

Международное право

Правильная ссылка на статью:

Дубень А.К. — Принципы правового обеспечения информационной безопасности в системе принципов международного права // Международное право. – 2023. – № 2. DOI: 10.25136/2644-5514.2023.2.40089 EDN: KREABN URL: https://nbpublish.com/library_read_article.php?id=40089

Принципы правового обеспечения информационной безопасности в системе принципов международного права

Дубень Андрей Кириллович

Научный сотрудник Института государства и права Российской академии наук

119019, Россия, Москва область, г. Москва, ул. Знаменка, 10

✉ k.duben@mail.ru



[Статья из рубрики "Теория и философия международного права"](#)

DOI:

10.25136/2644-5514.2023.2.40089

EDN:

KREABN

Дата направления статьи в редакцию:

27-03-2023

Дата публикации:

03-04-2023

Аннотация: В теории права и отраслевых юридических науках вопросу, связанному с правовыми принципами уделено достаточное внимание, тем не менее, имеются некоторые проблемы, требующие доктринального осмысления. Одним из таких вопросов является место и роль принципов правового обеспечения информационной безопасности в системе принципов международного права. Автор отмечает, что правовые принципы определяют сущность рассматриваемой отрасли права и в силу их юридического закрепления в нормах конкретной отрасли права, имеют общеобязательное значение. В данной статье рассматриваются принципы построения системы информационной безопасности. Сложность построения такой системы заключается в необходимости рассматривать защитные меры в комплексе, которые должны охватить правовую, организационную и техническую составляющую. В статье на основе анализа международных нормативных правовых актов и научно-правовых источников определены основные векторы развития международного и информационного права, рассмотрены внешние и внутренние угрозы в информационной сфере, раскрывается содержание основных принципов информационной безопасности.

Автор делает вывод о том, что в условиях глобальной цифровой трансформации и необходимости построения информационного общества проблемы, касающиеся определения основополагающих принципов правового обеспечения информационной безопасности приобретают особое значение. В связи с этим достаточно актуальным становится вопрос о научном осмыслении системы указанных принципов, их развитии и соотношении друг с другом, а также влиянии на информационные правоотношения.

Ключевые слова:

принципы права, международное право, информационное право, система принципов, теория права, новые вызовы, цифровизация, трансформация права, правовое обеспечение, информационное общество

В условиях глобальной цифровой трансформации и необходимости построения информационного общества проблемы, касающиеся определения основополагающих принципов правового обеспечения информационной безопасности приобретают особое значение. В связи с этим достаточно актуальным становится вопрос о научном осмыслении системы указанных принципов, их развитии и соотношении друг с другом, а также влиянии на информационные правоотношения. При этом обусловленность подобного осмыслиения связана не только с научным интересом ученых в сфере науки международного и информационного права, но и с более практическими целями, касающимися совершенствования правового регулирования и формирования правоприменительной практики.

В теории права определение правовых принципов имеет различные формулировки, большинство из которых содержат в себе ключевые признаки данного понятия. Так, в работе М.Н. Марченко принципы представляют собой «основные идеи, исходные положения или ведущие начала процесса формирования, развития и функционирования права» [1, с. 249]. Согласно позиции Л.А. Морозовой, принципами права являются «основополагающие идеи, закрепленные в официальных источниках права или получившие признание в юридической практике и отражающие закономерности развития общественных отношений» [2, с. 193]. Таким образом, принципы права имеют фундаментальное значение для регулирования общественных отношений и при этом могут находить нормативно-правовое закрепление как на государственном, так и на международном уровне.

Значение правовых принципов с точки зрения их роли в формировании правоприменительной практики и нормативно-правового материала является особенно высоким, в том числе в сфере обеспечения информационной безопасности. Правовые принципы служат ориентиром для законодателя, так как нормы, формулируемые им, не должны противоречить принципам права и в то же время должны представлять их детализированное выражение. Указанные аспекты имеют место и применительно к сфере обеспечения информационной безопасности.

