

Международное право и международные организации / International Law and International Organizations

*Правильная ссылка на статью:*

Дубень А.К. — Международно-правовые основы информационной безопасности: итоги и новые вызовы // Международное право и международные организации / International Law and International Organizations. – 2023. – № 1. DOI: 10.7256/2454-0633.2023.1.40054 EDN: ANNCOP URL: [https://nbpublish.com/library\\_read\\_article.php?id=40054](https://nbpublish.com/library_read_article.php?id=40054)

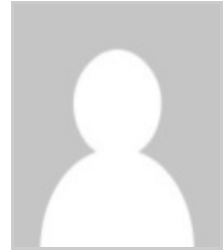
## Международно-правовые основы информационной безопасности: итоги и новые вызовы

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](mailto:k.duben@mail.ru)



[Статья из рубрики "Нормотворческая и правоприменительная деятельность международных организаций"](#)

**DOI:**

10.7256/2454-0633.2023.1.40054

**EDN:**

ANNCOP

**Дата направления статьи в редакцию:**

24-03-2023

**Дата публикации:**

31-03-2023

**Аннотация:** Актуальность проведенного исследования вызвана трансформацией права в условиях больших вызовов и угроз, а без понимания глобальности проблематики данного явления невозможно осуществлять активное межгосударственное сотрудничество. Целью исследования стало межгосударственное сотрудничество по обеспечению информационной безопасности, а также разработка мер по повышению его эффективности (в первую очередь международного законодательства, а также и иных межгосударственных мер по предупреждению новых вызовов и угроз). Объектом исследования стали современные общественные отношения, складывающиеся в сфере межгосударственного сотрудничества по обеспечению информационной безопасности. В качестве предмета выступили международно-правовые акты, регулирующие отношения в сфере кибербезопасности, материалы и публикации в области информационной безопасности, интернет-ресурсы по проблемам данной темы. В процессе исследования автором делаются выводы о том, что сегодня динамика конкурентных отношений в России детерминирована рядом факторов, которые следует развивать на площадках межгосударственных региональных объединений ШОС, БРИКС, ОДКБ, СНГ и других для

роста взаимосвязи участников рынка, интеграции производств, нивелирования санкционных издержек. Указанные условия ставят задачу поиска правовых средств, направленных на активизацию развития экономической сферы и обеспечения безопасности в информационной сфере. Это ставит задачу формирования эффективного механизма технического регулирования. В условиях, когда в Российской Федерации имеются значимые предпосылки для прорывного развития цифровых технологий как драйвера ее экономического роста, необходимы адекватные правовые решения, позволяющие устранить существующие препятствия на этом пути.

**Ключевые слова:**

информационная безопасность, сотрудничество, международная безопасность, международное право, международные организации, информационное право, угрозы и риски, правовое регулирование, трансформация права, информационное общество

Проблемы правового обеспечения информационной безопасности являются актуальными как для отечественной правовой доктрины, так и для законодательства. Каждое государство имеет свои национальные интересы и заинтересовано в поддержании мира и международной информационной безопасности. В свете тесного взаимодействия различных стран, вступающих в партнерские и союзнические отношения друг с другом, проблемы информационной защищенности одного государства могут стать бременем и для другого. В связи с этим важным представляется вопрос о зарубежном опыте правового обеспечения информационной безопасности.

Достаточно распространенным явлением стала политика ряда зарубежных стран, направленная на развитие своего информационно-технического потенциала в целях негативного воздействия на информационную инфраструктуру других государств.

В тоже время, Н.В. Бекетов справедливо отмечает что, понятие «информационная безопасность» является сложным правовым явлением с точки зрения информационного права, поскольку вышеуказанную дефиницию следует рассматривать в праве как самостоятельный наднациональный вид всеобщей безопасности, поскольку на сегодняшний день информационное право затрагивает все сферы общественной жизни и обеспечивает развитие государства в целом [\[1, с. 33\]](#).

