ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДИПЛОМАТИЧЕСКАЯ АКАДЕМИЯ
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

Мартиросян Аревик Жораевна

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

5.1.5. Международно-правовые науки

Диссертация на соискание ученой
степени кандидата юридических наук

Научный руководитель:
Яковенко Александр Владимирович
доктор юридических наук, профессор

Москва – 2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Международно-правовое регулирование обеспечения безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) является одной из насущных тем в современном международном праве в связи с повышенной важностью ИКТ в XXI в. и их становлением неотъемлемым элементом обеспечения международной безопасности. Широкое распространение в мире ИКТ создало условия для формирования глобального информационного общества (ГИО), нормативным документом которого была провозглашена Хартия информационного общества – Окинавская Хартия, принятая 22 июля 2000 г. лидерами стран «Большой восьмерки». Однако несмотря на то, что с момента ее принятия прошло более 20 лет, международно-правовые инструменты регулирования отношений в ИКТ-среде находятся все еще на стадии формирования.

Проблемы международно-правового регулирования обеспечения безопасности в сфере использования ИКТ нашли отражение в ежегодных резолюциях Генеральной Ассамблеи Организации Объединенных Наций (ООН) «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности», докладах Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ ООН) и Рабочей группы ООН открытого состава по вопросам безопасности в сфере ИКТ и самих ИКТ 2021–2025 (РГОС ООН). Правовые пробелы в регулировании обеспечения безопасности в сфере использования ИКТ, а также существующие и потенциальные угрозы в исследуемой области определяют необходимость регулирования использования ИКТ и исследования данного вопроса.

Актуальность темы диссертационного исследования обусловлена также недостаточной разработанностью теоретических подходов к международно-правовому регулированию обеспечения безопасности в сфере использования ИКТ, активным развитием ИКТ-среды, а также отсутствием системного международно-

правового регулирования отношений в ней. Беспрерывное развитие и повсеместное внедрение ИКТ, а также процессы, протекающие с начала третьего тысячелетия, предопределяют необходимость формирования признанных на международном уровне механизмов, направленных на обеспечение международной информационной безопасности. С учетом того, что на данный момент в международном праве отсутствует унифицированное международно-правовое регулирование обеспечения безопасности в сфере использования ИКТ, это обуславливает актуальность темы диссертационного исследования.

Степень разработанности темы исследования. Исследование отдельных аспектов регулирования обеспечения безопасности в сфере использования ИКТ на текущий момент находится в фокусе внимания ученых, особенно в свете активной переговорной линии в рамках ООН, проводимой Российской Федерацией. Однако большинство научных исследований относится к политическим, либо историческим наукам. Тема диссертационного исследования имеет низкую степень разработанности в отечественной доктрине международного права, но ее отдельные элементы находят частичное отражение в ряде работ. Так, в диссертационном исследовании А.В. Кубышкина «Международно-правовые проблемы обеспечения информационной безопасности государства» изучены непосредственно проблемы обеспечения информационной безопасности государства с международно-правовой точки зрения, а не регулирование использования ИКТ как таковое. Помимо этого, работа была актуальна для своего периода исследования, на момент его проведения в 2002 г., в связи с чем не отражает современные аспекты исследуемой тематики, в частности, деятельность учрежденных позднее международных организаций, соответствующие правовые аспекты и инициативы по выработке универсального международно-правового акта, регулирующего ИКТ-среду. Ранее проведенное диссертационное исследование А. И. Мысиной по теме «Международно-правовое регулирование сотрудничества государств по противодействию преступлениям в сфере информационных технологий» направлено на выявление закономерностей и особенностей международно-правового регулирования сотрудничества

государств по противодействию преступлениям в сфере ИТ, однако не включает вопросы общего регулирования ИКТ вне системы уголовного правосудия. Диссертация на соискание ученой степени доктора юридических наук В. П. Талимончик «Международно-правовое регулирование отношений в сфере информации» имеет своей целью проанализировать систему правового регулирования международных информационных отношений, складывающихся в условиях формирования информационного общества. В работе, помимо прочего, рассматриваются формирующиеся специальные принципы правового регулирования международных информационных отношений, но не учитывается необходимость выделения новой отрасли международного права, что может объясняться датированием рассматриваемого исследования. В. И. Федулов в своем исследовании «Международно-правовые аспекты защиты компьютерной информации» сконцентрировался на международно-правовых аспектах защиты компьютерной информации, являющейся одной из трех составных элементов информационной безопасности (безопасность информации, безопасность информационной инфраструктуры, безопасность информационного пространства), настоящая работа посвящена безопасности не информации как таковой, а информационной инфраструктуры и информационного пространства. В диссертации на тему «Международно-правовые проблемы обеспечения международной информационной безопасности в сети Интернет», автором которой является К. В. Прокофьев, объектом выступают отношения, возникающие между субъектами международного права в рамках обеспечения информационной безопасности в сети Интернет, при этом системно не исследована роль иных составляющих ИКТ, в то время как в настоящем диссертационном исследовании объект – общественные отношения, складывающиеся в процессе обеспечения безопасности в сфере использования ИКТ в целом. Д. Д. Штодина в своей диссертационной работе «Международно-правовой режим киберпространства: позиция США» также выбрала более узкий объект, который исследуется относительно позиции Соединенных Штатов.

Несмотря на наличие указанных исследований, можно констатировать, что

комплексного изучения международно-правового регулирования обеспечения безопасности в сфере использования ИКТ не проводилось. Помимо этого, авторы учитывали тенденции, которые существовали в международных отношениях на период проведения соответствующих исследований, а непрерывная эволюция ИКТ, их повсеместное внедрение и рост исходящих от них угроз обуславливает потребность научного анализа для восполнения теоретических пробелов и поиска практических решений.

Теоретическая основа диссертационного исследования. Международно-правовое регулирование обеспечения безопасности в сфере использования ИКТ – составная проблематика международного права, в этой связи важно отметить научные труды, посвященные общетеоретическим вопросам, связанным с темой исследования. Значительный вклад в изучение современного международного публичного права и теоретическую основу работы внесли отечественные юристы как в сфере международного права, так и общей теории права: А. Х. Абашидзе, А. В. Алтухова, И. О. Анисимов, В. В. Архипов, Б. М. Ашавский, П. Н. Бирюков, А. Н. Вылегжанин, Е. Е. Гуляева, А. А. Данельян, С. А. Егоров, А. А. Ефремов, Б. Л. Зимненко, П. А. Калиниченко, А. Я. Капустин, О. Г. Карпович, М. Б. Касенова, С. Ю. Кашкин, Н. И. Костенко, И. И. Лукашук, Е. Г. Ляхов, А. Ю. Марченко, П. В. Меньшиков, А. В. Минбалеев, Б. Н. Мирошников, А. И. Мысина, Б. И. Осминин, Т. А. Полякова, Э. Л. Сидоренко, А. А. Смирнов, Т. М. Смыслова, А. А. Стрельцов, В. П. Талимончик, О. И. Тиунов, В. Н. Трофимов, Г. И. Тункин, Г. Г. Шинкарецкая, В. М. Шумилов, А. В. Яковенко, С. Н. Ярышев, Ю. А. Ясносокирский, А. Ю. Ястребова и др.; а также иностранные правоведы: Дж. П. Барлоу, Г. Г. Браун, Дж. Л. Голдсмит, К. Гринвуд, К. Джоан, Д. Р. Джонсон, М. К. Кеттеманн, Л. Лессиг, О. С. Макаров, Ж.-П. Панкрацио, П. П. Полански, Д. Пост, К. Поэллет, Р. Е. Эннан и др.

Помимо этого, теоретическую основу диссертационного исследования также составляют труды представителей различных областей научного знания – математики, технических наук, социальных наук, гуманитарных наук, которые занимаются изучением проблемы безопасности в сфере использования ИКТ. Так,

например, среди политологов, историков, социологов значительный вклад в изучение международной информационной безопасности внесли следующие отечественные исследователи – М. Б. Алборова, Н. С. Бабекина, А. В. Бирюков, С. М. Бойко, О. В. Демидов, Е. С. Зиновьева, А. В. Зинченко, В. Б. Козюлин, А. В. Крутских, О. А. Мельникова, Е. С. Михалева, Е. Н. Пашенцев, Н. П. Ромашкина, А. И. Смирнов, И. В. Сурма и др., а также иностранные – А. Гаврилович, П. Иттельсон, Х. Капалидис, И. Кислица и др.

Автор также опирался на междисциплинарные исследования зарубежных ученых, среди которых Г. Барам и О. Векслер; Р. А. Бургельман, К. М. Кристенсен и С. С. Уилрайт; К. Джайлс и У. Хагестад II; Б. Уиден и В. Самсон; В. Г. Г. Фустер и Л. Жасмонтайте; а также М. Альшаер, Х. К. Мендонки, Т. Стремлау, Л. Шэдболт и др.

Объектом диссертационного исследования выступают общественные отношения, складывающиеся в процессе обеспечения безопасности в сфере использования ИКТ.

Предмет исследования – принципы и нормы международного права, нормы национального законодательства Российской Федерации, применяемые с целью обеспечения безопасности в сфере использования ИКТ, а также практика их реализации.

Цель исследования – формирование нового юридического знания и разработка совокупности теоретических положений о международно-правовом регулировании обеспечения безопасности в сфере использования ИКТ.

Основываясь на цели диссертационного исследования, в работе поставлены следующие **задачи**:

1) выявить различные подходы к терминологическому аппарату относительно регулирования обеспечения безопасности в сфере использования ИКТ и определить их особенности;

2) сформулировать концептуальные подходы к информационно-коммуникационным технологиям и регулированию обеспечения безопасности в сфере их использования в доктрине международного права и дать оценку

обоснованности выделения новой отрасли международного права, предметом которой являются международные правовые отношения в информационной области;

3) обобщить, систематизировать и раскрыть нормативно-правовые и доктринальные основы регулирования обеспечения безопасности в сфере использования ИКТ в Российской Федерации;

4) очертить перспективы развития системы правового обеспечения безопасности в сфере использования ИКТ с точки зрения международно-правовой основы регулирования, а также механизмов международного сотрудничества в исследуемой области;

5) раскрыть и обосновать особенности регулирования использования ИКТ в рамках международного морского права, а также выработать рекомендации по прогрессивному развитию современного международного права в части обеспечения безопасности в сфере использования ИКТ в контексте международного морского судоходства;

6) выявить отдельные проблемы и перспективы международно-правового регулирования использования ИКТ в международном космическом праве, а также выработать рекомендации для совершенствования правовых основ обеспечения безопасности ИКТ в международном космическом праве;

7) выработать рекомендации для дальнейшего международно-правового регулирования обеспечения безопасности в сфере использования ИКТ и его совершенствования в рамках ООН.

Научная новизна заключается в том, что проведено комплексное исследование с целью формирования нового юридического знания и разработки совокупности теоретических положений о международно-правовом регулировании обеспечения безопасности в сфере использования ИКТ. Несмотря на наличие научных работ по разным юридическим и техническим аспектам информационной безопасности, всестороннее исследование обеспечения международной безопасности в сфере использования ИКТ с точки зрения международного права не проводилось. Для попытки его проведения автором были изучены различные

аспекты данного вопроса. Новизна работы также заключается в изучении проблем, недостаточно либо вовсе не исследованных в литературе, – системного анализа отдельных отраслей международного публичного права относительно регулирования обеспечения безопасности в сфере использования ИКТ: выявлены тенденции, проблемы и перспективы, существующие в международном морском праве и международном космическом праве относительно регулирования использования ИКТ, а также предложены практические и теоретические рекомендации в целях содействия прогрессивному развитию международного права и его кодификации в исследуемой области.

Теоретическая значимость определяется возможностью использования полученных результатов исследования в проведении лекций в рамках учебных курсов образовательных организаций высшего образования по направлениям «Международное публичное право», «Информационное право» и др. Результаты исследования вносят определенный вклад в развитие доктрины международного права применительно к международно-правовому регулированию обеспечения безопасности в сфере использования ИКТ. Формулирование и систематизация отдельных норм международного права, регулирующих ИКТ, определение тенденций и перспектив развития международно-правового регулирования обеспечения безопасности в сфере использования ИКТ, а также выработанные в рамках настоящей диссертации теоретические и практические рекомендации относительно разработки новых норм могут быть использованы для кодификации и прогрессивного развития международного права.

Практическая значимость определяется возможностью использовать результаты настоящей работы в качестве методологического и практического материала в процессе дальнейшего развития международно-правового регулирования обеспечения безопасности в сфере использования ИКТ, в том числе в рамках переговорных процессов по исследуемой тематике. Предложения, сформулированные в результате исследования, могут служить рекомендательной базой или концептуальной основой для совершенствования международной,

а также внутригосударственной правотворческой деятельности и правоприменительной практики.

Методологическая основа диссертации базируется на общенаучных методах: анализ, синтез, обобщение, аналогия, индуктивный и дедуктивный методы, диалектический и системный метод. Все они в своей совокупности применялись для изучения процесса становления и развития современного международно-правового регулирования обеспечения безопасности в сфере использования ИКТ. Формально-логический метод исследования в сочетании с такими логическими приемами, как анализ, синтез, индукция, дедукция, сравнение, аналогия, абстрагирование и обобщение, позволил обеспечить обоснованность и достоверность сформулированных по результатам исследования выводов.

Из специальных методов юридической науки были использованы такие методы, как историко-правовой метод, сравнительно-правовой метод, формально-юридический метод и метод интерпретации. Специфика рассмотрения процессов формирования норм правового регулирования ИКТ определила особую роль историко-правового метода исследования. Изучение понятий в международных и национальных правовых актах обусловило необходимость применения сравнительно-правового метода. Для использования согласованного понятийно-категориального аппарата в исследовании применен формально-юридический метод. Указанные методы позволили проанализировать и упорядочить обширный фактический материал, касающийся исследуемых в работе проблем. Также использован подход социального конструктивизма, который позволил проанализировать и установить связи между эволюцией ИКТ и их влиянием на международную информационную безопасность, с одной стороны, а также кодификацией и прогрессивным развитием международного права в сфере использования ИКТ, с другой стороны. Междисциплинарный подход способствовал выработке совокупности теоретических положений о международно-правовом регулировании обеспечения безопасности в сфере использования ИКТ, а также практических рекомендаций.

Положения, выносимые на защиту. В соответствии с целями и задачами диссертационного исследования на защиту выносятся следующие новые и содержащие элементы новизны основные идеи:

1. В связи с отсутствием в доктрине и практике международного права единого понимания ИКТ автором предлагается определение данного термина в широком смысле: «совокупность методов, процессов и средств, используемых для сбора, обработки, хранения и распространения графической, звуковой, текстовой и числовой информации с помощью электронно-вычислительных устройств, а также телекоммуникационных аппаратных и программных средств».

2. Ввиду наличия терминологических разногласий в понимании международной информационной безопасности и кибербезопасности автором обоснована необходимость использования в рамках международного нормотворчества единого термина «безопасность в сфере использования ИКТ».

3. Вносится вклад в формирование новой отрасли международного права – международного информационного права, посредством определения его отраслеобразующих элементов:

– специальный предмет – межгосударственные отношения в информационной области, включая складывающиеся в процессе обеспечения безопасности в сфере использования ИКТ;

– специальный объект – информационная область как развивающаяся система качественно однородных общественных информационных отношений и специфическая обособленная область международных отношений;

– специальные принципы – суверенитет в информационной области; использование информационного пространства и его составляющих, в том числе ИКТ, в мирных целях; равенство государств в информационном пространстве; принцип инклюзивного доступа к информационному пространству; принцип совместного управления информационным пространством; принцип обеспечения свободного доступа к источникам информации; принцип обеспечения культурного разнообразия в информационном пространстве; принцип ответственности государств в ИКТ-среде; принцип атрибуции кибератак и др.

Автор предлагает следующее определение международного информационного права: «совокупность специальных международных принципов и норм, определяющих права и обязанности субъектов международного права в информационном пространстве».

4. Автором доказано, что преобладающим источником международного информационного права являются нормы «мягкого права», которые носят рекомендательный характер и содержатся в специальных источниках – актах органов международных организаций, стандартах, регламентах, рекомендациях, «кодексах», разработанных с целью регулирования общественных отношений в информационном пространстве, включая обеспечение безопасности в сфере использования ИКТ.

5. Автором выявлено более эффективное правовое регулирование обеспечения безопасности в сфере использования ИКТ на региональном уровне по сравнению с универсальным. В связи с чем предлагается при разработке международно-правовых норм универсального характера использовать наиболее передовой и прогрессивный опыт регионального нормотворчества в рассматриваемой области.

6. Выявлены пробелы в регулировании безопасности морской ИКТ-инфраструктуры – систем в общей среде, на борту судов и на берегу, в связи с чем обоснована необходимость совершенствования международно-правового регулирования обеспечения безопасности в сфере использования ИКТ в рамках международного морского права. Автором предлагается системное регулирование проблем обеспечения безопасности в сфере использования ИКТ, возникающих в результате кибератак против морской ИКТ-инфраструктуры, а также совершенствование института морского страхования с учетом угроз, исходящих от прямого или косвенного использования или эксплуатации в качестве средства для причинения вреда ИКТ.

7. Предлагается включить в объект международно-правового регулирования обеспечения безопасности в сфере использования ИКТ космическую деятельность с целью минимизации рисков потенциальной атаки

против космической ИКТ-инфраструктуры – физического наземного сегмента, космического сегмента, каналов передачи данных и цепочек поставок космической инфраструктуры.

8. Обоснована необходимость учреждения специализированной Организации ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ, в мандат которой вошли бы разработка и принятие универсального международно-правового акта по обеспечению безопасности в сфере использования ИКТ и самих ИКТ, в связи с чем предлагается соответствующий проект конвенции.

Степень достоверности и обоснованности настоящего исследования подтверждается использованием правил научной логики и различных методов исследования, большого объема анализируемых источников международного права, обширностью актуальной нормативно-правовой и информационной базы по теме исследования и смежным вопросам, позволяющих всесторонне изучить рассматриваемую проблему. Кроме того, выводы и рекомендации, изложенные в диссертационном исследовании, основываются на системном анализе существующих российских и зарубежных научных работ по проблематике исследования. В совокупности это способствовало комплексному и объективному изучению различных аспектов темы диссертации. Также достоверность настоящего исследования подтверждена апробацией результатов исследования.

Апробация результатов исследования. Результаты исследования были апробированы при обсуждении диссертации на заседании кафедры международного права ФГБОУ ВО «Дипломатическая академия МИД России», а также представлены на ежегодной международной научной конференции «Актуальные проблемы мировой политики: итоги и перспективы» 2020–2023 гг., на конференции «Право индивида на защиту персональных данных», на круглом столе Совета молодых ученых Дипломатической Академии МИД России «Информационное пространство и обеспечение международной безопасности» 2021 г., на I Международной молодежной конференции по информационной безопасности 2023 г., проходившими в Дипломатической Академии МИД России;

на научно-практических мероприятиях Национальной Ассоциации международной информационной безопасности 2021–2023 гг.; на Международной конференции «Киберстабильность: подходы, перспективы, вызовы» 2022 г. и 2023 г., на научном круглом столе «Международное право в киберэпоху: проблемы, вызовы и перспективы» МГЮА имени О.Е. Кутафина 2022 г., на XIII Конвенте Российской ассоциации международных исследований в рамках работы секции «Проблемы применимости международного права к информационной сфере» 2021 г.; на Всероссийской студенческой научной конференции «Право, общество, государство: проблемы теории и истории» Российского университета дружбы народов 2021 г. и др.

Выводы диссертационного исследования базируются на практической деятельности соискателя в качестве научного сотрудника Института актуальных международных проблем Дипломатической академии МИД России и были использованы при подготовке аналитических материалов по информационной проблематике для Министерства иностранных дел Российской Федерации. Отдельные элементы исследования были представлены в качестве тезисов на второй (март 2022 г.), третьей (июль 2022 г.), четвертой (март 2023 г.), пятой (июль 2023 г.), шестой (декабрь 2023 г.), седьмой (март 2024 г.) субстантивных сессиях и неформальных межсессионных встречах РГОС ООН, на семинаре Совещания по взаимодействию и мерам доверия в Азии «Безопасное и устойчивое развитие сети Интернет» 2022 г., на Форумах ООН по Управлению Интернетом 2021–2023 гг., на Российском форуме по управления Интернетом 2022–2023 г.; а также в формате образовательных лекций на Специальных сессиях Шанхайской организации сотрудничества (ШОС), Летней школе по управлению Интернетом Координационного центра доменов .RU/.РФ 2023 г. и 2024 г. и в рамках научно-аналитического и образовательного проекта «Школа международной информационной безопасности» Института актуальных международных проблем Дипломатической академии МИД России, аккредитованного в РГОС ООН.

По теме исследования опубликовано 14 научных работ, в том числе 6 статей в научных изданиях, рецензируемых Высшей аттестационной комиссии

при Министерстве образования и науки Российской Федерации. Теоретические основы диссертации также имеют свое отражение в монографии автора, раскрывающей особенности формирования концепции обеспечения международной информационной безопасности в части регулирования Интернета.

Структура работы. Диссертационное исследование состоит из введения, трех глав, разделенных на параграфы, заключения, списка сокращений и условных обозначений, списка использованной литературы, а также приложения.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Настоящая глава посвящена первоочередным задачам диссертационного исследования – определению основных терминов, выявлению различных подходов к терминологическому аппарату относительно регулирования обеспечения безопасности в контексте использования ИКТ и его особенностей, оценке обоснованности выделения новой отрасли международного права, предметом которой являются международные правовые отношения в информационной области. Помимо этого, в первой главе обобщены нормативно-правовые и концептуальные основы исследуемой проблематики в Российской Федерации.

1.1. Понятийно-категориальный синтез информационно-коммуникационных технологий

На сегодняшний день вопросы регулирования ИКТ имеют большую актуальность и составной элемент исследуемой проблематики, который представляет научный интерес, – это обеспечение безопасности в контексте использования ИКТ с точки зрения лингвистики и герменевтики.

Начнем с базового понятия «технология», которая не вызывает споров и предполагает способ, с помощью которого мы достигаем целей, и может рассматриваться как средство их выполнения. Технологию также определяют как это знания и процессы, которые люди используют для удовлетворения своих потребностей. Существует также определение, согласно которому технологию рассматривают как практическое и теоретическое ноу-хау и способности, которые могут быть использованы при разработке продуктов или услуг, обеспечивающих их систем, а также которые могут быть интегрированы в процессы, оборудование, материалы и системы, используемые в производстве товаров или оказании услуг[1].

[1] Burgelman R. A., Christensen C. M., Wheelwright S. C. Strategic Management of Technology and Innovation. – 5th edition. – New York: McGraw-Hill, 2009. – P. 31.

