Дата поступления рукописи в редакцию: 25.04.2026 г.
Дата принятия рукописи в печать: 13.07.2026 г.
DOI: 10.24412/2782-3830-2026-7-504-508

ОЛЕЙНИКОВ Олег Владимирович,
к.ю.н., доцент, Академия маркетинга и социально-информационных технологий, Краснодар, Россия,
e-mail: oleynikovnvr@mail.ru

ДРОГИН Егор Валерьевич,
студент, Академия маркетинга и социально-информационных технологий, Краснодар, Россия,
e-mail: mail@law-books.ru

ПАРШИН Дмитрий Сергеевич,
студент, Академия маркетинга и социально-информационных технологий, Краснодар, Россия,
e-mail: mail@law-books.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ КИБЕРПРОСТРАНСТВА В УСЛОВИЯХ ГЛОБАЛЬНОЙ НЕОПРЕДЕЛЕННОСТИ

Аннотация. *В статье разбираются главные проблемы правового регулирования киберпространства в современной международной правовой системе. Автор исследует глубинный конфликт между природой интернета – который не имеет границ и децентрализован — и классическим международным правом, которое исторически опирается на четкие территории и контроль государств. В работе подробно рассматривается идеологический раскол между либеральной моделью управления (ее поддерживают США и ЕС) и концепцией кибер-суверенитета (которую отстаивают Россия и Китай). Именно это противостояние мешает созданию единых правил игры. Также анализируются три острые проблемы: применение международного права к кибероперациям, борьба с транснациональной киберпреступностью и защита прав человека в сети. Отдельное внимание уделено влиянию IT-корпораций, которые фактически сами диктуют стандарты безопасности, и региональным инициативам (ЕС, ШОС), которые наглядно показывают сценарий «управляемой фрагментации» глобальной сети.*

Ключевые слова: *киберпространство, международное право, кибербезопасность, цифровой суверенитет, многостороннее управление, управляемая фрагментация, права человека, негосударственные организации.*

OLEYNIKOV Oleg Vladimirovich,
candidate of Law, associate Professor, Academy of Marketing and Social and Information Technologies, Krasnodar, Russia

DROGIN Egor Valerievich,
student, Academy of Marketing and Social and Information Technologies, Krasnodar, Russia

PARSHIN Dmitry Sergeevich,
student, Academy of Marketing and Social and Information Technologies, Krasnodar, Russia

CURRENT PROBLEMS OF LEGAL REGULATION OF CYBERSPACE IN THE CONDITIONS OF GLOBAL UNCERTAINTY

Annotation. *The article analyzes the main problems of legal regulation of cyberspace in the modern international legal system. The author explores the deep-rooted contradictions between the cross-border, decentralized nature of cyberspace and the state-oriented nature of classical international law. The work reveals the key ideological differences between the liberal concept of multilateral governance (supported by the United States and the European Union) and the doctrine of cyber sovereignty (advocated by Russia and China), which are the main obstacles to the formation of a unified legal regime. Three key issues are being addressed: the implementation of international law norms regarding cyber operations, countering cross-border cybercrime, and ensuring human rights in the digital environment. Special attention is paid to the influence of non-state actors who actually set security standards, as well as to the analysis of regional initiatives (the European Union, the Shanghai Cooperation Organization) that demonstrate the scenario of "managed fragmentation".*

Key words: *cyberspace, international law, cybersecurity, digital sovereignty, multilateral governance, managed fragmentation, human rights, and non-governmental organizations.*

Интернет давно перестал быть просто набором компьютерных технологий. Сегодня это фундамент, на котором держится современное общество, мировая экономика и вся система международных отношений. Киберпространство стало главной площадкой для общения, бизнес-конкуренции и даже прямых конфликтов. Оно проникло абсолютно во все сферы: от наших личных переписок до вопросов национальной безопасности и дипломатии. Однако есть одна большая проблема: технологии развиваются настолько быстро, что правовая система просто не успевает за ними. Мы до сих пор не создали полноценной и понятной системы управления этой цифровой средой, что породило массу юридических, политических и этических проблем [8, 14]. Из-за того что в сети нет единых и общепринятых правил, под угрозой оказываются международная безопасность, права обычных людей и даже государственный суверенитет. Именно поэтому вопрос о том, как эффективно регулировать киберпространство, сегодня является одним из самых острых в мировой повестке.

