УДК 341

Морекаев Е.А.
Студент, магистрант
Сибирский федеральный университет
г. Красноярск, Россия

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ПРЕДМЕТ ПРАВОВЫХ СОГЛАШЕНИЙ В РАМКАХ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА

Аннотация: *актуальность исследования обусловлена отождествлением информационной безопасности государства с национальной безопасностью в современных геополитических условиях. В статье анализируется процесс формирования международно-правовой архитектуры обеспечения международной информационной безопасности (МИБ) в рамках Шанхайской организации сотрудничества (ШОС) с участием Российской Федерации. Автор рассматривает правовые основы МИБ, включая региональные соглашения и акты «мягкого права», а также выявляют проблемы отсутствия универсального международного договора. Особое внимание уделяется нормам ответственного поведения государств в ИКТ-среде как перспективному механизму снижения глобальных угроз и стабилизации международных отношений.*

Ключевые слова: *международная информационная безопасность, информационная безопасность, Шанхайская организация сотрудничества, международное право, кибербезопасность, информационно-коммуникационные технологии.*

Morekaev E.A.
Student, Master's Degree Candidate
Siberian Federal University
Krasnoyarsk, Russia

INTERNATIONAL INFORMATION SECURITY AS A SUBJECT OF LEGAL AGREEMENTS WITHIN THE *SHANGHAI COOPERATION ORGANISATION*

Abstract: *the relevance of the study stems from the fact that in modern geopolitics, state information security is becoming virtually synonymous with national security. The article examines the formation of the international legal framework for international information security (IIS) within the Shanghai Cooperation Organization (SCO) involving the Russian Federation. The author analyzes the legal foundations of IIS, including regional agreements and soft law instruments, while identifying the challenges posed by the absence of a universal international treaty. Special attention is paid to voluntary, non-binding norms of responsible state behavior in the ICT environment as a promising mechanism for reducing global threats and stabilizing international relations.*

Keywords: *international information security, Shanghai Cooperation Organisation, international law, cybersecurity, information and communication technologies.*

В современном мире информационная безопасность государства фактически становится тождественной понятию национальной безопасности. Выработка консенсуса на уровне мирового сообщества является важным этапом в формирования архитектуры международного права по вопросам обеспечения международной информационной безопасности (далее – МИБ). Этот процесс находится в стадии становления для стран участниц Шанхайской организации сотрудничества (далее – ШОС). Учитывая угрозы и риски современной геополитики важным для научного анализа представляется исследование взаимодействия государств участников шанхайского соглашения, в состав которых входит и Российская Федерация, по вопросам и проблемам МИБ.

Методологическую основу исследования составляют общенаучные методы (анализ, синтез, сравнение), а также специальные методы, такие как системный подход, проблемный подход к исследуемому предмету, критический анализ проблем МИБ, научно-правовой и сравнительный анализ международных регламентов в области информационной безопасности стран-участниц ШОС.

В ФЗ «О безопасности» дано определение термина безопасность в качестве функции, как приоритета государства - положение, при котором от внешних и внутренних угроз защищены значимые для жизни интересы человека, общества, а также государства в целом [1]. В данном определении в понятие включены такие компоненты, как государство, общество, субъекты хозяйствования, социальные группы, общности, индивиды. М. А. Гундорова раскрывает содержание безопасности как вида деятельности, сущность которой определяется во время разрешения противоречий между объективной реальностью, содержащей компоненты угроз функционирования субъектов, нуждами субъектов, стремящихся избежать этих угроз, ограничении в ликвидации отрицательных результатов [2].

Легальное определение термина МИБ отсутствует в официальных документах Организации объединенных наций (далее – ООН). Однако это понятие закреплено в ряде региональных соглашений:

Во-первых, это соглашение между правительствами государств членов Шанхайской организации сотрудничества, о сотрудничестве в области обеспечения международной информационной безопасности. В нём МИБ определяется как «состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве» [3].

Во-вторых, основы государственной политики Российской Федерации в области международной информационной безопасности, утверждённые Указом Президента РФ от 12 апреля 2021 года №213. В них МИБ определяется как такое «…состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнёрства обеспечивается поддержание международного мира, безопасности и стабильности» [4].

Далее, в положениях «Правила поведения в области международной информационной безопасности», которые были представлены Российской Федерацией на рассмотрение Генеральной Ассамблеи ООН в 2015 году. В 2018 году свод правил поведения в области информационной безопасности был поддержан в качестве резолюции Генеральной Ассамблеи ООН [5].

