Взаимодействие международного права и национальной безопасности: правовые механизмы и вызовы современности

Чеботарева Ирина Юрьевна
кандидат юридических наук, доцент, доцент кафедры правовых, психолого-педагогических и экономических дисциплин, филиал Адыгейский государственный университет, vetal_01@list.ru,

Алкесов Руслан Темботович
кандидат социологических наук, ст. преподаватель кафедры административного и уголовного права, Майкопский государственный технологический университет, ira.ch00@bk.ru,

Хлебникова Анна Андреевна
Кандидат юридических наук, доцент кафедры юриспруденции факультета управления и права, Краснодарский кооперативный институт Российский университет кооперации, stakhova69@mail.ru,

Мамишева Зара Аскарбиевна
кандидат юридических наук, доцент, доцент кафедры теории и истории государства и права, конституционного строительства и политологии, Институт права, АГУ, mamicheva.zara@mail.ru

Исследование посвящено соотношению международного права и национальной безопасности через призму правовых средств, применяемых на универсальном, региональном и внутригосударственном уровнях. Актуальность темы связана с расширением круга угроз, смещением значительной части конфликтов в цифровую среду, усилением санкционного давления и ростом споров о пределах государственного суверенитета. Научная новизна состоит в сведении разрозненных направлений доктрины в единую аналитическую схему, где совместно рассмотрены стратегическое регулирование, международная информационная безопасность, цифровой суверенитет, санкционные режимы и международное сотрудничество по борьбе с киберпреступностью. Цель работы — выявить правовые механизмы сопряжения международно-правовых норм с задачами охраны национальных интересов. Методическую основу составили анализ научных публикаций, сравнительно-правовой анализ, классификация, обобщение и логико-аналитическое толкование. Корпус исследования образован десятью русскоязычными публикациями 2024–2026 гг. Аналитическая часть раскрывает устройство нормативных связей между суверенитетом, безопасностью и международным регулированием. Практическая ценность связана с применением выводов при подготовке статей, учебных курсов и экспертных материалов по международному публичному праву.

Ключевые слова: международное право, национальная безопасность, государственный суверенитет, международная информационная безопасность, цифровой суверенитет, киберпространство, санкционные режимы, международное сотрудничество, правовые механизмы, ООН.

Введение

Актуальность темы определяется тем, что безопасность давно перестала ограничиваться военной сферой. Правовое поле охватывает информационные сети, критическую инфраструктуру, трансграничные данные, санкционные ограничения, международное сотрудничество правоохранительных органов и договорные исключения, связанные с защитой национальных интересов. На таком фоне международное право перестраивается под давление новых рисков, а национальные правопорядки усиливают защитные конструкции, не выходя за пределы международной легитимности. Наиболее заметное смещение произошло в цифровой плоскости, где спор о пределах суверенитета, допустимых мерах реагирования и формах многостороннего согласования приобрел устойчивый доктринальный характер.

Цель исследования — выявить правовые механизмы взаимодействия международного права и национальной безопасности в современных условиях. Поставлены три задачи:

1) систематизировать каналы правового сопряжения международных норм с внутригосударственным регулированием безопасности.

2) Раскрыть зоны напряжения, возникающие при охране суверенитета, цифровой инфраструктуры, экономических интересов и процессуальных гарантий.

3) Определить направления доктринального упорядочения изучаемой сферы на базе современного корпуса русскоязычной литературы.

Научная новизна работы связана с объединением в одном аналитическом поле нескольких обычно разнесенных линий исследования: стратегии национальной безопасности, нормотворчества ООН в киберсфере, цифрового суверенитета, санкционного давления на международные процедуры и международно-правовой квалификации действий в киберпространстве. Подобная компоновка позволяет увидеть не разрозненный набор специальных режимов, а целостную систему правового согласования суверенных интересов и международных обязательств.

Материалы и методы

Материалы. В исследовательский корпус вошли публикации, раскрывающие разные уровни изучаемой проблемы. А. Ассаф [1] анализирует нарушение суверенитета в киберпространстве через нормы Устава ООН; А.И. Бедаев [2] рассматривает правовую линию Европейского союза в сфере международной информационной безопасности; В.И. Булва [3] прослеживает переход от классической дипломатии к сетевым форматам регулирования; Н.Ю. Жуковская, Е.В. Калинина, А.М. Радолин [4] систематизируют этапы формирования правовых основ международной информационной безопасности в формате ООН; А.Г. Игнатьев [5] исследует проблему фрагментации Интернета на площадке ООН; С.В. Коротков [6] разбирает пределы применения оговорок о национальной безопасности в инвестиционном арбитраже; А.А. Мохов [7] раскрывает правовую природу Стратегии национальной безопасности и перспективы развития законодательства; Цзян Сыюань, Сунь Чэнь [8] обращаются к правовой охране цифрового суверенитета в рамках ШОС; А.К. Чоботова, Д.Д. Холматов [9] изучают влияние санкций на процессуальную ткань международного арбитража; Д.Д.

