УДК 341.2
МРНТИ 10.87.01
DOI 10.56525/DRGF3094

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И МНОГОПОЛЯРНОГО МИРА

Сеюбергенова Д., Исманов Т. К.
Международный университет Кыргызстана, Бишкек, Кыргизия
e-mail: didar__81@mail.ru, ismanov-61@mail.ru

Аннотация. В статье исследуются актуальные проблемы и современные тенденции развития международно-правового регулирования в сфере информационной безопасности в условиях стремительной цифровой трансформации общества и формирования многополярного информационного пространства. Особое внимание уделяется анализу международных универсальных и региональных нормативно-правовых актов, регулирующих вопросы защиты информации, обеспечения кибербезопасности, противодействия киберпреступности, а также соблюдения и защиты прав человека в цифровой среде. Рассматриваются основные международные документы, принятые в рамках Организации Объединенных Наций, Совета Европы, Шанхайской организации сотрудничества и Содружества Независимых Государств. В ходе исследования выявлены ключевые проблемы современного международного регулирования, включая фрагментарность правовых норм, отсутствие единых подходов к квалификации кибератак, сложности установления юрисдикции и недостаточную эффективность механизмов международного сотрудничества в борьбе с трансграничными киберугрозами. Обоснована необходимость разработки универсального международного правового акта под эгидой ООН, способного обеспечить комплексное регулирование отношений в сфере информационной безопасности с учетом современных технологических, политических и геополитических вызовов. Сделан вывод о необходимости консолидации усилий государств, международных организаций и научного сообщества для формирования эффективной и устойчивой системы защиты глобального информационного пространства.

Ключевые слова. Информационная безопасность, кибербезопасность, международное право, киберпреступность, цифровая трансформация, международное сотрудничество, защита информации, права человека.

Введение

Стремительное развитие цифровых технологий и глобальная взаимосвязанность информационных систем радикально трансформируют современное общество, формируя новую реальность, в которой информация становится ключевым стратегическим ресурсом. В этих условиях вопросы обеспечения информационной безопасности выходят за рамки исключительно технической проблематики и приобретают комплексный правовой, политический и социальный характер. Особую значимость они приобретают в контексте усиливающейся цифровизации государственного управления, экономики и международных отношений.

Современный этап развития международных отношений характеризуется ростом зависимости государств от устойчивости и защищенности информационной инфраструктуры. Нарушения в данной сфере способны повлечь серьезные последствия - от дестабилизации отдельных институтов до угроз национальной и международной безопасности. При этом киберпространство, обладая трансграничной природой, усложняет применение традиционных механизмов правового регулирования и требует поиска новых подходов к формированию эффективных инструментов взаимодействия государств.

Актуальность исследования обусловлена нарастающим числом киберугроз, усложнением их характера, а также отсутствием универсальных международно-правовых механизмов, способных обеспечить комплексное противодействие таким вызовам. Существующие нормативные акты, как на глобальном, так и на региональном уровнях, охватывают лишь отдельные аспекты информационной безопасности, что приводит к фрагментации правового регулирования и снижает эффективность международного сотрудничества.

Целью настоящего исследования является анализ современных тенденций и проблем формирования международно-правовых механизмов обеспечения информационной безопасности в условиях цифровой трансформации. В рамках достижения поставленной цели предполагается рассмотреть существующую нормативно-правовую базу, выявить ее ограничения, а также определить перспективные направления развития международного регулирования в данной сфере.

Методологическую основу исследования составляют общенаучные и специальные методы познания, включая системный, сравнительно-правовой и формально-юридический анализ. Их применение позволяет комплексно оценить текущее состояние международного правового регулирования и выявить ключевые проблемы и противоречия.

Таким образом, исследование направлено на формирование целостного представления о состоянии и перспективах развития международной информационной безопасности как одного из ключевых элементов глобальной системы безопасности в условиях цифровой эпохи.