В первую очередь стоит затронуть общепризнанные принципы международного права. Источником закрепления указанных принципов является Устав ООН, Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН и Декларация тысячелетия ООН. Первые два из вышеназванных актов упоминают принцип, согласно которому государства разрешают свои международные споры мирными средствами таким

образом, чтобы не подвергать угрозе международный мир, безопасность и справедливость. Информационное пространство абсолютным большинством современных стран определяется в качестве нового театра боевых действий. В связи с этим стоит сделать вывод, что понятие международного мира и безопасности, упомянутое в рамках содержания указанного принципа, относится и к сфере международной информационной безопасности. Следовательно, понятия «международная безопасность» и «международная информационная безопасность» соотносятся друг с другом как общее и частное. При этом в сфере международной информационной безопасности указанный принцип является наиболее актуальным, так как преимущества использования информационного оружия делают ведение информационных войн более предпочтительным для стран.

Высокое значение имеет принцип неприменения силы и угрозы силой для сферы обеспечения информационной безопасности. В настоящее время данный принцип может толковаться расширительно и предполагать не только посягательство на территориальную целостность другого государства и возможность ведения боевых действий на его территории, но и акты информационной агрессии и использования информационного оружия, в том числе пропаганда войны, запрет которой закреплен в ст. 20 Международного пакта о гражданских и политических правах [\[3\]](#).

Обязанность государств сотрудничать друг с другом в сфере обеспечения информационной безопасности проявляется в выработке координированных мер по противодействию информационным угрозам, посягающим на безопасность глобального информационного пространства и затрагивающим национальные интересы нескольких государств. В настоящее время указанный принцип представляется еще более актуальным ввиду повышения уровня интеграционного взаимодействия и взаимозависимости между странами, обусловленных трансграничным характером информационного пространства.

Принцип суверенного равенства государств предполагает возможность всех государств равным образом участвовать в решении проблем международной информационной безопасности и быть участниками глобального информационного пространства независимо от различий политического, социального, экономического или иного характера. Указанный принцип играет значительную роль в повышении уровня межгосударственного взаимодействия по проблемам защиты информационного пространства от негативного воздействия источников информационных угроз.

Принцип добросовестного выполнения обязательств реализуется посредством надлежащего исполнения государствами обязанностей, вытекающих из международных договоров в сфере обеспечения информационной безопасности или в соответствии с общепризнанными принципами и нормами международного права. Понятие «добросовестность» в данном случае предполагает добровольное исполнение, исключающее необходимость использования международно-правовых рычагов давления.

Характеризуя источники международного информационного права, многие авторы упоминают принцип уважения прав человека и основных свобод. Указанный принцип, применительно к сфере обеспечения информационной безопасности, конкретизируется в Международном пакте о гражданских и политических правах, Международном пакте об экономических, социальных и культурных правах [\[4\]](#) и Всеобщей декларации прав человека [\[5\]](#). В частности, указанные акты закрепляют нормы о тайне корреспонденции и

запрете незаконного посягательства на честь и репутацию.

В Декларации тысячелетия ООН подчеркивается приверженность целям и принципам ООН, а также повышение их актуальности «по мере того, как страны и народы становятся все более взаимосвязанными и взаимозависимыми». Последнее утверждение в полной мере соответствует и развитию информационной среды и информационных технологий в условиях глобализации, следовательно, относится и к обеспечению информационной безопасности.

Общепризнанные принципы международного права в сфере обеспечения информационной безопасности нашли выражение и в резолюциях ООН, посвященных проблемам кибербезопасности и научно-техническому прогрессу [6]. Большинство указанных принципов согласуются с документами стратегического планирования зарубежных стран и подчеркивают важность открытости и транспарентности деятельности государства в информационном пространстве, а также необходимость формирования глобальной культуры информационной безопасности.

Окинавская хартия глобального информационного общества также закрепила ряд принципов, некоторые из которых имеют прямое отношение к области обеспечения международной информационной безопасности [7]. Так, среди прочих принципов закрепляется: « дальнейшее развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций; развитие эффективного и значимого механизма защиты частной жизни потребителя, а также защиты частной жизни при обработке личных данных, обеспечивая при этом свободный поток информации ». Таким образом, в указанном международном акте делается акцент прежде всего на информационной безопасности личности, а также на развитии информационно-технических средств обеспечения безопасности.

На формирование принципов правового обеспечения информационной безопасности повлияла также Декларация принципов, принятая в Женеве в 2003 году [8]. В документе указывается на важность соблюдения принципа законности, который предполагает неукоснительное соблюдение национальных законов и норм, а также соответствующих международных соглашений. Одним из наиболее важных принципов, имеющих непосредственное отношение к сфере международной информационной безопасности является принцип укрепления доверия и безопасности при использовании ИКТ. Из анализа Декларации следует, что данный принцип состоит из следующих элементов: 1) упрочение основы для доверия, включая информационную безопасность и безопасность сетей, аутентификацию, защиту неприкосновенности частной жизни и прав потребителей; 2) формирование, развитие и внедрение глобальной культуры кибербезопасности; 3) предотвращение использования информационных ресурсов и технологий в преступных и террористических целях.