Штодина [10] оценивает Конвенцию ООН против киберпреступности 2024 г. как результат сложного переговорного компромисса.

Методы. Методическая база охватывает анализ научных публикаций, сравнительно-правовой анализ, классификацию, обобщение, синтез и логико-аналитическое толкование. Применение названных методов позволило сопоставить универсальные и региональные модели правового регулирования, выделить устойчивые группы механизмов и установить, где проходит граница между допустимой защитой национальных интересов и размыванием международно-правовых ограничителей.

Результаты

Взаимодействие международного права и национальной безопасности формируется как многослойная система, где нормы разных уровней не изолированы друг от друга. Внутригосударственные акты стратегического планирования задают язык национальных интересов и приоритетов, международные площадки производят нормы координации и стандарты поведения, а специальные правовые режимы регулируют действия государств в кризисных ситуациях. В научной литературе подобная связка раскрывается через сочетание стратегического законодательства, дипломатических процедур, режимов информационной безопасности и механизмов юридической ответственности [3; 4; 7; 8].

Первая группа правовых механизмов связана с внутренним закреплением национальных интересов и последующим выводом таких интересов на международный уровень. В работе А.А. Мохова Стратегия национальной безопасности рассматривается как программный нормативный ориентир для развития законодательства о безопасности [7]. Подобная постановка вопроса значима по двум линиям. С одной стороны, формируется внутренняя система приоритетов, компетенций и направлений правотворчества. С другой стороны, внешнеполитическая и договорная активность получает ясную нормативную опору. На цифровом направлении подобная логика усиливается: публикации В.И. Булвы и Цзян Сыюань, Сунь Чэнь показывают, что безопасность все чаще связывается с сетевой инфраструктурой, данными, платформами и цифровым суверенитетом [3; 8].

Вторая группа механизмов складывается вокруг универсальных международных процедур. Н.Ю. Жуковская, Е.В. Калинина, А.М. Радолин прослеживают, как площадка ООН последовательно вырабатывала основы международной информационной безопасности — от раннего обсуждения угроз до более оформленных переговорных форматов [4]. А.Г. Игнатьев, обращаясь к теме фрагментации Интернета, показывает, что дискуссия в ООН уже не ограничивается вопросами технической совместимости: предметом обсуждения становятся суверенизация сетевых сегментов, управление инфраструктурой и соотношение глобальной связности с национальным регулированием [5]. Д.Д. Штодина рассматривает Конвенцию ООН против киберпреступности 2024 г. как итог сложного согласования интересов государств, стремившихся совместить расширение сотрудничества с сохранением суверенного контроля над уголовно-правовыми и процессуальными инструментами [10]. В совокупности названные работы позволяют выделить универсальный договорно-процедурный механизм, где безопасность обеспечивается через переговоры, координацию, выработку терминологии и закрепление процедур правовой помощи [4; 5; 10].

Третья группа механизмов раскрывается на региональном уровне. А.И. Бедаев исследует правовую линию Европейского союза, где международная информационная безопасность проходит через сеть институтов, актов и специальных программ, ориентированных на защиту критической инфраструктуры и унификацию киберполитики [2]. Иная модель просматривается в работе Цзян Сыюань и Сунь Чэнь, где цифровой суверенитет государств — членов ШОС осмыслен как правовая ценность, требующая отдельной охраны, согласования национальных режимов и недопущения цифровой гегемонии [8]. Сопоставление двух моделей позволяет сделать вывод: региональные объединения формируют не единый, а дифференцированный набор средств, где одна линия тяготеет к институциональной унификации, другая — к усилению суверенной автономии при сохранении кооперации [2; 8].