Конкретная технология может быть электрическим или механическим компонентом, машиной или сборкой, программным кодом, химическим процессом, руководством, документацией, чертежами, рабочими процедурами, техникой, патентом или даже человеком. Таким образом, суммируя указанные выше определения, можно заключить, что технология, может быть в целом понята как сущность, как материальная, так и нематериальная, произведенная путем приложения умственных и физических усилий для достижения некоторой цели.

Прежде чем перейти к понятийному и смысловому анализу ИКТ, важно отметить две особенности. Во-первых, понятия «информационные технологии», «информационно-коммуникационные технологии», и используемое в российских нормативно-правовых актах понятие «информационные и коммуникационные технологии» в российской правовой доктрине рассматриваются как синонимы[2]. Во-вторых, в правовой доктрине нет общепринятого определения ИКТ в связи с их комплексным характером и разнообразием подходов, поскольку в различных исследованиях используются разные определения ИКТ. Обратимся к некоторым из них и на основе сравнительно-правового анализа отследим эволюцию данного понятия.

Информационная[3] технология – это общий термин, который охватывает создание, отбор, обработку, преобразование, хранение и распространение информации. Существует мнение, что термин «информационная технология» был разработан в Harvard Business Review, чтобы провести различие между специально построенными машинами, предназначенными для выполнения ограниченного круга функций, и универсальными вычислительными машинами, которые могут быть запрограммированы для различных задач. В 1958 г. термин «информационные технологии» был введен в статью под названием «Менеджмент

[2] Мельникова О. А. Манипуляция общественным мнением и глобальная кибербезопасность: монография. – Москва: Гнозис, 2021. – С. 24; Костенко Н. И. Право международной информационной безопасности: (становление, тенденции и проблемы развития): монография. – Москва: Юрлитинформ, 2019. – С. 60–66.

[3] Происхождение слова «информация», датируемого концом XIV в., относится к тому же периоду, что и «акт информирования» от старофранцузского «information, enformacion» – информация, совет, наставление, и от латинского «informationem» (номинативное informatio) со значением «передаваемое знание».

в 1980-е годы»[4]. Информационные технологии как техническая поддержка человеческого мышления и коммуникации развивались на протяжении тысячелетий. История созданных человеком информационных технологий – это история медленной эволюции, которая насчитывает около 5000 лет. Она пошла по механическому, а позднее электронному пути, начиная от примитивных знаков, иероглифов, алфавитного письма, книгопечатания и дойдя до языка программирования. Телефон, радио, телевидение, спутниковая передача, компьютер и микропроцессоры представляют собой яркие примеры качественных изменений в ИКТ.

ИКТ выступают относительно новым термином для правовой доктрины[5], при этом они стали предметом изучения различных наук. Сегодня этот термин широко используется в научной литературе, и некоторые его определения включают технологическую сторону информационных систем (ИС)[6]. Технология включает в себя компьютерные ИС[7] и совокупность используемых компьютерных систем[8]. Они были определены как технологии, которые используются с целью любой манипуляции информации во всех ее видах[9]. Данное определение охватывает части ИКТ-оборудования (компьютеры, принтеры, сканеры и т.д.), программное обеспечение (операционные системы, приложения, языки разработки, офисные

[4] Говоря о новой технологии, которая начинает осваиваться в американском бизнесе, Ливитт и Томас писали: новая технология еще не имеет единого устоявшегося названия. Она состоит из нескольких взаимосвязанных частей. Один из них включает в себя методы быстрой обработки больших объемов информации, и он воплощается в быстродействующем компьютере. Вторая часть сосредоточена вокруг применения статистических и математических методов к задачам принятия решений; она представлена такими методами, как математическое программирование и исследование операций. Она предполагает применение вычислительных машин и коммуникационных технологий с целью обработки информации, передачи информации и информационных потоков от уровня генерации до уровня использования. Она ограничена системами, зависящими от микроэлектроники, основанной на комбинации вычислительных машин и телекоммуникационных технологий. Перспективные и диверсифицированные возможности ИТ сократили пространство и время между людьми, странами, континентами и в конечном итоге привели к появлению концепций «глобального общества».

[5] Шинкарецкая Г. Г. Роль информационно-коммуникационных технологий (ИКТ) в обеспечении устойчивого развития человеческого общества // Право и управление. – 2023. – № 9. – С. 153.

[6] Hollander A., Denna E., Cherrington J. O. Accounting, information technology, and business solutions. – 2nd edition. – New York: McGraw-Hill Higher Education, 1999. – P. 3–5.

[7] Laudon K. C., Laudon J. P. Management information systems: Organization and technology in the networked enterprise. – Upper Saddle River: Prentice Hall, 2000. – P. 11.

[8] Turban E., McLean E., Wetherbe J., Leidner D. Information technology for management: Transforming organizations in the digital economy. – Hoboken: John Wiley and Sons, 2004. – P. 15.

[9] Boar B. H. Strategic Thinking for Information Technology: How to Build the IT Organization for the Information Age. – New York, NY: John Wiley and Sons, Inc., 1997. – P. 7.

приложения и т.д.), и телекоммуникационные устройства (модемы, концентраторы, сетевые адаптеры и интерфейсы и т.д.).

ИКТ определяются как возможности, предоставляемые компьютерами, программными приложениями и телекоммуникациями для передачи данных, информации и знаний отдельным лицам и процессам[10]. ИКТ также рассматривается как наука об обработке информации, в частности с помощью компьютеров, используемая для обеспечения передачи знаний в технической, экономической и социальной областях.

Существует разнообразие подходов к определению ИКТ со стороны международных организаций. Так, согласно материалам Департамента по экономическим и социальным вопросам ООН, являющегося частью Секретариата ООН, ИКТ включают любое коммуникационное устройство или приложение, такое как радио, телевидение, сотовые телефоны, компьютеры, спутниковые системы, а также сетевое оборудование и программное обеспечение и связанные с ними услуги[11]. Эксперты Всемирного банка определяют ИКТ как совокупность видов деятельности, которые облегчают с помощью электронных средств обработку, передачу и отображение/воспроизведение информации[12], а также устройств, принципов, используемых для обработки информации, и электронной связи, которая включает в себя все аппаратное и программное обеспечение[13]. Согласно ЭКСКАТО, определение ИКТ должно охватывать как новые, так и старые информационные технологии. Словарь Института статистики ЮНЕСКО определяет ИКТ как разнообразный набор технологических инструментов и ресурсов, используемых для передачи, хранения, создания, совместного

---

[10] Attaran M. Information technology and business-process redesign // Business Process Management Journal. – 2003. – Т. 4. – С. 440–458.

[11] Toolkit on disability for Africa. Information and communication technology (ICT) and disability / The Division for Social Policy and Development (DSPD) of the Department of Economic and Social Affairs (DESA). – 2016. – P. 11.

[12] Rodriguez F., Wilson E. Are Poor Countries Losing the Information Revolution [Электронный ресурс]. MfoDev Working Paper. – Washington D.C.: World Bank, 2000. – URL: https://documents1.worldbank.org/curated/en/600361468762019045/pdf/266510WP0Scode1tries0losing0Infodev.pdf (дата обращения: 10.08.2024).

[13] World Development Report 2006. Equity and Development [Электронный ресурс]. – A copublication of the World Bank and Oxford University Press. – URL: https://documents1.worldbank.org/curated/en/435331468127174418/pdf/322040World0Development0Report02006.pdf (дата обращения: 10.08.2024).

использования или обмена информацией[14]. Данные технологические инструменты и ресурсы включают компьютеры, Интернет (веб-сайты, блоги и электронную почту), технологии прямого вещания (радио, телевидение и веб-трансляция), технологии «записанного» вещания (подкастинг, аудио- и видеоплееры, а также устройства хранения данных) и телефонию (фиксированную или мобильную, спутниковую, видео/видеоконференцсвязь и т.д.).

Примечателен также социологический подход, согласно которому ИКТ рассматриваются как нервная система современного общества, передающая, распределяющая информацию, и управляющая ею и возникающими взаимосвязями, а также множеством независимых единиц[15].

Резюмируя вышесказанное, в связи с отсутствием в доктрине и практике международного права единого понимания ИКТ автором предлагается в наиболее широком смысле определить ИКТ как «совокупность методов, процессов и средств, используемых для сбора, обработки, хранения и распространения графической, звуковой, текстовой и числовой информации с помощью электронно-вычислительных устройств, а также телекоммуникационных аппаратных и программных средств». Основываясь на проделанном сравнительно-правовом анализе понятий, можно сделать вывод, что термин «ИКТ» недавно стал использоваться в качестве собирательного термина для всего спектра технологий, обеспечивающих способы и средства получения, хранения, передачи, извлечения и обработки информации. То есть ИКТ включает в себя такие технологии, как радио и телефонная связь, видео, спутниковые системы, информационные сети, аппаратное и программное обеспечение. Наблюдается конвергенция трех направлений технологий: вычислительной техники, микроэлектроники и связи. Они связаны не только с новыми видами оборудования, но и с гораздо более

[14] Information and communication technologies (ICT) [Электронный ресурс]. UNESCO Institute of Statistics. Glossary. – URL: https://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict (дата обращения: 10.08.2024).

[15] Ifeanyi A. The impact of Information and Communication Technology (ICT) on News Processing, Reporting and Dissemination on Broadcast stations in Lagos, Nigeria [Электронный ресурс]. – 2012. – URL: http://www.researchgate.net/publication/280049026_The_impact_of_Information_and_Communication_Technology_ict_on_News_Processing_Reporting_and_Dissemination_on_Broadcast_stations_in_Lagos_Nigeria/ (дата обращения: 10.08.2024).

широким спектром информационной деятельности[16], так как система ИКТ состоит из компьютерных технологий, коммуникационных технологий, оптических систем связи и технологий спутниковой связи.

Таким образом, рассмотрев различные подходы к определению ИКТ, можно заключить, что в доктрине международного права не существует конкретного, общепризнанного определения ИКТ. В международно-правовом контексте ИКТ могут рассматриваться как объект международного права в их широком понимании в тот момент времени, когда относительно них возникают международно-правовые отношения. Нормы международного права регулируют ИКТ в различных их ипостасях, ИКТ-среда в контексте международного права представляет собой сложную и динамичную область, охватывающую широкий спектр правовых вопросов относительно регулирования ИКТ. К ним относят обеспечение информационной (кибер) безопасности, противодействие киберпреступности, ответственность государства за свои действия в ИКТ-среде, защиту данных и их конфиденциальность, распределение полос частот, координацию спутниковой связи и регулирование международных телекоммуникационных услуг, электронную коммерцию, регулирование интеллектуальной собственности и обеспечение права человека в цифровую эпоху, а также международное сотрудничество в области ИКТ и многие другие вопросы.

Беспрерывное развитие и повсеместное внедрение ИКТ преобразуют все сферы деятельности человека и встроены во все аспекты жизни, начиная от возможности общаться с пользователями Интернета из любой точки мира в режиме реального времени и заканчивая обеспечением социально важной инфраструктуры и национальной безопасности. ИКТ несут в себе как положительные, так и отрицательные стороны[17]. В то время как глобальная связь и развитие ИКТ принесли неоспоримые положительные выгоды, зависимость от ИКТ и их повсеместный характер создали новые уязвимости с точки зрения безопасности.

[16] Информационная технология охватывает такие различные объекты, как книга, печать, репрография, телефонная сеть, радиовещание и компьютеры.

[17] Крутских А., Стрельцов А. Международное право и проблема обеспечения международной информационной безопасности [Электронный ресурс] // Международная жизнь. – 2014. – № 11. – URL: https://interaffairs.ru/jauthor/material/1167 (дата обращения: 10.08.2024).

Как справедливо отмечает Г. Г. Шинкарецкая, комплекс негативных последствий и рисков, которые могут возникнуть в результате широкого распространения и интенсивного использования информационных технологий, выступает как неотъемлемая сторона их использования[18]. Угрозы и вызовы в ИКТ-среде приобрели глобальный характер наряду с иными, что установлено в резолюции 72/200 «Использование информационно-коммуникационных технологий в целях устойчивого развития», принятой Генеральной Ассамблеей 20 декабря 2017 г. по итогам доклада Второго комитета (A/72/417).

На основании вышеуказанного можно сделать вывод, что ИКТ становятся важнейшим стратегическим ресурсом, определяющим состояние и уровень национальной и международной безопасности, а пробелы в международном праве, касающиеся регулирования отношений в ИКТ-среде, создают барьеры для создания эффективной системы обеспечения безопасности в области применения ИКТ[19], что, в свою очередь, становится обоснованием необходимости совершенствования международно-правового регулирования ИКТ.

В российской правовой доктрине безопасность ИКТ входит в более широкий термин – информационную безопасность, так как ИКТ рассматривается как цифровой вид информации как таковой. Согласно Доктрине информационной безопасности Российской Федерации 2016 г., под информационной безопасностью понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[20]. Для обозначения международного аспекта

[18] Шинкарецкая Г. Г. Проблема выработки определения кибератаки // Международное право. – 2023. – № 2. – С. 11.
[19] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074. – URL: http://www.jurizdat.ru/editions/official/lcrf/archive/2016/50.htm (дата обращения: 10.08.2024).
[20] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.

информационной безопасности отечественные ученые используют термин «международная информационная безопасность»[21]. Автор диссертационного исследования оперирует наиболее оптимальным термином с учетом специфики ИКТ-среды и различий трактовок ее категориального аппарата; он отражает как понимание обеспечения безопасности ИКТ с точки зрения отечественной доктрины международного права, так и зарубежной: безопасность в сфере использования ИКТ.

Право государств на обеспечение безопасности закреплено в международных правовых актах, основополагающую роль среди которых играет Устав ООН[22]. Хотя мировое сообщество обсуждает вопрос необходимости регулирования ИКТ и единогласно признает его важность, до сих пор наблюдается отсутствие единства и общего понимания по терминологии и сущности определений относительно ИКТ. Рассмотрим и проанализируем некоторые из них.

Согласно российскому национальному стандарту, «безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность»[23]. Схожее определение можно найти в международном стандарте Международной организации по стандартизации (ИСО) ISO 27000: «безопасность информации – сохранение конфиденциальности, целостности и доступности информации»[24]. Термин «безопасность информации (данных)» практически идентично определяется и не вызывает каких-либо споров с точки зрения своей сущности.

---

[21] Может быть определена как эффективно функционирующая система международной информационной безопасности, направленная на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета государств в информационном пространстве. Источник: Бойко С. М. Международная информационная безопасность: Россия в ООН. Два формата диалога (2018-2021 гг.) [Электронный ресурс] // Международная жизнь. – 2024. – № 3. – URL: https://interaffairs.ru/virtualread/ia_rus/32024/files/assets/downloads/publication.pdf (дата обращения: 10.08.2024).

[22] Устав Организации Объединенных Наций [Текст]: принят в г. Сан-Франциско 26.06.1945 // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. XII. – М, 1956. – С. 14–47.

[23] Национальный Стандарт Российской Федерации ГОСТ Р 50922-2006. Защита информации: основные термины и определения [Электронный ресурс]. Дата введения 01.02.2008 / Федеральное агентство по техническому регулированию и метрологии. – URL: https://protect.gost.ru/document.aspx?control=7&id=129024 (дата обращения: 10.08.2024).

[24] ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary [Электронный ресурс]. – URL: http://www.iso.org/standard/73906.html/ (дата обращения: 10.08.2024).

Термин «информационная безопасность» рассматривается в диссертационном исследовании в понимании российской юридической доктрины[25].

Однако наибольший терминологический вызов с точки зрения обеспечения безопасности в контексте применения ИКТ обусловлен применением так называемой «кибертерминологии», которая, несмотря на факт ограничения смыслов, широко используется «коллективным Западом» для реализации собственных интересов и целей. Господствующий подход так называемого «коллективного Запада» определяется через дискурс «кибербезопасности». Иными словами, западный подход в каком-то смысле подменяет термины информационной безопасности и международной информационной безопасности, продвигаемые Российской Федерацией и единомышленниками, «кибертерминологией», подразумевая под кибербезопасностью как деятельность на национальном уровне с широким охватом направлений, а также на внешнеполитическом уровне[26].

Позиция Российской Федерации заключается в использовании более широкого термина «информационная безопасность», частью которой также является и «кибербезопасность». Отечественная правовая доктрина не признает отделения понятия кибербезопасности от более широкого понятия информационной безопасности, что можно проследить в российском

---

[25] В отличие от «безопасности информации» «информационная безопасность» «представляет собой более широкий термин, который включает помимо безопасности информации (данных) также и защиту субъектов информационных отношений от негативного информационного воздействия». При этом важно отметить, что с лингвистической точки зрения возникают сложности перевода с английского языка, где данные определения имеют одно и то же написание «information security», что, в свою очередь, приводит к герменевтическим сложностям. Источник: Жуков Ю., Кузьмин А., Финогенов Д. Терминология в сфере международной информационной безопасности [Электронный ресурс] // BIS Journal. – 2015, 16 сентября. – № 3 (18). – URL: https://ib-bank.ru/bisjournal/post/385 (дата обращения: 10.08.2024).

[26] Это можно увидеть на примере основополагающих документов США, регулирующих различные аспекты обеспечения «кибербезопасности»: Конституция США, Стратегия национальной безопасности 2022 г., Стратегия национальной обороны 2022 г., Стратегия национальной кибербезопасности 2023 г., Киберстратегия Министерства обороны США 2023 г., Закон о конфиденциальности 1974 г., Акт патриотов 2001 г., Закон о свободе 2005 г., Закон о защите детей в Интернете от 2000 г., Закона о приличиях в области связи 1996 г. и др. В более широком смысле «кибербезопасность» определяется как «стратегии, политики и стандарты, касающиеся безопасности и операций в киберпространстве, и охватывающие полный спектр мер по снижению угроз, снижению уязвимости, сдерживанию, международному взаимодействию, политики и мероприятия в области реагирования на киберинциденты, включая операции с компьютерными сетями, обеспечение информационной безопасности, а также правоохранительные, дипломатические, военные и разведывательные миссии, поскольку они связаны с безопасностью и стабильностью глобальной информационной и коммуникационной инфраструктуры».

законодательстве[27]. При этом существование «кибертерминологии» и ее целевое использование не оспаривается[28]. Термин «кибербезопасность» на первый взгляд соотносится с российским подходом, однако в отличие от российского подхода, он фокусируется на определении «киберпространства» через «физическую» инфраструктуру. В контексте наличия терминологических разногласий примечательно, что уже в обновленной редакции международного стандарта ISO/IEC 27032[29] применяются термины «кибербезопасность» (защита людей, общества, организаций и наций от киберрисков) и «Интернет-безопасность» (сохранение конфиденциальности, целостности и доступности информации через Интернет). С точки зрения отечественного терминологического подхода чаще всего используется понятие «ИКТ-среда»[30], которое выступает синонимом терминов «ИКТ-инфраструктура» и «киберпространство». Также «кибертерминология» используется в российской доктрине применительно к западному подходу.

С точки зрения юридической лингвистики и герменевтики важно отметить особенность российской терминологии, которая формируется вне рамок западного понимания и трактовок и стремится к более широким смыслам. Это касается не только теоретического уровня отечественной юридической доктрины, но и практической реализации деятельности Российской Федерации на внешнеполитическом направлении. Примером могут считаться термины, толкование которым давалось российской стороной и среди них фигурирует «международная информационная безопасность», которая, согласно Принципам,

---

[27] Концепция кибербезопасности разошлась с государственной стратегией [Электронный ресурс]. – 2013, 29 ноября. – URL: https://www.kommersant.ru/doc/2355154 (дата обращения: 10.08.2024).

[28] Так, в предыдущей редакции международного стандарта ISO/IEC 27032 используются понятия «кибербезопасность» или «безопасность киберпространства», которая определяется как «защита конфиденциальности, целостности и доступности информации данных в киберпространстве». Источник: ISO/IEC 27032:2012 Information technology, Security techniques. Guidelines for cybersecurity [Электронный ресурс]. – URL: https://www.iso.org/ru/standard/44375.html (дата обращения: 10.08.2024).

[29] ISO/IEC 27032:2023 Cybersecurity. Guidelines for Internet security [Электронный ресурс]. – URL: https://www.iso.org/ru/standard/76070.html (дата обращения: 10.08.2024).

[30] Как справедливо отмечает А. А. Стрельцов, «в достаточно общем виде его содержание может быть раскрыто как совокупность средств, систем и сетей, используемых для оказания услуг телекоммуникационной связи и автоматизированной обработки информации, а также организационной инфраструктуры, предназначенной для создания и эксплуатации соответствующих средств, систем и сетей». Источник: Стрельцов А. А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности. Указ. соч.

касающихся международной информационной безопасности от 12 мая 1999 г., определяется как «состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве»[31].

Что касается международно-правовой практики применения терминов на глобальном уровне, то здесь необходимо обратиться к некоторым документа ГА ООН по данной проблематике. Так, в резолюции ГА ООН от 5 декабря 2018 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» A/RES/73/27[32] используется понятие «информационной безопасности»[33].

Тем не менее в большинстве стран на национальном уровне приняты документы стратегического планирования, стратегии, руководства по информационной безопасности, которые регулируют информационную безопасность в целом и определенные ее аспекты в частности, однако наблюдается подмена понятий на «кибертерминологию».

Ключевым фактором для России в области информационной безопасности является ее активная поддержка на международном уровне, которая способствует формированию целостного взгляда на безопасность информации и её защиту, при этом кибербезопасность считается одним из компонентов этой системы наравне с другими, а информация рассматривается как естественная (аналоговая)[34], либо как искусственная (созданная в ИКТ-среде). Последняя как раз и подразумевает

---

[31] Международная информационная безопасность: подходы России [Электронный ресурс]. Доклад ЦМИБ МГИМО. – 2021. – URL: https://mgimo.ru/upload/2022/03/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii.pdf (дата обращения: 10.08.2024).

[32] United Nations General Assembly Resolution 73/27, Developments in the field of information and telecommunications in the context of international security, A/RES/73/27, 5 December 2018. Resolutions and Decisions adopted by the General Assembly during its 73rd session. Vol. I. 18 September – 22 December 2018 // General Assembly Official Records, 73rd session, Supplement No. 49 (A/73/49 (Vol. I). – New York: United Nations, 2019. – P. 274–277.

[33] В резолюции Генеральной Ассамблеи от 8 октября 2021 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» A/C.1/76/L.13 также используется термин «информационная безопасность».

[34] Молчанов Н. А., Матевосова Е. К. Информационный терроризм в международно-правовом контексте [Электронный ресурс] // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2018. – № 5. – Доступ из справочно-правовой системы «ГАРАНТ». – URL: https://ivo.garant.ru/#/document/77584175 (дата обращения: 10.08.2024).