На наш взгляд, такая позиция могла бы иметь под собой более прочное обоснование, если бы государства стремились к обеспечению всеобщей международной информационной безопасности. Однако каждое государство, учитывая рассмотренные в предыдущем параграфе стратегические документы зарубежных стран, преимущественно заботится о собственном информационном суверенитете. Информационная безопасность иных государств зачастую заботит остальных участников геополитической борьбы лишь в той мере, в которой информационные угрозы, затрагивающие интересы одного государства, могут затронуть национальные интересы другого государства. Подобная ситуация возможна при тесном интеграционном сотрудничестве между странами, которое предполагает взаимную защиту секретной информации. Выстраивание партнерских и союзнических отношений предполагает и взаимную ответственность за информационную защищенность каждого из участников интеграционного объединения.

Вместе с тем следует отметить, что в информационном праве правовое регулирование вопросов информационной безопасности отображается в Доктрине информационной

безопасности РФ. Данный нормативно-правовой акт регулирует часть общественных отношений в информационной сфере, благодаря которым демонстрируется защищенность государства в информационной сфере и определяется дальнейшее совершенствование правовых институтов с целью балансирования интересов личности, общества и государства в информационной среде.

Особое внимание в науке информационного права отнесено вопросам состояния правового обеспечения исследуемой подотрасли права, так в соответствии с п. 8 Доктрины информационной безопасности РФ можно выделить следующие особенности национальных интересов:

- 1) прозрачность и транспарентность деятельности государства в информационной сфере;
- 2) гарантия защиты конституционных прав и свобод граждан, касающихся информационной безопасности;
- 3) взаимное и согласованное функционирование государства и гражданского общества, в том числе в рамках укрепления нравственных ценностей общества;
- 4) обеспечение надлежащего функционирования информационной инфраструктуры как в случае непосредственного влияния информационных угроз (в том числе в военное время), так и в период стабильной мирной обстановки в стране;
- 5) стимулирование научно-технического прогресса и развития экономических отраслей, способствующих обеспечению информационной безопасности;
- 6) интеграционное взаимодействие с другими странами для обеспечения международной информационной безопасности и стратегической стабильности [\[2\]](#).

Национальные интересы в сфере информационной безопасности представляют собой общие ориентиры для органов публичной власти, на которых возложена роль нейтрализатора информационных угроз и конфликтов. Закрепленный в документах стратегического планирования перечень национальных интересов является правовым фундаментом (наряду с целями и задачами), на котором стоит вся система национальной безопасности.

Довольно актуальными являются подходы к разрешению проблем, связанных с обеспечением информационной безопасности международно-правовыми средствами. Проблема состоит в том, что любые условия, касающиеся транспарентности и информационной прозрачности, могут восприниматься странами в качестве ограничения суверенитета (прежде всего, информационного). Этим объясняется то, что в настоящий момент отсутствует международный договор, в котором были бы закреплены базовые принципы обеспечения информационной безопасности. Единственным способом для разрешения данной проблемы является заключение международных соглашений в рамках наднациональных институтов.

Как мы ранее отмечали, Российская Федерация является активным участником различных интеграционных объединений: объединение БРИКС, ОДКБ, ШОС, ЕАЭС, СНГ. В рамках указанных организаций заключаются соглашения, касающиеся защиты информации и иных вопросов в сфере обеспечения информационной безопасности. Такой подход выбран неслучайно, так как разрешение вопросов, касающихся такой чувствительной к различного рода угрозам среды, как информационное пространство, требует не только поиска точек соприкосновения со стороны иных государств и формирования единых подходов к разрешению проблем информационного характера, но

и определенного доверия. Лишь при взаимодействии со странами, с которыми Россию связывают партнерские и союзнические отношения, можно надеяться на неукоснительное соблюдение единых целей и задач в информационном пространстве.