Материалы и методы исследования

Эмпирическую и нормативную основу исследования составили международно-правовые акты универсального и регионального характера, регулирующие вопросы информационной безопасности, защиты прав человека в цифровой среде и противодействия киберпреступности. В качестве ключевых источников были использованы резолюции Генеральной Ассамблеи ООН, международные договоры, включая многосторонние конвенции, а также межправительственные соглашения в рамках региональных объединений. Дополнительно проанализированы научные публикации отечественных и зарубежных исследователей, посвященные проблемам международной информационной безопасности, а также материалы правоприменительной практики и экспертные доклады.

Методологическая база исследования сформирована с учетом междисциплинарного характера рассматриваемой проблематики. В работе использован системный подход, позволивший рассмотреть информационную безопасность как комплексное явление, включающее правовые, технические и институциональные элементы. Сравнительно-правовой метод применялся для сопоставления международных и региональных механизмов регулирования, выявления их сходств, различий и уровня эффективности. Формально-юридический метод обеспечил анализ содержания нормативных актов, их структуры и юридической техники.

Для выявления тенденций развития международного регулирования использован метод правового моделирования, позволивший определить возможные направления совершенствования нормативной базы. Кроме того, применялся аналитический метод, направленный на обобщение существующих научных подходов и формирование авторской позиции по исследуемой проблеме.

В рамках исследования также использованы элементы проблемно-ориентированного анализа, позволившие выделить ключевые пробелы и противоречия в действующей системе международно-правового регулирования информационной безопасности. Комплексное применение указанных методов обеспечило целостность исследования и обоснованность полученных выводов.

Результаты исследования

Формирование многополярного информационного пространства представляет собой сложный и многоуровневый процесс, требующий комплексного подхода к регулированию международной информационной безопасности. Данная трансформация неизбежно

порождает новую область межгосударственной конкуренции, оказывающую существенное влияние на глобальную архитектуру безопасности. При этом принципиально важно разграничивать безопасность глобального и национального информационного пространства, поскольку уровень международной информационной безопасности напрямую зависит от защищенности национальных информационных систем. Это, в свою очередь, обуславливает необходимость разработки и заключения межгосударственных соглашений, направленных на обеспечение устойчивости функционирования информационной инфраструктуры в условиях многополярности.

Отдельные элементы информационной безопасности уже получили закрепление в международном праве. Так, одним из базовых положений является право на информацию, закрепленное в Резолюции Генеральной Ассамблеи ООН A/RES/59 (I), где оно рассматривается как фундаментальное право человека и критерий реализации всех свобод, включая свободу информации, трактуемую как право свободно собирать, передавать и распространять сведения [1]. Данное положение получает развитие во Всеобщей декларации прав человека 1948 года [2], в частности, в статье 19, закрепляющей право каждого на свободу убеждений, а также на поиск, получение и распространение информации независимо от государственных границ. Одновременно статья 12 Декларации гарантирует защиту личной информации от произвольного вмешательства [2].

В 2011 году Генеральная Ассамблея ООН признала доступ к сети Интернет неотъемлемым правом человека [3], что свидетельствует о его ключевой роли в современном обществе. В дальнейшем, в Резолюции 68/167 от 2013 года [4], было подчеркнуто, что развитие информационных технологий значительно расширяет возможности наблюдения и сбора данных, что может привести к нарушению права на неприкосновенность частной жизни, закрепленного в статье 12 Всеобщей декларации прав человека [2] и статье 17 Международного пакта о гражданских и политических правах [5]. В этой связи подчеркивается необходимость обеспечения защиты указанных прав как в офлайн-, так и в онлайн-среде, а также предотвращения правонарушений в данной сфере [4]. Кроме того, в документе отмечается, что технологический прогресс способствует появлению новых форм киберпреступности, что требует принятия комплексных мер, включая совершенствование законодательства и развитие международного сотрудничества [4].

Существенное значение в регулировании международного обмена информационными ресурсами имеют Конвенция о международном обмене изданиями и Конвенция об обмене официальными изданиями и правительственными документами (1958 г.), направленные на развитие некоммерческого обмена информацией между государственными и негосударственными структурами при исключении конфиденциальных данных.