кибернетический аспект информации, рассматриваемый как техническую ипостась информации[35].

Различия подходов также можно обосновать тем, что в то время, как правовая доктрина США постепенно перешла от основного внимания к информационной безопасности к безопасности сетей и приложений, российская доктрина постепенно увеличивала свое внимание к информационной безопасности, расширив географию проблем[36]. Существует также мнение, что в стремлении сохранить и приумножить свои возможности по организации масштабных операций в информационном пространстве других стран, США и их союзники стараются использовать все возможные способы для того, чтобы противодействовать международно-правовому ограничению таких операций[37]. именно с этой целью «коллективный Запад» является сторонником того, что существующие нормы международного права могут быть применимы к ИКТ-среде без адаптации и необходимости разработки новых норм. С противоположной позицией выступает Российская Федерация, которая обосновывает свой подход потребностью принятия согласованного и отчетливого международно-правового регулирования использования ИКТ и обеспечения безопасности. Также она считает необходимым противостоять милитаризации ИКТ-среды. Под «кибертерминологией» скрывается не только понимание «кибербезопасности» с точки зрения обеспечения защиты, но легализация реализации наступательных операций, в том числе с применением информоружия, из-за правового вакуума в действующем международном праве в части отсутствия ограничение на проведение информационных операций. При этом сторонники данной концепции аргументируют свой подход тем, что использование термина «информационная безопасность» считается неприемлемым из-за возможности ограничения свободы слова и реализации политики цензуры в ИКТ-среде.

---

[35] Godwin III J. B., Kulpin A., Rauscher K. F., Yaschenko V. Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2. [Электронный ресурс] East West Institute and the Information Security Institute of Moscow State University. – 2014. – URL: https://www.files.ethz.ch/isn/178418/terminology2.pdf (дата обращения: 10.08.2024).

[36] US-Russia Cybersecurity Cooperation: Future Paths and Historical Perspective [Электронный ресурс]. – 2021, December 4. – URL: https://geohistory.today/us-russia-cybersecurity-cooperation/ (дата обращения: 10.08.2024).

[37] Жуков Ю., Кузьмин А., Финогенов Д. Терминология в сфере международной информационной безопасности. Указ. соч.

С учетом наличия терминологических расхождений важно упомянуть инициативу Российской Федерации: еще в 2010 г. российская стороны выступила с предложением использовать компромиссный термин «безопасность при использовании ИКТ и самих ИКТ»[38], который возможно рассматривать как допустимый для использования на международном уровне с сохранением ИКТ-терминологии в национальном законодательстве. Данная инициатива была поддержана ГПЭ ООН в 2015 г.

Еще одним компромиссным использованием терминов стала формулировка, используемая в наименовании профильного переговорного механизма ООН – РГОС ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025. Как ранее было отмечено автором диссертационного исследования, именно данная формулировка рассматривается наиболее целесообразной ввиду отсутствия взаимоприемлемого понятийного аппарата для описания концепций понимания ИКТ и обеспечения безопасности в сфере их использования, в связи с чем предлагается реализовывать дальнейшее международное нормотворчество в соответствии с данной терминологией.

Однако факт существования глубоких терминологических расхождений сохраняет возможность нахождения реальной общности взглядов на природу и управление ИКТ далекой[39]. Так как инициативы, направленные на гармонизацию терминологии в русском и английском языках, в основном исходят от российской стороны, они не имеют положительного исхода из-за политической составляющей. В связи с этим автором видится полезным для достижения прогресса в переговорах по формированию системы международно-правового обеспечения безопасности в контексте применения ИКТ рассмотрение возможности создания специализированного экспертного механизма в рамках системы ООН, объединяющего юристов-международников и специалистов по ИКТ-проблематике

[38] Жуков Ю., Кузьмин А., Финогенов Д. Терминология в сфере международной информационной безопасности. Указ. соч.

[39] Keir G., Hagestad W. Divided by a common language: Cyber definitions in Chinese, Russian and English [Электронный ресурс] // 5th International Conference on Cyber Conflict. – 2013. – URL: https://www.researchgate.net/publication/261300676_Divided_by_a_common_language_Cyber_definitions_in_Chinese_Russian_and_English (дата обращения: 10.08.2024).

на равной географической основе и в полномочия которого входило бы исследование особенностей терминологии в исследуемой области и выработка рекомендаций для государств для гармонизации понимания и трактовки терминов, связанных с ИКТ. Создание такого механизма имеет потенциал внести вклад в кодификацию международного права, а также заложить основу для формирования необходимых условий в виду необходимости согласования различных подходов к регулированию использования ИКТ в контексте международной безопасности и гармонизации национальных правовых систем с конечной целью разработать соответствующий международно-правовой акт.

1.2. Концептуализация информационно-коммуникационных технологий и регулирование обеспечения безопасности в сфере их использования в международно-правовой доктрине

Общая значимость исследуемой проблематики обуславливает постановку перед наукой международного права задачи определить основные цели и принципы выстраивания отношений в области информацбезопасности. Появление все большего количества юридических трудов и совокупности теоретических знаний, в свою очередь, ведет к формированию новой отрасли права, представляющей собой совокупность специальных международных принципов и норм, определяющих права и обязанности субъектов международного права в информационном пространстве в целом. Обеспечения безопасности в сфере использования ИКТ как направление международного сотрудничества признается проблемой как на национальном, так и на глобальном уровнях, находясь на повестке дня различных международных организаций. Данная проблематика, будучи составным институтом международного информационного права (МИП), получает свое юридическое оформление в виде однородной группы норм,

регулирующих общественные отношения в процессе обеспечения информационной безопасности[40].

Важно отметить, что на уровне национального законодательства многие правовые семьи признали за информационным правом отраслевой статус. Тем не менее, в отечественной и зарубежной доктрине международного права стоит вопрос о наличии достаточных свойств для признания за совокупностью международно-правовых норм в информационной сфере статуса отрасли международного права. В данном контексте важно упомянуть о наличии разных подходов в доктрины международного права по этому вопросу[41], такое разнообразие может объясняться помимо комплексного объекта регулирования тем, что в основе первых документов, в которых наблюдаются попытки юридически оформить информационное пространство, лежит бессистемный характер[42]. Как верно отмечает, А. Я. Капустин обозначенный фактор обусловил отставание доктрины международного права от технологического развития и необходимость научного осмысления международного правотворчества относительно ИКТ-среды.

Тезис приверженцев идеи появления права международной информационной безопасности в качестве новой отрасли основывается на включении последней в общую концепцию всеобъемлющей глобальной безопасности[43]. Иными словами,

---

[40] Полякова Т. А., Смирнов А. А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы [Электронный ресурс] // Российский юридический журнал. – 2022. – № 3. – Доступ из справочно-правовой системы «ГАРАНТ». – URL: https://ivo.garant.ru/#/document/76906647 (дата обращения: 10.08.2024).

[41] В том числе такие формулировки, как «международные режимы информационно-коммуникационных технологий», «международные режимы и информационная инфраструктура» и многие другие. Выделяют различные наименования отрасли международного права, предметом которой в той или иной степени выступает информационное пространство или его отдельные элементы, в том числе ИКТ и информационная безопасность: международное информационное право (International Information Law), «право международной информационной безопасности» (International Information Security Law), «международное кибер-право» (International Cyber Law), «международное право Интернета» (International Internet Law), «международное платформенное право» (International Platform Law), «международное цифровое право» (International Digital Law), «международное право массовой информации» (International Mass Media Law), «международное телекоммуникационное право» (International Telecommunications Law) и другие. Источник: Мартиросян А. Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы [Электронный ресурс] // Вестник ученых-международников. – 2022. – № 2 (20). – С. 179–187. – URL: https://elibrary.ru/item.asp?id=49808514 (дата обращения: 10.08.2024).

[42] Капустин А. Я. Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. – 2022. – Т. 18, № 6. – С. 100.

[43] Костенко Н. И. Право международной информационной безопасности: (становление, тенденции и проблемы развития): монография. Указ. соч.

мы можем говорить о том, что рассматриваемая отрасль выступает сформировавшейся системой принципов и норм, которые регулируют отношение субъектов международного права в области обеспечения как информационной безопасности, так и безопасности информации, а также защиты информации государства и других субъектов в мирное и военное время[44]. По мнению автора диссертационного исследования, данная научная концепция имеет слабую сторону в части искусственного вычленения из комплексного спектра международно-правовых отношения в информационной области лишь тех аспектов, которые касаются регулирования информбезопасности на международном уровне.

Наибольшую популярность среди зарубежных исследователей приобрел термин «международное кибер-право» и «международное право Интернета»[45], что обусловлено историей научной дискуссии вокруг необходимости международно-правового регулирования ИКТ-среды и восприятия информационной области с точки зрения кибернетического подхода. «Кибер-право» как дисциплина получила широкое распространение благодаря обсуждениям в американском научном сообществе вокруг проблематики регулирования «киберпространства». Данные подходы к изучению информационной области имеют недостаток с точки зрения определения предмета регулирования в его кибернетическом измерении, так как они не дают возможности ее комплексного изучения.

Проблематика регламентации ИКТ-среды на глобальном уровне стала активно изучаться с 90-х гг. XX в.[46], когда велись дискуссии на тему формулирования норм международного права, определяющих регулирование отношений в киберпространстве. Аксиологическое значение исследований американской школы права в рамках международно-правового регулирования ИКТ

---

[44] Кроме того, данная парадигма также включает в эту систему недопущение информационной войны, информационного терроризма, киберпреступности и агрессии в информационном пространстве. Вместе с этим она концентрируется на защите информационно-телекоммуникационной инфраструктуры, которая включаете в себя компьютеры и расположенные в них данные, защищающие от деструктивных угроз и иных негативных воздействий. Источник: Костенко Н. И. Теоретические проблемы формирования права международной информационной безопасности: монография. – М.: Юрлитинформ, 2019. – С. 27; Костенко Н. И. Право международной информационной безопасности: (становление, тенденции и проблемы развития): монография. Указ. соч.

[45] Kulesza J. International Internet Law. – Routledge Research in Information Technology and E-Commerce Law. – 1st edition. – 2012. – 196 p.

[46] Мартиросян А. Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы. Указ. соч.

в области информационной безопасности заключается в изучение регулирования ИКТ-среды. На основе проведенного исследования автор предлагает выделить три основные правовые школы: кибернигилисты или киберлибертарианцы[47] – сторонники свободного Интернета[48], чья позиция заключается в том, что он не должен становится объектом государственного регулирования, его основной принцип – самоуправление[49], который исторически обусловлен особенностями возникновения и эволюции Интернета; институционалистский подход сводится к необходимости формирования соответствующих институтов механизмов регулирования киберпространства[50] (через трактовку реалистической теории определяет государство как основного регулятора отношений в Интернете, обосновывает формирование международных режимов, в том числе регулирующих ИКТ-среду, интересами государства[51]); наконец, либеральный подход, согласно которому государственного регулирование Интернета будет зависеть от субъекта, интересы которого будут продвигаться[52]. При этом сторонники рассматриваемого подхода отмечают, что суверенитет всемирной сети берет свое начало в консенсусе, который достигается акторами экосистемы Интернета[53].

Что касается международного информационного права, то автор диссертационного исследования разделяет идею выделения данной отрасли наряду

---

[47] Barlow J. P. A Declaration of the Independence of Cyberspace [Электронный ресурс]. – URL: https://www.eff.org/cyberspace-independence/ (дата обращения: 10.08.2024).

[48] Johnson D.R., Post D. Law and Borders: The Rise of Law in Cyberspace [Электронный ресурс]. // Stanford Law Review. – 1996. – Vol. 48, No. 5. – P. 1367–1402. – URL: https://www.researchgate.net/publication/220167912_Law_and_Borders_The_Rise_of_Law_in_Cyberspace (дата обращения: 10.08.2024).

[49] Lessig L. The Path of Cyberlaw [Электронный ресурс] // University of Chicago Law School Chicago Unbound Journal Articles. – 1995/ – URL: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=11678&context=journal_articles/ (дата обращения: 10.08.2024).

[50] Иванова К. А., Мылтыкбаев М. Ж., Штодина Д. Д. Понятие киберпространства в международном праве // Правоприменение. – 2022. – Т. 6, № 4. – С. 37.

[51] А сам Интернет как «регулируемое пространство посредством четырех форм регулирования: закона, социальных норм, рынка и кодовой архитектуры». Источник: Goldsmith J. L. Against Cyberanarchy [Электронный ресурс] // University of Chicago Law Review. – 1998. – Vol. 65, Iss. 4, Article 2. – URL: https://chicagounbound.uchicago.edu/uclrev/vol65/iss4/2/ (дата обращения: 10.08.2024); Lessig L. Code and Other Laws of Cyberspace [Электронный ресурс]. – URL: https://books.google.ru/books/about/Code.html?id=swD6jNulNYEC&redir_esc=y/ (дата обращения: 10.08.2024).

[52] Slaughter A.-M. International Law and International Relations Theory: A Dual Agenda [Электронный ресурс] // American Journal of International Law. – 1993. – Vol. 87, Issue 2. – P. 205–239. – URL: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/international-law-and-international-relations-theory-a-dual-agenda/04816F63C68ACF71DEF4555E1C470D27 (дата обращения: 10.08.2024).

[53] Мартиросян А. Ж. Формирование системы обеспечения безопасности киберпространства: монография / отв. ред. И. О. Анисимов. – М.: Дипломатическая академия МИД России, 2021. – С. 24.

с такими юристами-международниками, как Р. Е. Эннан[54], Т. М. Смыслова[55], А. В. Пазюк[56], А. В. Задорожний и др. При этом для формирования полной научной картины целесообразно упомянуть, что также существует мнение, сторонником которого, например, является д. ю.н. В. П. Талимончик, о том, что преждевременно говорить о МИП в качестве самостоятельной отрасли международного права в виду того, что международно-правовая основа (специализированные нормы и принципы) находятся все еще в процессе формирования[57]. Однако В. П. Талимончик делает важную оговорку, что можно говорить о МИП по мере эволюции специального регулирования ИКТ[58]. Именно в связи нормотворческим процессом в информационной области, который наблюдается в последнее время на международном уровне и в связи с тем, что данная отрасль развивается, целесообразно говорить о ней, хотя ее формирование все еще активно продолжается.

В широком смысле МИП может быть определено следующим образом: «совокупность специальных международных принципов и норм, определяющих права и обязанности субъектов международного права в информационном пространстве. Объектом выступает информационная область в целом, которая рассматривается в качестве «развивающейся системы общественных информационных отношений, осуществляемых субъектами права независимо от расстояний между ними и национальных границ, посредством глобальной информационной инфраструктуры» и как специфическая обособленная область международных отношений. К предмету международного информационного права

---

[54] Эннан Р. Е. Формирование международного информационного права // Правове життя сучасної України: матеріали Міжнар. наук. конф. проф.-викл. та аспірант. складу (м. Одеса, 16–17 травня 2013 р.) / відп. за вип. В. М. Дрьомін; НУ "ОЮА". Півд. регіон. центр НАПрН України. – Одеса: Фенікс, 2013. – Т. 2. – С. 661–664.

[55] Смыслова Т. М. Международное информационное право: Методические материалы к междисциплинарному спецкурсу / сост. Т. М. Смыслова. – М.: СТЭНСИ, 2002. – 192 с.

[56] Пазюк А. В. Понятие международного информационного права как комплексной отрасли международного права [Электронный ресурс] // Actual Problems of International Relations. – 2012. – Vol. 1, No 111. – URL: https://www.academia.edu/4459264/Понятие_международного_информационного_права_как_комплексной_отрасли_международного_права (дата обращения: 10.08.2024).

[57] Талимончик В. П. Международно-правовое регулирование отношений информационного обмена. – Санкт-Петербург: Юридический центр Пресс, 2011. — 382 с.

[58] Там же.

можно отнести международно-правовые отношения[59] в информационной области в целом»[60].

Говоря о субъектной характеристике, важно подчеркнуть, что, отвечая на вопрос того, кого именно можно отнести к субъектам МИП, необходимо обратится к теории международного публичного права, где мы найдем ответ на данный вопрос. Среди субъектов международного информационного права как новой отрасли международного публичного права выделяются первичные и вторичные субъекты как такового международного права в их классическом понимании[61]. При этом некорректно детерминировать всех субъектов отношений в информационной области как субъектов МИП в частности и международного права в целом. Все субъекты (акторы ИКТ-среды)[62] в данной области не являются субъектами международного права, так как не обладают всеми элементами правосубъектности[63]. Примечательно, что в рамках переговорного процесса по исследуемой проблематике наблюдается тенденция со стороны некоторых государств, которая сводится к попыткам предоставить доступ негосударственным субъектам к дискуссиям, а также поднять вопрос их правосубъектного статуса в рамках международного права. В данном случае интересна для рассмотрения концепция, выдвинутая И. И. Лукашуком, который считает индивида не субъектом, а «бенефициарием» международного права. По принципу аналогии

---

[59] Информационные отношения и информационно-инфраструктурные, обеспечивающие обращение (коммуникацию) информационных ресурсов, межгосударственные отношения в информационной области и др.

[60] Мартиросян А. Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы [Электронный ресурс] // Вестник ученых-международников. – 2022. – № 2 (20). – URL: www.dipacademy.ru/documents/5584/Вестник_СМУ_ДА_220_2022_ред2__финал-2.pdf (дата обращения: 10.08.2024).

[61] Там же.

[62] Например, согласно Доктрине информационной безопасности Российской Федерации 2016 г., «участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности». Источник: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.

[63] Международная правоспособность, международная дееспособность и международная деликтоспособность.

можно заключить, что в случае, если НПО смогут принимать участие в международном правовом регулировании вопросов обеспечения безопасности ИКТ, они будут являться «бенефициарием» международного права»[64]. Интересна также позиция А. В. Пазюка. Согласно ему, отдельные категории акторов международных отношений, а именно физические и юридические лица, могут рассматриваться как «дестинаторами» прав и обязанностей[65]. Статус негосударственных субъектов и модальности их участия в РГОС ООН неоднократно обсуждались. Так, первая субстантивная сессия РГОС ООН 2021-2025 гг. началась с горячих дебатов по нерешенному вопросу об условиях участия многих заинтересованных сторон в официальных заседаниях, поскольку он не был согласован на организационном совещании в июне 2021 г. Председатель РГОС ООН предложил сохранить прецедент первой РГОС ООН в отношении участия заинтересованных сторон в официальных заседаниях, РГОС ООН может продолжать привлекать заинтересованные стороны к проведению непосредственно неофициальных консультативных совещаний. Данный вопрос вызвал дискуссии в части способа участия негосударственных заинтересованных сторон в переговорных процессах[66]. Так как РГОС ООН должна принимать решения консенсусом, данный вопрос был перенесен на обсуждение в ходе второй субстантивной сессии. Право государств выступать против участия определенных заинтересованных сторон было рассмотрено в контексте ряда предложений по повышению прозрачности принятия данных решений, чтобы это способствовало лучшему пониманию озабоченностей других стран и закладывало основы для прозрачного, инклюзивного и ориентированного на результат переговорного

[64] Правовые проблемы формирования межгосударственных объединений (на примере зоны свободной торговли и таможенного союза ЕВРАЗЭС) [Электронный ресурс]: монография / отв. ред. В. Ю. Лукьянова. – Доступ из справочно-правовой системы «ГАРАНТ». – URL: https://ivo.garant.ru/#/document/57736662 (дата обращения: 10.08.2024).

[65] Они «в силу международного-правового урегулирования информационных отношений на международном уровне являются конечными приобретателями – «дестинаторами» тех или иных информационных прав и обязанностей, которыми их наделяет государство как первичный и полноправный субъект международного права». Источник: Пазюк А. В. Международное информационное право. Общая часть. Международное информационное право – отрасль современного международного права [Электронный ресурс]. – URL: http://cyberpeace.org.ua/files/razdel-1.pdf (дата обращения: 10.08.2024).

[66] Modalities of multistakeholder participation, 13 Dec 2021 15:00h – 18:00h [Электронный ресурс]. – URL: https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/modalities-of-multistakeholder-participation (дата обращения: 10.08.2024).

процесса. При этом отмечалось, что РГОС ООН является межправительственным процессом, возглавляемым государствами, и нынешняя схема проведения заседаний, в частности неофициальные консультации, установленные предыдущей РГОС ООН, уже предоставили неправительственным организациям достаточно времени и возможностей для выражения своих мнений.

По мнению автора диссертационного исследования, ответ на вопрос, будут ли негосударственные субъекты, в числе которых неправительственные организации, частный сектор, экспертное и техническое сообщества, а также индивиды, выступать субъектами новой отрасли права однозначен, так как согласно нормам международного права, они не обладают международной правосубъектностью. Автор считает целесообразным иной подход, согласно которому негосударственные субъекты относят к категории функциональных субъектов международного права в случае, если они будут реализовывать свою правосубъектность в том или ином варианте.

Верховенство права зиждется на принципах международного права, которые выполняет регулирующую и др. функции международных отношений. Разработка и принятие принципов обеспечения безопасности в контексте применения ИКТ является повесткой ООН на протяжении долгого времени, однако на данный момент в связи с разногласиями государств относительно регулирования ИКТ-среды, процесс сосредоточен в рамках переговорного формата и попытках достичь компромисса. Основные принципы МИП имеют своим фундаментом статью 2 Устава ООН, которая определяет общие принципы международного права. Декларация о принципах международного права 1970 г. дала им дальнейшее развитие. В ней было конкретизировано нормативное содержание каждого из них. Следующей важной вехой в развитии принципов международного права стало 1 августа 1975 г. – день подписания тридцатью пятью странами Заключительного акта СБСЕ. Акт закрепляет десять принципов, дополняя семь принципов Устава ООН еще тремя, которые отражали новые особенности обеспечения международного правопорядка в свете его гуманизации: нерушимость государственных границ, территориальная целостность государств, уважение прав

человека и основных свобод. Так, например, рассмотрим принцип суверенного равенства применительно к информационной области: все государства должны уважать право друг друга на выбор собственного пути реализации информационной политики, а также на равноправной основе участвовать в управлении информационным пространством. В данном контексте важно отметить, что историческая особенность норм международного права вызывает дискуссию в части применимости действующих норм к ИКТ. Существует две основные позиции по данному вопросу: первая раскрывает подход России, Китая и ряда других государств и сводится к необходимости выработки новых норм международного права, которые будут применимы непосредственно ИКТ и будут соответствовать особенностям их продолжающейся эволюции; вторая отражает мнение коллективного Запада в лице США и ряда европейских стран и подразумевает возможность применения действующих норм к ИКТ без необходимости их адаптации и выработки новых норм. Отсутствие единства по рассматриваемому вопросу предопределяет переменный успех переговорного процесса в рамках ООН, характеристика которого более подробно дана в Главе 2 настоящего диссертационного исследования. Кроме основополагающих принципов международного права, выделяют формирующиеся специальные отраслевые принципы, которые применяются непосредственно в международном информационном праве и имеют пока больше политическое, чем юридическое значение. «Международные принципы создания информационного общества и подходы к его созданию, декларируемые Окинавской хартией глобального информационного общества 2000 г., Декларацией принципов «Построение информационного общества – глобальная задача в новом тысячелетии» 2003 г., Планом действий Тунисского обязательства 2005 г.»[67], лежат в их основе. Помимо них, можно обозначить некоторые другие отраслевые принципы, при этом они все еще находятся в стадии формирования, к ним можно отнести следующие:

[67] Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. – 2017. – № 20. – Ст. 2901.