Четвертая группа механизмов относится к международно-правовой квалификации поведения государств в киберпространстве. А. Ассаф связывает проблему суверенитета с вопросом о том, подпадают ли посягательства на киберинфраструктуру и данные под режимы запрета силы и невмешательства по Уставу ООН [1]. Из подобного подхода вытекает принципиальный вывод: правовая оценка цифрового инцидента зависит не от одной лишь технической формы атаки, а от степени затрагивания функций государства, инфраструктуры и способности публичной власти осуществлять свои полномочия. Названная линия дополняется публикацией Д.Д. Штодиной [10], где борьба с киберпреступностью осмыслена уже не как внутреннее дело отдельного государства, а как предмет международно-правового сотрудничества с процедурно оформленными каналами взаимной помощи. Следовательно, защита национальной безопасности в цифровой среде проходит одновременно через нормы о суверенитете, запрете вмешательства и договорные формы уголовно-правовой кооперации [1; 10].

Пятая группа механизмов связана с использованием аргумента национальной безопасности в международных экономических и процессуальных режимах. С.В. Коротков, анализируя инвестиционный арбитраж, показывает, что оговорки о защите национальной безопасности порождают спор о стандарте контроля над решениями государства и о пределах арбитражного пересмотра [6]. А.К. Чоботова и Д.Д. Холматов рассматривают санкционные ограничения уже в плоскости процессуальной целостности арбитража: под удар попадают финансирование спора, выбор представителей, нейтральность процедуры и исполнимость решений [9]. На таком материале отчетливо видно, что язык безопасности выходит далеко за пределы классического публичного права и начинает перестраивать международные частноправовые механизмы разрешения споров [6; 9].

Особое место занимает дипломатико-правовое измерение международной информационной безопасности. В.И. Булва связывает развитие российской линии с переходом к сетевой дипломатии [3], а Н.Ю. Жуковская, Е.В. Калинина, А.М. Радолин показывают последовательность формирования правовых основ в формате ООН [4]. При соединении с наблюдениями А.Г. Игнатьева о фрагментации Интернета [5] и с оценкой Д.Д. Штодиной новой конвенционной стадии [10] возникает более широкая картина: современное регулирование движется от политико-декларативных форм к более плотным процедурам согласования, где безопасность, связность сети, юрисдикция и суверенитет обсуждаются в одном нормативном поле.

По сумме рассмотренных работ взаимодействие международного права и национальной безопасности предстает как режим постоянного согласования суверенной дискреции и внешних юридических ограничителей. Исследованный корпус литературы позволяет выделить три опорных узла такой конструкции: внутреннее стратегическое нормирование [7], международное и региональное

производство правил безопасности [2–5; 8; 10], специальные механизмы реагирования в киберсфере, санкционной политике и международном арбитраже [1; 6; 9]. Сопряжение названных узлов образует правовую матрицу современного обеспечения безопасности, где суверенитет сохраняет исходное значение, но уже не мыслится вне договорных процедур, кооперации и международной правовой оценки действий государства.

Обсуждение

Сопоставление исследованных публикаций позволяет увидеть две крупные линии доктринального движения. Первая опирается на универсалистскую логику: безопасность нуждается в многостороннем согласовании, в единых процедурах, в институциональной памяти ООН и в расширении международной правовой помощи. Подобный ход мысли прослеживается в работах о нормотворчестве ООН, сетевой дипломатии, фрагментации Интернета и конвенционном оформлении борьбы с киберпреступностью. Вторая линия тяготеет к усилению суверенного измерения: приоритет получает охрана национального сегмента цифровой среды, защита внутренней компетенции государства, развитие собственных стратегий безопасности и более жесткая правовая реакция на внешнее давление. Обе линии не исключают друг друга, но задают разные центры тяжести.

Существенное расхождение проходит по вопросу о мере допустимой автономии государства. В публикациях, связанных с киберпространством и цифровым суверенитетом, усиливается стремление придать государству более широкий объем правовой самозащиты. Напротив, исследования, посвященные международным процедурам и арбитражу, подчеркивают риск чрезмерного расширения оговорок о национальной безопасности, поскольку подобная практика снижает предсказуемость правоприменения и осложняет контроль над мерами государства. На стыке названных позиций возникает центральная проблема современной доктрины: где проходит юридическая граница между правомерной самозащитой и размыванием международных ограничителей.

Ограниченность современного корпуса исследований связана с высокой фрагментацией предметного поля. Одна группа работ сосредоточена на стратегических документах и национальном законодательстве, другая — на киберпространстве, третья — на санкциях и международном арбитраже. Из-за такой специализации редко появляется единая схема, способная совместить внутригосударственное стратегическое регулирование, международное нормотворчество, цифровой суверенитет и процессуальные последствия санкционного давления. Пробел особенно заметен там, где требуется связать правовую квалификацию цифрового инцидента с последующими процедурами международного сотрудничества и с механизмами защиты прав участников спора.

