Международное право
Правильная ссылка на статью:
Горбунов И.А. Информационная безопасность: международно-правовые аспекты ее обеспечения // Международное право. 2024. № 1. DOI: 10.25136/2644-5514.2024.1.70440 EDN: FQXKYN URL: https://nbpublish.com/library_read_article.php?id=70440

Информационная безопасность: международно-правовые аспекты ее обеспечения

Горбунов Игорь Андреевич

аспирант, кафедра Административного и финансового права, Российский университет дружбы народов

117198, Россия, г. Москва, ул. Миклухо-Маклая, 6

igoragor97@mail.ru

Статья из рубрики "Развитие отдельных отраслей международного публичного права"

DOI:

10.25136/2644-5514.2024.1.70440

EDN:

FQXKYN

Дата направления статьи в редакцию:

09-04-2024

Дата публикации:

16-04-2024

Аннотация: Актуальность рассматриваемой темы обусловлена глобализацией информационного пространства, возникающей в связи с интенсивным развитием информационных технологий, что предполагает необходимость разработки новых подходов к обеспечению информационной безопасности. На основании принципов суверенного равенства и международного сотрудничества государства взаимодействуют друг с другом в общем интересе (в том числе в правовом поле), разрабатывают базовые принципы и нормы, на которых основывается юридический фундамент правового обеспечения международной информационной безопасности. Автор констатирует, что важность реализации скоординированных мер участниками международно-правового взаимодействия в указанной сфере обуславливается тем, что если информационная безопасность является неотъемлемой частью национальной безопасности, то

международная информационная безопасность представляет собой имманентный элемент международной безопасности, без которого в современных реалиях невозможно выстроить систему безопасного межгосударственного сотрудничества. Автором в процессе исследования применен метод теоретического анализа, в основе выводов лежит формально логический метод. Основным выводом автора исследования является следующее положение: цели по поддержанию состояния защищенности глобального информационного пространства могут оказаться недостижимыми без должной кооперации (в частности, организационного и правового характера) в решении задач, связанных с обеспечением международной информационной безопасности на нескольких уровнях взаимодействия: двустороннем, региональном, общемировом. Высокий уровень взаимозависимости стран и необходимость обеспечения принципа неделимости безопасности формируют глобальную потребность в поиске компромиссов и единых подходов в обеспечении международной информационной безопасности. Определение единого понятийного аппарата, не допускающего двусмысленности, противоречий и терминологической неопределенности, а также базовых принципов, являющихся юридическим фундаментом правового регулирования обеспечения международной информационной безопасности, должно быть реализовано путем разработки единого международного договора. Подобный вывод обусловлен неэффективностью норм «мягкого права» и международной морали, основанных на принципах добровольного исполнения обязательств, реализуемых в процессе межгосударственного взаимодействия.

Ключевые слова:

угрозы информационной безопасности, цифровизация, международно-правовое взаимодействие, национальная безопасность, информационное пространство, глобальное информационное пространство, международные соглашения, геополитика, международные документы, межгосударственные декларации

Трансграничный характер угроз информационной безопасности формирует неоспоримую потребность в консолидации сил различных стран для противодействия таким угрозам, что в том числе связано с процессом цифровизации [1]. Каждое государство, защищая в первую очередь свои национальные интересы, стремится утвердить господство в информационном пространстве. Однако при этом информационная политика стран должна быть направлена не только на обеспечение их собственного информационного суверенитета, но и на осуществление данной политики таким образом, чтобы не нарушались национальные интересы других участников международно-правового взаимодействия. В таких условиях цели по поддержанию состояния защищенности глобального информационного пространства могут оказаться недостижимыми без должной кооперации (в частности, организационного и правового характера) в решении задач, связанных с обеспечением международной информационной безопасности на нескольких уровнях взаимодействия: двустороннем, региональном, общемировом.

Международно-правовые аспекты обеспечения информационной безопасности в условиях ныне существующих глобальных проблем и международных конфликтов представляют научный интерес как для политологов, так и для ученых-юристов. Проблемы, возникающие в указанной сфере, носят междисциплинарный характер и включают в себя «блок теоретико-методологических правовых вопросов применения норм, правил и принципов ответственного поведения государств, призванных

способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды» [2].

