Дата поступления рукописи в редакцию: 13.05.2026 г.
Дата принятия рукописи в печать: 19.06.2026 г.
DOI: 10.24412/2224-9133-2026-5-34-39

ЗАРИФОВА Вероника Баходуровна,
Финансовый университет при Правительстве Российской Федерации Россия, Москва, магистр,
e-mail: nika.zarifova@yandex.ru

СЕЛЮКОВА Арина Андреевна,
Финансовый университет при Правительстве Российской Федерации Россия, Москва, магистр
e-mail: seluykovaa@gmail.com

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОТ ГЛОБАЛЬНОГО СОТРУДНИЧЕСТВА К НАЦИОНАЛЬНОЙ ПРАКТИКЕ

Аннотация. *Статья посвящена исследованию системы международных стандартов информационной безопасности в их взаимодействии с национальными правовыми режимами. Автор прослеживает эволюцию нормативного регулирования в сфере международной информационной безопасности (МИБ). Рассматриваются ключевые институциональные площадки выработки международных стандартов: Группа правительственных экспертов ООН (ГПЭ) и Рабочая группа открытого состава (РГОС). Особое внимание уделено сравнительному анализу национальных доктринальных документов (России, Казахстана, Беларуси, Вьетнама) в контексте их соответствия или отступления от международных ориентиров. Исследование выявляет устойчивое противоречие между стремлением к универсализации норм МИБ и суверенным правом государств на самостоятельное регулирование национального информационного пространства. Сделан вывод о постепенном складывании «мягкого» нормативного слоя в международном киберправе при сохраняющемся отсутствии юридически обязывающего универсального договора.*

Ключевые слова: *международная информационная безопасность, кибербезопасность, национальные стратегии, международное право, Конвенция о киберпреступности, информационное пространство.*

ZARIFOVA Veronika Bahodurovna,
Financial University under the Government of the Russian Federation Russia, Moscow
Master's degree

SELYUKOVA Arina Andreevna,
Financial University under the Government of the Russian Federation Russia, Moscow
Master's degree

INTERNATIONAL INFORMATION SECURITY STANDARDS: FROM GLOBAL COOPERATION TO NATIONAL PRACTICE

Annotation. *The article is devoted to the study of the system of international information security standards in their interaction with national legal regimes. The author traces the evolution of regulatory regulation in the field of international information security (IIB). The key institutional platforms for the development of international standards are considered: the UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG). Special attention is paid to the comparative analysis of national doctrinal documents (Russia, Kazakhstan, Belarus, Vietnam) in the context of their compliance or deviation from international guidelines. The study reveals a persistent contradiction between the desire for the universalization*

of the IIB norms and the sovereign right of states to independently regulate the national information space. The conclusion is drawn about the gradual formation of a "soft" regulatory layer in international cyber law, while the continued absence of a legally binding universal treaty.

Key words: *international information security, cybersecurity, national strategies, international law, Convention on Cybercrime, information space.*

Введение.

Переход человечества в цифровую эпоху породил угрозы, которых международное право прежде не знало. Государства, корпорации, отдельные граждане оказались уязвимы перед атаками, не признающими государственных границ. Именно эта реальность поставила перед юридическим сообществом вопрос, не имеющий пока убедительного ответа: как урегулировать поведение субъектов международного права в глобальном информационном пространстве?

Международная информационная безопасность – состояние глобального информационного пространства, при котором обеспечивается поддержание мира, безопасности и стабильности на основе общепризнанных принципов международного права и равноправного партнёрства. Формулировка кажется исчерпывающей, пока не начинаешь анализировать конкретные механизмы её реализации. Здесь и обнаруживается ключевая проблема: механизмы существуют, но их обязательная сила вызывает серьёзные сомнения.

Ещё в конце 1990-х годов Россия первой обозначила в рамках ООН «триаду» угроз, сопряжённых с использованием информационно-коммуникационных технологий, – военно-политических, криминальных и террористических. С тех пор международное сообщество ведёт переговоры, вырабатывает рекомендации, принимает резолюции. Универсальный юридически обязывающий договор по МИБ так и не появился. Вместо него возникла многоуровневая, нередко противоречивая система стандартов, рекомендаций и двусторонних соглашений.