Актуальность этой работы продиктована главным конфликтом нашего времени. С одной стороны, интернет не знает границ, он виртуален и децентрализован. С другой стороны, классическое международное право веками строилось на четких физических границах и полном контроле государств над своими территориями. Каждый год мы видим, как растет число мощных хакерских атак на важнейшие объекты, как цифровые инструменты используются в гибридных войнах, как распространяются фейки и как расцветает транснациональная киберпреступность. Все это кричит о том, что нам срочно нужны новые рабочие механизмы международного права [9, 106]. Сейчас мировому сообществу нужно решить невероятно сложную задачу: как найти баланс между обеспечением безопасности, защитой прав человека и сохранением интернета открытым и свободным. А усложняет эту задачу то, что правила в сети все чаще диктуют не государства, а крупные негосударственные игроки [10, 342].

Суть проблемы кроется в самой природе киберпространства. Его главные черты – отсутствие границ, анонимность, виртуальность и мгновенная скорость передачи данных. Это ломает привычную Вестфальскую систему международных отношений, которая веками опиралась на принцип государственного суверенитета. В старой модели каждое государство было полновластным хозяином на своей территории. Но традиционные методы контроля и юрисдикции в интернете просто не работают. Человек или хакерская группа в одной стране могут за секунду обрушить инфраструктуру в другой части света. Из-за этого многие устоявшие нормы международного права оказываются бесполезными. К этому технологическому вызову добавляется еще и глубокий идеологический раскол: страны до сих пор не могут договориться о том, как именно нужно управлять глобальной сетью. На мировой арене четко видны два совершенно разных подхода [6, 112].

Первый подход – это либеральная модель, которую продвигают США, страны Евросоюза и их союзники. Они считают, что управлять интернетом должны не только государства, но и бизнес, инженеры, и само гражданское общество. Их главная идея – применять к кибероперациям уже существующее международное право, жестко защищать права человека в сети (свободу слова и приватность) и опираться на добровольные нормы поведения, например, на соответствующие правила ООН.

Второй подход – это модель «киберсуверенитета». Ее последовательно отстаивают Россия, Китай и ряд других государств. Главный принцип этой модели прост: каждое государство имеет полное и безусловное право контролировать свой собственный сегмент интернета [5]. Сторонники этого подхода хотят принять новый, большой международный договор под эгидой ООН. Этот документ должен закрепить, что именно государство отвечает за безопасность, порядок и контент в сети на своей территории.

Есть, конечно, страны, которые пытаются найти компромисс между этими двумя полюсами, но их попытки лишь подчеркивают, что глобального согласия нет. Именно этот спор – что важнее, открытость сети или контроль, права личности или безопасность государства – является главным тормозом на пути к созданию единых правил игры в киберпространстве [11, 206].

На фоне этого идеологического спора отчетливо видны три конкретные проблемы, которые требуют срочного решения.

Первая проблема – как вообще применять нормы международного права к кибероперациям. Главная неясность заключается в толковании Устава ООН. Статья 2(4) запрещает применение силы, а статья 51 дает право на самооборону [1]. Но как это применить в сети? Какой масштаб кибератаки можно считать «вооруженным нападением», чтобы ответить на нее, в том числе с помощью реальной армии? Четких критериев нет. Из-за этой «серой зоны» государства могут проводить агрессивные операции в сети почти безнаказанно, что постоянно рискует перерасти в реальную эскалацию [7].

Вторая проблема — борьба с транснациональной киберпреступностью. Преступники действуют глобально, а правоохранительные системы привязаны к территориям. Из-за проблем с юрисдикцией, экстрадицией и сбором цифровых улик киберпреступники часто остаются безнаказанными. Главный инструмент здесь — Будапештская конвенция 2001 года [2]. Но такие крупные игроки, как Россия и Китай, ее не подписали, считая, что она ущемляет их суверенитет. Это сильно тормозит создание единого глобального фронта против киберугроз [3].