Проблемы международно-правового регулирования обеспечения информационной безопасности усугубляются не только желанием каждой из сторон международно-правовых отношений утвердить свое исключительное господство в информационном пространстве и обеспечить прежде всего защиту своего информационного суверенитета, но и тем, что в настоящий момент на международно-правовом уровне отсутствует единый документ, комплексно регулирующий вопросы международной информационной безопасности, в том числе определяющий ответственность государств за ведение дестабилизирующей информационной политики.

Интересной представляется инициатива Российской Федерации, представившей в 2021 году обновленный вариант концепции Конвенции ООН об обеспечении международной информационной безопасности. Указанный документ так и не был принят ввиду противодействия США и ряда европейских стран. Подобное поведение стран Запада диктуется наличием противоречий и сложностью в достижении соглашения между интересами крупных геополитических субъектов, каждый из которых стремится занять наиболее доминирующую позицию в глобальном информационном пространстве.

В целом стоит отметить, что позиция Российской Федерации в вопросах разработки международных принципов и механизмов обеспечения информационной безопасности является довольно активной. Еще в 1998 году по представлению Российской Федерации Генеральной Ассамблеей ООН была принята Резолюция A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которой были сформулированы угрозы международной информационной безопасности, реализуемые в трех целевых плоскостях – военно-политической, преступной и террористической (триада угроз). В 1999 году принята новая резолюция, в которой констатировалась возможность применения информационно-коммуникационных технологий в военной и гражданской сферах [3].

В настоящее время основной целью информационно-правовой деятельности России в ООН является продвижение идеи о необходимости принятия универсального юридически обязывающего документа, регулирующего вопросы информационной защищенности в общемировом масштабе. Так, 15 мая 2023 года Россия вместе с Белоруссией, КНДР, Никарагуа и Сирией внесла концепцию конвенции ООН об обеспечении международной информационной безопасности. Концептуальные основы указанного документа предполагают реализацию принципов суверенного равенства государств и невмешательства в их внутренние дела.

По мнению автора, потребность в принятии единого международного договора в сфере обеспечения международной информационной безопасности все еще является актуальной, в связи с чем следует поддержать активную роль России в реализации данной идеи с использованием международно-правовых механизмов и участием в интеграционных объединениях.

Фундаментальные правовые начала, на которых основывается система правового обеспечения информационной безопасности, должны быть закреплены в едином международном договоре, что, во-первых, станет заключительным этапом в достижении консенсуальных подходов между крупными субъектами международно-правовых отношений, во-вторых, будет способствовать единообразию в процедурах и механизмах обеспечения международной информационной безопасности. В связи с этим нельзя не

согласиться со следующим утверждением А.К. Дубеня: «основополагающие принципы в сфере обеспечения международной информационной безопасности требуют закрепления на общемировом уровне, так как наднациональный уровень правового обеспечения в масштабах региона, предполагающий участие нескольких (либо нескольких десятков) государств не может в полной мере удовлетворить потребность мирового сообщества в решении проблем международной информационной безопасности» [4].

Стоит отметить, что регулирование отношений в сфере обеспечения международной информационной безопасности осуществляется международными нормами общего характера, устанавливающими базовые принципы межгосударственного взаимодействия.

Устав Организации Объединенных Наций устанавливает ряд основополагающих целей и принципов, которые имеют отношение в том числе к сфере информационной безопасности (ст. 1, 2). Согласно утверждению Н.А. Молчанова и Е.К. Матевосовой, положения Устава ООН «не отвечают на многие вопросы обеспечения международной информационной безопасности, которые, надо признать, возникли перед стремящимся к всеобщему миру человечеству гораздо позднее принятия данного Устава» [5].

Тем не менее стоит признать, что ряд норм указанного документа имеют обширный предмет международно-правового регулирования. Так, принципы суверенного равенства, разрешения международных споров мирными средствами, неприменения силы или угрозы силой, а также иные принципы международного права, реализуемые в целях поддержания международного мира и безопасности, в равной степени относятся и к конфликтам между странами в информационной сфере.

Важным источником международно-правового регулирования обеспечения информационной безопасности является Окинавская хартия глобального информационного общества, в которой изложены официальные взгляды государств-участников группы G8 (в том числе России) на перспективы развития информационного общества в XXI веке. В указанном документе упоминаются проблемы, связанные с обеспечением международной информационной безопасности, например, отмечается, что «усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства» (п. 8). Также в Окинавской хартии уделяется особое внимание следующим вопросам:

1) защита интеллектуальных прав на информационные технологии;

2) защита частной жизни при обработке личных данных;

3) развитие и эффективное функционирование средств обеспечения безопасности и достоверности операций;

4) привлечение специалистов для защиты важных информационных инфраструктур.