Однако, по мнению некоторых авторов, достичь международного соглашения, как универсального и обязательного документа для стран-участников ООН, в сфере МИБ пока не удалось. Для выработки единых положений международного права в сфере МИБ является невозможность достичь консенсуса по таким вопросам, как запрет использования информационно-коммуникационных технологий (далее – ИКТ) в военно-политических целях, атрибуция кибератак, трактовка терминов сферы МИБ, определение национальных границ виртуального пространства и другие [6].

Авторы отмечают, что решением проблем глобальной информационной безопасности мировое сообщество занимается как на институциональном (в рамках отдельных международных организаций и структур), так и на конвенциональном (создание общих норм международного права) уровнях. Между тем, как показывает практика, длящийся уже четверть века процесс выработки взаимоприемлемых решений по способам обеспечения ответственного поведения государств в глобальном информационном пространстве пока далек от завершения т.к. «… государства−лидеры технологического развития не стремятся брать на себя обязательства по ограничению собственного господства в инфосфере» [6]. Однако, сам процесс выработки решений по обеспечению МИБ, способных удовлетворить интересы большого числа членов мирового сообщества, безусловно, заслуживает внимания. Его изучение позволяет:

а) определить позиции договаривающихся сторон;

б) установить содержание основных представлений о границах МИБ и способах ее обеспечения;

в) выявить слабые и сильные стороны достигнутых соглашений;

г) оценить итоги и перспективы договорного процесса.

МИБ как правовое понятие получило начало в российской системе права благодаря осознанию роли цифровизации в экономическом развитии страны и формировании информационного общества, изменение ситуации происходило быстро. В 1998 году была одобрена Концепция государственной информационной политики, включавшая задачи модернизации информационно-телекоммуникационной инфраструктуры, развития ИКТ, интеграции в мировое информационное пространство.

В Стратегии национальной безопасности среди национальных интересов указаны развитие безопасного информационного пространства и устойчивое развитие российской экономики на новой технологической основе, а к стратегическим национальным приоритетам отнесены информационная и экономическая безопасность, что включает обеспечение

технологического суверенитета, укрепление достигнутых лидирующих позиций и конкурентных преимуществ в сфере ИКТ, развитие радиоэлектронной промышленности, производства информационных технологий и оборудования, необходимых для решения задач в области цифровизации экономики и государственного управления [7].

Правовая основа МИБ в странах участницах ШОС включает ряд официальных документов:

№	Нормативный акт, год принятия	Значение для развития системы МИБ
1	Декларация глав государств-членов Шанхайской организации сотрудничества», 2005	впервые был упомянут информационный терроризм, что положило начало сотрудничеству в области информационной безопасности в рамках ШОС.
2	Заявление глав государств-членов ШОС по международной информационной безопасности, 2006	первый официальный документ ШОС в области информационной безопасности, который постановил создать группу экспертов по МИБ.
3	Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности, 2009	впервые на международно-правовом уровне зафиксировал наличие конкретных угроз в области информационной безопасности, а также определил основные направления, принципы, формы и механизмы сотрудничества в этой сфере
4	Заявление Совета глав государств-членов Шанхайской организации	Страны выступают за совершенствование механизма и мер по предотвращению межгосударственных конфликтов и

	сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности,2020 г	преодолению дефицита доверия между государствами. Подчёркивание необходимости достижения баланса между безопасностью и развитием. Страны требуют совместных усилий всех стран для обеспечения равной, справедливой и недискриминационной среды для ведения бизнеса в области новых технологий.
5	План взаимодействия государств-членов ШОС по вопросам обеспечения международной информационной безопасности на 2022-2023 годы, 2021	Включён в «Душанбинскую декларацию двадцатилетия ШОС. План был важен в условиях роста онлайн-активности и нарастания киберугроз. Выработка единых подходов и мер позволяла минимизировать риски и не допустить использования информационно-коммуникационных технологий в противоправных целях

По мнению Поляковой Т.А. процессы цифровой трансформации обусловливают необходимость «модернизации правовых подходов к урегулированию новых общественных отношений» [8].

А.В. Минбалеев указывает, что в современную цифровую эпоху методы правового регулирования должны быть достаточно гибкими и обеспечивать оперативную выработку системы способов и средств реагирования на новые угрозы и вызовы [9]. Эти выводы особенно значимы для международно-правового регулирования сферы МИБ, где традиционные правовые источники регулирования в виде международных договоров пока недостаточно развиты. В этой ситуации большое значение имеют принятие и

реализация иных международных актов в данной сфере, включая политико-декларативные документы и акты «мягкого права».