Важным этапом развития международного сотрудничества в сфере кибербезопасности стала Резолюция Генеральной Ассамблеи ООН №55/63 [6], направленная на противодействие преступному использованию информационных технологий. Данный документ акцентирует внимание на необходимости координации усилий государств на глобальном уровне для минимизации киберугроз, а также подчеркивает важность формирования национальных правовых систем, способных оперативно реагировать на вызовы цифровой эпохи [6].

Резолюция 57/239 [7] дополняет данный подход, формируя концепцию глобальной культуры кибербезопасности. В документе подчеркивается, что эффективная защита информационного пространства требует не только технических решений, но и комплексного подхода, включающего управление, планирование и превентивные меры. Среди ключевых элементов выделяются осведомленность, ответственность, этика, оценка рисков и внедрение механизмов защиты [7].

Значимым международным актом является Конвенция Совета Европы «О киберпреступности» 2001 года [8], ставшая первым документом, предложившим государствам унифицированный подход к уголовно-правовому регулированию киберпреступлений. В ней определены основные составы правонарушений, включая несанкционированный доступ, перехват данных, вмешательство в работу систем, а также преступления, связанные с

использованием информационных технологий. Конвенция также регулирует процессуальные аспекты и механизмы международного сотрудничества, включая взаимную правовую помощь и создание круглосуточных контактных пунктов [8].

Вместе с тем отдельные положения Конвенции, в частности статья 32, допускающая доступ к общедоступным данным без согласия государства, вызывают дискуссии в контексте соблюдения принципа государственного суверенитета [8], что требует дополнительного научного осмысления.

Следует отметить, что современное международное право, включая его уголовно-правовую составляющую, находится в стадии трансформации. Несмотря на наличие отдельных механизмов противодействия киберпреступности, универсальная система пока не сформирована. Существующие меры носят фрагментарный характер, а их эффективность во многом зависит от уровня международного сотрудничества. Дополнительную сложность создают геополитические противоречия, способствующие снижению роли международных институтов и формированию альтернативных блоков взаимодействия [9, с. 107].

Российская Федерация играет активную роль в развитии международного правового регулирования в данной сфере. В частности, в 1998 году была инициирована резолюция ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Существенное значение также имеет Окинавская хартия глобального информационного общества 2000 года [10], закрепившая ключевую роль информационных технологий в развитии современного мира.

Несмотря на признание важности информационной безопасности, единый подход к ее регулированию до сих пор не выработан. Это обусловливает необходимость разработки нового универсального международного документа, способного учитывать современные вызовы цифровой эпохи. Существующая Конвенция о киберпреступности уже не в полной мере отвечает актуальным требованиям, что обуславливает потребность в создании более комплексного и адаптивного акта под эгидой ООН.

На региональном уровне предпринимаются попытки унификации подходов. Так, в рамках ШОС было заключено Соглашение 2009 года [11], определяющее основные угрозы информационной безопасности, включая кибертерроризм, информационные войны и незаконное вмешательство в информационные системы. Аналогичные цели преследует Соглашение стран СНГ 2001 года [12], направленное на борьбу с преступлениями в сфере компьютерной информации.

В современных условиях цифровизации особую актуальность приобретает проблема соотношения стремительного технологического развития и способности правовых систем своевременно адаптироваться к новым общественным отношениям. Развитие искусственного интеллекта, технологий больших данных, облачных сервисов и глобальных цифровых платформ формирует качественно новые вызовы для международного права и системы обеспечения информационной безопасности. Как отмечается в исследовании, посвященном взаимодействию новых технологий и законодательства, существующие правовые механизмы зачастую не успевают за темпами технологических изменений, что приводит к возникновению правовых пробелов и снижению эффективности регулирования цифровой среды [13]. В этой связи особое значение приобретает разработка гибких международно-правовых механизмов, способных обеспечить баланс между технологическим развитием, защитой прав человека и обеспечением безопасности информационного пространства.

Однако процесс формирования международных норм сталкивается с рядом проблем, включая сложность квалификации киберпреступлений, определение статуса кибератак и их соотношение с актами агрессии. Особую актуальность приобретает вопрос оценки последствий кибератак и возможности их квалификации как вооруженного нападения.