равенство государств в ИКТ-среде, право государств на осуществление и санкционирование трансграничного телерадиовещания, принцип инклюзивного доступа к ИКТ, принцип обеспечения свободного доступа к источникам информации, принцип мирного использования информационного пространства, принцип ответственности государств в ИКТ-среде, принцип атрибуции, принцип совместного управления информационным пространством в целом и Интернетом в частности, принцип обеспечения культурного разнообразия в ИКТ-среде и др.

Наблюдается также становление специальных институтов МИП, которые учитывают специфику ИКТ-среды[68]. Это, например, институт обеспечения безопасности в сфере использования ИКТ, институт регулирования трансграничного информационного обмена, институт защиты прав человека в информационной сфере, институт ответственности в рамках регулирования ИКТ, который, согласно Комиссии международного права, отражает факт прогрессивного развития международного права, он нашел свое закрепление в резолюциях Генеральной Ассамблеи ООН благодаря деятельности ГПЭ ООН, РГОС ООН, Специального комитета ООН по разработке всеобъемлющей международной конвенции по противодействию использованию ИКТ в преступных целях и многие другие.

Что касается источников международного информационного права, то несмотря на отсутствие на сегодняшний день универсального международно-правового акта, который регулирует все направления деятельности в информационной области и который имеет общеобязательный характер, существует многочисленное количество источников международного права, предметом которых являются определённые аспекты данной области, подробнее о них будет написано в пунктах 1.3. и 2.2. диссертационного исследования. При этом ведется активная работа с целью разработки и принятия подобного документа.

Несмотря на наличие теоретических разногласий и различных подходов к определению и содержанию новой отрасли права, существует общая черта – все

[68] Мартиросян А. Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы. Указ. соч.

они имеют своим объектом информационную области или ее составляющие. При этом факт того, что существует разнообразие подходов к выделению новой отрасли международного права обусловлен спецификой эволюции международно-правовых отношений исследуемой области[69]. Во-первых, это связано с тем, что предмет регулирования достаточно нов, постоянно развивается, а международное право не поспевает за прогрессом ИКТ-среды. Во-вторых, на данный факт влияет также фрагментированное регулирование ИКТ и отсутствие единого терминологического аппарата. Несмотря на эти сложности, автор заключает и научно обосновывает, что происходит процесс формирования самостоятельной отрасли международного права, а сама идея выделения международного информационного права соотносится с системным подходом к изучению информационной области.

1.3. Регулирование обеспечения безопасности в сфере использования информационно-коммуникационных технологий в Российской Федерации

Исторически основой регулирования использования ИКТ выступает законодательство и юридическая практика отдельных государств. Исходя из этого, эволюцию международно-правового регулирования обеспечения безопасности в контексте применения ИКТ нельзя исследовать без национальных законодательств, которые в значительной мере влияют на его формирование. Данная часть диссертации будет ограничена анализом концептуальных и правовых основ Российской Федерации в части регулирования ИКТ с целью обеспечения безопасности в сфере их применения в контексте внешнеполитической деятельности. В РФ регулирование использования ИКТ обеспечивается самостоятельной отраслью – законодательством в области информации[70]. Нормативно-правовая база Российской Федерации, определяющая регулирование

[69] Мартиросян А. Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы. Указ. соч.

[70] Меньшиков П. В. Особенности государственного регулирования информационной сферы России [Электронный ресурс] // Международные коммуникации. – 2018. – № 1 (6). – URL: https://intcom-mgimo.ru/2018/2018-06/state-regulation-of-russian-information-sphere (дата обращения: 10.08.2024).

обеспечения информбезопасности, сравнительна нова. Тем не менее она связана с непрерывным развитием ИКТ, которая ставит перед законодателем постоянной адаптации законодательства. Последнее, в свою очередь, выступает движущей силой для развития информационного законодательства в целом и его подотрасли – законодательства об обеспечении информационной безопасности – в частности. В целях настоящего параграфа проанализируем нормативно-правовую базу Российской Федерации, которая регулирует обеспечение безопасности в сфере использования информтехнологий.

К источникам законодательства РФ можно отнести действующее федеральное и иное законодательство, общепризнанные принципы и нормы международного права и международные договоры. Фундаментом законодательства России в целом и регулирования использования ИКТ в частности является основной закон российского государства – Конституция. Статьи 2, 17, 23, 24, 29, 42 имеют важное значение с точки зрения обеспечения реализации международно-правовых обязательств Российской Федерации в области прав человека. Так, статья 2 определяет человека, его права и свободы высшей ценностью, статья 24 закрепляет один из основополагающих принципов прав человека в эпоху глобального информационного общества – невмешательство в личную и семейную жизнь. Часть 4 статьи 15 Конституции[71] устанавливает, что международные договоры России наряду с общепризнанными принципами и нормами международного права выступают составным элементов правовой системы РФ.

Далее обратимся к федеральному законодательству и обозначим основные нормативно-правовые акты, которые в той или иной степени регулируют использование ИКТ с целью обеспечения безопасности в сфере их использования[72]. Ключевым среди них – это Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об

[71] Конституция Российской Федерации: принята всенародным голосованием 12.12.1993: с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации 30 декабря 2008 года № 6-ФКЗ, от 30 декабря 2008 года № 7-ФКЗ, от 5 февраля 2014 года № 2-ФКЗ, от 21 июля 2014 года № 11-ФКЗ, от 14 марта 2020 года № 1-ФКЗ, от 4 октября 2022 года № 5-ФКЗ, от 4 октября 2022 года № 6-ФКЗ, от 4 октября 2022 года № 7-ФКЗ, от 4 октября 2022 года № 8-ФКЗ // Официальный интернет-портал правовой информации (www.pravo.gov.ru). – 6.10.2022. – Ст. 0001202210060013.

[72] Проведен неисчерпывающий обзор.

информации, информационных технологиях и защите информации». Он «регулирует осуществление права на поиск, получение, передачу, производство и распространение информации, применение информационных технологий и обеспечение их защиты»[73], а также наиболее детально отвечает на вопрос, как должен осуществляться правовой режим информационных ресурсов.

Что касается регулирования обеспечения безопасности в области применения ИКТ с точки зрения защиты персональных данных, то ключевым документом российского законодательства выступает Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ[74]. Также помимо регулирования защиты данных Конституцией Российской Федерации, Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и защите информации» 2006 г., отдельными положениями отраслевых законов, данный аспект информационной безопасности урегулирован также многочисленными юридическими и техническими требованиями, изложенными в нормативных актах, изданных Правительством Российской Федерации и специализированными государственными органами в области защиты данных.

Отдельным направлением регулирования обеспечения безопасности в контексте применения новых технологий представляются правовые отношения, на которые распространяются положения о государственной тайне. Законодательство по данному аспекту представлено Законом от 21 июля 1993 г. № 5485-1 «О государственной тайне», Федеральным законом от 28 декабря 2010 г. № 390-ФЗ «О безопасности» и др. Федеральный закон № 187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры» определяет порядок обеспечения безопасности критической информационной инфраструктуры в целях ее функционирования при столкновении с компьютерными атаками и дает характеристику государственной системе

---

[73] Угрозы информационной безопасности в кризисах и конфликтах XXI века [Электронный ресурс] / под ред. А. В. Загорского, Н. П. Ромашкиной. – М.: ИМЭМО РАН, 2015. – 151 с. – URL: www.imemo.ru/files/File/ru/publ/2015/2015_027.pdf (дата обращения: 10.08.2024).

[74] Он был принят в 2005 г. после ратификации Конвенции Совета Европы о защите физических лиц в отношении автоматической обработки персональных данных (Страсбургская конвенция) и основан на международных документах о конфиденциальности и защите данных.

обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы.

Помимо этого, принимаются рамочные программы, направленные на осуществление целей и задач государственной политики с конечной целью обеспечения безопасности в контексте применения ИКТ. Так, была принята госпрограмма «Информационное общество» и национальная программа «Цифровая экономика Российской Федерации».

Международный аспект обеспечения безопасности в контексте применения ИТ выступает также предметом регулирования не только нормативно-правовых актов и норм международного права, но концептуальных программных документов Российской Федерации, которые представлены Стратегией национальной безопасности (СНБ) 2021 г., Основами государственной политики в области международной информационной безопасности 2021 г., Доктриной информационной безопасности (ДИБ) 2016 г., Концепцией внешней политики (КВП) 2023 г. и рядом иных документов, регламентирующими обеспечение национальной безопасности России. Рассмотрим основополагающие из них более подробно.

СНБ 2021 г., рассматривается как «базовый документ стратегического планирования, который определяет национальные интересы и стратегические национальные приоритеты России»[75] как во внутриполитической, так и внешнеполитической линии. Согласно документу, обеспечение информационной безопасности определяется как стратегический национальный приоритет[76]. В документе отмечается рост угроз безопасности, сопряженных с использованием ИКТ, их повсеместным внедрением, особенностями современного информационного пространства и внешнеполитической конъюнктурой, а также стремлением к технологическому доминированию иностранных технологических

[75] Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 4 января 2016 г. – № 1-2, ст. 212.

[76] Среди задач, которые лежат в основе достижения целей обеспечения государственной и общественной безопасности, значится «предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий. Источник: Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 5 июля 2021 г. – № 27-2, ст. 5351.

компаний. С целью достижения обеспечения информационной безопасности определяется 16 задач, среди которых установлена также необходимость расширения взаимодействия России на внешнеполитическом направлении «в области обеспечения информационной безопасности, в том числе в целях установления международно-правового режима обеспечения безопасности в сфере использования ИКТ»[77]. Примечательно, что в предыдущей редакции рассматриваемого документа – СНБ от 31 декабря 2015 г.[78] – также уделялось внимание данной проблематике.[79] Отмечалось, что усиливающееся противостояние на глобальной информационной арене оказывает воздействие на международную обстановку. СНБ 2015 г. также определяла задачу укрепления технологической безопасности, включая информационную сферу, как одно из основных направлений обеспечения национальной безопасности. Сравнив действующую и предыдущую версию стратегии национальной безопасности, можно сделать вывод, о том, что ранее акцент был сделан больше на внутреннюю линию обеспечения информационной безопасности. Данный факт обусловлен тем, что за короткий период с момент принятия предыдущей редакции Стратегии национальной безопасности – 6 лет, данный вопрос приобрел особую актуальность в связи с возросшим угрозами в контексте обеспечения безопасности в сфере использования ИКТ.

ДИБ 2016 г.[80] гласит о важной роли ИКТ в государственном развитии, а также об угрозах, исходящих от их использования. Документ конкретизирует положения, содержащие в предыдущей редакции Стратегии. Положения доктрины, посвященные международному аспекта обеспечения информбезопасности,

---

[77] Указ Президента Российской Федерации от 02 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». Указ. соч.

[78] Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». Указ. соч.

[79] Международная безопасности в среде информационно-коммуникационных технологий [Электронный ресурс]: коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / Национальная ассоциация международной информационной безопасности; под редакцией проф. А. А. Стрельцова, проф. А. Я. Капустина, проф. Т. А. Поляковой, проф. А. С. Маркова, Б. Н. Мирошникова. – Москва, 2023. – URL: https://namib.online/wp-content/uploads/2023/03/Международная-Безопасность-в-Среде-ИКТ.pdf (дата обращения: 10.08.2024).

[80] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 2016. – № 50, ст. 7074.

детерминируют основополагающие направления «содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве»[81]. Научный интерес с точки зрения цели настоящего диссертационного исследования представляет положение о необходимости выработки системы норм международного права, которые будут регулировать международные отношения в информационной области с учетом специфики развития ИКТ, а также будут направлены на инклюзивное сотрудничество в данной области и достижение стратегической стабильности.

Ранее действующая КВП от 30 ноября 2016 г.[82] включала также положения, которые касаются использования ИКТ и обеспечения безопасности в контексте применения информтехнологий как на национальном, так и международном уровнях. В документе была установлена важность укрепления позиций российских СМИ в глобальном информационном пространстве в качестве одной из задач в области обеспечения национальных интересов во внешнеполитической области. В контексте характеристики особенностей реализации российского внешнеполитического курса отмечался наряду с остальными факторами и информационный. ИКТ также упоминаются как элемент комплексной политики «мягкой силы». Помимо этого, было подчеркнуто особое значение выработки новых норм международного права с учетом особенностей развития современных ИКТ и глобального информационного сообщества, а также использования ИКТ, в том числе Интернета, на равной справедливой основе. В рамках информационного сопровождения внешнеполитической деятельности Концепция внешней политики России 2016 г. определяла одним из направлений деятельности достоверное

[81] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 2016. – № 50, ст. 7074.
[82] Указ Президента Российской Федерации от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // Собрание законодательства Российской Федерации. – 2016, 5 декабря. – № 49, ст. 6886.

информирование мирового сообщества о взглядах России на различные международные процессы, реализациях внутри- и внешнеполитического курса страны. При этом также говорилось о стремлении России использовать ИКТ для формирования национальной и международной информационной безопасности. Также документ устанавливал задачу выработки совокупности правовых и этических основ[83] применения ИКТ. Часть IV документа, посвящённая обзору российских региональных приоритетов, содержала положение об осуществлении коллективным Западом информационного давления на Россию, что несомненно представляет угрозу как региональной, так глобальной стабильности, и отображает текущее реалии современных международных отношений.

Действующая КВП от 31 марта 2023 г. во II разделе среди прочих новшеств развития международных отношений отмечает «структурную перестройку мировой экономики, ее перевод на новую технологическую основу (в том числе внедрение технологий искусственного интеллекта, новейших информационно-коммуникационных, энергетических, биологических технологий и нанотехнологий)»[84]. В части, посвященной использованию противоправных инструментов и методов, числятся наступательные и подрывные операции в ИКТ-среде. Использование ИКТ в противоправных целях детерминировано как транснациональный вызов и угроза, а информационное пространство – как новая сфера военных действий. Третий раздел КВП имеет самостоятельный подраздел, который непосредственно охватывает вопросы международно-правового регулирования обеспечения безопасности в контексте применения ИКТ и формирования глобального режима управления ИКТ[85]. Среди приоритетных направлений России отмечены: «1) укрепление и совершенствование международно-правового режима предотвращения и разрешение

[83] Указ Президента Российской Федерации от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации». Указ. соч.

[84] Указ Президента Российской Федерации от 31 марта 2023 г. № 229 «Об утверждении Концепции внешней политики Российской Федерации» [Электронный ресурс] // Собрание законодательства Российской Федерации. – 2023, 3 апреля. – № 14, ст. 2406. – URL: http://www.jurizdat.ru/editions/official/lcrf/archive/2023/14.htm (дата обращения: 10.08.2024).

[85] Путин утвердил новую концепцию внешней политики России [Электронный ресурс] / Агентство информационных сообщений. – URL: https://vg-news.ru/n/165216 (дата обращения: 10.08.2024). – Дата публикации: 31.03.2023.

межгосударственных конфликтов и регулирования деятельности в глобальном информационном пространстве; 2) формирование и совершенствование международно-правовых основ противодействия использованию информационно-коммуникационных технологий в преступных целях; 3) обеспечение безопасного и стабильного функционирования и развитие информационно-телекоммуникационной сети «Интернет» на основе равноправного участия государств в управлении данной сетью и недопущению установления иностранного контроля над ее национальными сегментами; 4) принятие политико-дипломатических и иных мер, направленных на противодействие политике недружественных государств по милитаризации глобального информационного пространства, по использованию информационно-коммуникационных технологий для вмешательства во внутренние дела государств и в военных целях, а также по ограничению доступа других государств к передовым информационно-коммуникационным технологиям и усилению их технологической зависимости»[86]. Примечательно, что среди приоритетных направлений в этом вопросе числится «дальнейшее формирование общего информационного пространства Российской Федерации и государств – участников СНГ, наращивание сотрудничества в информационной сфере с государствами, проводящими конструктивную политику в отношении России»[87], что подчеркивает потенциал организационно-правового (институционального) развития переговорного процесса и международно-правового регулирования обеспечения безопасности в области применения информтехнологий на региональном уровне.

Стратегия развития информационного общества в Российской Федерации на 2017-–030 гг. от 9 мая 2017 г.[88] дифференцирует приоритетные направления, которые считаются необходимыми для успешного развития российских ИКТ, в том числе: нового поколения электронных сетей, эффективной обработки больших

[86] Указ Президента Российской Федерации от 31 марта 2023 г. № 229 «Об утверждении Концепции внешней политики Российской Федерации» [Электронный ресурс] // Собрание законодательства Российской Федерации. – 2023, 3 апреля. – № 14, ст. 2406. – URL: http://www.jurizdat.ru/editions/official/lcrf/archive/2023/14.htm (дата обращения: 10.08.2024).
[87] Там же.
[88] Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». Указ. соч.

данных, ИИ, электронной идентификации и аутентификации (с особым акцентом на банковскую отрасль), облачных вычислений, промышленного Интернета и Интернета вещей, робототехники и биотехнологии; а также информационной безопасности. В рассматриваемом документе подчеркивается необходимость выработки на международном уровне правовых механизмов, которые будут способствовать реализации принципа государственного суверенитета в информационном пространстве, в контексте регулирования национального сегмента Интернета, и которые также будут устанавливать его безопасное и устойчивое функционирование. При этом крайне важен принцип равноправного и инклюзивного участия государств в управлении Интернетом. Выделяется стратегическая задача обеспечения конкурентоспособности российских ИКТ на международном уровне, что крайне важно в условиях стремления ряда стран к технологическому доминированию.

Наконец, 12 апреля 2021 г. были утверждены действующие Основы государственной политики Российской Федерации в области международной информационной безопасности[89]. Данный программный документ является отражением российской позиции на сущность международного аспекта обеспечения безопасности в области применения информтехнологий. По сравнению с предыдущими Основами от 2013 г., наблюдается эволюция подхода к определению МИБ. В Основах от 2013 г., она определяется следующим образом: «такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры». То есть внимание сконцентрировано на правочеловеческой проблематике, обществе и государстве, необходимости формирования системы обеспечения национальной информабезопасности и недопустимости нарушения ее целостности извне. Можно проследить, что национальная информационная безопасность стала

[89] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Собрание законодательства Российской Федерации. – 2021. – № 16-1, ст. 2746.

рассматриваться без отрыва от МИБ на основе принципа неделимости безопасности. При этом особое внимание уделяется непосредственно нормам международного публичного права, которые должны стать юридическим фундаментом системы МИБ. Данный подход отражает факт того, что Российская Федерация является приверженцем принципов и норм, закрепленных в Уставе ООН, и ее позиция полностью с ним согласуется. Также в документе определена главная цель российской государственной политики – установление международного режима обеспечения безопасности в сфере использования ИКТ в целях минимизации угроз в данной области и установления равного сотрудничестве государств, подобные положения мы уже встречали в ранее рассмотренных программных документах, в том числе в ДИБ 2016 г. Эволюция российского видения угроз в области применения ИКТ в данных документах[90] стала отображением отечественного подхода в связи с укоренившейся тенденцией ряда государств использовать ИКТ-среду для дестабилизации общественной и политической обстановки других государств. Обращаясь к угрозам, изложенным в действующей редакции Основ госполитики в области МИБ, можно проследить влияние последствий пандемии, вызванной коронавирусной инфекцией (COVID-19). Несколько изменился характер криминальных угроз: если ранее речь шла только о компьютерной сфере, то в новой редакции основ уже учитываются также угрозы для различного вида мошенничеств, распространённого не только в компьютерной сфере, но и в экономической. Пандемия COVID-19 подтвердила важность обеспечения безопасности информационных ресурсов государств, особенно критической информационной инфраструктуры, наличие угрозы

[90] Российской Федерацией на площадках ООН с начала 2000-х гг. «традиционно выделялась «триада угроз» – использование ИКТ в террористических, преступных и военно-политических целях (под военно-политическими целями понимается использование ИКТ в межгосударственных конфликтах)» // Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. от 24 июля 2013 г. «Наряду с ними также обозначают угрозу использования ИКТ с целью вмешательства во внутренние дела государств различными путями, в том числе посредством манипулирования общественным сознанием и воздействием на внутриполитические и социально-экономические процессы, подрыва и ущемления суверенитета, территориальной целостности». Источник: Зиновьева Е. С. Анализ внешнеполитических инициатив РФ в области международной информационной безопасности [Электронный ресурс]. // Вестник МГИМО-Университета. – 2014. – № 6 (39). – С. 47–52. – URL: https://www.vestnik.mgimo.ru/jour/article/view/240/240/ (дата обращения: 10.08.2024); Lilly B., Cheravitch J. The Past, Present, and Future of Russia’s Cyber Strategy and Forces, 2020 [Электронный ресурс] // 12th International Conference on Cyber Conflict (CyCon), Estonia, 2020. – P. 129–155. – URL: https://ieeexplore.ieee.org/document/9131723 (дата обращения: 10.08.2024).

применения ИКТ с целью атак на них, а также угрозы стремления ряда стран к технологическому доминированию, что также было зафиксировано в документе. Дальнейшую реализацию Основ госполитики в области МИБ в части необходимости достижения технологического суверенитета и обеспечения безопасности информационных ресурсов России в ответ на системную политику западных технологических гигантов монополизировать рынок ИКТ и ограничить доступ к ним мы можем проследить также на примере документов, затрагивающих вопросы запрета использования иностранного программного обеспечения и перехода на отечественное программное обеспечение на объектах критической информационной инфраструктуры[91].

Анализ нормативно-правовых и доктринальных основ регулирования обеспечения безопасности в сфере использования ИКТ в национальном законодательстве России позволяет сделать вывод о преемственности и прозрачности российского подхода, основная цель которого заключается в установлении международно-правового режима, направленного на формировании системы международно-правового обеспечения безопасности в области применения информтехнологий, которая должна строиться на равноправном и инклюзивном участии всех государств, принципе мирного использования информационного пространства, технологическом суверенитете государств, открытом рынке ИКТ, ответственном поведении в ИКТ-среде, расширении международного взаимодействия с целью минимизации угроз в исследуемой области. Таким образом, проведенный сравнительно-правовой анализ позволяет сделать заключение о том, что подход России к обеспечению безопасности в сфере использования ИКТ как на национальном, так и международном уровнях логически эволюционирует, отражая потребности текущего периода развития межгосударственных отношений и международного права с учетом особенностей ИКТ. Автор также полагает, что фундаментальным элементом юридического каркаса обеспечения безопасности в сфере использования ИКТ с точки зрения

[91] К ним можно отнести, например, Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

правотворчества является непрерывное совершенствование правовой базы с учетом особенностей развития ИКТ.

