизмов территориального контроля.

Однако данное представление оказалось недостаточным для описания реальной структуры управления киберпространством. В отличие от Договора об Антарктике (1959) или Договора о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела (1967), известного как Договор о космосе, которые регулируют использование пространств общего пользования, киберпространство не подпадает под действие единого международного соглашения, что создает правовой вакуум и затрудняет разработку универсальных норм регулирования цифровой сферы.

Со временем идея киберпространства как *res communis* стала подвергаться критике. На практике его управление оказалось сконцентрированным в руках отдельных структур. Ключевые организации, определяющие технические и административные аспекты интернета, такие как ICANN (Internet Corporation for Assigned Names and Numbers) и Internet Society, зарегистрированы в Соединенных Штатах [Mueller 2010:110]. Это вызвало озабоченность со стороны ряда государств по поводу концентрации контроля над интернетом в пределах юрисдикции одной страны и возможного влияния Вашингтона на глобальные процессы.

На фоне этих процессов возникли разногласия по поводу модели управления киберпространством. Некоторые страны (например, США, Германия, Великобритания) выступают за многосторонний (multistakeholder) подход, включающий участие не только государств, но и частного сектора, гражданского общества и технического сообщества. Другие (например, Россия, Китай) настаивают на межправительственной модели, где ключевую роль играют государства, аргументируя это необходимостью защиты национальных интересов и обеспечения безопасности [Данельян 2020б:266].

Таким образом, осознание концентрации власти в киберпространстве привело к переосмыслению подходов и послужило катализатором перехода к концепции киберсуверенитета.

В ответ на дискуссии о власти в киберпространстве возникло требование его суверенизации. Это повлекло за собой адаптацию традиционной концепции государственного суверенитета (закрепленной в Вестфальской системе международных отношений) к цифровой сфере [Kello 2017].

Принцип государственного суверенитета традиционно подразумевает полный контроль государства над своей территорией, населением и ресурсами, что зафиксировано в Конвенции о правах и обязанностях государств (Конвенция Монтивидео, 1933) и Уставе ООН (1945). Однако киберпространство не имеет физических границ – информация может перемещаться в режиме реального времени, что ставит под сомнение применимость классических принципов [Schmitt 2009:435].

На практике переход от идеализированной модели открытого интернета к концепции киберсуверенитета проявился в изменении стратегий регулирования цифрового пространства различными государствами.

Китай в «Стратегии международного сотрудничества в киберпространстве 2017 г.»[6] закрепил принцип «информационного суверенитета», подчеркивая право государства контролировать национальный сегмент интернета. Китайская позиция основывается на том, что каждое государство имеет право самостоятельно определять политику в области кибербезопасности, регулировать интернет на своей территории и защищать свои национальные интересы в цифровой сфере. Китай выделяет четыре основных принципа: мир, суверенитет, совместное управление и общий прогресс.

Россия также активно продвигает идею киберсуверенитета. В «Доктрине информационной безопасности Российской Федерации»[7] 2016 г. подчеркивается важность обеспечения национального суверенитета в информационном пространстве и развития независимой национальной информационной инфраструктуры.

Более того, если в «Международной стратегии киберпространства»[8] США опубликованной в 2011 г., основной акцент делался на свободе информации, защите частной жизни и гражданских правах, при этом суверенитет как концепция не играл ключевой роли, то с усилением геополитической конкуренции и ростом киберугроз США отошли от принципа открытого интернета в пользу расширения национального контроля.

Этот переход зафиксирован в «Облачном акте» CLOUD Act (2018)[9], который расширил юрисдикцию США на данные, хранящиеся за пределами страны, фактически распространив американское законодательство на трансграничные цифровые потоки. В результате Вашингтон перешел к модели контроля над цифровыми ресурсами, утверждая национальный приоритет над данными независимо от их местоположения.

