УДК 327:004.056

КИБЕРУГРОЗЫ КАК ФАКТОР ТРАНСФОРМАЦИИ ПРАВОВОЙ КУЛЬТУРЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

CYBER THREATS AS A FACTOR IN THE TRANSFORMATION OF THE LEGAL CULTURE OF INTERNATIONAL SECURITY

Б. И. Шумская
Белорусский государственный экономический университет,
аспирант, магистр политических наук

Аннотация. *В статье анализируется влияние киберугроз на трансформацию правовой культуры международной безопасности, рассматриваются специфика угроз, практика атрибуции инцидентов и роль государств в формировании норм поведения в киберпространстве; делается вывод о фрагментации правовой культуры и необходимости ее дальнейшей институционализации.*

Ключевые слова: *международная безопасность, киберугрозы, правовая культура, киберпространство, цифровой суверенитет, международные отношения.*

Annotation. *The article analyzes the impact of cyber threats on the transformation of international security legal culture, examines the specifics of threats, incident attribution practices, and the role of states in shaping norms of behavior in cyberspace; the author concludes on the fragmentation of legal culture and the need for its further institutionalization.*

Keywords: *international security, cyber threats, legal culture, cyberspace, digital sovereignty, international relations.*

Исторически сложилось так, что международная безопасность изучается в политологической науке как состояние защищенности международной системы и ее ключевых акторов от угроз, нарушающих стабильность миропорядка. При классическом реалистском подходе безопасность ассоциировалась преимущественно с военной силой и балансом мощи между государствами. На конец XX ст. и в начале XXI ст. данное понятие расширилось из-за внесения в него немилитаризованных и транснациональных угроз, таких как терроризм, экономическая нестабильность, природоохранные риски и информационные воздействия.

Современные исследования международной безопасности описывают ее как комплексное и многоуровневое явление, содержащее не только военно-политическое измерение, но и совокупность правовых, институциональных и нормативных механизмов регулирования международных отношений. В рамках подхода устойчивость международной системы определяется не столько балансом сил, сколько степенью согласованности ее норм, правил и процедур,

регулирующих поведение государств при появляющихся технологических вызовах [1, с. 16].

Диджитализация международных отношений послужила причиной признания киберпространства как независимого измерения мировой политики. Увеличение объема информационно-коммуникационных технологий в сфере государственного управления, экономики и обороны обусловило появление киберугроз, обладающих разрушительным потенциалом, вследствие чего киберпространство стало составляющей повестки международной безопасности, а реагирование на цифровые угрозы — компонентом внешнеполитической стратегии государств. При данных выводах актуальным становится изучение правовой культуры международной безопасности; именно она определяет рамки допустимого поведения акторов в ситуации нормативной неопределенности и нанотехнологических изменений.

Международная безопасность в чистом виде является результатом взаимодействия объективных (существующих, измеримых факторов) угроз и субъективных (зависящих от восприятия, оценок государств) представлений государств о степени индивидуальной уязвимости. Политологический подход основывается на том, что угрозы не существуют вне интерпретации, а формируются в процессе политической коммуникации и их институционального закрепления.

На волне глобализации и взаимозависимости государств международная безопасность обеспечивается и гарантируется не за счет национальных ресурсов, а исключительно через международное сотрудничество и правовое регулирование. Существенную роль в данном процессе играют международные организации, формирующие нормативные ожидания и стандарты поведения в переломных и кризисных ситуациях.

Правовая культура международной безопасности в рамках заявленной парадигмы трактуется как совокупность устойчивых нормативных установок о допустимом инструментарии обеспечения безопасности, легитимных формах принуждения и режимах ответственности за нарушение международных обязательств. Ее формирование опосредовано системным институциональным взаимодействием государств, международных организаций и экспертных сообществ, что отражает степень нормативной консолидации международной системы. Достаточно высокий уровень развития правовой культуры обеспечивает прогностическую стабильность стратегий акторов и нивелирует риски неконтролируемой эскалации при нарастающей неопределенности.