Резюмируя первую главу диссертационного исследования целесообразно отметить, что, проведя анализ терминологического аппарата и его особенностей, можно сделать вывод, что существует фундаментальный теоретико-правовой разрыв между евроатлантическим взглядом на безопасность ИКТ и подходами России и ее единомышленниками. Российский подход отличается целостным пониманием информационной безопасности в отличие от фрагментарного кибернетического подхода к ИКТ «коллективного Запада». Неспособность достичь соглашения по основополагающим терминам, влияющим на формирование международно-правового регулирования обеспечения безопасности в сфере использования ИКТ, свидетельствует о том, что, несмотря на возросшую готовность стран взаимодействовать, это остается чрезвычайно сложной задачей из-за отсутствия общепринятых концепций того, что представляют собой ИКТ, информационная безопасность, кибербезопасность и остальные, связанные с ними термины. Отсутствие консенсуса в основополагающей терминологии в области регулирования ИКТ, а также единства в доктрине международного права относительно понимания терминов приводит к достаточно медленному переговорному процессу по формированию международно-правового регулирования обеспечения безопасности в сфере использования ИКТ[92]. Российской стороне и ее союзникам необходимо и дальше придерживаться ИКТ-терминологии, не допуская признания на глобальном уровне «кибертерминологии», которая в своей перспективе имеет конфликтогенный потенциал. Автором также поддерживается использование компромиссной формулировки – обеспечение безопасности в сфере использования ИКТ, а также предлагается идея учреждения специализированного механизма в рамках системы ООН, деятельность которого будет сосредоточена на способствовании формирования международно-правового регулирования обеспечения безопасности в сфере

[92] Stadnik I. What Is an International Cybersecurity Regime and How We Can Achieve It? [Электронный ресурс] // Masaryk University Journal of Law and Technology. – 2017. – URL: https://www.researchgate.net/publication/318075735_What_Is_an_International_Cybersecurity_Regime_and_How_We_Can_Achieve_It (дата обращения: 10.08.2024).

использования ИКТ с точки зрения юридической лингвистики и герменевтики. Его мандат должен включать исследования особенностей ИКТ-терминологии и ее понимания, а также выработку рекомендаций, направленных на гармонизацию различных концепций.

Помимо этого, автором проведен анализ отечественной и зарубежной доктрины международного права с точки зрения изучения ИКТ и регулирования обеспечения безопасности в сфере их использования, а также идей о формировании новой отрасли международного права. Сделан вывод, что наблюдается отсутствие единого теоретическо-правового подхода к определению и содержанию новой отрасли международного права, предметом которой выступает информационная сфера и ее составляющие, в частности ИКТ. Среди научных идей наиболее оптимальной рассматривается выделение международного информационного права[93].

Что касается анализа нормативно-правовых и доктринальных основ регулирования обеспечения безопасности в сфере использования ИКТ в российском законодательстве, то на основе результатов его проведения можно заключить, что подход Российской Федерации относительно регулирования использования ИКТ и обеспечения безопасности в сфере использования ИКТ отличается преемственностью, транспарентностью, адаптацией к конъюнктуре и потребностям системы международных отношений. Заслуживает быть отмеченным факт того, что основной целью российской информационной политики является обеспечение национальной и международной безопасности на основе принципов, закреплённых в Уставе ООН. Достижение безопасности в сфере использования информтехнологией, согласно проведенному исследованию, определяется Россией в выработке и принятии отраслевых норм и принципов. Они должны стать основой международно-правового регулирования обеспечения безопасности в сфере использования ИКТ, а основополагающими принципами выступают принцип неделимой безопасности, суверенитет и равенство государств в ИКТ-среде, использование ИКТ и ИКТ-среды в мирных целях.

[93] Мартиросян А. Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы. Указ. соч.

ГЛАВА 2. ФОРМИРОВАНИЕ СИСТЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Основная обеспокоенность в сфере использования ИКТ связана с возможностью их применения в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, что актуализирует вопрос формирования системы международно-правового обеспечения безопасности в сфере использования ИКТ и ее составляющих – международно-правовой основы регулирования использования ИКТ, а также институциональных механизмов (организационно-правовой формы регулирования) международного сотрудничества в исследуемой области, в рамках которых ведется деятельность по регламентации ИКТ-среды. В связи с чем данная глава диссертационного исследования посвящена анализу перспектив развития системы международно-правового обеспечения безопасности в сфере использования ИКТ. В частности, в ней отражены теоретические основы международно-правового регулирования использования ИКТ, систематизированы и проанализированы источники международного права, регулирующие обеспечение безопасности в сфере использования ИКТ; изучены особенности развития переговорного процесса исследуемой проблематике; проведена оценка перспектив развития системы международно-правового обеспечения безопасности в сфере использования ИКТ с точки зрения теоретических и институциональных (организационно-правовых) основ международного регулирования ИКТ; выработаны рекомендации для ее дальнейшего формирования в рамках системы ООН; выявлена роль российских инициатив.

2.1. Обеспечение безопасности в сфере использования информационно-коммуникационных технологий: современное состояние и перспективы развития международного сотрудничества

Принцип сотрудничества государств выступает фундаментом международных отношений: он обязывает международное сообщество к эффективному сотрудничеству во всех областях международных отношений. Принцип сотрудничества государств, несмотря на свою общеобязательность, носит относительного когентный характер в части свободы воли государства в установлении сотрудниических отношений и выбора партнеров. В данном контексте важно отметить, что в связи повсеместным внедрением ИКТ и их непрерывной эволюцией изменился характер вызовов и угроз, стоящих перед международным сообществом, а также условия и средства обеспечения безопасности в области применения информтехнологий. Это обусловлено изменением восприятия угроз международной и национальной безопасности государствами и другими субъектами международного права[94], что, в свою очередь, преобразует характер международного сотрудничества. В рамках международно-правового обеспечения безопасности в сфере ИКТ данный принцип занимает важное место. Так, например, в докладе ГПЭ ООН за 2015 г. подчеркивается важность сотрудничества: рекомендовано принять меры укрепления доверия для укрепления международного мира и безопасности, что повысило бы межгосударственное сотрудничество. Иными словами, государствам было рекомендовано стремиться «содействовать трансграничному сотрудничеству в целях устранения уязвимостей критической инфраструктуры» и укреплять сотрудничество на всех уровнях. В пункте 19 доклада также отмечается, что «международное сотрудничество и помощь могут сыграть важную роль в предоставлении государствам возможности обезопасить ИКТ и обеспечить их мирное использование». Помимо этого, доклад РГОС ООН от 2021 г. также содержит положение, согласно которому признается

[94] Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции [Электронный ресурс]. Диссертация на соискание ученой степени доктора политических наук. – Москва, 2019. – URL: https://viewer.rsl.ru/ru/rsl01010014439 (дата обращения: 10.08.2024).

важность принципа международного сотрудничества в данной области: распространение и применение информационных технологий не должны нарушать международные нормы и принципы в области обеспечения мира, стабильности и безопасности, однако использование ИКТ может быть несовместимым с целями поддержания международного мира, стабильности или безопасности. В связи с этим Генеральная Ассамблея признала, что широкое международное сотрудничество могло бы стать эффективным способом для предотвращения негативных последствий использования ИКТ[95].

Благодаря усилиям международного сообщества по достижению соглашения о том, как необходимо регламентировать безопасность в сфере использования ИКТ, были разработаны многообразные механизмы, основой которых выступают «двусторонние и многосторонние договоры о сотрудничестве в области информационной безопасности, многосторонние отношения в данной области могут быть разделены на два вида в зависимости от субъектов отношений в ИКТ-среде, участвующих в них: многосторонние отношения государственного и негосударственного характера»[96]. Исследование всех механизмов, занимающихся информбезопасностью ввиду их значительного объема не представляется возможным, поэтому остановимся на некоторых из них.

Исследуемая проблематика устойчиво вошла в повестку дня ООН с 1998 г., когда от России был внесен проект резолюции по этому вопросу в Первый комитет ГА ООН. Он был принят без голосования в качестве резолюции 53/70. Таким образом, данная резолюция содержала исторически первый призыв в адрес государств-членов ООН с просьбой рассмотреть возможные угрозы в области информационной безопасности на международном уровне[97]. С того момента началось активное международное сотрудничество, в том числе по учреждению

---

[95] Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report [Электронный ресурс]. – 2021, 10 March. – A/AC.290/2021/CRP.2. – URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 10.08.2024).

[96] Мартиросян А. Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы. Указ. соч.

[97] 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 (190). – С. 138.

межправительственных процессов для решения вопросов информационной безопасности и применения ИКТ в контексте международной безопасности. В рамках нормотворческого процесса в данном направлении самыми важными инициативами являются такие механизмы ООН, как ГПЭ ООН и РГОС ООН.

В ООН вопрос обеспечения безопасности в сфере использования ИКТ, помимо этого, был рассмотрен в 1999 г. на 53-й сессии Генеральной Ассамблеи ООН. Двойственный характер достижений науки и техники в гражданской и военной сферах был признан резолюцией 53/73, в которой также отмечалось, что научно-технический прогресс следует использовать во благо человечества в целях обеспечения устойчивого экономического и социального развития всех стран, а также обеспечения безопасности на международной арене[98]. Данная резолюция продемонстрировала готовность подавляющего большинства государств активизировать совместные усилия в целях противодействия транснациональным угрозам от использования ИКТ с целью обеспечения международной безопасности.

После нескольких попыток использовать различные площадки ООН для начала дискуссий было решено, что наилучшим способом является учреждение ГПЭ ООН при Комитете по разоружению. Так, 8 декабря 2003 г. состоялось принятие «резолюции 58/32. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[99], согласно ее положениям, был обеспечен запуск практического решения данной проблематики благодаря учреждению механизма ГПЭ ООН. ГПЭ ООН была создана для исследования угроз в ИКТ-среде и концепций обеспечения безопасности в ней, это стало историческим событием в рамках организационного-правового обеспечения безопасности в сфере использования ИКТ.

---

[98] United Nations General Assembly Resolution 53/73. Role of science and technology in the context of international security and disarmament. – A/RES/53/73. – 4 January 1999. – Resolutions and Decisions adopted by the General Assembly during its 53rd session. – Volume I, Resolutions 9 September – 18 December 1998 // General Assembly Official Records, 53rd Session. – Supplement No. 49 (A/53/49). – New York: United Nations, 1999. – P. 84.

[99] United Nations General Assembly Resolution 58/32. Developments in the field of information and telecommunications in the context of international security. – A/RES/58/32. – 8 December 2003. – Resolutions and Decisions adopted by the General Assembly during its 58th session. – Volume I, Resolutions 16 September – 23 December 2003 // General Assembly Official Records, 58th Session. – Supplement No. 49 (A/58/49). – New York: United Nations, 2004. – P. 131.

Первая ГПЭ ООН собралась под эгидой Комитета ООН по разоружению в 2004–2005 гг., ее деятельность не привела к принятию консенсусного доклада по многочисленным причинам, среди которых в том числе нежелание постоянных членов СБ ООН согласовать направление доклада и отсутствие понимания серьезности проблем обеспечения безопасности в области применения ИКТ, так как в основном использование ИКТ и их регулирование рассматривались в техническом контексте[100].

На фоне того, что в 2000-е гг. последовала волна значительных атак с использованием ИКТ на правительственные учреждения, оборонные и высокотехнологичные компании[101] и увеличилось число таких инцидентов, актуальность вопроса о необходимости принятия соответствующих мер по обеспечению безопасности в сфере использования ИКТ на международном уровне стала более ощутимой.

В 2006 г. Российская Федерация предложила резолюцию Генеральной Ассамблеи ООН о создании новой ГПЭ ООН в 2009 г.[102] Деятельность второй ГПЭ знаменовала собой разработку и принятие первого успешного доклада в 2010 г., который представляет собой лаконичный документ, включающий положения о существующих угрозах сфере использования ИКТ, меры сотрудничества и рекомендации. В нем признавались рост угроз международной и национальной информационной безопасности, исходящий от применения ИКТ, а также необходимость активизации и углубление международного взаимодействия с целью обеспечения безопасности в области применения ИКТ, были выработаны рекомендации «по разработке мер укрепления доверия и прочих мер в целях снижения риска возникновения неправильного восприятия в результате

---

[100] Tiirmaa-Klaar H. The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body [Электронный ресурс] // Cyberstability Paper Series. – 2021, December. – URL: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf (дата обращения: 10.08.2024).

[101] Significant Cyber Incidents Since 2006 [Электронный ресурс]. – URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/220404_Significant_Cyber_Incidents.pdf?6baqc92oMg0w.0wCwZLP6OATs9MmMmLG (дата обращения: 10.08.2024).

[102] United Nations General Assembly Resolution 61/54. Developments in the field of information and telecommunications in the context of international security. – A/RES/61/54. – 6 December 2006. – Resolutions and Decisions adopted by the General Assembly during its 61st session. – Volume I, 12 September – 22 December 2006 // General Assembly Official Records, 61st session. – Supplement No. 49 (A/61/49 (Vol. I). –New York: United Nations, 2007. – P. 127.

дезорганизации или нарушений, связанных с применением ИКТ», в том числе посредством «обсуждения норм, касающихся государственного использования ИКТ, сокращения коллективного риска и защиты критической национальной и международной инфраструктуры», а также выработки терминологической основы[103]. Данный доклад и деятельность ГПЭ ООН второго созыва подготовили основу к дальнейшему переговорному процессу.

Данный путь продолжила третья ГПЭ ООН, которая реализовывала свою деятельность с 2012 по 2013 гг. В ее заключительном документе были определены элементы, которые будут в дальнейшем использованы как основы «ответственного поведения государств в ИКТ-среде[104]. В докладе были, помимо этого, представлены главы, посвященные угрозам, рискам и факторам уязвимости; сотрудничеству, направленному на формирование устойчивого и открытого ГИО, в котором ключевую роль должны играть государства и ООН, важное место занимает также деятельность в рамках иных международных структур регионального и субрегионального характера. В докладе также установлена необходимость продолжения работы по достижению единой позиции по поводу того, как именно нормы международного права должны применяться к использованию ИКТ, а также подчеркивается, что специфика развития ИКТ открывает вопрос разработки новых норм международного права. Данный аспект был наиболее спорным с самого начала деятельности ГПЭ ООН, по нему сформировалось одно из основных расхождений в проблематике обеспечения безопасности в сфере использования ИКТ. Так, «коллективный Запад» выступает

[103] United Nations General Assembly Sixty-fifth session. Item 94 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security [Электронный ресурс] / Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. – A/65/201. – 30 July 2010. – URL: https://digitallibrary.un.org/record/688507?ln=ru (дата обращения: 10.08.2024).

[104] Добровольные, не имеющие обязательной силы нормы ответственного поведения государства в мирное время, меры укрепления доверия и обмена информацией, а также меры по наращиванию потенциала. Источник: United Nations General Assembly Sixty-eighth session. Item 94 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security [Электронный ресурс] / Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. – A/68/98. – 24 June 2013. – URL: https://digitallibrary.un.org/record/753055 (дата обращения: 10.08.2024).

за применимость существующего международного права, в том числе гуманитарного, к ИКТ-среде. Российская Федерации считает необходимым выработку специализированных норм. В этом контексте первым шагом стало предложение еще в 1998 г. Кодекса поведения в области информбезопасности. Предусматривалась выработка специального документа ООН с учетом специфики развития ИКТ. В данном контексте особенно важно упомянуть инициативу Китая и России 2011 г. и государств-членов ШОС 2015 г.

Доклад ГПЭ ООН за 2013 г. лег в основу следующего заключительного документа ГПЭ ООН, функционирующей с 2014 по 2015 гг. Его центральной повесткой стали добровольные нормы ответственного поведения государств в мирное время, рассмотрение дополнительных аспектов международного права, в том числе принципов, среди которых гуманность, необходимость, соразмерность. Международное гуманитарное право (МГП) не упоминалось из-за опасности использования ИКТ-среды в военных целях.

ГПЭ ООН 2013 г. и 2015 г. добились важных результатов в части некоторых вопросов международного права, в том числе о том, что международное право и принципы суверенитета и невмешательства применимы к ИКТ-среде. Было достигнуто соглашение по 11 нормам ответственного поведения государств, мерам укрепления доверия и скоординированному наращиванию потенциала в рамках обеспечения безопасности в сфере использования ИКТ.

ГПЭ ООН, проводя свою деятельность в 2016–2017 годах, не смогла добиться значительных результатов в связи с нестабильной международной ситуацией и разногласий между государствами по различным аспектам обеспечения безопасности в сфере использования ИКТ[105]. Отсутствие консенсуса по мандату группы в 2017 г. в части того, должна ли она обсуждать только вопросы обеспечения информационно-технологического или социально-гуманитарного компонента безопасности. Вопросы о применении силы и международного

[105] Сборник докладов участников XIII международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Москва, 22–25 апреля 2019 г. [Электронный ресурс] / Национальная ассоциация международной информационной безопасности. – URL: https://elibrary.ru/item.asp?id=45719883 (дата обращения: 10.08.2024).

гуманитарного права к деятельности государств[106] также деструктивно повлияли на итоги ее работы[107]. Учитывая сложности, региональные механизмы попытались заполнить вакуум в создании норм, регулирующих обеспечение безопасности в области применения ИКТ. ГПЭ ООН 2016-2017 г. не смогла согласовать консенсусный доклад из-за отсутствия единой позиции государств и обеспокоенности некоторых государств милитаризацией ИКТ-среды.

Семьдесят третья сессия Генеральной Ассамблеи ООН 2018 г. с обсуждениями в Первом комитете завершились тем, что было выработано две резолюции. Резолюция под авторством США 73/266 включала предложение о созыве новой ГПЭ ООН для дальнейшей работы по достижению понимания о том, как должны применяться нормы международного права к ИКТ[108]. Автором второй резолюции выступила Российская Федерация, которая выступила с предложением о создании РГОС ООН с возможностью участия всех государств-членов ООН[109], в отличие от ограниченного формата ГПЭ ООН[110]. Это привело к необычной ситуации, когда два механизма в рамках ООН параллельно занимаются почти одними и теми же вопросами, но в разных форматах.

Первые два совещания ГПЭ ООН проходили относительно гладко до второй сессии в Женеве в 2020 г., однако пандемия коронавирусной инфекции повлияла на формат проведения переговоров: как ГПЭ ООН, так и РГОС ООН перешли в

---

[106] Moynihan H. The Application of International Law to State Cyberattacks [Электронный ресурс]. Research paper. – 2019, December 2. – URL: www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/6-processes-reaching-agreement-application/ (дата обращения: 10.08.2024).

[107] Kyslytsya I. International Cooperation in Ensuring International Information Security [Электронный ресурс]. Thesis for the degree of Master of Arts in International Relations. – Central European University Department of International Relations Vienna, Austria, 2021. – URL:https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwix8uH2zob3AhXBAxAIHd9_ApQQFnoECA8QAQ&url=https%3A%2F%2Fwww.etd.ceu.edu%2F2021%2Fkyslytsya_ian.pdf&usg=AOvVaw2jaEt9GZg1Thw0CJ8SjYsV/ (дата обращения: 10.08.2024).

[108] United Nations General Assembly Resolution 73/266. Advancing responsible State behaviour in cyberspace in the context of international security. – A/RES/73/266. – 22 December 2018. – Resolutions and Decisions adopted by the General Assembly during its 73rd session. – Volume I, 18 September – 22 December 2018. – General Assembly Official Records, 73rd session. – Supplement No. 49 (A/73/49, Vol. I). – New York: United Nations, 2019. – P. 410–412.

[109] Мысина А. И. Международно-правовое регулирование сотрудничества государств по противодействию преступлениям в сфере информационных технологий [Электронный ресурс]. Диссертация на соискание ученой степени кандидата юридических наук. – Москва, 2021. – URL: https://viewer.rsl.ru/ru/rsl01010794479 (дата обращения: 10.08.2024).

[110] United Nations General Assembly Resolution 73/27. Developments in the field of information and telecommunications in the context of international security. – A/RES/73/27. – 5 December 2018. – Op. cit.

виртуальные залы заседаний с неопределенной перспективой их результатов[111]. Итоговый доклад ГПЭ ООН 2019-2021 гг. стал символом многосторонней дипломатии, который охватил интересы всех сторон и продемонстрировал стремление стран к достижению консенсусных рекомендаций.

Что касается РГОС ООН, то она начала свое функционирование в 2019 г. на основе резолюции, автором которой выступила Российская Федерация. В сентябре 2019 г. все государства, участвующие в ГПЭ ООН 2019-2021 гг., приняли участие в первом предметном обсуждении РГОС ООН в Нью-Йорке, США. Ожидалось, что ГПЭ ООН создаст дополнительный уровень понимания «норм ответственного поведения государства в ИКТ-среде и будет проводиться относительно небольшой группой, в то время как РГОС ООН станет инклюзивным органом по повышению осведомленности и дискуссий по применимости норм международного права, норм ответственного поведения государств, мер укрепления доверия и наращивания потенциала, в том числе с привлечением негосударственных субъектов ИКТ-среды. В мандат РГОС ООН вошло изучение существующих норм, которые содержались в предыдущих итоговых документах ГПЭ ООН. В соответствии со своим мандатом, определенном в резолюции 73/27 Генеральной Ассамблеи ООН, РГОС ООН должна была обсудить и представить доклад[112]. РГОС ООН провела три субстантивные сессии 9-13 сентября 2019 г., 10–14 февраля 2020 г., а заключительная сессия была проведена в период с 8 по 12 марта 2021 г. Итог первой сессии РГОС ООН в сентябре 2019 г. продемонстрировал, что большинство государств придерживаются использования рекомендации ГПЭ ООН за 2015 г. Однако множество вопросов, связанных с международным правом, оставались не разрешенными, например, как международное право применяется к ИКТ и какие необходимо определить пути содействия соблюдению существующих норм. Через полтора года деятельности на консенсусной основе был принят доклад РГОС ООН

[111] Tiirmaa-Klaar H. The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body. Op. cit.

[112] По шести пунктам: 1) существующие и потенциальные угрозы; 2) правила, нормы и принципы; 3) применимость международного права; 4) меры укрепления доверия; 5) наращивание потенциала; 6) регулярный институциональный диалог.