Таким образом, тенденция к национализации киберпространства становится глобальной, отражая отход от концепции единого цифрового пространства в пользу фрагментированной сети цифровых юрисдикций. Однако возникает вопрос: каким образом принцип территориального суверенитета может быть адаптирован к киберпространству и какие правовые механизмы необходимы для его реализации?

2. Применение принципа территориального суверенитета в киберпространстве

В международном праве суверенитет государства традиционно имеет два измерения: внутреннее и внешнее. Внутренний суверенитет подразумевает исключительную власть государства над своей территорией и населением, включая право устанавливать законы и регулировать внутренние дела без вмешательства извне. Внешний суверенитет связан с независимостью государства в международных отношениях и его правом свободно взаимодействовать с другими государствами при соблюдении международного права.

В контексте киберпространства внутренний суверенитет означает право государства контролировать и регулировать киберинфраструктуру на своей территории, а также деятельность, связанную с киберпространством, осуществляемую физическими и юридическими лицами под его юрисдикцией. Внешний суверенитет отражается в способности государства защищать свои интересы в киберпространстве на международной арене, участвовать в разработке международных норм и сотрудничать с другими государствами в области кибербезопасности.

---

[6] Министерство иностранных дел Китайской Народной Республики: Международная стратегия сотрудничества в киберпространстве.

[7] Доктрина информационной безопасности Российской Федерации.

[8] США. Белый дом: Международная стратегия киберпространства (май 2011 г.).

[9] Закон CLOUD (Clarifying Lawful Overseas Use of Data Act) (2018).

Определение того, какие действия в киберпространстве могут считаться нарушением территориального суверенитета, остается предметом дискуссий. Традиционно нарушение суверенитета ассоциируется с физическим вторжением на территорию другого государства без его согласия, как это было определено в решениях Международного суда ООН по делам «Никарагуа против США»[10], «О проливе Корфу»[11] и С.С. Лотус (Франция против Турции)[12].

Однако в киберпространстве физическое присутствие не всегда необходимо для причинения ущерба. Кибератаки могут осуществляться удаленно, при этом их последствия могут быть сопоставимы с традиционными вооруженными действиями. Некоторые исследователи предлагают рассматривать несанкционированные кибероперации, приводящие к значительному ущербу, как нарушение суверенитета [Данельян 2020б:265]. Одновременно указывается, что отсутствие универсальных критериев затрудняет единообразие правоприменения [Lin 2016:78].

Несмотря на отсутствие всеобъемлющих международных норм, государства начинают формировать свою практику и позиции по этому вопросу. Франция в своем документе «Международное право, применимое к операциям в киберпространстве»[13] заявляет, что несанкционированные кибероперации, нарушающие функционирование ее информационных систем, могут рассматриваться как нарушение суверенитета.

Нидерланды, ссылаясь на «Таллиннское руководство 2.0», также признают, что кибероперации, причиняющие значительный ущерб или затрагивающие критическую инфраструктуру, могут представлять собой нарушение суверенитета[14]. Такие позиции отражают стремление государств установить определенные границы допустимого поведения в киберпространстве и защитить свои национальные интересы.

3. Дебаты о суверенитете: принцип или норма?

В международном праве суверенитет традиционно рассматривается как фундаментальный принцип, на котором основываются отношения между государствами. Однако возникает вопрос: является ли суверенитет самостоятельной юридически обязательной нормой или же он служит общим принципом, из которого вытекают конкретные правовые нормы?

Этот вопрос приобретает особую значимость в контексте киберпространства, где традиционные границы и механизмы регулирования часто не работают. От ответа на него зависит, какие действия в киберпространстве могут считаться нарушением международного права и какие меры могут предприниматься государствами для защиты своих интересов [Moynihan 2019:5].

Генеральный прокурор Великобритании Дж. Райт в 2018 г. отметил, что хотя суверенитет является фундаментальным принципом международного права, трудно выделить конкретную норму, запрещающую любые формы кибердеятельности на территории другого государства без его согласия, за исключением случаев, когда такая деятельность приводит к значительному ущербу или нарушает другие международные обязательства[15].