Дополнительные трудности связаны с идентификацией субъектов киберпреступлений, что обусловлено анонимностью цифровой среды и трансграничным характером информационных технологий. Это требует разработки новых методов расследования и межгосударственного взаимодействия.

Таким образом, существующие международно-правовые акты, несмотря на их значимость, не обеспечивают комплексного регулирования и во многом носят фрагментарный или региональный характер. В условиях отсутствия единого глобального соглашения возрастает риск использования информационных технологий в противоправных целях, включая политическое давление, шпионаж и кибертерроризм.

В этой связи особую актуальность приобретает разработка универсальных международных стандартов и создание новой Конвенции ООН, способной обеспечить комплексное регулирование вопросов информационной безопасности. Такой документ должен учитывать современные технологические реалии и предусматривать эффективные механизмы международного сотрудничества.

Заключение

Проведенное исследование позволило комплексно оценить текущее состояние международно-правового регулирования в сфере информационной безопасности и выявить его ключевые системные недостатки. Установлено, что существующая нормативная архитектура носит разрозненный характер и не обеспечивает должного уровня согласованности между государствами, что снижает эффективность противодействия современным киберугрозам.

Анализ показал, что развитие цифровых технологий значительно опережает процесс формирования правовых механизмов их регулирования. В результате возникает дисбаланс между уровнем технологической оснащенности и степенью правовой обеспеченности безопасности информационного пространства. Это создает благоприятные условия для роста трансграничной киберпреступности, усложняет идентификацию правонарушителей и затрудняет привлечение их к ответственности.

Особое внимание в ходе исследования было уделено проблеме отсутствия единых подходов к квалификации кибератак и определению их правовой природы. Установлено, что разночтения в национальных правовых системах препятствуют формированию универсальных механизмов реагирования и подрывают потенциал международного сотрудничества. Кроме того, выявлены противоречия между необходимостью обеспечения безопасности и соблюдением принципов государственного суверенитета и прав человека в цифровой среде.

Важным выводом является признание необходимости перехода от фрагментарного регулирования к формированию целостной и универсальной системы международных норм. Такая система должна учитывать не только правовые, но и технологические особенности функционирования киберпространства, а также обеспечивать баланс интересов государств и личности. При этом особую роль играет институционализация механизмов взаимодействия, включая обмен информацией, координацию расследований и разработку единых стандартов реагирования на киберинциденты.

Перспективным направлением развития представляется разработка нового универсального международного соглашения, способного объединить существующие подходы и устранить выявленные пробелы. Его формирование должно основываться на принципах открытости, взаимного доверия и равноправного участия государств, что позволит повысить легитимность и эффективность будущего правового режима.

Таким образом, обеспечение международной информационной безопасности в условиях цифровой трансформации требует консолидации усилий мирового сообщества, углубления научных исследований и выработки согласованных правовых решений. Только при условии системного и координированного подхода возможно создание устойчивой и эффективной модели защиты глобального информационного пространства.

ЛИТЕРАТУРЫ

1. Резолюция Генеральной Ассамблеи ООН A/RES/59 (I) «Созыв международной Конференции по вопросу о свободе информации» 14 декабря 1946 года [Электронный ресурс]. - Режим доступа: http://un.org

2.Всеобщая декларация прав человека. Принята резолюцией 217 A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года [Электронный ресурс]. - Режим доступа: https://clck.ru/3MzXvW

3. Доклад Генеральной Ассамблеи ООН от 16 мая 2011 года [Электронный ресурс]. - Режим доступа: https://clck.ru/3MzXwF

4. Резолюция Генеральной Ассамблеи ООН 68/167 «Право на неприкосновенность личной жизни в цифровой век» 8 декабря 2013 года [Электронный ресурс]. - Режим доступа: https://online.zakon.kz/Document/?doc_id=31499342

5. Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 года [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzXxi

6. Резолюция Генеральной Ассамблеи ООН 55/63 «Борьба с преступным использованием информационных технологий» [Электронный ресурс]. – Режим доступа: http://un.org/

7. Резолюция Генеральной Ассамблеи ООН 57/239 «Создание глобальной культуры кибербезопасности» [Электронный ресурс]. – Режим доступа: http://un.org/

8. Конвенция Совета Европы о киберпреступности от 23 ноября 2001 года // Международное уголовное право в документах. В 2 т. Т. 1. – Казань: Казан. гос. ун-т, 2005. – С. 467–482.