в марте 2021 г.[113] Согласно одобренному ГА ООН 28 апреля 2021 г. докладу РГОС ООН[114], государства подтвердили, что международное право применимо к ИКТ-среде. В связи с дебатами по окончательной формулировке данного тезиса он заслуживает отдельного анализа. Согласно эксперту DiploFoundation П. Иттельсону, существует несколько позиций: первая группа государств была удовлетворена финальной формулировкой (Форум Тихоокеанских островов, Движение неприсоединения, Греция), вторая коалиция выступала за то, чтобы международное право и Устав ООН применялись во всей своей полноте к ИКТ-среде, наконец, третья группа стран[115] – за включение конкретного упоминания о том, что применяется МГП, право прав человека и обычное международное право[116]. Последняя позиция встретила возражения со стороны Китая, Кубы, Белоруссии и России, которые аргументировали это тем, что это узаконило бы милитаризацию ИКТ-среды. Отсутствие упоминания международного гуманитарного права в тексте заключительного доклада стало камнем преткновения.

Помимо этого, обсуждалось внесение в итоговой документ конкретных принципов международного права. Камнем преткновения стали отраслевые принципам международного гуманитарного права. Тем не менее, в итоговом докладе упоминается общий принцип международного права – урегулирование споров мирными средствами. Доклад содержит также призыв избегать и воздерживаться от принятия любых мер, которые противоречат действующему международному праву. Исходя из этого, государства пришли к общему решению, что требуется выработка единого понимание того, как международное право

---

[113] Мартиросян А.Ж. Формирование системы обеспечения безопасности киберпространства: монография / отв. ред. И.О. Анисимов. – Дипломатическая академия МИД России, 2021. – С. 50; Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. – 10 March 2021. – A/AC.290/2021/CRP.2. – Op. cit.

[114] Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security established pursuant to General Assembly resolution 73/27 of 5 December 2018 [Электронный ресурс]. – 28 April 2021. – A/DEC/75/564. – URL: https://digitallibrary.un.org/record/3924426?ln=en/ (дата обращения: 10.08.2024).

[115] Нидерланды, Лихтенштейн, Чешская Республика, Австралия и др.

[116] Ittelson P. What's new with cybersecurity negotiations? [Электронный ресурс]. UN Cyber OEWG Final Report analysis. –2021, 19 March. – URL: https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis/ (дата обращения: 10.08.2024).

применяется к ИКТ[117]. В нем подчеркивается важность мер укрепления доверия, которые могут способствовать повышению общей безопасности, устойчивому и мирному использованию ИКТ, а также внедрению норм ответственного поведения государств. В докладе также излагаются принципы наращивания потенциала (пункт 56). Еще одним направлением дискуссий был формат будущих переговоров по обеспечению безопасности в области применения ИКТ. По данному вопросу взгляды государств разделились на две линии. Сторонники первой, среди которых числятся США, ЕС, Япония, Нидерланды, Швеция, Украина, Канада и другие, поддерживают Программу действий и идею создания постоянного форума ООН по вопросам использования ИКТ в контексте международной безопасности[118]. Другая группа государств[119] отстаивала продолжение работы в рамках новой РГОС ООН на 2021–2025 г.[120] В докладе рекомендуется продолжать регулярный институциональный диалог под эгидой ООН. В заключительной части доклада содержится положение о возможности обсуждения юридически обязательных норм[121].

Работа данной РГОС ООН в целом может быть охарактеризована положительно с точки зрения международно-правового обеспечения безопасности в области применения информтехнологий, поскольку это первый доклад, принятый консенсусом за шестилетний период работы, после доклада ГПЭ ООН в 2015 г. Успешный итог деятельности РГОС ООН привел к принятию решения о создании второй РГОС ООН со сроками работы с 2021 по 2025 гг. Так, 1 июня 2021 г. РГОС ООН провела свою организационную сессию[122]. В ходе субстантивной сессии

---

[117] Сборник докладов участников XVI международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Москва, 19–21 сентября 2022 г. [Электронный ресурс] // Национальная ассоциация международной информационной безопасности. – URL: https://elibrary.ru/item.asp?id=50460981 (дата обращения: 10.08.2024).

[118] Мартиросян А. Ж. Международная информационная безопасность: некоторые итоги 2021 г. и политический контекст 2022 г. [Электронный ресурс]. // Интернет сегодня и завтра. Сборник авторских статей к Двенадцатому российскому форуму по управлению интернетом (RIGF 2022), 28–29 сентября 2022 г. – URL: https://cgitc.ru/upload/iblock/ff1/zzzc5u5zgad3ywxomp10xq0foe8fbss5.pdf (дата обращения: 10.08.2024).

[119] Россия, Китай, Южная Африка, Индонезия, Куба и Индия.

[120] Учрежденной резолюцией 75/240.

[121] В дополнение к существующему правовому обеспечению безопасности в области применения ИКТ на международном уровне, основой которого выступает «мягкое право».

[122] РГОС ООН избрала своим Председателем посла Б. Гафура, Постоянного представителя Сингапура при ООН. Государства согласились с тем, «что мандат РГОС на 2021–2025 гг. основывается на резолюции 75/240 Генеральной Ассамблеи ООН и что решения будут приниматься на базе консенсуса». Государства также обсудили возможности

РГОС ООН, состоявшейся в декабре 2021 г., на повестке дня были модальности участия многих заинтересованных сторон (субъектов ИКТ-среды), транспарентность переговорных процессов, ИКТ-угрозы, международное право и Устав ООН, атрибуция атак с использованием ИКТ, наращивание потенциала, меры укрепления доверия, а также регулярный институциональный диалог. Что касается угроз, то большинство государств, выступавших по этому вопросу, подчеркивали угрозы критической инфраструктуре и рост атак, совершаемых посредством программ-вымогателей[123]. Также обсуждались возможные совместные меры по предотвращению и противодействию угрозам в сфере международной безопасности и важность наращивания потенциала[124]. В данном контексте особенно важно упомянуть заявление России, согласно которому для противодействия существующим и потенциальным новым угрозам необходима глобальная система обеспечения безопасности в сфере использования ИКТ под эгидой ООН, которая должна формироваться на основе уважения принципов равноправной безопасности государств и справедливого разрешения споров, которые возникают в результате использования ИКТ.

Несколько государств, а именно Куба, Китай, Иран, Пакистан и Россия, призвали к созданию нового международного юридически обязательного документа, обосновывая это тем, что наблюдается отсутствие согласия по терминологии в отношении ИКТ и прав и обязанностей государств, наличие нерегулируемых вопросов или пробелов в международном праве[125]. Более детально дискуссии велись относительно конкретных принципов и положений Устава ООН. В контексте ст. 51 Устава ООН рассматривались вопросы вооруженного конфликта и право на самооборону. Россия выступила со своей неизменной позицией, согласно которой нет никаких оснований для оценки законности использования

создания тематических подгрупп, вовлечение других заинтересованных сторон, Программу действий, взаимодополняемость процессов ООН и другие вопрос организационного характера.

[123] Помимо этого, упоминались другие угрозы, включающие киберпреступность, экстремизм и терроризм с использованием ИКТ, фейк-ньюс, дезинформацию, угрозы безопасности данных, прав человека, безопасности детей в Интернете, использование ИКТ в военных целях, цифровой разрыв, фрагментация Интернета и многие другие угрозы.

[124] Existing and potential threats, 14 Dec 2021 20:00h – 23:00h. [Электронный ресурс]. – URL: https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/existing-and-potential-threats (дата обращения: 10.08.2024).

[125] International law, 14 Dec 2021 20:00h - 23:00h. Op. cit.

ИКТ, в том числе с точки зрения международного гуманитарного права, так как у международного сообщества нет консенсуса по вопросу квалификации злонамеренного использования ИКТ как вооруженного нападения в соответствии со статьей 51 Устава ООН[126].

На повестке также находился вопрос об атрибуции атак с использованием ИКТ[127]. Некоторые государства выдвинули предложение о том, чтобы РГОС ООН провела дальнейший анализ правовых ограничений – предварительных условий и процедурных требований контрмер. Было принято решение в ходе обсуждений в РГОС ООН продолжить изучение вопроса о том, каким образом международное право должно применяться к ИКТ, а также выработать общее понимание по нему.

В ходе обсуждения регулярного институционального диалога делегацией Индонезии было отмечено, что РГОС ООН рассматривается как единственный многосторонний и всеобъемлющий межправительственный орган, занимающийся вопросами обеспечения международной безопасности в сфере использования ИКТ[128]. Российская Федерация подчеркнула, что формат РГОС ООН уже доказал свою эффективность и актуальность: как показал опыт первой РГОС ООН, она обладает всеми функциями, которые требуются международному сообществу. При этом, Россия не исключает возможности превращения РГОС ООН в долгосрочный механизм или его преобразования в постоянный механизм, если государства сочтут это необходимым в ходе дальнейшего переговорного процесса.

Что касается Программы действий, то Франция в ходе представления ряда положений Рабочего документа предложила учредить механизм, в чью компетенцию входили бы проведение периодически совещаний и реализация контрактные задач, таких как меры по наращиванию потенциала[129]. Ряд государств

---

[126] Угрозы информационной безопасности в кризисах и конфликтах XXI века / под ред. А. В. Загорского, Н. П. Ромашкиной. Указ. соч.

[127] Отмечалось, что «обычное право, регулирующее ответственность государств, отраженное в проектах статей Комиссии международного права об ответственности государств, обеспечивает механизм применения большей части международного права, включая Устав ООН, и детализирует строгие правила присвоения, предусматривает, какие меры государство может принимать меры в ответ на незаконные акты и определяет последствия международно-противоправных деяний, включая возмещение ущерба. Источник: International law. 14 Dec 2021. 20:00h - 23:00h. Op. cit.

[128] Regular institutional dialogue. 17 Dec 2021 20:00h – 23:00h. [Электронный ресурс]. – URL: https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/regular-institutional-dialogue (дата обращения: 10.08.2024).

[129] Ibid.

считают, что Программа действий представляет собой отправную точку на пути к созданию юридически обязательного документа в будущем, однако важно не дублировать существующие мандаты или усилия ООН. Делегация Российской Федерации рассматривает Программу действий как механизм для обзора выполнения норм и предложила обсудить его в рамках тематической дискуссии о правилах, нормах и принципах поведения.

В ходе второй субстантивной сессии РГОС ООН (28 марта – 1 апреля 2022 г.) были обсуждены вопросы в рамках мандата группы[130] и ряд других вопросов. Прежде, чем перейти к содержательной части обсуждений, автор считает целесообразным отметить некоторые организационные вопросы, влияющие на институциональные механизмы сотрудничества в данной области: некоторые государства предпринимали попытки торпедирования как переговорного процесса, посредством антироссийской риторики[131]. Так, Соединенное Королевство, аргументируя тем, что государства-члены не могут договориться о формах участия заинтересованных сторон, предложило государствам не принимать программу работы РГОС ООН и перейти к неофициальному режиму обсуждения, что предполагало созыв неофициальной сессии с целью подорвать статус процесса. Кроме того, это могло бы повлиять на принятие ежегодного доклада Группы, который должен был быть обсужден и подготовлен на следующей субстантивной сессии. Бразилия, Индонезия и Российская Федерация подняли вопрос о неопределенности в отношении того, будут ли национальные заявления, сделанные в неофициальном режиме, приняты к сведению в окончательном докладе группы. Ряд стран предложили, чтобы работа РГОС ООН продолжалась на основе того, как была проведена первая субстантивная сессия в декабре 2021 г., т.е. отложить в сторону вопрос о принятии программы работы и начать предметные обсуждения

[130] Существующие и потенциальные угрозы в рамках обеспечения безопасности в сфере использовании ИКТ; правила, нормы и принципы ответственного поведения государств в ИКТ-среде; как международное право применяется к использованию ИКТ государствами; меры укрепления доверия, наращивание потенциала, регулярный институциональный диалог.

[131] Мартиросян А. Ж. Международная информационная безопасность: некоторые итоги 2021 г. и политический контекст 2022 г. Указ. соч.

на официальной основе[132]. Однако Председатель прервал заседание, и делегации приступили к обсуждению вопросов существа в неофициальном режиме. Данный инцидент является наглядным примером блокирования работы РГОС ООН группой западных стран.

Отдельного внимания заслуживает проблематика разработки норм по международно-правовому регулированию ИКТ в области информационной безопасности. В связи с частым блокированием документов под конкретным авторством логичным представляется рассмотрение анонимного предложения документов.

Дискуссия в ходе второй субстантивной сессии относительно применения международного права к ИКТ стала разделяющим фактором: первая группа стран выступила с позицией, согласно которой международное право, включая Устав ООН во всей его полноте, применяется к использованию ИКТ государствами; вторая отметила, что Устав ООН не содержит конкретных положений о применимости, что обуславливает необходимость разработки нового единого международного юридически обязательного документа, регулирующего обеспечение безопасности в сфере использования ИКТ, в том числе поведение государств в ИКТ-среде.

На повестке также был вопрос об организационно-правовой составляющей[133]. Франция подчеркнула, что 57 государств-членов ООН, а также ЕС в настоящее время содействуют созданию Программы действий в качестве постоянного институционального механизма, который мог бы работать скоординированным и дополняющим образом с текущей работой и обсуждениями в рамках нынешней РГОС ООН. «Ряд государств высказался против данной инициативы, аргументируя свою позицию тем, что выступают против

[132] UN OEWG 2021–2025. – Organisation of work [Электронный ресурс]. – 28 Mar 2022 15:00h – 1 Apr 2022 23:00h.– URL: https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/oewg-2021-2025-organisation-of-work (дата обращения: 10.08.2024).

[133] OEWG 2021-2025. – Regular institutional dialogue [Электронный ресурс]. – 1 Apr 2022 14:00h – 17:00h.– URL: https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/oewg-2021-2025-regular-institutional-dialogue (дата обращения: 10.08.2024).

параллельных механизмов, которые стремятся заменить работу РГОС ООН»[134]. Делегация Российской Федерации настояла на сохранении за РГОС ООН статуса единственного переговорного механизма при ООН по решению вопросов, связанных с ИКТ-средой.

В рамках диссертационного исследования и идей, высказанных автором, актуальным и отвечающим интересам международного сообщества также рассматривается идея Шри-Ланки, которая предложила организовать институциональный диалог на трех уровнях: национальном, региональном и международном. Национальные обсуждения могут создавать идеи для дальнейшего обсуждения и развития в рамках региональных механизмов, которые в свою очередь, будут содействовать принятию решений и обсуждениям в международных организациях, таких как ООН[135]. Помимо этого, трёхуровневая система позволит создать почву для формирования полностью транспарентной системы обеспечения безопасности в сфере использования ИКТ.

РГОС ООН 2021–2025 гг. провела свою следующую – третью субстантивную сессию 25–29 июля 2022 гг., основным итогом которой стало принятие консенсусом годового доклада о проделанной работе. Проанализируем правовые аспекты поднимавшихся вопросов на основе обзора DiploFoundation[136] и отчетных документов заседаний. Перед обсуждением вопросов существа, члены должны были сначала утвердить процедурный пункт: условия взаимодействия заинтересованных сторон в РГОС, то есть субъектный состав переговорного механизма РГОС. В преддверии сессии заинтересованные стороны подали заявки на внесение вклада в работу РГОС. Государства имели возможность наложить вето на участие заинтересованных сторон, которые не обладают консультативным статусом при ЭКОСОС ООН[137]. Модальности участия заинтересованных сторон

---

[134] Мартиросян А. Ж. Международная информационная безопасность: некоторые итоги 2021 г. и политический контекст 2022 г. Указ. соч.

[135] Демидов О. В., Касенова М. Б. Кибербезопасность и управление интернетом [Электронный ресурс]. – Москва: Статут, 2013. – URL: http://pircenter.org/media/content/files/12/13969745490.pdf (дата обращения: 10.08.2024).

[136] What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted [Электронный ресурс]. – 13 August 2022. – URL: www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/ (дата обращения: 10.08.2024).

[137] Словари. Краткий словарь [Электронный ресурс]. – URL: http://slovo.yaxy.ru/96.html (дата обращения: 10.08.2024).

были утверждены консенсусом. Обсуждения вопросов существа (т.е. пункта 5 повестки дня) были основаны на пересмотренном варианте первого ежегодного доклада РГОС ООН о ходе работы, представленного делегациям 20 июля 2022 г. Дискуссия по юридическим вопросам была в основном сконцентрирована вокруг того, следует ли РГОС ООН сосредоточиться на внедрении существующих добровольных норм ответственного поведения государства, разработке новых норм или и на том, и на другом. Большинство государств, среди которых Германия, США, Канада, Чехия, заявили, что основное внимание следует уделять внедрению существующих норм, при этом государства должны совместно работать над предоставлением дополнительных указаний для продвижения внедрения норм, а также над разработкой выводов и рекомендаций. Кения предложила создать рабочие группы РГОС ООН для обмена передовым опытом, особенно в отношении того, как существующие правила, нормы и принципы могут быть контекстуализированы при внедрении в национальную политику. Иран и Россия придерживались позиции, согласно которой существует необходимость выработки и принятия новых норм, причем Россия предложила новые юридически обязывающие нормы, против чего выступили Канада и Маврикий. Некоторые страны, такие как Перу, Никарагуа, Индонезия, Республика Корея и Сингапур, подчеркнули важность соблюдения существующих норм, но не выступали против разработки новых. Сингапур отметил, что области, которые могли бы выиграть от обсуждения новых норм или дальнейшего применения существующих норм, включают защиту избирательной инфраструктуры и общую целостность и доступность Интернета.

Вопрос разработки специализированной международной конвенции по регулированию использования ИКТ также активно обсуждался: Пакистан, Демократическая Республика Конго, Россия, Иран, Никарагуа, Египет подчеркнули необходимость продолжения обсуждения универсального юридически обязывающего документа с целью формированию международно-правовой основы обеспечения безопасности в сфере использования ИКТ.

Еще одним направлением обсуждения юридических вопросов была выработка общего понимания ИКТ-терминологии. Китай, Иран, Куба, Лаосская народно-Демократическая Республика и Никарагуа приветствовали это. Австралия была против этого, в то время как Нидерланды и США предложили, чтобы государства могли обмениваться национальным пониманием терминов ИКТ в целях прозрачности. Примечательно, что в ежегодном докладе признается, что государства предложили продолжить разработку дополнительных норм, а выработка общего понимания технических терминов ИКТ не была включена в доклад.

Вопрос применения МГП к ИКТ-среде также продолжает оставаться спорной юридической темой. Группа шестнадцати государств[138], чья позиция была представлена делегацией Швейцарии, выступила с заявлением, в котором говорилось, что МГП применяется в ИКТ-среде, а приоритетной задачей является разъяснение того, как оно применяется в отношении кибероперaций в вооруженных конфликтах. Никарагуа и Куба заявили, что неуместно даже говорить о применимости МГП к использованию ИКТ в контексте международной безопасности, поскольку это означало бы, что государства молчаливо признают возможность вооруженного конфликта, который способствовал бы милитаризации в ИКТ-среде. Куба, Россия и Исламская Республика Иран выступили против упоминания МГП в ежегодном докладе. Пакистан отметил, что МГП требует дальнейших политически нейтральных дискуссий между государствами для выработки общего понимания. Республика Корея приветствовала упоминание принципа должной осмотрительности и МГП. Иран, с другой стороны, предпочел исключить любые конкретные ссылки на должную осмотрительность и обмен передовым опытом в области международного права, сочтя их преждевременными. Проблематика кибератрибуции также была обсуждена и выдвинута Пакистаном, Индонезией, Малайзией и Германией.

[138] Аргентины, Бразилии, Канады, Чили, Колумбии, Чешской Республики, Эстонии, Германии, Индонезии, Японии, Иордании, Мексики, Нидерландов, Республики Корея, Сенегала, Швеции.

В рамках четвертой субстантивной сессии, март 2023 г., состоялась очередная серия дискуссий. Что касается универсального международно-правового акта об обеспечении безопасности в сфере использования ИКТ, то также продолжается его обсуждение без значительного прогресса. Куба, Иран, Ирак и Сирия поддержали идею юридически обязывающего документа. Иран отметил необходимость включения в юридически обязывающий документ определения терминологии и принципов международного права относительно ИКТ-среды[139]. Данное обсуждение, как и прежде, встретило сопротивление со стороны группы государств[140], не поддерживающих новый юридически обязательный документ.

Четвертая субстантивная сессия ознаменовалась представлением обновленной версией концепции Конвенции ООН об обеспечении МИБ со стороны российской делегации с Беларусью и Никарагуа в качестве соавторов. Конвенция преследует три цели, такие как предотвращение и урегулирование межгосударственных конфликтов, укрепление доверия и развитие сотрудничества между государствами-членами ООН с целью обеспечения безопасности в сфере использования ИКТ, поддержка наращивания потенциала государств. Вьетнам заявил, что, если идея нового юридически обязательного документа преждевременна, РГОС ООН могла бы разъяснить нормы международного права посредством (а) запроса консультативного заключения в Международный суд; (б) мандата на проведение исследования Комиссией международного права ООН; или (в) путем представления темы для обсуждения в Шестом комитете ООН. Обсуждалось также будущее институционального диалога. Великобритания, Канада и США отметили, что РГОС ООН могла бы способствовать общему пониманию того, какие возможности необходимо создать. Тем не менее, наращивание потенциала будет входить в компетенцию Программы действий, создание которой приветствовалось некоторыми государствами в резолюции 77/37. Бразилия, Сальвадор, Южная Африка, Индия и Малайзия еще раз предупредили о

[139] Международная безопасность в среде информационно-коммуникационных технологий: коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде. Указ. соч.
[140] Австралия, Австрия, Бельгия, Канада, Чешская Республика, Эстония, Ирландия, Израиль, Нидерланды, Малави, Республика Корея, Соединенное Королевство и Новая Зеландия.

проблеме параллельных направлений дискуссий ГПЭ ООН и РГОС ООН, для участия в которых требуется больше ресурсов. Китай отметил, что государства, поддержавшие резолюцию по Программе действий, подрывают статус РГОС как единого и инклюзивного процесса под эгидой ООН. Куба заявила, что РГОС доказала свою ценность и должна стать центральным механизмом регулярного институционального диалога до 2025 года. Иран, Пакистан и Сирия подчеркнули, что любые предложения о регулярном институциональном диалоге должны обсуждаться в рамках РГОС ООН на равноправной основе. Иран повторил идею, которую он выдвинул на декабрьской сессии: МСЭ мог бы стать постоянным форумом для диалога, консультаций, сотрудничества и координации между государствами-членами, включая развитие технического потенциала. Куба поддержала эту идею. Россия, Беларусь и Никарагуа предложили альтернативу Программе действий, в которой также предлагается создать постоянный орган с механизмами обзора[141]. Доклад РГОС ООН[142] также содержит положение, согласно которому государства признали центральную роль РГОС как механизма в рамках ООН для диалога по вопросам безопасности при использовании ИКТ.