Еще одна лакуна касается критериев правовой оценки. В литературе просматривается согласие относительно того, что цифровая среда уже вошла в сферу безопасности, но единые юридические пороги для квалификации вмешательства, недопустимого давления, санкционного воздействия и допустимых исключений разработаны не полностью. Отсюда вытекает нестабильность терминологии, различие в подходах к суверенитету и неодинаковая плотность международных процедур в смежных сегментах регулирования. Наиболее устойчиво оформлена линия международного сотрудничества по борьбе с киберпреступностью, менее оформлена — линия квалификации кибероперации как нарушения суверенитета или невмешательства, еще более спорна — линия влияния санкций на частноправовые и арбитражные процедуры.

Заключение

Первая задача исследования решена через выделение основных правовых механизмов сопряжения международного права и национальной безопасности. К ним отнесены внутреннее стратегическое нормирование, универсальные и региональные процедуры международного согласования, специальные режимы цифровой безопасности, договорные формы сотрудничества по борьбе с киберпреступностью, оговорки о национальной безопасности и процессуальные конструкции международного арбитража.

Вторая задача раскрыта через анализ зон напряжения. Наиболее остро противоречия проявляются при правовой охране суверенитета в киберпространстве, при фрагментации сетевой среды, при регионализации режимов цифровой безопасности и при переносе аргумента национальной безопасности в сферу санкций и международного разрешения споров. Названные линии показывают, что современное право безопасности развивается не по модели изолированного отраслевого массива, а через пересечение публично-правовых и частноправовых процедур.

Третья задача решена путем определения направления дальнейшего доктринального упорядочения темы. Перспективной представляется модель, при которой суверенное усмотрение государства сочетается с более ясными международными критериями квалификации цифровых инцидентов, с процедурно оформленным сотрудничеством и с сохранением юридических гарантий в трансграничных спорах. Подобный подход лучше всего соответствует логике исследованного корпуса литературы и позволяет связать национальную безопасность с международной легитимностью без разрыва между внутренним и внешним правовым регулированием.

Литература

1. Ассаф А. Нарушение государственного суверенитета в «киберпространстве»: взгляд через призму Устава ООН // Журнал ВШЭ по международному праву. 2024. Т. 1, № 3. С. 4–20. DOI: 10.17323/jil.2023.18848.

2. Бедаев А.И. Международная информационная безопасность в рабочей повестке Евросоюза: угрозы, направления работы и проблемы // Caspium Securitatis: журнал каспийской безопасности. 2024. Т. 4, № 1. С. 11–22.

3. Булва В.И. Международная информационная безопасность: от классической к сетевой дипломатии России // Вестник Санкт-Петербургского университета. Международные отношения. 2024. Т. 17, вып. 3. С. 325–341. DOI: 10.21638/spbu06.2024.306.

4. Жуковская Н.Ю., Калинина Е.В., Радолин А.М. Формирование правовых основ обеспечения международной информационной безопасности в формате ООН: этапы и результаты // Международное право и международные организации. 2024. № 4. С. 74–86. DOI: 10.7256/2454-0633.2024.4.72650.

5. Игнатьев А.Г. Фрагментация Интернета в повестке Организации Объединенных Наций // Журнал ВШЭ по международному праву. 2025. Т. 3, № 1. С. 98–114. DOI: 10.17323/jil.2025.27032.

6. Коротков С.В. Неточное решение: применение стандарта оценки к вопросам определения и реализации мер по защите интересов национальной безопасности в споре Майкл Энтони Ли-Чин против Доминиканской Республики // Журнал ВШЭ по международному праву. 2024. Т. 1, № 4. С. 92–101. DOI: 10.17323/jil.2023.19792.

7. Мохов А.А. Стратегия национальной безопасности Российской Федерации: правовой взгляд на содержание и перспективы развития законодательства о национальной безопасности // Вестник Российской правовой академии.

2024. № 2. С. 98–108. DOI: 10.33874/2072-9936-2024-0-2-98-108.

8. Цзян Сыюань, Сунь Чэнь. Система правовой охраны цифрового суверенитета государств — членов Шанхайской организации сотрудничества // Вестник Санкт-Петербургского университета. Право. 2025. Т. 16, № 2. С. 572–584. DOI: 10.21638/spbu14.2025.219.

9. Чоботова А.К., Холматов Д.Д. Влияние санкций на процессуальные аспекты арбитража // Журнал ВШЭ по международному праву. 2026. Т. 3, № 4. С. 56–74. DOI: 10.17323/jil.2025.31994.