Министерство обороны Великобритании в 2020 г. также заявило, что в настоящее время нет достаточно распространенной и последовательной практики государств, свидетельствующей о существовании нормы обычного

[10] МС ООН: Военные и паравоенные действия в Никарагуа и против нее (Никарагуа против США) (1986). Суд признал противоправным вмешательство государства во внутренние дела и подрыв независимости другого. По аналогии, кибератаки, направленные на дестабилизацию, могут трактоваться как незаконное вмешательство.

[11] МС ООН: Дело пролива Корфу (Великобритания против Албании) (1949). Государство обязано не допускать, чтобы с его территории осуществлялись действия, наносящие ущерб другому государству. Это может быть экстраполировано на кибератаки или киберпреступную деятельность, исходящую из национальной инфраструктуры.

[12] Постоянная палата международного правосудия: Дело С.С. Лотус (Франция против Турции) (1927). Государства не вправе осуществлять власть на территории другого государства без специального разрешения, если иное не предусмотрено нормами международного права. Для киберпространства это означает, что несанкционированные кибероперации против иностранных систем потенциально могут расцениваться как нарушение суверенитета.

[13] Министерство вооруженных сил Франции: Международное право, применимое к операциям в киберпространстве. (сентябрь 2019 г.).

[14] Руководство Таллинн 2.0 по международному праву, применимому к кибероперациям.

[15] Дж. Райт QC MP. Киберпространство и международное право в XXI веке (май 2018 г.)

международного права, запрещающей кибероперации на территории другого государства без его согласия[16]. Таким образом, Великобритания склоняется к тому, что суверенитет в киберпространстве следует рассматривать скорее как принцип, чем как конкретную правовую норму.

В противоположность этому, некоторые исследователи и государства считают, что суверенитет в киберпространстве должен рассматриваться как юридически обязательная норма, нарушение которой влечет за собой международно-правовую ответственность. Они аргументируют это тем, что суверенитет является основой международного порядка и его нарушение недопустимо независимо от сферы, будь то физическое пространство или киберпространство [Schmitt 2009:439].

Аналогично тому, как принцип невмешательства запрещает государствам вмешиваться во внутренние дела других государств, суверенитет может интерпретироваться как запрет на несанкционированные кибероперации, которые затрагивают территорию или интересы другого государства. Такой подход требует признания того, что киберпространство не является правовой пустотой и подчиняется общепризнанным принципам международного права. Как указывает Rid, подобный спор во многом упирается в проблему доказательства физического или экономического ущерба, сопоставимого с «классическими» нарушениями [Rid 2012:12].

4. Различия в трактовках киберсуверенитета среди государств

Государства предлагают свои интерпретации понятия киберсуверенитета, отражающие их национальные интересы и приоритеты. Финляндия, например, утверждает, что киберпространство в целом не может быть объектом присвоения каким-либо государством[17]. Она признает, что государства обладают юрисдикцией над своей киберинфраструктурой и лицами, осуществляющими кибердеятельность на их территории, но не претендует на контроль над глобальным киберпространством.

Этот подход основан на признании транснациональной природы киберпространства и необходимости международного сотрудничества для его эффективного регулирования. Финляндия выступает за сохранение открытого и свободного интернета, поддерживая многосторонний подход к управлению цифровой сферой.

Франция предлагает более комплексную концепцию киберсуверенитета. В документе «Международное право, применимое к операциям в киберпространстве» она заявляет об осуществлении суверенитета над информационными системами, расположенными на ее территории[18]. Это включает не только физическую инфраструктуру, но и связанные с ней логические компоненты и данные.

Таким образом, Франция подчеркивает право государства на регулирование и защиту как материальных, так и нематериальных элементов киберпространства на своей территории. Этот подход отражает стремление обеспечить безопасность и защиту национальных интересов в цифровой сфере, учитывая сложность и многоуровневость киберпространства.