С 24 по 28 июля 2023 г. в ходе пятой субстантивной сессии РГОС ООН утвердила проект доклада[143]. Итоги обсуждения были следующими: международное право применимо к ИКТ-среде, требуется дальнейшее обсуждение

---

[141] Под эгидой ГА ООН в качестве рабочей группы/комиссии/комитета открытого состава/обзорной конференции. Мандат будущего органа должен включать весь спектр вопросов, связанных с обеспечением безопасности в сфере использования ИКТ. Она должна быть ориентирована на практические имплементационные соглашения, достигнутые в РГОС ООН. В частности, его мандат мог бы включать: (a) разработку юридически обязательного международного документа по международной информационной безопасности; (b) внедрение мер укрепления доверия путем разработки механизмов практического сотрудничества между государствами; (c) создание механизмов для оказания государствам помощи в укреплении их потенциала по защите национальных информационных ресурсов.

[142] United Nations General Assembly Seventy-seventh session. Item 95 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security [Электронный ресурс] / Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General. Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. – A/77/275. – 2022, 8 August. – URL: https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports (дата обращения: 10.08.2024).

[143] United Nations General Assembly Seventy-eighth session. Item 96 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security [Электронный ресурс] / Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General. Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. – A/78/265. – 2023, 1 August. – URL: https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports (дата обращения: 10.08.2024).

о том, как оно применяется к использованию ИКТ. В ходе целенаправленных дискуссий РГОС о том, как международное право применяется к использованию ИКТ, государства подтвердили статью 2 и 33 Устава ООН.

В докладе также говорится о возможности будущей разработки дополнительных юридически обязательных норм: государства рассмотрели необходимость рассмотрения вопроса о том, существуют ли какие-либо пробелы в том, как применяется существующее международное право при использовании ИКТ, а также определили возможность дальнейшей разработки дополнительных юридических обязательств.

В части институционального диалога отчетный документ гласит, что государства признали основополагающую роль РГОС ООН в качестве диалогового механизма по вопросам безопасности при использовании информтехнологий; в дополнение к рекомендации, содержащейся в докладе РГОС ООН за 2021 г. и в первом обзоре РГОС ООН, государства углубили обсуждение предложения о разработке Программы действий. Были выдвинуты и другие предложения относительно регулярного институционального диалога. Государства в целом согласны с тем, что будущий механизм регулярного институционального диалога будет основываться на следующих общих элементах:

1) это будет единый постоянный механизм под эгидой ООН, подотчетный Первому комитету ГА ООН;

2) цель будущего механизма будет заключаться в продолжении содействия открытой, безопасной, стабильной, доступной и мирной ИКТ-среде;

3) будущий механизм будет использовать в качестве основы своей работы достигнутые соглашения об ответственном поведении государств при использовании ИКТ, содержащиеся в предыдущих докладах ГПЭ ООН и РГОС ООН;

4) это будет открытый, инклюзивный, прозрачный, устойчивый и гибкий институциональных механизм, который сможет развиваться в соответствии с потребностями государств, а также в соответствии с изменениями в ИКТ-среде

стоящими задачами с целью обеспечения безопасности в сфере использования ИКТ;

5) важность принципа консенсуса в отношении как создания самого будущего механизма, так и процессов принятия решений в рамках механизма;

6) другие заинтересованные стороны (субъекты ИКТ-среды) смогут вносить свой вклад в деятельность будущего регулярного институционального диалога.

Дальнейшее обсуждение в рамках РГОС ООН состоится в ходе предстоящих 6 субстантивных сессиях до окончания срока действия мандата группы в 2025 г.

С одной стороны, существование двух параллельных переговорных механизмом в ООН – ГПЭ ООН и РГОС ООН – открывает возможность для дальнейшего диалога между государствами. РГОС ООН, открытая для всех заинтересованных государств-членов ООН, позволяет участвовать большему и более разнообразному числу государств. Однако, с другой стороны, это также является свидетельством наличия серьезных разногласий в части международного нормотворчества и правоприменения в информационном пространстве[144]. В целом каждая из этих групп говорит о существующих и потенциальных угрозах и благодаря их деятельности была выработана система рекомендаций и основа будущего переговорного процесса, институционального механизма и международно-правовой основы регулирования обеспечения безопасности в области применения ИКТ.

ИКТ-технологии имеют глобальный характер, что требует международного сотрудничества в их использовании, в частности в вопросе обеспечения безопасности в сфере их применения. Это приводит к тому, что данная проблематика в дополнение к работе на уровне ООН в рамках ГПЭ ООН и РГОС ООН является также повесткой иных как профильных (МСЭ), так и непрофильных (ЮНЕСКО, ЮНКТАД и др.) механизмов системы ООН, которые занимаются регулированием и/или исследованием ИКТ в рамках своих полномочий.

[144] Moynihan H. The Application of International Law to State Cyberattacks. Research paper. – 2 December 2019. Op. cit.

Так, ЮНЕСКО, как заявляется, вносит вклад в создание глобального общества знаний, которое использует ИКТ для борьбы с нищетой, содействия развитию, обеспечения образования для всех и обеспечения культурного и языкового разнообразия. ЮНЕСКО играет важную роль в части достижения Целей устойчивого развития (ЦУР), в частности посредством таких инициатив, как программа «Информация для всех» (ПИДВ) и «Международная программа развития коммуникации» (МПРК)». ЮНСИТРАЛ в связи с растущим использованием электронной торговли и передовых ИКТ в международной торговле ЮНСИТРАЛ в 1996 г. разработала Типовой закон об электронной торговле[145], основанный на резолюции ГА ООН от 1985 г., призывающей государства и международные организации принять меры для обеспечения правовой безопасности в контексте широкого использования автоматизированной обработки данных в международной торговле. Одним из руководящих факторов при разработке данного типового закона было то, что закон должен способствовать использованию электронной торговли, приемлемой для государств с различными правовыми, социальными и экономическими системами с тем, чтобы внести значительный вклад ИКТ в развитие гармоничных международных экономических отношений. Типовой закон призван помочь всем государствам в разработке соответствующего законодательства, регулирующего использование альтернативных бумажным методам передачи и хранения информации. ГА ООН в своей резолюции 51/162 от 30 января 1997 г. рекомендовала всем государствам опираться на типовой закон при разработке или пересмотре национального законодательства по использованию ИКТ в торговле[146]. Положения рассматриваемого типового закона вскоре легли в основу нескольких национальных законодательств, например, Закона Индии об информационных технологиях 2000 г. В 2005 г. ЮНСИТРАЛ выступила с Конвенции об

[145] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bisas adopted in 1998. – United Nations Publication Sales No. E. 99. – V. 4. – 76 p. – ISBN 92-1-133607-4.
[146] United Nations General Assembly Resolution 51/162. Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. – A/RES/51/162. – 30 January 1997. – Resolutions and Decisions adopted by the General Assembly during its 51st session. – Volume I, 17 September – 18 December 1996 // General Assembly Official Records, 51st Session. – Supplement No. 49 (A/51/49 Vol. I). – New York: United Nations, 1997. – P. 336–340.

использовании электронных сообщений в международных договорах, которую приняла ГА ООН 23 ноября 2005 г.[147] Конвенция направлена на повышение правовой определенности и коммерческой предсказуемости в тех случаях, когда электронные сообщения используются в связи с международными договорами. Функционируют также механизмы координации ИКТ в чрезвычайных ситуациях, созданные Управлением ООН по координации Гуманитарные вопросы (УКГВ). Ключевое место в обеспечении информационной безопасности международного судоходства занимает ИМО, одним из последних событий стало принятие резолюции MSC.428 (98) в ответ на растущую угрозу преступности в ИКТ-среде.

Наиболее активным учреждением ООН в достижении согласованности в обеспечении безопасности в сфере использования ИКТ рассматривается МСЭ[148]. ГА ООН признала в 2001 г. необходимость проведения многоэтапной Всемирной встречи на высшем уровне по вопросам информационного общества (ВВИУО) и просила МСЭ рассмотреть возможность взять на себя ведущую роль в координации данного мероприятия. После саммитов ВВИУО[149] и Полномочной конференции МСЭ 2006 г. МСЭ взял на себя важную роль в координации усилий по укреплению доверия и обеспечению безопасности в сфере использования ИКТ.

Необходимо отметить, что в настоящее время существует множество региональных и двусторонних инициатив, которые не входят в систему ООН, но являются важным инструментом для международного взаимодействия по ИКТ-повестке. в целях обеспечения безопасности в сфере использования ИКТ. Они вносят важный вклад в формирование правил и практик, в особенности тех, которые внедряются на региональном или отраслевом уровне, в рассматриваемой

---

[147] United Nations Convention on the Use of Electronic Communications in International Contracts. Adopted in New York, 23 November 2005 // United Nations, Treaty Series, Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. Vol. 2898. – New York, 2018. – 411 p.

[148] Является «специализированным учреждением ООН с 1947 г. с базирующимся в Швейцарии межправительственным органом с тремя секторами, занимающимися разработкой и публикацией рекомендаций для радиосвязи (МСЭ-R), стандартизацией электросвязи (МСЭ-T) и содействием развитию электросвязи (МСЭ-D)». Источник: О Международном союзе электросвязи [Электронный ресурс]. – URL: http://www.itu.int/ru/about/ (дата обращения: 10.08.2024).

[149] Всемирный саммит проходил в два этапа: первый – в 2003 г. в Женеве (Швейцарии) и второй – в 2005 г. в Тунисе (Тунис) в соответствии с резолюцией 73, принятой Полномочной конференцией МСЭ на сессии 1998 г.[149] состоявшейся в Миннеаполисе (США). Источник: Мартиросян А. Ж. Формирование системы обеспечения безопасности киберпространства: монография / отв. ред. И.О. Анисимов. – М.: Дипломатическая академия МИД России, 2021. – С. 33.

области. Именно этот уровень позволяет в дальнейшем перейти на следующий уровень – глобальный. Среди наиболее значимых региональных механизмов, инициативы которых также были реализованы с целью обеспечения безопасности в сфере использования ИКТ, определяют ШОС, СНГ, ОДКБ, ОБСЕ[150], Совет Европы, ЕС, АСЕАН, ЛАГ, Африканский союз, НАТО[151]. Подчеркивая важность таких механизмов, в течение 2019 г. ГПЭ ООН провела консультации с региональными институтами (Африканский союз, ЕС, Организация американских государств, ОБСЕ и Региональный форум АСЕАН). Применение международного права к ИКТ также было на повестке было ряде других региональных форумов, включая Афро-Азиатскую консультативно-правовую организацию[152]. Помимо того, что государства-члены ШОС заключили Соглашение между правительствами о сотрудничестве в области обеспечения МИБ от 16 июня 2009 г., внеся вклад в развитие региональных инициатив в данной области, они также сыграли важную роль с точки зрения глобального уровня, когда предложили Генеральной Ассамблее ООН проект Международного кодекса поведения в области информационной безопасности, представленный сначала в 2011 г., а затем в пересмотренном виде в 2015 г. (Письмо от 9 января 2015 г. постоянных представителей Китая, Казахстана, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при ООН на имя генерального секретаря, ГА ООН A/69/723). Предлагаемый кодекс не получил большого распространения, отчасти из-за опасений по поводу отсутствия ссылок на международное право в области прав человека.

На примере АСЕАН рассмотрим потенциал регионального уровня сотрудничества рассматриваемой проблематики. С точки зрения внешнеполитических интересов Российской Федерации в направлении

---

[150] ОБСЕ приняла два набора мер укрепления доверия в области информационной безопасности в 2013 и 2016 гг. и продолжает осуществлять эти меры через свою рабочую группу по кибербезопасности. Региональный форум АСЕАН обсуждает вопросы укрепления доверия в ИКТ-среде с 2012 г., а Министерская конференция АСЕАН по кибербезопасности одобрила одиннадцать норм ответственного поведения государств из доклада ГПЭ ООН 2015 г. Европейский союз включил вопрос информационной безопасности в свою политику с момента принятия первой Стратегии ЕС по кибербезопасности 2013 г. Источник: Tiirmaa-Klaar H. The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body. Op. cit.

[151] Международная информационная безопасность: подходы России. Доклад ЦМИБ МГИМО. Указ. соч.

[152] Moynihan H. The Application of International Law to State Cyberattacks. Research paper. – 2 December 2019. Op. cit.

международно-правового регулирования использования ИКТ и формирования системы международно-правового обеспечения безопасности в сфере использования ИКТ важным видится продолжать налаживать стратегические партнерские отношения со странами-единомышленниками и региональными объединениями, которые разделяют опасения по поводу различных вопросов, связанных с ИКТ-средой, и технологического доминирования отдельных стран. Так, например, учитывая стремление некоторых государств ослабить центральную роль АСЕАН в регионе АТР, важно продолжать предпринимать меры по укреплению центральной роли АСЕАН в развивающейся региональной архитектуре безопасности, а также расширять диалог и улучшать обмен информацией между Россией и АСЕАН по различным аспектам безопасности, таким как противодействие традиционным и нетрадиционным угрозам и вызовам, для содействия миру, безопасности и стабильности в АТР. В контексте меняющегося геополитического ландшафта в сторону незападного полицентричного мира взаимодействие может быть полезным для обеих сторон. Значительный потенциал в новых геополитических условиях имеет проект «Большой Евразии», важно отметить, что данная концепция может благоприятно повлиять на двусторонние отношения между Россией и АСЕАН посредством выстраивания института сотрудничества через связку АСЕАН – ШОС – ЕАЭС, которая открывает возможности наращивания взаимосвязей на евразийском пространстве[153]. Помимо этого, позитивный потенциал имеет укрепление сотрудничества между АСЕАН и Россией в рамках механизмов, возглавляемых АСЕАН, в частности Восточноазиатского саммита, Регионального форума АСЕАН[154], Совещания министров обороны стран членов АСЕАН и диалоговых партнеров[155], а также реализация Всеобъемлющего плана действий по реализации Стратегического партнерства Россия-АСЕАН (2021–2025 гг.). Российская Федерация также вовлечена в деятельность профильных региональных

[153] Канаев Е. А., Королев А. С. Большая Евразия, Индо-Тихоокеанский регион и отношения России с АСЕАН. – DOI 10.23932/2542-0240-2019-12-1-26-43 // Контуры глобальных трансформаций: политика, экономика, право. – 2019. – Т. 12, № 1. – С. 26–43.
[154] ASEAN Regional Forum.
[155] ADMM Plus.

механизмов, например, Регионального форум АСЕАН по безопасности (АРФ)[156]. Если исходить из логики положений Стратегии сотрудничества АСЕАН в области кибербезопасности 2021–2025 гг.[157], то стоит обратить внимание на некоторые пункты, которые соотносятся с интересами Российской Федерации и могут благоприятно повлиять на сотрудничество со странами-членами АСЕАН. Что касается концептуальных основ, то Стратегия на 2021–2025 гг.[158], то она содержит положения, которые могут стать направлениями взаимодействия с Россией на фоне геополитических изменений с точки зрения выработки норм, в том числе «мягкого права», на основе которых должна функционировать ИКТ-среда. В данном контексте важно учитывать роль АСЕАН в многостороннем мироустройстве и потенциал объединения в обеспечении безопасности ИКТ-среды. Можно проследить также принцип, которой отвечает интересам Российской Федерации и красной нитью идет через весь документ: политический нейтралитет в данной сфере. Стратегия на 2021–2025 гг. предусматривает пять направлений работы: наращивание регионального потенциала; укрепление региональной координации киберполитики; развитие сотрудничества в области киберподготовки; повышение доверия в киберпространстве; международное сотрудничество. Все пять пунктов также соответствуют интересам Российской Федерации. Наличие надежной региональной стратегии сотрудничества с целью обеспечения безопасности в сфере использования ИКТ имеет важное значение для государств – членов АСЕАН. Данная стратегия имеет потенциал масштабирования на трансрегиональное и глобальное сотрудничество. В связи с чем в этом направлении важно сотрудничать в разработке региональных систем защиты данных и нормативных актов, в которых приоритетное внимание уделяется суверенитету и безопасности данных России и стран АСЕАН, например, посредством разработки единых стандартов защиты

[156] Лобанова О., Нархова Е. Новые тенденции формирования системы международной информационной безопасности в Азии [Электронный ресурс] // Международная жизнь. – 2021. – № 11. – URL: https://interaffairs.ru/jauthor/material/2586 (дата обращения: 10.08.2024).
[157] The ASEAN Cybersecurity Cooperation Strategy 2021–2025 [Электронный ресурс]. – URL: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf (дата обращения: 10.08.2024).
[158] Ibid.

данных и сертификаций, отражающих уникальные потребности и вызовы, с которыми сталкиваются Россия и страны АСЕАН в области применения ИКТ.

Более эффективное правовое регулирование обеспечения безопасности в сфере использования ИКТ на региональном уровне по сравнению с универсальным обусловлено наличием множества разногласий, которые достаточно сложно преодолеть на глобальном уровне. Последнее создает предпосылки для торможения развития международного права в части регулирования ИКТ в контексте международной безопасности. В связи с чем целесообразно при разработке международно-правовых норм универсального характера использовать наиболее передовой и прогрессивный опыт регионального нормотворчества в рассматриваемой области.

Помимо международных организаций также существуют отдельные инициативы, которые направлены на международное сотрудничество по вопросам обеспечения безопасности в сфере использования ИКТ. Ряд первичных субъектов международного права также выступили инициаторами многосторонних инициатив, наиболее ярким примером представляется Парижский призыв к доверию и безопасности в киберпространстве[159]. Он подтверждает ключевую роль ООН, при этом акцент делается на том, что сотрудничество государств следует выстраивать в многоуровневом формате на равной основе и с привлечением ИТ-сектора и гражданского общества. С точки зрению юридической природы Парижский призыв обладает лишь декларативным характером[160]. В соответствии с Парижским призывом к доверию и безопасности, подписанты обязуются: предотвращать деятельность, которая намеренно и существенно наносит ущерб общей доступности или целостности публичного ядра Интернета; принять меры по предотвращению ответных хакерских атак негосударственных субъектов; пропагандировать международные нормы ответственного поведения. В нем отмечается, что «международное право вместе с добровольными нормами

[159] Его инициатором выступил президент Франции Э. Макрон, представив его на Форуме по управлению Интернетом в Париже в 2018 г.

[160] Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции. Указ. соч.

ответственного поведения государства в мирное время и связанными с ними мерами доверия и укрепления потенциала, – это основа международного мира и безопасности». Помимо этого, к глобальным инициативам также относят Программу действий по продвижению ответственного поведения государств в киберпространстве, Инициативу по борьбе с вымогателями, Глобальную инициативу по безопасности данных и др.[161] Однако в современных геополитических условиях есть и такие инициативы, которые имеют своей целью саботировать глобальный переговорный процесс, несут деструктивный характер, а также декларируют блоковость и разделение государств. К ним могут быть отнесены Саммит за демократию и Декларация о будущем Интернета.

Особенности эволюции ИКТ в современных международных отношениях определяют научную ценность изучения роли инициатив с участием негосударственных субъектов, включая гражданское общество, научное и экспертной сообщество, бизнес-сектор[162]. Российские негосударственные субъекты также вовлечены в данную деятельность и в данном контексте важно упомянуть об инициативах Национальной ассоциации международной информационной безопасности и Школы международной информационной безопасности ИАМП ДА МИД России, которые выработали свои предложения по обеспечению безопасности в сфере использования ИКТ, в том числе по международно-правовому регулированию использования ИКТ[163]. Также в данном направлении функционируют негосударственные международные организации. Наиболее ярким примером выступает ИСО – это базирующаяся в Швейцарии независимая неправительственная международная организация по разработке и изданию международных стандартов, состоящая из представителей различных национальных организаций по стандартизации с несколькими комитетами, некоторые из которых осуществляют деятельность, связанную с информационной

[161] Международная информационная безопасность: подходы России. Доклад ЦМИБ МГИМО. Указ. соч.
[162] Moynihan H. The Application of International Law to State Cyberattacks. Research paper. Op. cit.
[163] Written Input of the International Information Security School to the United Nations Open-ended Working Groupon Security of and in the Use of Information and Communications Technologies [Электронный ресурс]. – URL: https://documents.unoda.org/wp-content/uploads/2022/09/Written-input-of-the-IISS-to-the-UN-OEWG.pdf (дата обращения: 10.08.2024).

безопасностью[164]. Еще одной международной неправительственной организацией, занимающейся гуманитарными аспектами использования ИКТ является МККК. В соответствии со своей миссией и мандатом МККК, в первую очередь, занимается операциями с применением ИКТ, используемыми в качестве средств и методов ведения войны во время вооруженного конфликта, а также защитой, обеспечиваемой МГП от их последствий. МККК приветствует межправительственные дискуссии, проходящие в рамках двух процессов, санкционированных ГА ООН, а именно РГОС ООН и ГПЭ ООН. Однако стоит отметить, что вопрос применения МГП к ИКТ требует отдельного исследования, выходящего за рамки настоящей диссертации. Международный комитет по защите кабелей[165], созданный в 1958 г., является отраслевой международной неправительственной организацией, членами которой являются владельцы, операторы и поставщики более 97 процентов международных подводных кабельных систем в мире. В 2010 г. членство было открыто для государств. Данный механизм выдает рекомендации по различным вопросам, касающимся подводных кабелей, и играет важную роль в сотрудничестве с правительствами, международными организациями и другими пользователями морского дна в целях сохранения целостности подводной кабельной сети. Отдельное место в обеспечении безопасности в сфере использования ИКТ занимают неправительственные экспертно-технические механизмы, среди которых числятся Институт инженеров электротехники и электроники, Инженерный совет Интернета, Консорциум Всемирной Паутины, Интернет-Корпорация по присвоению имен и номеров, 3GPP, Форум CableLabs, и многие другие.

Можно сделать вывод о том, что международное сотрудничество в сфере использования ИКТ занимает важное место в деятельности международных организаций как глобального, так и регионального уровня. В связи с тем, что активизировались попытки международного сообщества, направленные на формирование системы международно-правового обеспечения безопасности в

[164] International Organization for Standardization [Электронный ресурс]. – URL: http://www.iso.org/ (дата обращения: 10.08.2024).
[165] The International Cable Protection Committee.

сфере использования ИКТ, включая выработку норм по использованию ИКТ в данной области, анализ деятельности международных организаций в части разработки правовых инструментов международного сотрудничества в ИКТ-среде представляет научный интерес.