В Тунисской программе для информационного общества от 15 ноября 2005 г. закреплен следующий комплекс действий, направленных реализацию принципов, ранее утвержденных:

1) защита безопасного, непрерывного и стабильного функционирования сети «Интернет», а также обеспечение безопасности при использовании ИКТ;

2) активизация международного сотрудничества и осуществление действий на внутригосударственном уровне с целью укрепления глобальной культуры

кибербезопасности;

3) защита детей и молодежи от растления и эксплуатации посредством использования ИКТ.

Некоторые отдельные аспекты международной информационной безопасности регулируются международными актами, затрагивающими сферу киберпреступности и информационных прав и свобод человека. В данном случае следует осознавать, что положения некоторых основополагающих международных договоров Совета Европы, в том числе Конвенции о защите прав человека и основных свобод не действуют в отношении Российской Федерации ввиду ее выхода из состава Совета Европы. Не вступая в дискуссию о политической обоснованности данного действия, автор считает нужным отметить, что многие из указанных актов, в том числе названная Конвенция содержали важные положения об информационных правах человека и информационной безопасности личности. Вместе с тем данные нормы также можно встретить в иных международных договорах, исполняемых Российской Федерацией.

Как справедливо отмечал В.А. Садовничий, «принятие норм безопасной деятельности в киберпространстве – императив нашего времени» [6]. Однако, учитывая наличие у каждой из стран своих национальных интересов и их нежелание отказываться от суверенитета в угоду международно-правовым договоренностям и компромиссу, достигнутому в целях решения глобальных проблем межгосударственного масштаба, все актуальнее становится вопрос о том, как должна регулироваться сфера обеспечения международной информационной безопасности. Большая часть ныне принятых документов в данной области носят рекомендательный характер, что, с одной стороны, является логичным результатом стремления государств к единоличному господству в информационном пространстве и нежеланием принимать на себя бремя обязательств, но, с другой стороны, показывает неэффективность действия норм «мягкого права» в сравнении с юридически обязывающими нормами.

Указанный вывод является еще одним явным свидетельством необходимости поддержания позиции России и ее союзников в принятии единого международного акта, на основании которого будут определены обязательства государств в сфере обеспечения международной информационной безопасности, так как рекомендательные нормы в международном праве, не подкрепленные реальным механизмом принуждения, отдаются на откуп «добропорядочности» государств, зачастую незаинтересованных в исполнении данных норм.

Очевидно, что так называемая международная мораль, под которой понимается «система норм, оценок, предписаний, образцов поведения, которые выполняют функции морального регулирования в системе международных отношений, в формировании ценности культуры мира, в становлении демократического и ненасильственного мироустройства» [7], не является действенным способом «призыва» к правомерному поведению. Этим объясняется тот факт, что Российская Федерация не стала подписантом Парижского призыва к доверию и безопасности в киберпространстве, с которым 12 ноября 2018 года выступил президент Франции на XIII Форуме по управлению Интернетом, несмотря на широкую поддержку данного документа другими странами, международными и иными организациями.

При этом в содержании названного документа должно уделяться особое внимание неравному соотношению информационного суверенитета государств. Государство, обладающее низким уровнем цифрового и технологического суверенитета, но формально

являющееся самостоятельным и равноправным субъектом международного права, не имеет реального суверенитета, так как самостоятельность во внутриполитических и внешнеполитических сферах, в условиях вовлеченности стран в глобальное информационное пространство и дисбаланса их цифрового потенциала, ставится в зависимость от способности противодействия информационным вызовам и угрозам. В этой связи следует констатировать, что эффективность нормотворческой деятельности в сфере обеспечения международной информационной безопасности зависит как от формы закрепления международно-правовых норм (в рекомендательных актах или юридически обязывающих), так и от содержания указанных норм, учитывающих неравноценный статус государств как субъектов международной политической системы.