10. Штодина Д.Д. Конвенция Организации Объединенных Наций против киберпреступности 2024 года — итог «киберкомпромисса»? // Московский журнал международного права. 2025. № 1. С. 110–124. DOI: 10.24833/0869-0049-2025-1-110-124.

The interaction of international law and national security: legal mechanisms and contemporary challenges

Chebotareva I.Yu., Alkesov R.T., Khlebnikova A.A., Mamisheva Z.A.

Adyghe State University, Maikop State Technological University, Krasnodar Cooperative Institute, Russian University of Cooperation, ASU

This study examines the relationship between international law and national security through the lens of legal instruments applied at the universal, regional, and domestic levels. The relevance of this topic is driven by the expanding range of threats, the shift of a significant portion of conflicts to the digital environment, the intensification of sanctions pressure, and growing debates over the limits of state sovereignty. The scientific novelty lies in consolidating disparate areas of doctrine into a single analytical framework that jointly examines strategic regulation, international information security, digital sovereignty, sanctions regimes, and international cooperation in combating cybercrime. The goal of the study is to identify legal mechanisms for aligning international legal norms with the objectives of protecting national interests. The methodological basis consists of an analysis of scientific publications, comparative legal analysis, classification, generalization, and logical-analytical interpretation. The research body comprises 10 Russian-language publications published between 2024 and 2026. The analytical section explores the normative relationships between sovereignty, security, and international regulation. The practical value stems from applying the findings in the preparation of articles, training courses, and expert materials on public international law.

Keywords: international law, national security, state sovereignty, international information security, digital sovereignty, cyberspace, sanctions regimes, international cooperation, legal mechanisms, UN.

References

1. Assaf, A. “Violation of State Sovereignty in Cyberspace: A View Through the Prism of the UN Charter” // HSE Journal of International Law. 2024. Vol. 1, No. 3. pp. 4–20. DOI: 10.17323/jil.2023.18848.
2. Bedayev, A.I. “International Information Security on the EU Working Agenda: Threats, Areas of Work, and Challenges” // Caspium Securitatis: Journal of Caspian Security. 2024. Vol. 4, No. 1. pp. 11–22.
3. Bulva, V.I. “International Information Security: From Classical to Network Diplomacy of Russia” // Bulletin of St. Petersburg University. International Relations. 2024. Vol. 17, issue. 3. pp. 325–341. DOI: 10.21638/spbu06.2024.306.
4. Zhukovskaya N. Yu., Kalinina E. V., Radolin A. M. Formation of the Legal Foundations for Ensuring International Information Security in the UN Format: Stages and Results // International Law and International Organizations. 2024. No. 4. pp. 74–86. DOI: 10.7256/2454-0633.2024.4.72650.
5. Ignatiev A. G. Internet Fragmentation on the United Nations Agenda // HSE Journal of International Law. 2025. Vol. 3, No. 1. pp. 98–114. DOI: 10.17323/jil.2025.27032. Korotkov S.V. Inaccurate Decision: Application of the Standard of Evaluation to the Issues of Determining and Implementing Measures to Protect National Security Interests in the Dispute Michael Anthony Lee-Chin v. Dominican Republic // HSE Journal of International Law. 2024. Vol. 1, No. 4. pp. 92–101. DOI: 10.17323/jil.2023.19792.
6. Mokhov A.A. National Security Strategy of the Russian Federation: A Legal View of the Content and Prospects for the Development of National Security Legislation // Bulletin of the Russian Law Academy. 2024. No. 2. pp. 98–108. DOI: 10.33874/2072-9936-2024-0-2-98-108.
7. Jiang Siyuan, Sun Chen. The System of Legal Protection of the Digital Sovereignty of the Shanghai Cooperation Organization Member States // Bulletin of St. Petersburg University. Law. 2025. Vol. 16, No. 2, pp. 572–584. DOI: 10.21638/spbu14.2025.219.
8. Chobotova A.K., Kholmatov D.D. The Impact of Sanctions on the Procedural Aspects of Arbitration // HSE Journal of International Law. 2026. Vol. 3, No. 4, pp. 56–74. DOI: 10.17323/jil.2025.31994.
9. Shtodina D.D. The 2024 United Nations Convention against Cybercrime: the Result of a “Cybercompromise”? // Moscow Journal of International Law. 2025. No. 1, pp. 110–124. DOI: 10.24833/0869-0049-2025-1-110-124.