Третья проблема – защита прав человека в цифре. Интернет стал не только местом, где права реализуются, но и площадкой для их массового нарушения. Стремясь к тотальному контролю и безопасности, государства и корпорации часто ущемляют право на приватность, свободу слова и доступ к информации. Массовая слежка, интернет-цензура и непрозрачные алгоритмы модерации в соцсетях создают угрозу демократии и ведут к риску построения «цифрового авторитаризма» [12, 294].

Отдельно стоит сказать о роли негосударственных игроков, в первую очередь – IT-гигантов. Эти корпорации давно перестали быть просто объектом регулирования. Фактически именно они пишут негласные правила кибербезопасности и приватности для миллиардов людей. Их внутренние политики влияют на нашу повседневную жизнь гораздо сильнее, чем национальные законы. Возник новый мощный слой управления – «частное правление» (private governance). Если мы не признаем эту реальность и не встроим эти корпорации в международную систему регулирования, любой наш анализ будет неполным, а рекомендации – просто красивыми словами, оторванными от жизни [10, 343].

Анализ переговоров в ООН и на других площадках показывает, что в ближайшие годы принять один идеальный глобальный договор по интернету не получится. Скорее всего, мир ждет сценарий, который можно назвать «управляемой фрагментацией». Это значит, что единого документа для всех не будет, но и полного раскола интернета на изолированные куски не произойдет. Вместо этого сформируется сложная система: базовые общепринятые нормы будут работать везде, но поверх них ляжет множество региональных и отраслевых соглашений [6, 178].

Эта фрагментация уже видна на практике. Яркий пример – Европейский Союз. Через свои жесткие регламенты (NIS2, GDPR, законы о цифровых услугах и рынках — DSA и DMA) [4] ЕС создает мощную систему правил и фактически экспортирует свои стандарты на весь мир (так называемый «эффект Брюсселя»). В противовес этому Шанхайская организация сотрудничества (ШОС) во главе с Россией и Китаем продвигает свою модель. Она базируется на идее информационной безопасности и абсолютного суверенитета государств, а в ООН продвигает альтернативные Будапештской конвенции инициативы [5]. Параллельно создаются и другие коалиции «единомышленников», которые на добровольной основе берут на себя обязательства по ответственному поведению в сети. Все это наглядно показывает, как «управляемая фрагментация» работает в реальности.

Подводя промежуточный итог, можно сказать, что регулирование киберпространства переживает глубокий кризис. Старые законы не работают из-за технологической природы сети, а идеологический спор между Западом и Востоком делает невозможным создание единого правового режима в обозримом будущем. Путь вперед – это именно «управляемая фрагментация», сложная мозаика из разных соглашений [11, 207].

В этих условиях успех зависит не от того, сможем ли мы подписать одну большую бумагу, а от гибкости дипломатов и готовности идти на прагматичные компромиссы. Чтобы перейти от пустых деклараций к реальным делам, нужно сделать три конкретных шага.

1) Необходимо создать международный орган по арбитражу и медиации киберконфликтов. Под эгидой ООН нужно учредить структуру, которая будет расследовать крупные хакерские атаки, помогать с технической атрибуцией (кто именно стоял за

атакой) и мирить стороны. Это закроет проблему «разрыва атрибуции» и снизит риск того, что страна нанесет непропорциональный ответный удар.

2) Необходимо навести порядок в вопросах взаимной правовой помощи и экстрадиции. Стоит разработать новый протокол или договор, посвященный именно киберпреступности. Он должен унифицировать понятия, чтобы решить проблему «двойной криминализации» (когда действие считается преступлением в одной стране, но не считается в другой). Также нужен упрощенный экстренный порядок обмена цифровыми уликами и четкие каналы для быстрой экстрадиции хакеров, но с обязательным соблюдением прав человека [7].
3) Необходимо официально включить «частное правление» в систему международного регулирования. Мировому сообществу пора признать, что IT-корпорации фактически стали равноправными субъектами мировой цифровой политики. Необходимо принять нормы, которые обяжут компании быть прозрачнее в работе своих алгоритмов, участвовать в международных консультациях по кибербезопасности и обеспечивать равный доступ к платформам. Диалог нужно вести не только с правительствами, но и напрямую с бизнесом [6, 198].