В Тунисской программе для информационного общества, принятой в 2005 году, подчеркивается важность обеспечения стабильности, безопасности и непрерывности сети Интернет, укрепления доверия и безопасности при использовании ИКТ, активизации международного сотрудничества с целью укрепления безопасности при обеспечении большей защиты информации личного характера, неприкосновенности частной жизни и данных [9]. В целом положения указанных документов мало чем отличаются от идей, изложенных в резолюциях ООН.

Как можно заметить, общие начала, призванные обеспечить международную

информационную безопасность, в настоящий момент уже можно считать сформированными. Однако нельзя сказать, что базовые принципы правового обеспечения международной информационной безопасности, закрепленные на международном уровне, представляют собой структурированную систему. Попытка структурировать и придать системный вид базовым принципам обеспечения информационной безопасности была осуществлена Российской Федерацией, предложившей еще в 1999 году в рамках ООН «Принципы, касающиеся международной информационной безопасности» [10]. Однако предложенный документ с пятью базовыми принципами так и не был принят в качестве резолюции. С течением времени, в связи со стремительным развитием информационных технологий и формированием глобального информационного общества, неизбежно будет появляться потребность в формулировании новых принципов, пересмотр ранее закрепленных либо их иная интерпретация.

Принципы обеспечения информационной безопасности могут формулироваться не только на общемировом уровне, но и региональном. Определенное значение имеют принципы, закрепленные в результате интеграционного взаимодействия России с другими странами.

С течением времени, в связи с изменением политической и экономической обстановки в мире, вызванной глобализацией, интеграционное сотрудничество между государствами лишь возрастает, в том числе по вопросам международной информационной безопасности. Указанные проблемы были предметом рассмотрения на XIII Форуме по управлению Интернетом, проведенном в штаб-квартире ЮНЕСКО, на котором выступил Президент Франции с Парижским призывом к доверию и безопасности в киберпространстве [11]. Однако среди более 50 стран, подписавших данный документ, России не оказалось. Думается, что связано это прежде всего с тем, что указанный документ носит декларативный характер, в связи с чем обязательность его исполнения юридически не подкреплена.

При этом в плане оперативного реагирования на проблемы международной информационной безопасности Российской Федерации также не является исключением в данном случае, в связи с чем и были приняты Основы государственной политики Российской Федерации в области международной информационной безопасности. Активная роль Российской Федерации в области обеспечения международной информационной безопасности прослеживается исходя из ее деятельности в ООН. Так, в декабре 2018 года было принято сразу два проекта резолюций, предложенных Россией: Резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [12] и Резолюция «Противодействие использованию информационно-коммуникационных технологий в преступных целях» [13].

Из анализа международных актов следует, что с участием Российской Федерации было заключено большое количество правовых актов в сфере обеспечения информационной безопасности. Целью интеграционного взаимодействия в данном случае является гармонизация законодательств различных государств в сфере обеспечения международной информационной безопасности, что позволит избежать такой актуальной проблемы, как недостаточная определенность понятийного аппарата, используемого в различных правовых актах, без решения которой невозможно полноценное сотрудничество между странами. Устойчивые интеграционные отношения между различными государствами позволяют им принять совместные координированные меры по борьбе с информационными угрозами и вызовами, затрагивающими региональные и общемировые интересы, для эффективного предотвращения которых требуется

консолидация международных государственных ресурсов.

Стоит отметить, что официальные документы, принятые в рамках одной интеграционной организации, порой оказывают позитивное влияние на нормативную правовую базу другой организации. Так, Модельный закон МПА СНГ «О международном информационном обмене» [14] и Концепция сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности [15] имели разные определения понятия «информационная безопасность», что было недопустимо с точки зрения необходимости обеспечения единого понятийного аппарата и терминологической определенности. В связи с этим понятие информационной безопасности в Стратегии обеспечения информационной безопасности государств - участников СНГ, принятой в 2019 году, стало определяться в соответствии с более подходящим определением, закрепленным в Соглашении между Правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности, то есть как состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.