Нидерланды ссылаются на «Таллиннское руководство 2.0», в котором расширяется понятие суверенитета, включая физический, логический и социальный уровни киберпространства. Согласно этому подходу, государство обладает суверенными правами не только над физической инфраструктурой, но и над программным обеспечением, данными и киберактивностью, связанной с его гражданами.

Этот многоуровневый подход позволяет более полно учитывать все аспекты киберпространства и отражает необходимость комплексного регулирования в условиях цифровизации [Lotsberg, Jellinek 2017]. Нидерланды поддерживают идею о том, что государство должно иметь возможность защищать свои интересы на всех уровнях киберпространства.

Разнообразие терминов и определений, таких как «киберсуверенитет», «суверенитет в киберпространстве», «цифровой суверенитет», свидетельствует об отсутствии единого понимания этой концепции на международном уровне.

[16] Министерство обороны Великобритании: Подход Великобритании к беспилотным летательным аппаратам, Joint Doctrine Note 2/11 (2020).

[17] Заявление Финляндии о международном праве и киберпространстве (2020).

[18] Министерство вооруженных сил Франции: Международное право, применимое к операциям в киберпространстве (сентябрь 2019 г.).

Различия в подходах отражают национальные интересы, культурные особенности и политические приоритеты различных государств.

Однако отсутствие согласованной терминологии и общепринятых принципов затрудняет разработку международных норм и может приводить к конфликтам и недопониманию между государствами. Это подчеркивает необходимость продолжения диалога и сотрудничества для достижения консенсуса в вопросах регулирования киберпространства. Отдельно подчеркивается, что правовая фрагментация может негативно отразиться на глобальной экономике и информационных потоках [Shackelford, Richards, Studio, Craig 2015:12].

5. Кибероперации низкой интенсивности и нарушение суверенитета

Кибероперации низкой интенсивности – это действия, которые не достигают уровня применения силы или вооруженного нападения, но могут причинять ущерб и нарушать суверенитет государства. «Таллиннское руководство 2.0» предлагает классифицировать такие операции следующим образом:

– кибероперации, вызывающие физический ущерб: например, использование вредоносного программного обеспечения, которое выводит из строя оборудование;

– операции, приводящие к утрате функциональности систем: как в случае с вирусом Shamoon, который поразил нефтяную компанию Saudi Aramco в 2012 г. [Bronk, Tikk-Ringas 2013:85];

– кибероперации, не вызывающие физического ущерба, но влияющие на данные или доступность систем: такие как DDoS-атаки или изменение информации.

Государства по-разному оценивают, какие кибероперации следует считать нарушением суверенитета. Некоторые придерживаются позиции, согласно которой любое несанкционированное вмешательство в их киберинфраструктуру является нарушением суверенитета. Финляндия придерживается сходной позиции, признавая нарушение суверенитета в случаях, когда кибероперации приводят к материальному ущербу[19]. Другие считают, что для признания нарушения суверенитета необходимо, чтобы кибероперация причинила значительный ущерб или затронула критически важные функции государства. Чехия, например, считает нарушением суверенитета кибероперации, которые причиняют ущерб ее критической инфраструктуре[20].

Такое разнообразие подходов подчеркивает необходимость международного диалога для выработки общепринятых критериев. В частности, Taddeo указывает на важность согласованных определений «допустимого» вмешательства в цифровую инфраструктуру, иначе «низкоинтенсивные» атаки могут так и остаться в серой зоне [Taddeo 2018:506].

6. Кибершпионаж и его правовая оценка

Кибершпионаж представляет собой одну из наиболее сложных и спорных тем в международном праве. В отличие от традиционного шпионажа, кибершпионаж может осуществляться удаленно и массово, затрагивая огромные объемы данных.