Сотрудничество государств по реализации задач безопасности в информационной сфере требует формирования и последующего принятия организационно-правовых мер по противодействию информационным угрозам, посягающим на безопасность информационного пространства и затрагивающим национальные интересы нескольких государств. В настоящее время указанный принцип представляется еще более актуальным ввиду повышения уровня интеграционного взаимодействия в рамках региональных межгосударственных союзов и взаимозависимости между государствами, обусловленных трансграничным характером информационного пространства. Учитывая существующие проблемы межгосударственного взаимодействия на площадках международных организаций в условиях геополитических рисков и общемирового цивилизационного кризиса, для Российской Федерации усиливается значение межгосударственного взаимодействия на площадках таких региональных интеграционных союзов, как БРИКС, СНГ, ШОС, ЕАЭС и ОДКБ. К примеру, в рамках межгосударственного сотрудничества принимаются модельные законы об информационной безопасности, так на заседании Совета Парламентской Ассамблеи ОДКБ отдельно отмечено, что на данный момент всем странам-участницам необходимо усилить противодействие киберпреступности посредством внесения изменений в нормативные акты национального законодательства, в основе которого должен лежать модельный закон ОДКБ «Об информационной безопасности», принятый в 2021 г.<sup>[3]</sup> В свою очередь, по результатам межгосударственных консультаций государств – участников СНГ по тематике международной информационной безопасности принято решение о разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях в рамках Специального межправительственного комитета экспертов ООН<sup>[4]</sup>. Таким образом, взаимодействие России в рамках региональных межгосударственных союзов и взаимозависимости между государствами способствует укреплению международного сотрудничества.

На сегодняшний день процесс формирования и развития международных норм в информационной сфере возникает по результатам межгосударственного сотрудничества в рамках международных организаций таких как ООН, Совет Европы, Европейский Союз, ШОС, БРИКС, ЕвразЭС, СНГ, ОДКБ и других. Совет Европы один из первых, кто рассматривал на высоком уровне вопросы информационной безопасности, в результате были приняты Белая книга «Экономический рост, конкуренция, занятость – задачи и пути их решения на пороге XXI века» и план действий «Путь Европы в информационное общество», которые содержат ряд норм по защите информации и условий для создания и формирования свободного доступа к информации<sup>[5, с. 548]</sup>.

В международных актах сформулированы основные принципы международной информационной безопасности, которые являются базисными в информационном праве. Одним из основных документов для правового регулирования безопасности в информационной сфере является Всеобщая декларация прав человека<sup>[6]</sup>. В данном нормативном правовом акте закреплены гарантии на права и свободы человека и гражданина в части свободы убеждений, мысли, совести, религии, право на образование, а также право искать, получать и распространять информацию. Следовательно, право на свободу информации является естественным общепризнанным правом человека.

Кроме того, Всеобщей декларацией прав человека и конвенциями ООН дополнительно гарантированы права на частую жизнь. Важное значение для информационной безопасности имеют общие принципы, закрепленные в Резолюции ГА ООН 2450 (XXIII) от 12 декабря 1968 г., которые предусматривают свободу получения, хранения и обмена информацией, а также информирование о деятельности органов государственной власти и местного самоуправления.

В условиях динамично развивающихся правоотношений и геополитических изменений России с 1998 г. ведется переговорный процесс по формированию международно-правовых механизмов обеспечения информационной безопасности. Международной организацией ООН активно обсуждаются вопросы информационной безопасности, включая проблемы формирования понятийного аппарата, и разработки международно-правового режима информационной безопасности. В этой связи Российской Федерацией подготовлен проект «Принципы, касающиеся международной информационной безопасности», в котором содержатся определения базовых понятий в сфере информационной безопасности. Подтверждением актуальности международной информационной безопасности является позиция Глав государств – членов ШОС [7].

Таким образом, система международной информационной безопасности строится на системе взаимосвязанных международных норм на основе международного и межрегионального сотрудничества [8, с. 45]. Вместе с тем одним из перспективных направлений в данной теме является создание международно-правовой базы и формирование понятийного аппарата в сфере обеспечения международной информационной безопасности [9, с. 25]. Анализ рассматриваемых базовых положений межгосударственных соглашений позволил определить, что общая цель состоит в формулировании единых правил поведения в информационном пространстве в целях обеспечения информационной безопасности в условиях новых вызовов и угроз посредством международного сотрудничества между всеми соответствующими заинтересованными сторонами.