Изучение этой системы – не академическое упражнение. Как справедливо подчёркивает А.К. Дубень, «особое внимание уделено интеграционному объединению» [1], поскольку именно через призму региональных структур – ШОС, БРИКС, СНГ, ОДКБ – государства ищут практические механизмы совместного реагирования на угрозы информационной безопасности. Между тем П.В. Агапов точно замечает: решение проблемы МИБ «не может быть достигнуто силами одного государства», что превращает международное сотрудничество из опции в необходимость [2].

Цель настоящего исследования – выявить и систематизировать закономерности формирования международных стандартов информационной безопасности, оценить эффективность их имплементации в национальных правовых системах и определить перспективы выработки универсального юридически обязывающего режима МИБ.

Поставленная цель предполагает решение следующих задач:

1. проследить эволюцию нормативного регулирования МИБ в системе ООН начиная с 1998 года;
2. охарактеризовать институциональные площадки, на которых вырабатываются международные стандарты в сфере кибербезопасности;
3. провести сравнительный анализ национальных доктринальных документов ряда государств в контексте их взаимодействия с международными нормами;
4. определить перспективы и препятствия на пути к созданию универсального договора по МИБ.

Методологическую основу исследования составляет диалектический подход к анализу международно-правовых отношений. Применялись общенаучные методы – индукция, дедукция, синтез и системный анализ. Среди специально-юридических методов использовались формально-юридический метод, необходимый для оценки нормативного материала; сравнительно-правовой, позволивший сопоставить законодательство различных государств; а также методы контент-анализа – при изучении международных резолюций, докладов экспертных групп и двусторонних соглашений.

1. Генезис международно-правового регулирования МИБ: от «триады» к конвенции

Отправная точка современного международно-правового регулирования МИБ – 1998 год. Именно тогда Россия внесла в Первый комитет Генеральной Ассамблеи ООН проект резолюции, в котором впервые была обозначена «триада» угроз, связанных с ИКТ: военно-политическое использование технологий, преступные цели и терроризм. Резолюция A/RES/53/70 была принята 4 декабря 1998 года – и с этого момента проблема МИБ не исчезает с повестки ГА ООН ни разу.

Значимость инициативы трудно переоценить. Россия фактически сформулировала понятийный аппарат нарождавшейся отрасли: «информационное пространство», «информаци-

онное оружие», «критически важные структуры» – термины появились в докладе Генерального секретаря ООН от 10 июля 2000 года именно в том виде, в каком их предложила российская сторона.

Реакция западных партнёров, однако, оказалась сдержанной. На протяжении почти двенадцати лет после 1999 года вопрос о выработке принципов МИБ в резолюциях ГА ООН не ставился в явном виде – прежде всего потому, что США не желали брать на себя обязательства, способные ограничить военный потенциал в киберпространстве. Как констатируют Н. Ю. Жуковская, Е. В. Калинина и А. М. Радолин, «государства-лидеры технологического развития не стремятся брать на себя обязательства по ограничению собственного господства в инфосфере» [3]. Вывод остаётся актуальным и сегодня.

Перелом наметился в 2010-х годах. В итоговых докладах Группы правительственных экспертов 2010, 2013 и 2015 годов, принятых консенсусом, закреплялись базовые принципы сотрудничества государств в области МИБ. Прорывным стал доклад 2015 года: 11 добровольных норм ответственного поведения государств в информационном пространстве вошли в свод рекомендованных ООН правил, закреплённых в резолюции ГА № 73/27.

Добровольность – принципиальное слово. Нормы не являлись обязывающими. Международное право ещё не выработало инструментов принуждения к их соблюдению. Но сам факт консенсусного принятия означал: государства признали наличие общего интереса в мирном использовании ИКТ.

Работа последней ГПЭ (2018–2021) оказалась безрезультатной: «участники разошлись во взглядах на применимость международного права к действиям государств в инфопространстве». Именно тогда Россия выступила с инициативой создания принципиально новой площадки – Рабочей группы открытого состава (РГОС), к участию в которой приглашаются все 193 государства – члена ООН. Первый состав РГОС завершил работу в марте 2021 года, и итоговый доклад был принят консенсусом. Практическим достижением РГОС стало учреждение межправительственного реестра контактных пунктов по обмену информацией о компьютерных атаках – механизма скромного, но вполне реального.

На этом фоне принятие в декабре 2024 года резолюцией 79/243 ГА ООН Конвенции ООН против киберпреступности выглядит подлинным прорывом – первым универсальным договором в сфере МИБ за всю историю обсуждений. Конвенция направлена на укрепление международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных систем, а также на обмен электронными доказательствами по серьёзным уголовным делам. Б. В. Сангаджиев и К. В. Сангаджиева справедливо усматривают в появлении подобных инструментов подтверждение тезиса о том, что «решение проблемы обеспечения информационной безопасности не может быть достигнуто силами одного государства» [4].