9. Сидорова Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН / Т.Ю. Сидорова // Сибирский юридический вестник. – 2020. – №3 (90). – С. 103–108. – EDN XQJXUJ

10.Окинавская хартия глобального информационного общества от 21 июля 2000 года [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=d…odXDwttG

11.Соглашение государств-членов ШОС «О сотрудничестве в области обеспечения международной информационной безопасности». Подписано 16 июня 2009 года [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzY2o

12. Соглашение стран СНГ «О сотрудничестве в борьбе с преступлениями в сфере компьютерной информации». Подписано 1 июня 2001 года // Собрание законодательства Российской Федерации. – 2009. – №13. – Ст. 1460.

13. Суюнова Д.Ж. «Взаимодействие между новыми технологиями и законодательством» YESSENOV SCIENCE JOURNAL No2(47)-2024. С.236–242. https://journal.yu.edu.kz

REFERENCES

1. United Nations General Assembly Resolution A/RES/59 (I) “Calling of an International Conference on Freedom of Information”, December 14, 1946 [Electronic resource]. – Available at: http://un.org

2. Universal Declaration of Human Rights. Adopted by United Nations General Assembly Resolution 217 A (III) of December 10, 1948 [Electronic resource]. – Available at: https://clck.ru/3MzXvW

3. Report of the United Nations General Assembly of May 16, 2011 [Electronic resource]. – Available at: https://clck.ru/3MzXwF (

4. United Nations General Assembly Resolution 68/167 “The Right to Privacy in the Digital Age”, December 8, 2013 [Electronic resource]. – Available at: https://online.zakon.kz/Document/?doc_id=31499342 (

5. International Covenant on Civil and Political Rights. Adopted by United Nations General Assembly Resolution 2200 A (XXI) of December 16, 1966 [Electronic resource]. – Available at: https://clck.ru/3MzXxi

6. United Nations General Assembly Resolution 55/63 “Combating the Criminal Misuse of Information Technologies” [Electronic resource]. – Available at: http://un.org/

7. United Nations General Assembly Resolution 57/239 “Creation of a Global Culture of Cybersecurity” [Electronic resource]. – Available at: http://un.org/ (accessed: 06.03.2025).

8. Council of Europe Convention on Cybercrime of November 23, 2001 // International Criminal Law in Documents. In 2 vols. Vol. 1. – Kazan: Kazan State University, 2005. – pp. 467–482.

9. Sidorova T.Yu. International Information Security: Legal Aspects and UN Activities / T.Yu. Sidorova // Siberian Legal Bulletin. – 2020. – No. 3 (90). – pp. 103–108. – EDN XQJXUJ.

10. Okinawa Charter on Global Information Society of July 21, 2000 [Electronic resource]. – Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=d…odXDwttG

11. Agreement of the Member States of the Shanghai Cooperation Organization “On Cooperation in the Field of Ensuring International Information Security”, signed on June 16, 2009 [Electronic resource]. – Available at: https://clck.ru/3MzY2o

12. Agreement of the CIS Member States “On Cooperation in Combating Crimes in the Field of Computer Information”, signed on June 1, 2001 // Collection of Legislation of the Russian Federation. – 2009. – No. 13. – Art. 1460.