Некоторые исследователи, в том числе Г. Браун и К. Поэллет, рассматривают кибершпионаж как сложившуюся международную практику, которая фактически приобрела характер международного обычая [Brown, Poellet 2012:130]. Они утверждают, что несмотря на вызванные им угрозы, кибершпионаж не получил четкого запрета в международном праве, а его широкое использование государствами свидетельствует о фактическом признании его допустимости в рамках существующей международной системы.

Однако данная позиция вызывает разногласия, поскольку ряд государств рассматривают кибершпионаж как прямое нарушение их суверенитета, особенно в контексте атак на критически важную инфраструктуру и утечки конфиденциальных данных [Buchan 2016:477]. Согласно «Таллиннскому руководству», удаленный кибершпионаж, если он не наносит физического ущерба, формально не считается нарушением суверенитета[21]. Тем не менее, учитывая рост таких операций, на международном уровне продолжаются дискуссии о необходимости формирования новых правовых норм, направленных на регулирование кибершпионажа.

[19] Заявление Финляндии о международном праве и киберпространстве (2020).
[20] Чешская Республика. Позиция по международному праву, применимому в киберпространстве (2020).
[21] См.: Руководство Таллинн 2.0 по международному праву, применимому к кибероперациям.

Соединенные Штаты придерживаются позиции, согласно которой шпионаж, включая кибершпионаж, не запрещен международным правом, хотя его отдельные аспекты могут регулироваться на национальном уровне[22]. Эта точка зрения основана на давней практике государств, которые занимаются разведывательной деятельностью в целях обеспечения национальной безопасности, однако остается предметом международных дискуссий.

Несмотря на это многие государства и международные организации выражают обеспокоенность в связи с кибершпионажем. После разоблачений Э. Сноудена в 2013 г., которые показали масштабные программы электронного слежения, ряд государств осудили такие действия как нарушение суверенитета и прав человека [Buchan 2016:480].

Южный общий рынок (МЕРКОСУР) в декларации 2013 г. осудил шпионаж в интернете как противоправное действие, подрывающее доверие между государствами[23]. Такие реакции свидетельствуют о растущем понимании того, что кибершпионаж может иметь серьезные последствия для международных отношений и требует правового регулирования.

Существует противоречие между ограничениями на правоохранительную деятельность государств в отношении других государств и относительно свободной разведывательной деятельностью. Если правоохранительные органы не могут проводить операции на территории другого государства без его согласия, то почему разведывательные службы могут осуществлять кибероперации без такого согласия?

Принцип, установленный в деле С.С. Лотус (Франция против Турции), гласит, что государство не может осуществлять свою власть на территории другого государства без его разрешения, если это не предусмотрено международным правом[24]. Это подразумевает, что несанкционированные кибероперации, включая кибершпионаж, могут рассматриваться как нарушение суверенитета и международного права.

Некоторые исследователи считают, что необходимо установить четкие международно-правовые нормы, регулирующие разведывательную деятельность в киберпространстве, чтобы избежать эскалации конфликтов и обеспечить уважение суверенитета государств [Moynihan 2019:5].

7. ООН и международные усилия по обеспечению кибербезопасности

Организация Объединенных Наций играет важную роль в обсуждении вопросов, связанных с кибербезопасностью и регулированием киберпространства на международном уровне. Впервые вопрос о международной информационной безопасности был поднят Россией в 1998 г., когда она внесла проект резолюции в Генеральную Ассамблею ООН[25].

С тех пор были созданы несколько групп правительственных экспертов (GGE), задачей которых является изучение и разработка мер по укреплению доверия и безопасности в использовании информационно-коммуникационных технологий. В 2013 г. группа экспертов представила доклад, в котором подтвердилось, что международное право, включая принципы государственного суверенитета, применимо к действиям государств в киберпространстве[26].

Несмотря на достигнутые договоренности, между государствами сохраняются разногласия по ряду ключевых вопросов. В 2015 г. на 70-й сессии Генеральной Ассамблеи ООН было подтверждено, что государства обязаны соблюдать принципы международного права при использовании информационно-коммуникационных технологий, включая суверенитет, невмешательство и мирное разрешение споров[27].