2. Институциональная архитектура: кто вырабатывает стандарты?

Архитектура международного регулирования МИБ многоуровнева. На универсальном уровне ключевую роль играют ГА ООН и её профильные структуры. Международный союз электросвязи (МСЭ) (специализированное учреждение ООН с 1947 года) внедряет обязательные и добровольные стандарты в области электросвязи. К началу 2023 года МСЭ принял свыше 1 тыс. Рекомендаций Сектора радиосвязи, 40 из которых обязательны для государств-членов. Вместе с тем в последние годы МСЭ всё сильнее втягивается в орбиту политического противостояния западных и незападных государств, что снижает его потенциал как нейтральной технической площадки.

На региональном уровне выделяется Европейское агентство по сетевой и информационной безопасности (ENISA), занимающееся разработкой превентивных мер, поддержкой совместного реагирования на трансграничные инциденты и содействием в создании систем кибербезопасности государств – членов ЕС. Директива ЕС о безопасности сетей и информационных систем (NIS Directive) установила требования к защите критической инфраструктуры, обязав государства-члены принимать конкретные меры по защите информационных систем.

Особое место в системе региональных механизмов занимают интеграционные объединения с участием России. В рамках ОДКБ ещё в 2017 году вступило в силу Соглашение о сотрудничестве в области обеспечения информационной безопасности, нацеленное на выработку практических механизмов совместного реагирования на угрозы. А. К. Дубень констатирует: «информационная безопасность каждого государства формирует общую безопасность и непосредственно влияет на состояние коллективной безопасности» [1]. Логика прослеживается и в документах СНГ – с 2013 года в рамках Содружества действует соглашение в области обеспечения информационной безопасности, а современные международные программы в сфере кибербезопасности содержат базовые положения, выработанные именно в соглашениях СНГ.

Двусторонние соглашения образуют отдельный пласт нормативного регулирования. К настоящему времени подписано более 20 соглашений о сотрудничестве в области МИБ. Их совокупная роль – не только правовое обеспечение информационной безопасности, но и унификация технических стандартов при создании и эксплуатации интегрированных информационных систем. Как справедливо заключает А. К. Дубень, «международное сотрудничество в рамках исследуемого вопроса основано на принципе социальной ответственности» [1], а взаимодействие осуществляется в целях восполнения пробелов в нормативном регулировании киберсреды.

3. Национальные стратегии

Государства разрабатывают национальные стратегии информационной безопасности, воспринимая международные стандарты через призму собственных политических приоритетов. Сравнение доктринальных документов ряда государств позволяет выявить как общие тенденции, так и принципиальные различия в подходах.

Российская Доктрина информационной безопасности 2016 года определяет стратегические цели и основные направления обеспечения МИБ через призму национальных приоритетов. Три ключевых направления – противодействие использованию ИКТ для пропаганды экстремизма, защита критической информационной инфраструктуры и пресечение деятельности, наносящей ущерб национальной безопасности, – прямо корреспондируют с «триадой» угроз, сформулированной Россией ещё в 1998 году.

Опыт Казахстана заслуживает отдельного внимания. Согласно Концепции кибербезопасности республики, «деятельность публичных органов в первую очередь направлена на автоматизацию и цифровизацию государственных услуг» [5]. Казахстан – одна из немногих стран, располагающих специализированным Центром мониторинга безопасности, выявляющим кибератаки и уязвимости критических объектов. Информационная доктрина 2023 года закрепила обеспечение безопасности единого информационного пространства в числе базовых приоритетов государственной политики.

Республика Беларусь пошла по пути формирования Концепции информационной безопасности, в которой государство выступает гарантом защиты информационных прав граждан. Характерная черта белорусского подхода – акцент на смарт-проектировании решений по безопасности объектов компьютерной инфраструктуры и развитии аудита государственных систем на основе собственных стандартов. В 2023 году в рамках Союзного государства была утверждена совместная Концепция информационной безопасности, предусматривающая защиту цифрового и информационного пространства Беларуси и России. Концепция закладывает основы согласованной политики и выработки мер по совершенствованию систем обеспечения информационной безопасности обоих государств.