При этом ввиду отсутствия системы информационной безопасности и понятийного аппарата, а также несогласованных моделей считаем целесообразным развитие межгосударственного сотрудничества на основе сближения евразийской и евроатлантической систем международной информационной безопасности с учетом общепризнанных принципов и норм международного права, при этом значимое место должно быть уделено вопросам безопасности личности и общества в информационной сфере, включая противодействие нежелательному информационно-психологическому воздействию.

В заключении можем отметить, что сегодня динамика конкурентных отношений в России детерминирована рядом факторов, которые следует развивать на площадках межгосударственных региональных объединений ШОС, БРИКС, ОДКБ, СНГ и других для роста взаимосвязи участников рынка, интеграции производств, нивелирования санкционных издержек. Указанные условия ставят задачу поиска правовых средств, направленных на активизацию развития экономической сферы и обеспечения безопасности в информационной сфере. Это ставит задачу формирования эффективного механизма технического регулирования. В условиях, когда в Российской Федерации имеются значимые предпосылки для прорывного развития цифровых технологий как драйвера ее экономического роста, необходимы адекватные правовые решения, позволяющие устранить существующие препятствия на этом пути и создать правовую основу эффективного и безопасного продвижения в указанном направлении. В этой

связи, обеспечение информационной безопасности в различных ее аспектах является приоритетной целью технического регулирования.

## Библиография

1. Бекетов Н.В. Информационная безопасность развития государства // Информационные ресурсы России. 2004. № 6. С. 32 – 35.
2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ, 12.12.2016, № 50, ст. 7074.
3. Андрейченко: объективная информация о событиях в мире Западом жестко фильтруется и блокируется // Официальный сайт Белорусского телеграфного агентства «Белта» URL: <https://www.belta.by/politics/view/andrejchenko-objektivnaja-informatsija-o-sobytijah-v-mire-zapadom-zhestko-filtruetsja-i-blokiruetsja-506249-2022> (дата обращения: 10.03.2023).
4. Об итогах межмидовских консультаций государств – участников СНГ по тематике международной информационной безопасности // Официальный сайт Министерства иностранных дел РФ. URL: [https://www.mid.ru/ru/foreign\\_policy/integracionnye-struktury-prostranstva-sng/sng/1819433/](https://www.mid.ru/ru/foreign_policy/integracionnye-struktury-prostranstva-sng/sng/1819433/) (дата обращения: 14.03.2023).
5. Тихонов В.Н., Маркова А.Ю. Международно-правовое регулирование информационной безопасности // Аллея науки. 2017. № 15 (2). С. 547-550.
6. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета, 10.12.1998.
7. О заявлении Совета глав государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности // Официальный сайт Министерства иностранных дел Российской Федерации. URL: [https://www.mid.ru/ru/foreign\\_policy/news/1446414/](https://www.mid.ru/ru/foreign_policy/news/1446414/) (дата обращения: 15.03.2023).
8. Марков А.А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник СПбГУ. 2011. Сер. 12. Вып. 1. С. 43-48.
9. Бачило И.Л., Бондуровский В.В., Вус М.А., Кучерявый М.М., Макаров О.С. О совершенствовании и гармонизации национального законодательства государств-участников СНГ в сфере обеспечения информационной безопасности // Информационное право. 2013. № 1. С. 24 – 27.

## 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 «Международно-правовые основы информационной безопасности: итоги и новые вызовы».

Предмет исследования.

Предложенная на рецензирование статья посвящена актуальным вопросам международно-правового регулирования отношений по поводу информационной безопасности. Автором рассмотрены некоторые аспекты регулирования данного вопроса, а также намечены перспективные направления совершенствования права. В

качестве предмета исследования выступили мнения ученых, положения международно-правовых актов.

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 перспективах развития международно-правового регулирования отношений по поводу 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 положений правовых актов.