Таким образом, 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. В условиях, когда информационное пространство фактически размывает границы между государствами, не ограничиваясь рамками одного государства, региона или континента, вопросы международной информационной безопасности, включая базовые принципы ее обеспечения, должны представлять собой универсальную и четко определенную систему, соблюдение правил которой будет обязательным для всего международного сообщества.

Библиография

1. Теория государства и права: учебник для вузов / под ред. М.Н. Марченко. М.: Зерцало, 2004. – 800 с.
2. Морозова Л.А. Теория государства и права: учебник. 4-е изд., перераб. и доп. М.: Эксмо, 2010. – 510 с.
3. Международный пакт о гражданских и политических правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН) // Бюллетень Верховного Суда РФ, № 12, 1994.
4. Международный пакт об экономических, социальных и культурных правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН) // Бюллетень Верховного Суда РФ, № 12, 1994.
5. Всеобщая декларация прав человека (принята Генеральной Ассамблей ООН 10.12.1948) // Российская газета, 10.12.1998.
6. Резолюция Генеральной Ассамблеи ООН A/RES/64/211 от 21 декабря 2009 г. «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» // Официальный сайт Организации Объединенных Наций. URL: <https://undocs.org/pdf?symbol=ru/A/RES/64/211> (дата обращения: 27.12.2022).
7. Окинавская хартия глобального информационного общества (Принята на о. Окинава 22.07.2000) // Дипломатический вестник. 2000. № 8. С. 51–56.

8. Женевская Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии», принятая 12.12.2003 г. // Официальный сайт Организации Объединенных Наций. URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения: 27.12.2022).
9. Тунисская программа для информационного общества, принятая 15.11.2005 г. // Официальный сайт Организации Объединенных Наций. URL: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения: 27.12.2022).
10. Доклад Генерального секретаря ООН A/55/150 «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» от 10.07.2000 г. // Официальный сайт Организации Объединенных Наций. URL: <https://undocs.org/ru/A/55/140> (дата обращения: 16.12.2022).
11. Парижский призыв к доверию и безопасности в киберпространстве. URL: https://www.diplomatie.gouv.fr/IMG/pdf/appel_de_paris_en_russe_cle8a41ae.pdf (дата обращения: 16.12.2022).
12. Резолюция № A/RES/73/27 Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принятая 05.12.2018 на 45-м пленарном заседании 73-й сессии Генеральной Ассамблеи ООН // Официальный сайт Организации Объединенных Наций. URL: <https://documents.un.org/prod/ods.nsf> (дата обращения: 16.12.2022).
13. Резолюция № A/RES/73/187 Генеральной Ассамблеи ООН «Противодействие использованию информационно-коммуникационных технологий в преступных целях», принятая 17.12.2018 на 56-м пленарном заседании 73-й сессии Генеральной Ассамблеи ООН // Официальный сайт Организации Объединенных Наций. URL: <https://documents.un.org/prod/ods.nsf> (дата обращения: 16.12.2022).
14. Модельный закон о международном информационном обмен СНГ (принят в г. Санкт-Петербурге 26.03.2002 Постановлением 19-7 на 19-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2002. № 29. С. 134-143.
15. Решение Совета глав государств СНГ «О Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и о Комплексном плане мероприятий по реализации Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности на период с 2008 по 2010 год» (документ опубликован не был) // СПС «Консультант плюс».

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 «Принципы правового обеспечения информационной безопасности в системе принципов международного права».

Предмет исследования. Предложенная на рецензирование статья посвящена принципам «...правового обеспечения информационной безопасности в системе принципов международного права». Автором выбран особый предмет исследования: предложенные вопросы исследуются с точки зрения информационного, международного и

международного информационного права, при этом автором отмечено, что «В условиях глобальной цифровой трансформации и необходимости построения информационного общества проблемы, касающиеся определения основополагающих принципов правового обеспечения информационной безопасности приобретают особое значение». Изучаются НПА России и СНГ, Устав ООН, Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами, международные пакты и декларации, имеющие отношение к цели исследования. Практически не изучается и не обобщается большой объем российской и зарубежной научной литературы по заявленной проблематике (в т. ч. и по статьям в журналах НВ), анализ и дискуссия с данными авторами-оппонентами соответственно отсутствует. При этом автор отмечает: «...принципы права имеют фундаментальное значение для регулирования общественных отношений и при этом могут находить нормативно-правовое закрепление как на государственном, так и на международном уровне».