Показателен случай Вьетнама. До 2019 года страна не располагала комплексным нормативным актом в сфере кибербезопасности. Принятый Закон о кибербезопасности вызвал критику со стороны США и Канады – в частности, посольство США указывало, что закон может привести к большим проблемам для будущего обеспечения кибербезопасности. При этом, как обращает внимание А.В. Минбалеев, вьетнамская система обеспечения информационной безопасности уже используется рядом государств при формировании национальных систем кибербезопасности, определяя «эффективный способ обеспечения критически важных информационных ресурсов от кибератак» [6]. Противоречие между западной критикой и практической востребованностью вьетнамской модели весьма показательно: оно обнажает политическое измерение, неотделимое от якобы технических споров о стандартах.

Сравнительный анализ выявляет устойчивую закономерность, которую фиксируют Б. В. Сангаджиев и К. В. Сангаджиева: в России акцент делается на государственном контроле и регулировании, тогда как в США и ЕС значительное внимание уделяется сотрудничеству с частным сектором и международными организациями. Различие в подходах – не просто технический вопрос: оно отражает принципиально разные концепции суверенитета в информационном пространстве.

4. Противоречия в системе МИБ

Барьер на пути к универсальному соглашению по МИБ носит не технический, а политический характер. Три проекта конвенции ООН об обеспечении МИБ, внесённых Россией в 2011, 2021 и 2023 годах, раз за разом встречали сопротивление западных государств.

Н. Ю. Жуковская, Е. В. Калинина и А. М. Радолин называют три узловых противоречия, препятствующих консенсусу. Первое – вопрос о запрете использования ИКТ в военно-политических целях: «Вашингтон неизменно отвергает любые обязательства, способные ограничить его потенциал в киберпространстве» [3]. Второе – проблема атрибуции кибератак: отсутствие согласованной методологии позволяет государствам уклоняться от ответственности, прикрывая операции «под чужим флагом». Третье – разногласия в толковании базовых терминов: понятия

«информационное оружие», «информационная война», «критически важные структуры» трактуются государствами по-разному.

К этим трём следует добавить четвёртое противоречие, не менее существенное: несовпадение взглядов на роль государства в управлении интернетом. Отказ США подписать на саммите в Дубаи (2012) договор о праве государств на участие в управлении сетью – наглядное тому подтверждение.

Противоречия сохраняются. Начатая 24 февраля 2022 года специальная военная операция России на Украине резко сузила переговорное пространство: она «положила конец возможности взаимодействия с США и их западными партнёрами по выработке договорённости в сфере МИБ» [3], констатируют Н. Ю. Жуковская, Е. В. Калинина и А. М. Радолин. С другой стороны, именно в этот период резко возросло число кибератак на российскую критическую инфраструктуру, что лишний раз подтверждает: информационное противостояние стало неотъемлемой частью современных геополитических конфликтов.

Ю.В. Косов точно формулирует суть проблемы: «глобальные информационные системы – новая сфера для столкновения национальных интересов – потребовали от органов государственного управления инновационных подходов к противодействию угрозам информационной безопасности» [7]. Инновационных подходов требует и международное право – но выработать их в условиях глубокого геополитического раскола крайне сложно.

5. Мягкое право как временное решение и его пределы

В отсутствие обязывающего универсального договора международное сообщество выстраивает систему МИБ на основе инструментов «мягкого права»: добровольных норм, руководящих принципов, рекомендаций и резолюций. Итоговый доклад РГОС 2021 года, принятый консенсусом всех 193 государств, – наглядное воплощение этой логики.

Потенциал «мягкого права» не следует недооценивать. Нормы, изначально лишённые обязательной силы, нередко получают её со временем: достаточно вспомнить, как рекомендательные акты в области прав человека постепенно приобретали статус обычных норм международного права. Те же процессы (пусть и медленнее) идут в сфере МИБ. Добровольные нормы ответственного поведения государств, закреплённые в докладах ГПЭ и резолюциях ГА ООН, получают признание в дипломатических, политических и академических кругах.

Вместе с тем пределы «мягкого права» очевидны. Ни одно государство не обязано соблюдать добровольные нормы, если политическая конъюнктура складывается иначе. Атрибуция кибератак по-прежнему остаётся предметом политических манипуляций. Механизмов ответственности нет. И.А. Горбунов прямо указывает: «трансграничный характер угроз информационной безопасности формирует неоспоримую потребность в консолидации сил различных стран для противодействия таким угрозам» [8] – но именно эта консолидация остаётся недостижимой без юридически обязывающих инструментов.