Киберугрозы приобретают статус критического фактора в системе вызовов международной безопасности. Природа угроз проявляется в ряде характерных черт, среди которых трансграничность, асимметричность, высокая

скорость реализации и сложность субъектной атрибуции. Действуя в так называемой серой зоне, кибервмешательства зачастую не достигают порога вооруженного конфликта, что затрудняет их международно-правовую квалификацию и применение норм международного гуманитарного права.

Проблема атрибуции кибератак остается одной из ключевых в современных исследованиях международной безопасности. Как отмечают Н. П. Ромашкина, А. С. Марков и Д. В. Стефанович, отсутствие унифицированных и общепризнанных процедур установления ответственности в киберпространстве существенно ограничивает возможности международно-правового реагирования и способствует росту взаимного недоверия между государствами [2, с. 10–11]. На фоне политизации киберинцидентов атрибуция выходит за рамки сугубо технической верификации, вбирая в себя выраженное политическое и дипломатическое измерение.

Политизация киберпространства находит отражение в практике публичной атрибуции киберинцидентов. В мае 2025 г. правительство Чешской Республики официально возложило ответственность за масштабную кибератаку на Министерство иностранных дел на структуры Китайской Народной Республики, что сопровождалось дипломатическими мерами и международной поддержкой со стороны союзников по Европейскому союзу (далее — ЕС) и Организации Североатлантического договора (НАТО) [3]. Схожая тенденция наблюдается в практике Китайской Народной Республики, которая в апреле 2025 г. официально обвинила Соединенные Штаты Америки в проведении «передовых кибератак» на критическую инфраструктуру во время Азиатских зимних игр в Харбине вместе с IT-системами предприятий и их технологических платформ [4]. Отмеченные кейсы указывают на зарождение новой политико-правовой практики, в рамках которой все без исключения кибератаки рассматриваются как компонент межгосударственного противоборства и используются в качестве инструмента внешнеполитического давления. Данная проблема напрямую трансформирует правовую культуру международной безопасности, смещая фокус с правовых механизмов урегулирования на политические интересы. Однако увеличивающиеся киберугрозы лишь усугубляют ситуацию: отсутствие универсального и юридически обязательного международного соглашения по урегулированию действий государств в киберпространстве приводит к фрагментации нормативных подходов и конкуренции правовых моделей.

Международные усилия по созданию общепризнанных норм ответственного поведения государств в киберпространстве осуществляются преимущественно в виде многосторонних процессов, инициированных Организацией Объединенных Наций (далее — ООН). К основным составляющим их усилий относятся деятельность Группы правительственных экспертов (GGE)

по вопросам ответственного поведения государств в контексте международной безопасности и работа Открытой рабочей группы (OEWG) по вопросам безопасности в сфере использования информационно-коммуникационных технологий в мирных целях [5]. Действующие форматы служат площадками для выработки принципов, норм и мер поддержания доверия, направленных на предотвращение конфликтов в цифровой среде и повышение транспарентности государственного поведения в киберпространстве.

На основе консенсусных выводов GGE 2015 г. Генеральная Ассамблея ООН подтвердила, что имеющееся международное право вместе с принципами Устава ООН, международного гуманитарного и международного прав человека полностью применимо к деятельности государств в киберпространстве. Такой аспект закреплен в поочередных резолюциях Генеральной Ассамблеи и международных заявлениях, отражающих единую позицию государств-членов о необходимости приведения поведения и действий государств в киберсреде в соответствие с универсальными юридическими нормами [6].

Региональные акторы привносят значительный вклад в развитие правовой культуры кибербезопасности. ЕС последовательно формирует собственную нормативно-правовую модель кибербезопасности, направленную на повышение устойчивости цифрового пространства и защиту единого внутреннего рынка от киберугроз. Центральным элементом модели является Закон ЕС «О киберустойчивости» [7], устанавливающий обязательные требования к безопасности продуктов с цифровыми элементами на всех этапах их жизненного цикла. В политико-правовом измерении данный акт отражает стремление ЕС по укреплению цифрового суверенитета и переход от рекомендательных мер к обязательному правовому регулированию в сфере кибербезопасности.