Более тесное сотрудничество в рамках обеспечения информационной безопасности осуществляется на региональном уровне. Российская Федерация является активным участником многих интеграционных объединений регионального масштаба, созданных для совместного достижения Россией и ее союзниками экономических, политических и иных целей. К таким организациям можно отнести ОДКБ, ШОС, СНГ, БРИКС, ЕАЭС, рамках которых заключены соглашения, регламентирующие порядок сотрудничества в сфере обеспечения международной информационной безопасности.

Наиболее развитое сотрудничество в рамках рассматриваемых вопросов осуществляется странами-участниками СНГ. В силу тесных и обусловленных историческим процессом интеграционных и партнерских связей между членами данной организации в настоящий момент принято большое количество правовых актов СНГ в сфере обеспечения информационной безопасности. При этом данные акты носят как юридически обязывающий, так и рекомендательный характер.

Учитывая существующую геополитическую ситуацию и интенсивное противоборство (в том числе предполагающее использование информационного оружия) между Россией и странами Запада, налаживание и выстраивание партнерских связей со странами-участниками данных интеграционных объединений является одним из приоритетных направлений внешней политики государства. Причиной необходимости такого сотрудничества является политика европейских стран и США, направленная на международную изоляцию России и санкционное давление на нее, что способствует нарастанию глобального кризиса и выстраиванию политико-правовых механизмов, исходя из идеологической близости стран и общности их политических целей.

В этой связи целесообразно согласиться со следующими словами председателя Конституционного Суда РФ В.Д. Зорькина: «нужно хорошо понимать, что у нас есть не только много серьезных врагов, но и немало друзей или союзников, остро заинтересованных в нашей поддержке» [8].

Российская Федерация развивает механизм двустороннего сотрудничества в сфере информационной безопасности, который является весьма мобильным и эффективным в сравнении с общемировыми и региональными форматами сотрудничества. В настоящий момент Россией заключено большое количество межправительственных соглашений, касающихся сотрудничества в сфере обеспечения международной информационной безопасности. Такое межгосударственное взаимодействие осуществляется преимущественно с дружественными странами, не разделяющими идею однополярного мира и взаимодействующими с Россией на началах взаимовыгодного союзничества и партнерства.

Нельзя не отметить особый уровень союзнического взаимодействия России и Беларуси.

Значимым результатом союзнических усилий России и Беларуси стало принятие Концепции информационной безопасности Союзного государства от 22 февраля 2023 г., утвержденной постановлением Высшего Государственного Совета Союзного Государства. Подобный шаг является следствием нарастания экономического и политического давления со стороны стран Запада, что требует особого уровня согласованности политических и правовых механизмов между Россией и Беларусью в целях противостояния информационным атакам со стороны недружественных стран.

Таким образом, высокий уровень взаимозависимости стран и необходимость обеспечения принципа неделимости безопасности формируют глобальную потребность в поиске компромиссов и единых подходов в обеспечении международной информационной безопасности. Определение единого понятийного аппарата, не допускающего двусмысленности, противоречий и терминологической неопределенности, а также базовых принципов, являющихся юридическим фундаментом правового регулирования обеспечения международной информационной безопасности, должно быть реализовано путем разработки единого международного договора. Подобный вывод обусловлен неэффективностью норм «мягкого права» и международной морали, основанных на принципах добровольного исполнения обязательств, реализуемых в процессе межгосударственного взаимодействия.

Библиография

1. Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: Моногр. / Под общ. ред. Т.А. Поляковой. Саратов: Амирит, 2020. – С. 36.
2. Полякова Т.А., Шинкарецкая Г.Г. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз // Право и государство: теория и практика. 2020. № 10. С. 138.
3. Крутских А.В., Зиновьева Е.С. Международная информационная безопасность: подходы России. М.: МГИМО МИД России, 2021. С. 11.
4. Дубень А.К. Принципы правового обеспечения информационной безопасности в системе принципов международного права// Международное право. 2023. № 2. С. 6.
5. Молчанов Н.А., Матевосова Е.К. Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. 2020. № 1. С. 136.
6. Выступление В.А. Садовничего на V международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму» // 28.05.2013. Институт проблем информационной безопасности МГУ имени М.В. Ломоносова. URL: http://www.iisi.msu.ru/articles/article28/ (дата обращения: 09.02.2024).
7. Капто А.С. Современная цивилизация: вызовы и альтернативы. М.: Издательство Московского университета, 2013. С. 137.
8. Зорькин В.Д. Право России: альтернативы и риски в условиях глобальной кризисности // Российская газета. 29.06.2022. URL: https://rg.ru/2022/06/29/pravo-rossii-alternativy-i-riski-v-usloviiah-globalnogo-krizisa.html (дата обращения: 13.02.2024)