Заключение

Международные стандарты информационной безопасности сложились как разветвлённая, многоуровневая система – и остаются принципиально незавершёнными. Двадцать шесть лет переговоров в рамках ООН дали ощутимые результаты: согласованную терминологию, добровольные нормы ответственного поведения государств, институциональные площадки для диалога, наконец – первую универсальную конвенцию против киберпреступности. Всё это – реальные достижения.

Но ключевой задачи – выработки юридически обязывающего универсального договора по МИБ – мировое сообщество не решило. Причины носят не технический, а политический характер: государства, располагающие наибольшим потенциалом в киберпространстве, не заинтересованы в самоограничении.

На национальном уровне государства движутся в сторону более детального доктринального оформления своей политики в сфере информационной безопасности. Россия, Казахстан, Беларусь, Вьетнам – при всём различии конкретных подходов – следуют общей логике: информационная безопасность рассматривается как стратегическое направление обеспечения национальной безопасности. Эта тенденция устойчива и, по всей видимости, необратима.

Перспективы развития МИБ определяются двумя конкурирующими векторами. С одной стороны – нарастающая взаимозависимость государств в информационном пространстве создаёт объективные стимулы к сотрудничеству: ни одна страна не застрахована от кибератак, а их последствия давно вышли за рамки отдельных государств. С другой – геополитическое противостояние, в котором информационные технологии занимают всё более заметное место, подталкивает к фрагментации глобального информационного пространства.

Выход из этого противоречия – постепенное наращивание обязательного нормативного слоя: сначала на уровне региональных соглашений, затем – через трансформацию добровольных норм в обычное международное право. Путь долгий. Но альтернативы – регулирование киберпространства как «пространства без права» – международное сообщество позволить себе не может.

Список литературы:

[1] Дубень А. К. Международные аспекты информационной безопасности России в условиях глобализации // Образование и право. – 2023. – №. 11. – С. 75-79.

[2] Агапов П. В., Ефремова М. А. Международно-правовые основы обеспечения информационной безопасности участников содружества независимых государств // Юридическая наука и правоохранительная практика. – 2015. – №. 1 (31). – С. 176-182.

[3] 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.

[4] Сангаджиев Б. В., Сангаджиева К. В. Международно-правовые основы обеспечения информационной безопасности // Образование и право. – 2024. – №. 8. – С. 23-27.

[5] Алиаскаров Р. Ж. Проблемы обеспечения информационной безопасности республики Казахстан в современных условиях // Universum: экономика и юриспруденция. – 2025. – Т. 1. – №. 4 (126). – С. 57-61.

[6] Минбалеев А.В. Правовое обеспечение кибербезопасности во Вьетнаме // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 1 (31). – С. 64-68.

[7] Косов Ю.В. Информационная безопасность и международное право II Управленческое консультирование. – 2016. – №3 (87). – С. 209-211.

[8] Горбунов И.А. Информационная безопасность: международно-правовые аспекты ее обеспечения // Международное право. – 2024. – №1. – С. 29-38.

References:

[1] Duben A.K. International aspects of information security of Russia in the context of globalization//Education and law. – 2023. – №. 11. - S. 75-79.

[2] Agapov P.V., Efremova M.A. International legal framework for ensuring information security of members of the Commonwealth of Independent States//Legal science and law enforcement practice. – 2015. – №. 1 (31). - S. 176-182.

[3] Zhukovskaya N. Yu., Kalinina E. V., Radolin A. M. Formation of the legal framework for ensuring international information security in the UN format: stages and results//International law and international organizations. – 2024. – №. 4. - S. 74-86.

[4] Sangadzhiev B.V., Sangadzhieva K.V. International legal framework for ensuring information security//Education and law. – 2024. – №. 8. - S. 23-27.

[5] Aliaskarov R. Zh. Problems of ensuring information security of the Republic of Kazakhstan in modern conditions//Universum: economics and jurisprudence. – 2025. - VOL. 1. – №. 4 (126). - S. 57-61.

[6] Minbaleev A.V. Legal support of cybersecurity in Vietnam//Bulletin of the Ural Federal District. Security in the information sphere. – 2019. – № 1 (31). - S. 64-68.

[7] Kosov Yu.V. Information Security and International Law II Management Consulting. – 2016. – №3 (87). - S. 209-211.

[8] Gorbunov I.A. Information security: international legal aspects of its provision//International law. – 2024. – №1. - S. 29-38.