Правовое регулирование киберпространства сегодня находится в системном кризисе. Анонимность и скорость сети делают классический территориальный суверенитет неэффективным. Мир расколот на два лагеря: сторонников открытого многостороннего интернета и сторонников жесткого государственного киберсуверенитета. Этот спор усугубляется тремя проблемами: непониманием того, как применять Устав ООН к хакерским атакам, бессилием перед транснациональной киберпреступностью и угрозой «цифрового авторитаризма». При этом реальные правила в сети часто диктуют IT-корпорации.

Вместо одного глобального договора мир движется к «управляемой фрагментации», где региональные блоки (как ЕС или ШОС) создают свои стандарты. Будущее цифровой среды зависит от того, сможем ли мы договориться о практических вещах: создать международный кибер-арбитраж, упростить экстрадицию хакеров и легализовать роль IT-гигантов в выработке глобальных стандартов. Выбор, который мы сделаем в ближайшие годы, определит облик интернета на десятилетия вперед.

Список литературы:

[1] Устав Организации Объединенных Наций (принят в г. Сан-Франциско 26.06.1945) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. XII. – М., 1956. – С. 14–47.

[2] Конвенция Совета Европы о преступности в сфере компьютерной информации (ETS № 185) (заключена в г. Будапеште 23.11.2001) // СПС Гарант.

[3] Конвенция Организации Объединенных Наций против киберпреступности (Ханойская конвенция) (принята Генеральной Ассамблеей ООН 24.12.2024, открыта для подписания 25.10.2025) // Официальный сайт ООН. – URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/

[4] Регламент (ЕС) 2022/2065 Европейского парламента и Совета от 19 октября 2022 года о едином рынке цифровых услуг (Digital Services Act — DSA) // Официальный журнал Европейского союза. – 2022. – № 277. – С. 1-102.

[5] Соглашение Шанхайской организации сотрудничества о сотрудничестве в области международной информационной безопасности (2009) // Официальный сайт ШОС. – URL: https://eng.sectsco.org/

[6] Концепция цифрового государства и цифровой правовой среды / Н. Н. Черногор, Д. А. Пашенцев, М. В. Залоило [и др.]. – Москва : Инфра-М, Норма, 2023. – 244 с.

[7] Новиков И. Ханойская конвенция ООН: сотрудничество или новое киберпротивостояние // Anti-Malware.ru. – 2026. – 20 января. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/UN-Hanoi-Convention

[8] Маглинова Т. Г. Влияние цифровых технологий на развитие экономических системы страны // Вестник ИМСИТ. – 2023. – № 1(93). – С. 14-17.

[9] Бондаренко И. А. Кибербезопасность как инвестиция / И. А. Бондаренко, А. О. Пахомова, А. О. Козлова // Исследование инновационного потенциала общества и формирование направлений его стратегического развития : сборник научных статей 12-й Всероссийской научно-практической конференции с международным участием, Курск, 30 декабря 2022 года. Том 1. – Курск: Юго-Западный государственный университет, 2022. – С. 104-111.

[10] Мадатова О. В. Искусственный интеллект и киберугрозы: новые вызовы экономической безопасности в эпоху цифровизации / О. В. Мадатова, О. С. Ткачев // Инновационное предпринимательство как фактор достижения технологического суверенитета России : Сборник научных статей по результатам работы VII Международной научно-практической конференции, Москва, 16 апреля 2025 года. – Москва: Общество с ограниченной ответственностью «Русайнс», 2025. – С. 341-344.

[11] Жидяева Е. С. Законность – фундаментальная категория юридической науки и практики // Международный журнал гуманитарных и естественных наук. – 2025. – № 1-1(100). – С. 205-208.

[12] Лаптева С. А. Цифровизация юридической отрасли / С. А. Лаптева, С. Ю. Субачев // Стратегия социально-экономического развития общества: управленческие, правовые, хозяйственные аспекты : сборник научных статей 14-й Международной научно-практической конференции, Курск, 21–22 ноября 2024 года. – Курск: ЗАО «Университетская книга», 2024. – С. 293-295.

References:

[1] Charter of the United Nations (adopted in San Francisco 26.06.1945) //Collection of existing treaties, agreements and conventions concluded by the USSR with foreign states. - Issue XII. - M., 1956. - S. 14-47.