Однако отсутствие единого понимания того, как именно эти принципы должны применяться в киберпространстве, приводит к продолжению дискуссий. В 2018 г. была создана Рабочая группа открытого состава (OEWG) с целью разработки рекомендаций по ответственному поведению

[22] Министерство обороны США: Руководство по ведению войны.
[23] МЕРКОСУР: Декларация о деятельности по кибершпионажу в интернете (2013).
[24] Постоянная палата международного правосудия: Дело S.S. Lotus (Франция против Турции).
[25] ООН: Резолюция Генеральной Ассамблеи ООН A/RES/53/70 «Достижения в области информатики и телекоммуникаций в контексте международной безопасности» (1998).
[26] ООН: Доклад группы правительственных экспертов ООН A/68/98 (2013).
[27] ООН: Доклад группы правительственных экспертов ООН A/70/174 (2015).

государств в цифровой сфере. В итоговом докладе группы за 2021 г. признается необходимость дальнейшей работы над детализацией и согласованием позиций государств[28].

Борьба с киберпреступностью является одним из важных направлений международного сотрудничества. В 2019 г. Генеральная Ассамблея ООН приняла резолюцию A/RES/74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях»[29]. Между тем, как отмечается в ряде исследований, формирование единой международно-правовой системы противодействия киберпреступности по-прежнему остаётся на раннем этапе и требует дальнейшей унификации подходов [Горелик 2021б:65]. На ее основе была создана специальная межправительственная группа экспертов для разработки всеобъемлющей международной конвенции по противодействию киберпреступности.

Эти инициативы свидетельствуют о признании международным сообществом необходимости совместных действий для обеспечения безопасности в киберпространстве и создания эффективных правовых механизмов противодействия киберугрозам.

Заключение

Стремительная цифровизация и растущая зависимость общества от киберпространства ставят перед международным сообществом сложные вызовы. Вопрос о применимости государственного суверенитета к киберпространству остается нерешенным, а отсутствие единых международных норм создает правовые вакуумы и увеличивает риск конфликтов.

Разнообразие трактовок киберсуверенитета среди государств отражает их различные интересы и приоритеты. Одни страны стремятся расширить суверенитет на киберпространство, усиливая контроль и регулирование, тогда как другие выступают за сохранение открытого и свободного интернета, опасаясь, что излишнее вмешательство государства может ограничить права и свободы граждан.

Необходимо признать, что традиционные принципы международного права не всегда эффективно применимы к киберпространству. Требуется разработка новых подходов и норм, учитывающих особенности цифровой среды. Международное сотрудничество и диалог между государствами являются ключевыми элементами в этом процессе.

В связи с этим рекомендуется продолжать активную работу в рамках ООН и других международных организаций по выработке общепринятых норм и правил поведения в киберпространстве, которые будут учитывать интересы всех государств. Укрепление международного сотрудничества в сфере кибербезопасности, включая обмен информацией, проведение совместных учений и разработку механизмов быстрого реагирования на киберугрозы, станет важным шагом на пути к обеспечению глобальной безопасности.

Кроме того, необходимо разработать четкие международно-правовые нормы, регулирующие кибершпионаж и кибероперации низкой интенсивности. Это позволит предотвратить эскалацию конфликтов и обеспечить уважение суверенитета государств в цифровой сфере. Поиск баланса между национальной безопасностью и защитой прав и свобод человека в цифровом пространстве также является приоритетной задачей. Обеспечение устойчивого и безопасного развития киберпространства возможно только при условии, что будут учтены как потребности государства в безопасности, так и права граждан на свободу информации и приватность.

Только через совместные усилия и взаимопонимание международное сообщество сможет преодолеть существующие разногласия и создать эффективную правовую основу для безопасного, свободного и справедливого киберпространства, способствующего развитию и благополучию всех государств и народов.