Применение автоматизированных технологий и искусственного интеллекта существенно трансформирует характер текущих кибероперации. Согласно отчету Microsoft о цифровой защите за 2025 г., системы киберзащиты ежедневно обрабатывают порядка 100 трлн цифровых сигналов, блокируют 4,5 млн вредоносных файлов и анализируют до 38 млн инцидентов, связанных с компрометацией идентичности, во многом за счет AI-алгоритмов. Такого типа технологии позволяют в автоматическом режиме выявлять угрозы и реагировать на них, но параллельно используются злоумышленниками для масштабирования атак, что усиливает асимметрию угроз и снижает прозрачность действий в киберпространстве. Государства интегрируют AI- и автоматизированные инструменты активнее в национальные киберстратегии, что подтверждается ростом масштабируемых и высокоавтоматизированных кибероперации. Актуализируется запрос на доработку норм международного права, поскольку

автономность алгоритмов усложняет атрибуцию, контроль эскалации и обеспечение ответственности государств в цифровой среде [8].

Таким образом, киберугрозы выступают одними из факторов трансформации международной безопасности и правовой культуры, генерируя новые концепции допустимых форм политического воздействия при тотальной цифровизации. Институционализация реагирования на угрозы в киберпространстве демонстрируется практикой публичной атрибуции кибератак, интенсификацией международного сотрудничества и укреплением регионального регулирования. Сохраняющаяся нормативная неопределенность, отсутствие универсальных императивных механизмов ответственности и конкуренция правовых парадигм объясняют выявленный фрагментарный характер формирующейся правовой культуры международной безопасности. Данный факт актуализирует потребность в дальнейшей теоретической и прикладной экспликации вопросов правового регулирования киберпространства на международном уровне.

---

1. Бартош А. А. Основы международной безопасности. Организации обеспечения международной безопасности : учеб. пособие для вузов. 3-е изд., перераб. и доп. М. : Юрайт, 2023. 429с. Вернуться к статье

2. Ромашкина Н. П., Марков А. С., Стефанович Д. В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А. В. Загорский, Н. П. Ромашкина. М. : ИМЭМО РАН, 2020. 97 с. Вернуться к статье

3. Czech Republic says China behind cyberattack on ministry, embassy rejects accusations [Electronic resource] // Reuters : [website]. URL: https://www.reuters.com/world/china/czech-republic-says-china-was-behind-cyberattack-ministry-summons-ambassador-2025-05-28/ (date of access: 26.01.2026). Перейти к источнику Вернуться к статье

4. China accuses US security agency of ‘advanced’ cyberattacks [Electronic resource] // BusinessDay : [website]. URL: https://www.businessday.co.za/bd/world/asia/2025-04-15-china-accuses-us-security-agency-of-advanced-cyberattacks/ (date of access: 26.01.2026). Перейти к источнику Вернуться к статье

5. Управление по вопросам разоружения [Электронный ресурс] // Организация Объединенных Наций : [сайт]. URL: https://disarmament.unoda.org/ru/who-we-are/about-unoda (дата обращения: 28.01.2026). Перейти к источнику Вернуться к статье

6. Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace // Council of the European Union : [website]. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/ (date of access: 29.01.2026). Перейти к источнику Вернуться к статье

7. Cyber Resilience Act [Electronic resource] // European Commission : [website]. URL: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (date of access: 01.02.2026). Вернуться к статье

8. Microsoft Digital Defense Report 2025 [Electronic resource] // Microsoft : [website]. URL: https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/?msockid=3601f268ea23670f2f2ce768eb0b6696 (date of access: 01.02.2026). Перейти к источнику Вернуться к статье