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ
на статью на тему «Информационная безопасность: международно-правовые аспекты ее обеспечения».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам международно-правовых аспектов обеспечения информационной безопасности. Автором анализируются различные подходы к тому, как следует направить деятельность в сфере обеспечения информационной безопасности с точки зрения международно-правового уровня. В качестве предмета исследования выступили, прежде всего, положения международно-правовых актов и мнения ученых.
Методология исследования.
Цель исследования прямо в статье не заявлена. При этом она может быть ясно понята из названия и содержания работы. Цель может быть обозначена в качестве рассмотрения и разрешения отдельных проблемных аспектов вопроса о международно-правовых аспектах обеспечения информационной безопасности. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.
В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из материалов практики.
Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства (прежде всего, положений международно-правовых актов). Например, следующий вывод автора: «В настоящее время основной целью информационно-правовой деятельности России в ООН является продвижение идеи о необходимости принятия универсального юридически обязывающего документа, регулирующего вопросы информационной защищенности в общемировом масштабе. Так, 15 мая 2023 года Россия вместе с Белоруссией, КНДР, Никарагуа и Сирией внесла концепцию конвенции ООН об обеспечении международной информационной безопасности. Концептуальные основы указанного документа предполагают реализацию принципов суверенного равенства государств и невмешательства в их внутренние дела. По мнению автора, потребность в принятии единого международного договора в сфере обеспечения международной информационной безопасности все еще является актуальной, в связи с чем следует поддержать активную роль России в реализации данной идеи с использованием международно-правовых механизмов и участием в интеграционных объединениях».
Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.
Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема международно-правовых аспектов информационной безопасности сложна и неоднозначна и требует уточнения и обсуждения. Сложно спорить с автором в том, что «Трансграничный характер угроз информационной безопасности формирует неоспоримую потребность в консолидации сил различных стран для противодействия таким угрозам, что в том числе связано с процессом цифровизации [1]. Каждое государство, защищая в первую очередь свои национальные интересы, стремится утвердить господство в информационном пространстве. Однако при этом

информационная политика стран должна быть направлена не только на обеспечение их собственного информационного суверенитета, но и на осуществление данной политики таким образом, чтобы не нарушались национальные интересы других участников международно-правового взаимодействия. В таких условиях цели по поддержанию состояния защищенности глобального информационного пространства могут оказаться недостижимыми без должной кооперации (в частности, организационного и правового характера) в решении задач, связанных с обеспечением международной информационной безопасности на нескольких уровнях взаимодействия: двустороннем, региональном, общемировом».

Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.

Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:

«высокий уровень взаимозависимости стран и необходимость обеспечения принципа неделимости безопасности формируют глобальную потребность в поиске компромиссов и единых подходов в обеспечении международной информационной безопасности. Определение единого понятийного аппарата, не допускающего двусмысленности, противоречий и терминологической неопределенности, а также базовых принципов, являющихся юридическим фундаментом правового регулирования обеспечения международной информационной безопасности, должно быть реализовано путем разработки единого международного договора. Подобный вывод обусловлен неэффективностью норм «мягкого права» и международной морали, основанных на принципах добровольного исполнения обязательств, реализуемых в процессе межгосударственного взаимодействия».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.

Во-вторых, автором предложены идеи по правильному пониманию положений международно-правовых актов, что может быть полезно специалистам в рассматриваемой сфере.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Международное право», так как она посвящена правовым проблемам, связанным с информационной безопасностью на международно-правовом уровне.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, в целом достиг цели исследования.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.

Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.

Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Полякова Т.А., Шинкарецкая Г.Г., Крутских А.В., Зиновьева Е.С., Молчанов Н.А., Матевосова Е.К. и другие). Многие из цитируемых ученых являются признанными учеными в области правовых аспектов обеспечения информационной безопасности.

Таким образом, труды приведенных авторов соответствуют теме исследования, обладают

признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.
Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.
Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к вопросам развития международно-правового регулирования отношений по обеспечению информационной безопасности.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи
«Рекомендую опубликовать»