Одним из таких сводов международных правил выступают добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде. Данные нормы были отражены в докладах Группы правительственных экспертов ООН (ГПЭ) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

В Заключительном докладе ГПЭ от 18 марта 2021 г. A/75/816 государствам было рекомендовано «добровольно анализировать национальные усилия по применению норм, накапливать опыт и передовую практику в части применения норм и обмениваться ими» (п. 30) [10].

Следует обратить внимание, что в 2011 г. Россия, КНР, Таджикистан и Узбекистан представили Генеральной Ассамблее ООН Правила поведения в области обеспечения международной информационной безопасности [11]. В 2015 г. был направлен обновленный вариант этого документа. Полагаем, что указанный документ был учтен при подготовке итоговых докладов ГПЭ.

В Докладе ГПЭ сказано: «Добровольные, не имеющие обязательной силы нормы ответственного поведения государств могут уменьшить риски для международного мира, безопасности и стабильности и могут играть важную роль в повышении предсказуемости и уменьшении риска неправильного восприятия, способствуя тем самым предотвращению конфликтов» (п. 24).

При этом нормы не заменяют собой обязательства или права государств по международному праву, а содержат дополнительные указания в отношении того, что представляет собой ответственное поведение государств при использовании ИКТ (п. 25). Вместе с тем эксперты группы обозначают возможность разработки в перспективе дополнительных юридически обязывающих международно-правовых норм.

Также эксперты отметили, что «нормы отражают ожидания и стандарты международного сообщества в отношении поведения государств при использовании ими ИКТ и позволяют международному сообществу оценивать действия государств» (п. 24 Доклада ГПЭ). Таким образом, данные нормы, несмотря на отсутствие обязательной юридической силы, могут рассматриваться в качестве определенных стандартов, позволяющих давать политико-правовую оценку действиям государств в ИКТ-среде.

Система правового обеспечения международной информационной безопасности находится на стадии формирования. Действующие международные договоры в сфере борьбы с преступностью, терроризмом и иными угрозами международной безопасности только частично затрагивают вопросы безопасного использования ИКТ. До настоящего времени отсутствует базовый, универсальный международный договор в области МИБ, хотя имеется положительный опыт разработки подобных документов в рамках региональных организаций с участием России (ОДКБ, ШОС). В связи с этим требуется продвижение российской инициативы по принятию Конвенции об обеспечении международной информационной безопасности [12].

Параллельно необходимо сосредоточить усилия на развитии международно-правового регулирования МИБ в рамках региональных международных организаций с участием России (СНГ, ОДКБ, ШОС, БРИКС, Союзное государство), а также на двустороннем уровне.

В условиях отсутствия юридически обязательных международно-правовых актов в области МИБ существенная роль отводится иным механизмам нормативного регулирования, включая документы политического характера и акты «мягкого права». Одними из перспективных источников видятся добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде. Данные нормы еще не получили полноценного юридического закрепления, однако в дальнейшем они могут стать основой для принятия международно-правовых актов. Тем не менее

даже сейчас они способны обеспечить снижение угрозы международному миру, безопасности и стабильности.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // Собрание законодательства РФ. – 2011. – № 1.

2. Гундорова, М. А. Экономическая безопасность: учеб. пособие / М. А. Гундорова; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2020. – С.5.

3. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности. URL: http://rus.sectsco.org/documents/20090616/203974.html.

4. Указ Президента Российской Федерации от 12.04.2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» URL: http://www.kremlin.ru/acts/bank/46614

5. Международная информационная безопасность. Большая российская энциклопедия. - URL: https://bigenc.ru/c/mezhdunarodnaia-informatsionnaia-bezopasnost-8cb6ae

6. 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.

7. Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации»//Собрание законодательства РФ, 05.07.2021, N 27 (часть II), ст. 5351.

8. Полякова Т.А. Цифровизация и синергия правового обеспечения информационной безопасности // Информационное право. 2019. N 2. С. 4.

9. Цифровая трансформация: вызовы праву и векторы научных исследований: Моногр. / Под общ. ред. А.Н. Савенкова; Отв. ред. Т.А. Полякова, А.В. Минбалеев. М.: РГ-Пресс, 2021. С. 62.

10. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: 75 сессия Генассамблеи ООН URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/74/PDF/N2106874.pdf?openElement.
11. Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359. URL: https://digitallibrary.un.org/record/710973/files/A_66_359-RU.pdf.
12. Рогачев И.А. Перспективы дальнейшего развития ШОС: некоторые задачи и проблемы / Материалы Третьего заседания Форума ШОС, Китай, г. Пекин, 2008 г. URL: http://mgimo.ru/files/37535/kb-05_shos-Lukin.pdf.