13. Suyunova D.Zh «The interactionbetween new technologies and law» Yessenov science journal 2024, Vol.47 (2) – pp. 236–242. https://journal.yu.edu.kz

ЦИФРЛЫҚ ТРАНСФОРМАЦИЯ ЖӘНЕ КӨППОЛЮСТІ ӘЛЕМ ЖАҒДАЙЫНДА АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ХАЛЫҚАРАЛЫҚ-ҚҰҚЫҚТЫҚ РЕТТЕУ

Сеюбергенова Д., Исманов Т. К.
Қырғызстан Халықаралық университеті, Бишкек қ., Қырғызстан
e-mail: didar__81@mail.ru, ismanov-61@mail.ru

Аннотация. Мақалада қоғамның қарқынды цифрлық трансформациясы және көпполярлы ақпараттық кеңістіктің қалыптасуы жағдайында ақпараттық қауіпсіздік саласындағы халықаралық-құқықтық реттеудің өзекті мәселелері мен қазіргі даму үрдістері зерттеледі. Ақпаратты қорғау, киберқауіпсіздікті қамтамасыз ету, киберқылмыспен күресу, сондай-ақ цифрлық ортада адам құқықтарын сақтау және қорғау мәселелерін реттейтін халықаралық әмбебап және өңірлік нормативтік-құқықтық актілерге ерекше назар аударылады. Біріккен Ұлттар Ұйымы, Еуропа Кеңесі, Шанхай ынтымақтастық ұйымы және Тәуелсіз Мемлекеттер Достастығы аясында қабылданған негізгі халықаралық құжаттар қарастырылады. Зерттеу барысында қазіргі халықаралық реттеудің негізгі проблемалары анықталды, олардың қатарында құқықтық нормалардың фрагменттілігі, кибершабуылдарды жіктеудің бірыңғай тәсілдерінің болмауы, юрисдикцияны анықтаудағы қиындықтар және трансшекаралық киберқауіптермен күрестегі халықаралық ынтымақтастық тетіктерінің жеткіліксіз тиімділігі бар. Цифрлық технологиялық, саяси және геосаяси сын-қатерлерді ескере отырып, ақпараттық қауіпсіздік саласындағы қатынастарды кешенді түрде реттеуді қамтамасыз ете алатын Біріккен Ұлттар Ұйымы аясында әмбебап халықаралық құқықтық акт әзірлеу қажеттілігі негізделеді. Глобалдық ақпараттық кеңістікті қорғаудың тиімді және

орнықты жүйесін қалыптастыру үшін мемлекеттердің, халықаралық ұйымдардың және ғылыми қауымдастықтың күш-жігерін біріктіру қажеттігі туралы қорытынды жасалады.

Түйін сөздер: ақпараттық қауіпсіздік, киберқауіпсіздік, халықаралық құқық, киберқылмыс, цифрлық трансформация, халықаралық ынтымақтастық, ақпаратты қорғау, адам құқықтары.

INTERNATIONAL LEGAL REGULATION OF INFORMATION SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION AND A MULTIPOLAR WORLD

Seyubergenova D., Ismanov T.
International University of Kyrgyzstan, Bishkek, Kyrgyzstan
e-mail: didar__81@mail.ru, ismanov-61@mail.ru

Abstract. The article examines current issues and modern trends in the development of international legal regulation in the field of information security under conditions of rapid digital transformation of society and the formation of a multipolar information space. Special attention is given to the analysis of international universal and regional legal instruments regulating the protection of information, ensuring cybersecurity, combating cybercrime, as well as the observance and protection of human rights in the digital environment. The study considers key international documents adopted within the framework of the United Nations, the Council of Europe, the Shanghai Cooperation Organisation, and the Commonwealth of Independent States. The research identifies major challenges in contemporary international regulation, including the fragmentation of legal norms, the lack of unified approaches to the qualification of cyberattacks, difficulties in establishing jurisdiction, and insufficient effectiveness of international cooperation mechanisms in combating transnational cyber threats. The necessity of developing a universal international legal instrument under the auspices of the United Nations is substantiated, which would provide comprehensive regulation of relations in the field of information security, taking into account modern technological, political, and geopolitical challenges. The study concludes that there is a need to consolidate the efforts of states, international organizations, and the academic community in order to form an effective and sustainable system for the protection of the global information space.

Keywords: information security, cybersecurity, international law, cybercrime, digital transformation, international cooperation, information protection, human rights, cyber threats.