[2] Council of Europe Convention on Crime in the Field of Computer Information (ETS No. 185) (concluded in Budapest 23.11.2001) //ATP Guarantor.

[3] United Nations Convention against Cybercrime (Hanoi Convention) (adopted by the UN General Assembly 24.12.2024, open for signature 25.10.2025) //Official website of the UN. – URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/

[4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the Digital Services Act (DSA)//Official Journal of the European Union. – 2022. – № 277. - S. 1-102.

[5] Agreement of the Shanghai Cooperation Organization on cooperation in the field of international information security (2009)//Official website of the SCO. – URL: https://eng.sectsco.org/

[6] The concept of a digital state and a digital legal environment/N. N. Chernogor, D. A. Pashentsev, M. V. Zaloilo [et al.]. - Moscow: Infra-M, Norma, 2023. - 244 s.

[7] Novikov I. UN Hanoi Convention: cooperation or new cyber confrontation// Anti-Malware.ru. – 2026. - January 20. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/UN-Hanoi-Convention

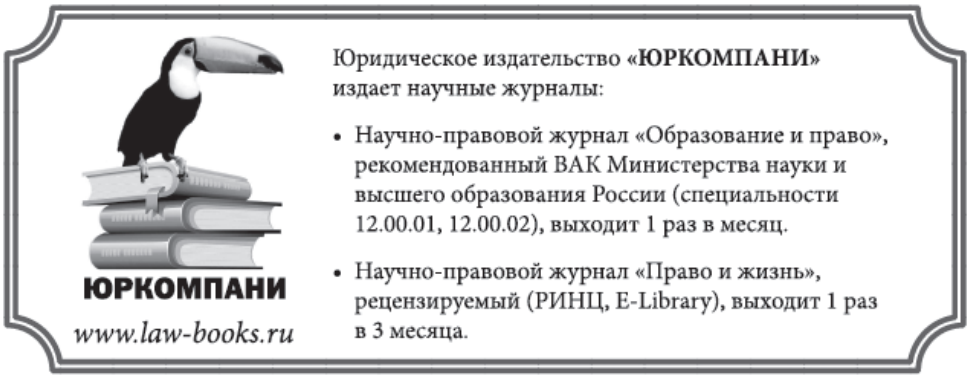
[8] Maglinova T. G. The influence of digital technologies on the development of the country's economic system//IMSIT Bulletin. – 2023. – № 1(93). - S. 14-17.

[9] Bondarenko I. A. Cybersecurity as an investment/I. A. Bondarenko, A. O. Pakhomova, A. O. Kozlova//Research of the innovative potential of society and the formation of directions for its strategic development: a collection of scientific articles of the 12th All-Russian Scientific and Practical Conference with international participation, Kursk, December 30, 2022. Volume 1. - Kursk: Southwestern State University, 2022. - S. 104-111.

[10] Madatova O. V. Artificial intelligence and cyber threats: new challenges to economic security in the era of digitalization/O. V. Madatova, O. S. Tkachev//Innovative entrepreneurship as a factor in achieving technological sovereignty of Russia: Collection of scientific articles based on the results of the VII International Scientific and Practical Conference, Moscow, April 16, 2025. - Moscow: Rusines Limited Liability Company, 2025. - S. 341-344.

[11] Zhidyaeva E. S. Legality is a fundamental category of legal science and practice//International Journal of Humanities and Natural Sciences. – 2025. – № 1-1(100). - S. 205-208.

[12] Lapteva S. A. Digitalization of the legal industry/S. A. Lapteva, S. Yu. Subachev//Strategy for the socio-economic development of society: managerial, legal, economic aspects: collection of scientific articles of the 14th International Scientific and Practical Conference, Kursk, November 21-22, 2024. - Kursk: University Book CJSC, 2024. - S. 293-295.



Юридическое издательство **«ЮРКОМПАНИ»** издает научные журналы:

- Научно-правовой журнал «Образование и право», рекомендованный ВАК Министерства науки и высшего образования России (специальности 12.00.01, 12.00.02), выходит 1 раз в месяц.
- Научно-правовой журнал «Право и жизнь», рецензируемый (РИНЦ, E-Library), выходит 1 раз в 3 месяца.