[28] ООН: Итоговый доклад Рабочей группы открытого состава ООН (2021).
[29] ООН: Резолюция Генеральной Ассамблеи ООН A/RES/74/247 (2019).

Список литературы

1. Горелик И.Б. 2021а. Роль международных организаций в процессе противодействия киберпреступности. – *Международное право и международные организации*. № 3. С. 28-41.
2. Горелик И.Б. 2021б. Формирование международно-правовой системы противодействия киберпреступности. – *Право и политика*. № 5. С. 60-71.
3. Данельян А.А. 2020а. Киберпространство и международное право. – *Международное право и международные организации*. № 2.
4. Данельян А.А. 2020б. Международно-правовое регулирование киберпространства. – *Образование и право*. № 1. С. 261-269.
5. Добринская Д.Е. 2018. Киберпространство: территория современной жизни. – *Вестник Московского университета*. Серия 18. Социология и политология. Т. 24. № 1. С. 52-70.
6. Мигулева М.В. 2018. История определения понятия «киберпространство». – *Этносоциум и межнациональная культура*. № 6 (120). С. 41-45.
7. Bronk C., Tikk-Ringas E. 2013. The Cyber Attack on Saudi Aramco. – *Survival*. Vol. 55. No. 2. P. 81-96.
8. Brown G., Poellet K. 2012. The Customary Law of Cyberspace. – *Strategic Studies Quarterly*. Vol. 6. No. 1. P. 126-145.
9. Buchan R. 2016. Cyber Espionage and International Law. – *Journal of Conflict and Security Law*. Vol. 21. No. 3. P. 461-493.
10. Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J. 2012. The Law of Cyber Attack. – *California Law Review*. Vol. 100, No. 4. P. 817-886
11. Johnson D.R., Post D.G. 1996. Law and Borders – The Rise of Law in Cyberspace. – *Stanford Law Review*. Vol. 8. No. 5. P. 1367-1402.
12. Kello L. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.
13. Lin H. 2016. Attribution of Malicious Cyber Incidents: From Soup to Nuts. – *Journal of International Affairs*. Vol. 70, No. 1. P. 75-92.
14. Lotsberg K., Jellinek H. 2017. Jurisdiction in Cyberspace. – *Journal of High Technology Law*. Vol. 17. No. 2.
15. Moynihan H. 2019. The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention. – *Chatham House Research Paper*. December. P. 1-40.
16. Mueller M. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge (MA): MIT Press. P. 1-280.
17. Rid T. 2012. Cyber War Will Not Take Place. – *Journal of Strategic Studies*. Vol. 35. No. 1. P. 5-32.
18. Schmitt M.N. 2009. Grey Zones in the International Law of Cyberspace. – *Vanderbilt Journal of Transnational Law*. Vol. 42. P. 427-448.
19. Shackelford S.J., Richards E., Studio J.D., Craig A.N. 2015. Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets Through Bilateral Investment Treaties. – *American Business Law Journal*. Vol. 52. No. 1. P. 1-86.
20. Taddeo M. 2018. Cybersecurity and Individual Rights, Striking the Right Balance. – *Philosophy & Technology*. Vol. 31. No. 4. P. 503-507.