Методология исследования. Цель исследования определена названием и содержанием работы: «Значение правовых принципов с точки зрения их роли в формировании правоприменительной практики и нормативно-правового материала является особенно высоким, в том числе в сфере обеспечения информационной безопасности», «Информационное пространство абсолютным большинством современных стран определяется в качестве нового театра боевых действий. В связи с этим стоит сделать вывод, что понятие международного мира и безопасности, упомянутое в рамках содержания указанного принципа, относится и к сфере международной информационной безопасности». Они могут быть обозначены в качестве рассмотрения и разрешения отдельных проблемных аспектов, связанных с вышеназванными вопросами. Исходя из поставленных цели и задач, автором выбрана определенная методологическая основа исследования. Автором используется некоторая совокупность частнонаучных, специально-юридических методов познания. Но в то же время автором не используются, в частности, методы анализа и синтеза, которые позволили бы обобщить подходы к предложенной тематике и повлияли бы на выводы автора. Определенную роль сыграли специально-юридические методы. В частности, автором применялись формально-юридический и сравнительно-правовой методы, которые позволили провести анализ и осуществить толкование норм актов российского законодательства и международных актов, сопоставить различные документы. В частности, делаются такие выводы: «... официальные документы, принятые в рамках одной интеграционной организации, порой оказывают позитивное влияние на нормативную правовую базу другой организации» и др. Таким образом, выбранная автором методология не в полной мере адекватна цели статьи, позволяет изучить лишь некоторые аспекты темы.

Актуальность заявленной проблематики не вызывает сомнений. Данная тема является важной в мире и в России, с правовой точки зрения предлагаемая автором работа может считаться актуальной, а именно он отмечает «...достаточно актуальным становится вопрос о научном осмыслении системы указанных принципов, их развитии и соотношении друг с другом, а также влиянии на информационные правоотношения». И на самом деле здесь должен следовать анализ работ оппонентов, но он не следует и автор никак не демонстрирует умение владеть материалом оппонентов. Тем самым, научные изыскания в предложенной области стоит только приветствовать.

Научная новизна. Научная новизна предложенной статьи не вызывает сомнения. Она выражается в конкретных научных выводах автора. Среди них, например, такой: «... вопросы международной информационной безопасности, включая базовые принципы ее обеспечения, должны представлять собой универсальную и четко определенную систему, соблюдение правил которой будет обязательным для всего международного сообщества». Как видно, указанный «теоретический» вывод может быть использован в

дальнейших исследованиях. Таким образом, материалы статьи в представленном виде могут иметь интерес лишь отчасти для научного сообщества.

Стиль, структура, содержание. Тематика статьи соответствует специализации журнала «Международное право», так как посвящена принципам «...правового обеспечения информационной безопасности в системе принципов международного права». В статье отсутствует аналитика по научным работам оппонентов, поэтому автор и не отмечает, что уже ставился вопрос, близкий к данной теме, а автор не использует их материалы, не дискутирует с оппонентами. Содержание статьи соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели своего исследования. Качество представления исследования и его результатов следует признать не до конца доработанным. Из текста статьи прямо следуют предмет, задачи, методология, результаты исследования, научная новизна. Оформление работы не во всем соответствует требованиям, предъявляемым к подобного рода работам. Существенные нарушения данных требований: отсутствие работ оппонентов и соответственно анализа современной ситуации, тем более в свете СВО и санкций в отношении России.

Библиография содержит только НПА и два учебника 2004 и 2010г.г., к которым автор обращается. Это не позволяет автору правильно определить проблемы и поставить их на обсуждение. Следует отрицательно оценить качество представленной и использованной литературы. Присутствие современной научной литературы показало бы обоснованность выводов автора и повлияло бы на его выводы. Труды приведенных авторов соответствуют теме исследования, но не обладают признаком достаточности, не способствуют раскрытию никаких аспектов темы.

Апелляция к оппонентам. Автор не провел серьезный анализ текущего состояния исследуемой проблемы. Автор не описывает разные точки зрения оппонентов на проблему, аргументирует свою, более правильную по его мнению позицию, опираясь только на международные акты и НПА, но не на работы оппонентов, предлагает варианты решения отдельных проблем.

Выводы, интерес читательской аудитории. Выводы являются логичными, общими «... 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» и др. Статья в данном виде может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к заявленным в статье вопросам только после доработки. На основании изложенного, суммируя все положительные и отрицательные стороны статьи «рекомендую отправить на доработку».