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 правовых актов). Например, следующий вывод автора: «В международных актах сформулированы основные принципы международной информационной безопасности, которые являются базисными в информационном праве. Одним из основных документов для правового регулирования безопасности в информационной сфере является Всеобщая декларация прав человека [6]. В данном нормативном правовом акте закреплены гарантии на права и свободы человека и гражданина в части свободы убеждений, мысли, совести, религии, право на образование, а также право искать, получать и распространять информацию. Следовательно, право на свободу информации является естественным общепризнанным правом человека».

Также автор статьи активно исследует опыт различных стран в анализируемой сфере. Так, отметим следующие рассуждения: «На сегодняшний день процесс формирования и развития международных норм в информационной сфере возникает по результатам межгосударственного сотрудничества в рамках международных организаций таких как ООН, Совет Европы, Европейский Союз, ШОС, БРИКС, ЕврАзЭС, СНГ, ОДКБ и други Совет Европы один из первых, кто рассматривал на высоком уровне вопросы информационной безопасности, в результате были приняты Белая книга «Экономический рост, конкуренция, занятость – задачи и пути их решения на пороге XXI века» и план действий «Путь Европы в информационное общество», которые содержат ряд норм по защите информации и условий для создания и формирования свободного доступа к информации».

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 обеспечения информационной безопасности сложна и неоднозначна. Информационная безопасность может быть гарантирована в полной мере на наднациональном уровне при активном участии различных государств, ведь онлайн-ресурсы, а также активные действия, связанные с распространением информации происходят вне каких-либо границ, а в масштабах различных государств. Следовательно, необходимо переосмысление международного взаимодействия по

указанному направлению. С практической стороны следует признать, что толкование международных актов, связанных с информационной безопасностью, может быть необходимо юристам, работающим в сфере международного права.

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

Научная новизна.

Определенная научная новизна предложенной статьи имеется. Во-первых, она выражается в авторских выводах. Например, следующий вывод:

«сегодня динамика конкурентных отношений в России детерминирована рядом факторов, которые следует развивать на площадках межгосударственных региональных объединений ШОС, БРИКС, ОДКБ, СНГ и других для роста взаимосвязи участников рынка, интеграции производств, нивелирования санкционных издержек. Указанные условия ставят задачу поиска правовых средств, направленных на активизацию развития экономической сферы и обеспечения безопасности в информационной сфере. Это ставит задачу формирования эффективного механизма технического регулирования. В условиях, когда в Российской Федерации имеются значимые предпосылки для прорывного развития цифровых технологий как драйвера ее экономического роста, необходимы адекватные правовые решения, позволяющие устранить существующие препятствия на этом пути и создать правовую основу эффективного и безопасного продвижения в указанном направлении. В этой связи, обеспечение информационной безопасности в различных ее аспектах является приоритетной целью технического регулирования».

Во-вторых, автором предложено оригинальное толкование положений международно-правовых актов в их системной взаимосвязи, что также может рассматриваться в качестве научной новизны и значимого аспекта исследовательской работы.

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

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Международное право и международные организации / International Law and International Organizations», так как она посвящена правовым проблемам, связанным с международно-правовым регулированием отношений по поводу обеспечения информационной безопасности.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, 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 средне оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Бекетов Н.В., Тихонов В.Н., Маркова А.Ю., Марков А.А. и другие). При этом самой «свежей» работой является статья 2017 года. Вместе с тем, автор рассматривает современные проблемы информационной безопасности. Странно, рассматривая именно современные проблемы, изучать работы, написанные в 2017 году и ранее.

Удивительно, что автор статьи, несмотря на тематику, не использовал работы ученых из зарубежных стран на иностранных языках. Представляется, что сложно или даже



невозможно раскрыть заявленную тему в отсутствие обсуждения мнения коллег из-за рубежа.

Таким образом, труды приведенных авторов соответствуют теме исследования, но не обладают признаком достаточности, не способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.

Вопрос об адекватности апелляции к оппонентам остается открытым. Следует расширить теоретическую базу исследования для однозначного ответа на этот вопрос.

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 регулирования отношений по поводу международно-правового обеспечения информационной безопасности.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи

«Рекомендую отправить на доработку»