References

1. Bronk C., Tikk-Ringas E. 2013. The Cyber Attack on Saudi Aramco. – *Survival*. Vol. 55. No. 2. P. 81-96.
2. Brown G., Poellet K. 2012. The Customary Law of Cyberspace. – *Strategic Studies Quarterly*. Vol. 6. No. 1. P. 126-145.
3. Buchan R. 2016. Cyber Espionage and International Law. – *Journal of Conflict and Security Law*. Vol. 21. No. 3. P. 461-493.
4. Danelyan A.A. Kiberprostranstvo i mezhdunarodnoe pravo [Cyberspace and International Law]. – *Mezhdunarodnoe pravo i mezhdunarodnye organizatsii [International Law and International Organizations]*. 2020a. No 2. (In Russ.).
5. Danelyan A.A. Mezhdunarodno-pravovoe regulirovanie kiberprostranstva [International Legal Regulation of Cyberspace]. – *Obrazovanie i pravo [Education and Law]*. 2020б. No 1. P. 261-269. (In Russ.).
6. Dobrinskaya D.E. Kiberprostranstvo: territoriya sovremennoi zhizni [Cyberspace: Territory of Contemporary Life]. – *Vestnik Moskovskogo universiteta. Seriya 18. Sotsiologiya i politologiya [Bulletin of Moscow University. Series 18. Sociology and Political Science]*. 2018. Vol. 24, No 1. P. 52-70. (In Russ.).
7. Gorelik I.B. Formirovanie mezhdunarodno-pravovoi sistemy protivodeistviya kiberprestupnosti [Formation of an International Legal System for Combating Cybercrime]. – *Pravo i politika [Law and Politics]*. 2021. No 5. P. 60-71. (In Russ.).
8. Gorelik I.B. Rol' mezhdunarodnykh organizatsii v protsesse protivodeistviya kiberprestupnosti [The Role of International Organizations in Countering Cybercrime]. – *Mezhdunarodnoe pravo i mezhdunarodnye organizatsii [International Law and International Organizations]*. 2021. No 3. P. 28-41. (In Russ.).
9. Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J. 2012. The Law of Cyber Attack. – *California Law Review*. Vol. 100, No. 4. P. 817-886
10. Johnson D.R., Post D.G. 1996. Law and Borders – The Rise of Law in Cyberspace. – *Stanford Law Review*. Vol. 48. No. 5. P. 1367-1402.
11. Kello L. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.
12. Lin H. 2016. Attribution of Malicious Cyber Incidents: From Soup to Nuts. – *Journal of International Affairs*. Vol. 70, No. 1. P. 75-92.
13. Lotsberg K., Jellinek H. 2017. Jurisdiction in Cyberspace. – *Journal of High Technology Law*. Vol. 17. No. 2.
14. Miguleva M.V. Istoriya opredeleniya ponyatiya "kiberprostranstvo" [History of Defining the Concept of "Cyberspace"]. – *Etnosotsium i mezhdunarodnaya kul'tura [Ethnosocium and Interethnic Culture]*. 2018. No 6 (120). P. 41–45. (In Russ.).
15. Moynihan H. 2019. The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention. – *Chatham House Research Paper*. December. P. 1-40.
16. Mueller M. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge (MA): MIT Press. P. 1-280.
17. Rid T. 2012. Cyber War Will Not Take Place. – *Journal of Strategic Studies*. Vol. 35. No. 1. P. 5-32.

18. Schmitt M.N. 2009. Grey Zones in the International Law of Cyberspace. – *Vanderbilt Journal of Transnational Law*. Vol. 42. P. 427-448.
19. Shackelford S.J., Richards E., Studio J.D., Craig A.N. 2015. Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets Through Bilateral Investment Treaties. – *American Business Law Journal*. Vol. 52. No. 1. P. 1-86.
20. Taddeo M. 2018. Cybersecurity and Individual Rights, Striking the Right Balance. – *Philosophy & Technology*. Vol. 31. No. 4. P. 503-507.

Информация об авторе

Константин Константинович ЛАЗАРЬ,
аспирант кафедры международного права, Дипломатическая академия МИД России

Остоженка ул., д. 53/2, стр. 1, г. Москва, 119021, Российская Федерация

lazariconstantin@yandex.ru
ORCID: 0009-0008-4763-1922

About the Author

Constantin C. LAZARI,
Post-graduate student of the Department of International Law, Federal State Educational Public Institution of Higher Education, "Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation"

53/2, bld. 1, Ostozhenka St., Moscow, Russian Federation, 119021

lazariconstantin@yandex.ru
ORCID: 0009-0008-4763-1922