Начиная с 2004 г. ГПЭ ООН изучала угрозы, исходящие от ИКТ в контексте международной безопасности, и способы их устранения. По мере того, как угрозы в сфере использования ИКТ приобретали все большее значение для международной безопасности и стабильности, членский состав группы расширился с первоначальных 15 до 25 к 2021 г. Четырем созывам ГПЭ удалось согласовать итоговые доклады, которые были одобрены всеми государствами – членами ООН. В частности, доклад ГПЭ ООН за 2015 г. был принят консенсусом в резолюции 70/237, в которой содержится призыв к государствам-членам руководствоваться при использовании ИКТ докладом ГПЭ ООН за 2015 год. Каждая группа опиралась на работу, проделанную предыдущей, добиваясь значительного совокупного прогресса по рассматриваемым вопросам. Два десятилетия спустя исторического событий 1998 г. Россия инициировала создание РГОС ООН – формата, который российское экспертное сообщество сравнивает со своего рода «кибер-Генеральной Ассамблеей»[166]. Таким образом, были сформированы две площадки ООН для международного сотрудничества с целью обеспечению безопасности в сфере использования ИКТ, что демонстрировало существование двух разных подходов к ее обеспечению. В данном контексте автором представляется важным отметить, что российские инициативы и деятельность имеют своей целью создание таких условий, в которых взаимодействие по вопросам ИКТ-среды оставалось направлением равного диалога и государств с сохранением за ними ключевой роли в принятии решений. Также задачей является укрепление центральной роли ООН как ключевой

[166] O'Connor T. As Biden Puts US on Alert, Russia Seeks Talks to Help Prevent Cyber War [Электронный ресурс]. – 22.03.2022. – URL: https://www.newsweek.com/biden-puts-us-alert-russia-seeks-talks-help-prevent-cyber-war-1690673/ (дата обращения: 10.08.2024).

переговорной площадки по вопросам информационной безопасности[167], в рамках которой необходима разработка международно-правового акта, регулирующего ИКТ-среду.

Отсутствие четко выстроенного институционального механизма (организационно-правовой основы) обеспечения безопасности в сфере использования ИКТ привело к формированию большого количества институтов, которые занимаются данной повесткой. Проведенный анализ документов и деятельности отдельных международных механизмов в исследуемой области подтверждает, что проблематика международно-правового обеспечения безопасности в сфере использования ИКТ требует дальнейшего развития на региональном и субрегиональном охвате как основы для глобального сотрудничества. Это позволяет сделать вывод о том, что с момента, когда данная тема стала повесткой международного сообщества, был заложен существенный фундамент для дальнейшего развития международного права по проблематике ИКТ и открываются новые возможности для формирования юридической основы обеспечения безопасности в области применения ИКТ.

Проведя краткий анализ организационно-правовых основ международного сотрудничества по обеспечению стабильности и устойчивости системы управления безопасностью в области использования ИКТ в рамках ООН, представляется целесообразным рассмотреть возможность внесения предложения для дальнейшего формирования соответствующего институционального механизма. Консолидация площадок ООН, занимающихся ИКТ требует особого внимания. Система ООН занимается проблематикой ИКТ в различных аспектах от интеграции их в свою работу по развитию и миру до создания и уточнения норм для «управления и обеспечения международной безопасности. Автором рассматривается необходимым начать работу над разработкой концепции координационного центра ООН по ИКТ-среде с постоянно действующими органами и механизмами сотрудничества с региональными и субрегиональными

[167] Мартиросян А. Ж. Международная информационная безопасность: некоторые итоги 2021 г. и политический контекст 2022 г. Указ. соч.

организациями, такими как АТЭС, ОБСЕ, ОАГ, ШОС, ОДКБ, СНГ и др., так как потенциал региональных подходов может способствовать более быстрой выработки единых позиции государств-членов на глобальном уровне в рамках переговорных площадках ООН. В связи с выше обозначенными причинами, а также с целью совершенствования организационно-правовой формы регулирования ИКТ-проблематики автором диссертационного исследования предлагается проект Конвенции по учреждению организации ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ (см. Приложение А).

2.2. Международно-правовая регламентация обеспечения безопасности в сфере использования информационно-коммуникационных технологий

Согласно нормативно-правовым основам деятельности РФ в сфере использования ИКТ, одним из приоритетов на внешнеполитическом направлении рассматривается выработка совокупности международно-правовых норм, которые будет обеспечивать регламентацию международных отношений в сфере использования ИКТ[168]. Именно в российских программных документах впервые появилась идея выработки международно-правовых основ обеспечения безопасности в сфере использования ИКТ. Исходя из этого, целесообразным видится после рассмотрения в первой главе российского законодательства перейти к анализу международных документов по обеспечению безопасности в области применения информтехнологий.

Научно-технический прогресс определяет кардинальные преобразования в обеспечении безопасности в сфере использования ИКТ и, соответственно, в правовом регулировании рассматриваемой проблематики. Формирование юридического фундамента, определяющего основы использования ИКТ выступает фактором, который непосредственно влияет на стратегическую стабильность и

[168] Мельникова О. А. Манипуляция общественным мнением и глобальная кибербезопасность: монография. – Москва: Гнозис, 2021. – С. 153.

международную безопасность[169]. Необходимость многостороннего сотрудничества в ответ на новые технологии была признана еще в 1865 г., когда был создан Международный телеграфный союз (МТС). МТС, переименованный в Международный союз электросвязи (МСЭ) в 1934 г., стал специализированным учреждением ООН в 1947 г. и является старейшей ныне существующей международной организацией. В последующие годы технологические изменения создали новые возможности для многостороннего сотрудничества в исследуемой области. Тем не менее на текущем этапе развития международного права все еще не разработан юридически обязательный международно-правовой акт, кодифицирующий и регламентирующий использование ИКТ в контексте международной безопасности. Однако уже можно говорить о том, что формируется система источников, которые определяют основы обеспечение безопасности в сфере использования ИКТ, несмотря на отсутствие всеобъемлющего международного документа по ИКТ-проблематике. Складывающаяся международно-правовая система, как и другой правовой режим, пройдет три этапа формирования: определение повестки, переговорный процесс и принятие международно-правового акта[170]. В контексте теоретических исследований формирования международно-правовых режимов также представляет интересен тезис, согласно которому в случае, когда участники переговоров осознают свою уязвимость друг перед другом, возрастает вероятность достижения эффективных и взаимовыгодных соглашений[171]. Если применить данный тезис к ИКТ-среде, то можно утверждать, что формирование режима обеспечения безопасности в области применения ИКТ обусловлено заинтересованностью ее участников обезопасить себя от непрерывно возрастающих рисков в данной области[172]. Сложность переговорного процесса заключается в принципиальном отличии ИКТ-среды от

---

[169] Яникеева И. О. Фактор международной информационной безопасности в двусторонних отношениях России и США в XXI веке [Электронный ресурс]. Диссертация на соискание степени кандидата политических наук: 5.5.4. – URL: https://viewer.rsl.ru/ru/rsl01011749760 (дата обращения: 10.08.2024).

[170] Young O. R. The Politics of International Regime Formation: Managing Natural Resources and the Environment [Электронный ресурс] // International Organization. – 1989. – Vol. 43, No. 3, P. 349–375. – URL: http://www.jstor.org/stable/2706651 (дата обращения: 10.08.2024).

[171] Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции. Указ. соч.

[172] Kyslytsya I. International Cooperation in Ensuring International Information Security. Op. cit.

иных. Тем не менее, уже можно говорить о том, что существуют контуры формирующейся системы обеспечения международной безопасности в сфере использования ИКТ и ее международно-правовой режим носит комплексный характер, представленный следующими уровнями правового регулирования: национальным, основанным на законодательстве отдельных государств и международным уровнем, который, в свою очередь, представлен двусторонним, региональным и универсальным, нормативная база которого все еще активно формируется в рамках системы ООН[173].

Рассмотрим систему источников, которые регулируют использования ИКТ с конечной целью формирования международного режима обеспечения безопасности в сфере использования ИКТ. Международное право может быть выражено через формулу сложения нормы и источника, где норма представляется внутренней формой воплощения международного права тогда, как источник – внешней, иными словами, официально-юридической формой существования международно-правовых норм. Под источником в этом контексте понимается формальный источник, который придает нормам их правовой характер[174]. Субъекты международного права придают значимость нормам посредством их закрепления в разнообразных источниках. При рассмотрении перечня источников международного права, традиционно упоминается[175] статья 38 Статута Международного суда. Настоящая статья, помимо основных источников международного права (международных конвенций и обычаев), определяет

[173] Фундаментом двустороннего уровня являются двусторонние соглашения между государствами и другими субъектами международного права. Региональный уровень основан на соглашениях, заключаемых в форматах субрегиональных и региональных объединений государств и других субъектов международного права. При этом универсальный, региональный и двусторонний уровни отражают основополагающий принцип международного права – международное сотрудничество. В свою очередь, национальный уровень правового регулирования призван учитывать национальные интересы государств, условия развития, внедрения и использования ИКТ.

[174] Первый доклад по теме «Формирование и доказательство существования международного обычного права», подготовленный Специальным докладчиком Майклом Вудом [Электронный ресурс] // Комиссия международного права. Шестьдесят пятая сессия. Женева, 6 мая – 7 июня и 8 июля – 9 августа 2013 года. – A/CN.4/663. – URL: https://legal.un.org/ilc/guide/1_13.shtml (дата обращения: 10.08.2024).

[175] Всестороннее исследование проблемы киберпреступности [Электронный ресурс]. Проект, февраль 2013 года // Управление Организации Объединенных Наций по наркотикам и преступности. – URL: www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 10.08.2024).

дополнительные (общие принципы права, судебные решения, доктрину)[176]. Помимо этого, данный список может быть пополнен актами международных правительственных организаций.

Международный договор – родовое понятие наиболее распространенной внешней формы существования международного права, международно-правовой акт, в котором закреплено согласованное волеизъявление субъектов международного права с целью установления юридически обязывающих отношений. Международный договор по своей форме может быть представлен как в письменной (классические и неформальные договоры), так и в устной форме. По числу участников он классифицируется на две категории: двусторонний и многосторонний, в свою очередь, разделяемый на универсальный, региональный, локальный уровни. По объекту регулирования подразделяется в зависимости от сферы, на которую распространяются правовые отношения, по способу присоединения – на открытый и закрытый, по срокам действия – бессрочный, определенно-срочный, неопределенно-срочный, наконец, по виду субъектов – межгосударственные, межправительственные, межведомственные.

Совокупность угроз, возникших с началом широкомасштабного внедрения ИКТ, дала толчок процессу формирования и развития правовых механизмов обеспечения безопасности в сфере использования ИКТ в рамках международного права. Что касается международных договоров в рассматриваемой области, то их характер очень разнороден, что обуславливает сложности в формировании единого международного-правового механизма. Наибольшую распространенность имеют международные договоры, предметом которых являются борьба с преступностью в информационной среде с применением ИКТ и уголовное правосудие. Рассмотрим на их примере особенности кодификации и развития международного права. Важной вехой в регулировании обеспечения безопасности в сфере использования ИКТ стал Восьмой Конгресс ООН по предупреждению преступности и обращению

[176] Grossman C. M. ILC Report on Prevention and Punishment of Crimes Against Humanity and Enforced Disappearance [Электронный ресурс] // American University Washington College of Law. – 2019, August 20. – URL: https://works.bepress.com/claudio_grossman/166/ (дата обращения: 10.08.2024).

с правонарушителями 1990 г.[177] Впервые среди других тем в рамках борьбы с транснациональной преступностью в нем был рассмотрен вопрос о преступлениях, связанных с использованием компьютеров[178]. Помимо этого, была признана необходимость достижения международного консенсуса по видам компьютерных преступлений, которые должны быть признаны уголовными преступлениями во всех государствах-членах ООН, чтобы расширить действие института ответственности физических лиц за подобные преступления, наносящие урон не только национальной, но и международной безопасности. Начало второго тысячелетия знаменовалось формированием ГИО, что было отражено в разработке и принятии таких документов, как Окинавская хартия Глобального информационного общества 2000 г., Декларация тысячелетия ООН 2000 г., а также проведением Десятого Конгресса ООН по предупреждению преступности и обращению с правонарушителями 2000 г. и двух этапов Всемирного саммита по информационному обществу – женевского и тунисского, по результату которых были приняты Декларация принципов «Построение информационного общества: глобальный вызов в новом тысячелетии»[179], «План действий Всемирной встречи на высшем уровне по информационному обществу»[180], «Тунисская повестка дня для информационного общества»[181]. Примечательно, что на фоне стремления ряда технологических компаний к доминированию в ИКТ-среде ключевой повесткой в рамках вызовов ГИО стали современная модификация государственного суверенитета – технологический суверенитет[182], преодоление «цифрового разрыва», а также равноправный доступ к ИКТ, использование их в мирных целях.

---

[177] Крупнейший межправительственный форум, оказавший влияние как на национальную политику, так и на разработку рекомендаций по международному сотрудничеству.

[178] Доклад, подготовленный Секретариатом // Восьмой Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, Гавана, 27 августа – 7 сентября 1990 г. – A/CONF.144/28/Rev.1. – Нью-Йорк: ООН, 1991. – 307 с.

[179] Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium [Электронный ресурс]. – WSIS-03/GENEVA/DOC/4. – 12 December 2003. – URL: https://digitallibrary.un.org/record/533621?ln=ru (дата обращения: 10.08.2024).

[180] Plan of Action of the World Summit on the Information Society [Электронный ресурс]. – Document WSIS-03/GENEVA/DOC/5-E. –2003, 12 December. – URL: https://www.itu.int/net/wsis/docs/geneva/official/poa.html (дата обращения: 10.08.2024).

[181] WSIS: Tunis Agenda for the Information Society [Электронный ресурс]. – WSIS-05/TUNIS/DOC/6 (Rev. 1)-E. –2005, 18 November. – URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (дата обращения: 10.08.2024).

[182] Ефремов А. А. Информационно-правовое обеспечение технологического суверенитета // Информационное право. – 2022. – № 4 (74). – С. 14.

В то время уже можно было наблюдать процесс формирования повестки обеспечения безопасности в области применения ИКТ, но акцент был сделан на вопросах сотрудничества, так как происходило развитие преступлений, которые связаны с применением ИКТ[183]. Данная проблематика способствовала разработке первых соответствующих международно-правовых документов в рамках региональных организаций, а именно Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 г., Конвенции Совета Европы о компьютерных преступлениях 2001 г., Соглашения между правительствами государств-членов ШОС о сотрудничестве в области МИБ 2009 г. Положения вышеупомянутых договоров легли в основу дальнейшей кодификации и прогрессивного развития международного права по ИКТ-проблематике, свидетельством чего стала выработка Конвенции ЛАГ о борьбе с преступлениями в области информационных технологий 2010 г., Проекта Конвенции Африканского союза (АС) о создании юридических основ кибербезопасности в Африке 2012 г. и Конвенции АС о кибербезопасности и защите персональных данных 2014 г., Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г., Общего регламента по Европейского союза защите данных 2018 г., Директив о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем 2016 г. и 2021 г. и так называемого пакета Закона о цифровых услугах 2022 г.[184], включающего Законы о цифровых рынках и цифровых услугах, и многих других документов регионального уровня[185].

В правовой доктрине Будапештская конвенция о киберпреступности часто определяется зарубежными правоведами как наиболее актуальный многосторонний документ, который направлен на борьбу с киберпреступностью, однако это достаточно спорный тезис, как минимум, из-за того, что предмет

---

[183] Международная безопасности в среде информационно-коммуникационных технологий. Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде. Указ. соч.

[184] Законодательное предложение Европейской комиссии, представленное Европейскому парламенту и Европейский совету 15 декабря 2020 г.

[185] Всестороннее исследование проблемы киберпреступности. Проект, февраль 2013 года // Управление Организации Объединенных Наций по наркотикам и преступности. Указ. соч.

договора достаточно узок, его членский состав не говорит о всеобъемлющем характере, а определяет его применение за исключением ключевых государств, участвующих в функционировании ИКТ-среды, не говоря уже о его спорном содержании. В этом контексте важно упомянуть еще одну инициативу Российской Федерации – учреждение Спецкомитета ООН по разработке договора по борьбе с киберпреступностью. Данный переговорный механизм был создан по инициативе РФ в соавторстве с 46 государствами и поддержке 87 государств в рамках резолюции ГА ООН 74/247, целью которой является создание универсального юридически обязательного документа, который бы обеспечивал международное сотрудничество и координацию в борьбе с киберпреступностью. Помимо этого, одна из задач предлагаемой Россией конвенции – это создание правовой альтернативы Будапештской конвенции на глобальном уровне под эгидой ООН. Ожидается, что итоговой текст будет представлен в ходе 78-й сессии ГА ООН (сентябрь 2024 г.)[186]. Тем не менее, проблематика киберпреступности является самостоятельным комплексным направлением, которое требует отдельного научного исследования и остается вне рамок настоящего диссертационного исследования.

В связи с актуальностью проблемы регулирования ИКТ в контексте международной безопасности появились конкретные предложения по выработке универсального международно-правового акта под эгидой ООН, примерами которых могут выступить российская концепция Конвенции об обеспечении МИБ 2011 г. и ее обновленная версия от 2023 г.[187] Однако, как было отмечено в первой главе диссертационного исследования, терминологические и сущностные разногласия государств по-прежнему торпедируют переговорный процесс, тем не менее, необходимость принятие такого на фоне укрепления государствами в

[186] О пятой сессии Спецкомитета ООН по разработке всеобъемлющей конвенции о противодействии использованию информационно-коммуникационных технологий (ИКТ) в преступных целях [Электронный ресурс]. – URL: https://mid.ru/ru/foreign_policy/news/1865216/ (дата обращения: 10.08.2024).

[187] 15 мая 2023 г. Россия в соавторстве с Белоруссией, КНДР, Никарагуа и Сирией внесла концепцию конвенции ООН об обеспечении международной информационной безопасности МИБ в качестве официального документа 77-й сессии Генеральной Ассамблеи ООН [Электронный ресурс]. Источник: Обновленная концепция конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности. Предложение Российской Федерации. – URL: http://www.scrf.gov.ru/media/files/file/ P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (дата обращения: 10.08.2024).

последние годы не только оборонительного, но и наступательного потенциала ИКТ диктуют настоятельную необходимость решения проблемы регламентации обеспечения безопасности в области применения ИКТ на универсальном уровне, а принятие подобного международно-правового акта признается всем международным сообществом, несмотря на наличие разногласий.

Что касается устной формы международных договоров, то можно обратиться к историческому примеру, связанному с ООН. В 1946 г. СССР, США, Англия и другие государства-члены ООН заключили джентельменское соглашение о принципе географического распределения мест для непостоянных членов Совета Безопасности ООН. Принцип равного географического участия далее лег в основу деятельности ряда международных организаций, которые занимаются информационной безопасностью, например, МСЭ[188].

Международный обычай занимает ведущее положение в развивающихся областях права, опережая международные договоры как источник международного права. В ситуациях, не урегулированных установившимся консенсусом относительно того, какой должен быть установлен международно-правовой режим, государства могут предпринимать действия, которые они сочтут целесообразными, исходя из общей и последовательной практики государств, длительности ее существования и признания в качестве общеобязательной нормы, то есть оперировать нормами международного обычного права. Что особенно актуально в случае с международно-правовым регулированием обеспечения безопасности в сфере использования ИКТ. Нормы обычного права могут помочь в толковании некоторых международных договоров, а также могут быть использованы для заполнения возможных пробелов[189]. Таким образом, еще один наиболее распространенный источник международного права – это обычай. Согласно

[188] В соответствии с основополагающим документом МСЭ «Ассамблея радиосвязи, Всемирная Ассамблея по стандартизации электросвязи (ВАСЭ), Всемирная конференция по развитию электросвязи обязаны назначать председателей и заместителей председателей исследовательских групп с учетом их компетентности и справедливого географического распределения, а также необходимости содействия более эффективному участию развивающихся стран». Источник: Constitution and Convention of the International Telecommunication Union (with annexes and optional protocol). Concluded at Geneva on 22 December 1992 // United Nations Treaty Series. Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. Vol. 1825, 1-3125. – New York, 1998. – P. 506.

[189] Первый доклад по теме «Формирование и доказательство существования международного обычного права», подготовленный Специальным докладчиком Майклом Вудом. Указ. соч.

И. И. Лукашуку, обычай можно классифицировать в зависимости от характера его формирования на две категории: традиционный и современный[190]. Международно-правовая регламентация реализуется также на основе международно-правовых обычаев, или норм международного обычного права, используя термин Венской конвенции о праве международных договоров 1969 г.[191] Что касается специфики международных обычаев, применимых к ИКТ, они пронизывают весь уровень их правового регулирования, являясь стержнем национального, двустороннего, регионального и универсального уровней правового регулирования. С целью установления существования обычной нормы, теория международного права требует, чтобы она отвечала следующим четырем критериям: устный характер, всеобщность признания, единообразия применения, признание в качестве opinion juris[192]. При этом, если норма отвечает только критериям всеобщности признания и единообразию применения, то это уже обыкновение, нарушение которого не будет, в отличие от нарушения обычая, восприниматься как правонарушение. ИКТ открывают новые возможности для международного обычного права. Во-первых, в процессе доказательства существования норм международного обычного права могут быть теперь использованы и Интернет-ресурсы. Во-вторых, изучение обычаев и практики их применения может эволюционировать с учетом развития ИКТ, например, посредством использования методологии обработки информации, основанной на автоматических или полуавтоматических средствах анализа объектов, содержащих информацию, или использования искусственного интеллекта.

---

[190] Как справедливо отметил А. В. Пазюк, «в формировании современного обычая ключевую роль играет opinion juris, т.е. всеобщее признание за обычаем правовой силы, а роль практики (usus) как элемента юридического состава отходит на второстепенный план». Источник: Пазюк А. В. Особенности создания и реализации международно-правовых обычных и договорных норм в сфере управления интернетом [Электронный ресурс]. – 2016, 03 августа. – URL: https://digital.report/upravlenie-internetom/ (дата обращения: 10.08.2024).

[191] Венская конвенция о праве международных договоров (Вена, 23 мая 1969 г.) // Ведомости ВС СССР. – 10 сентября 1986 г. – № 37. – Ст. 772.

[192] Международный суд в своей судебной практике редко стремился определить понятие обычая, прибегая к углубленному исследованию, охватывающему отдельно практику государств и opinio juris. Фактически, судьи обычно либо заявляли о существовании международного обычая (декларативный подход, который преобладает), либо делали вывод о его существовании на основе доказательств из государственной практики (логический подход). Источник: Brown G., Poellet K. The Customary International Law of Cyberspace [Электронный ресурс] // Strategic Studies Quarterly. – 2012. – Vol. 6, No. 3. – P. 126–145. – URL: https://www.jstor.org/stable/26267265 (дата обращения: 10.08.2024).

Далее необходимо рассмотреть, какие же существуют международные обычаи в сфере использования ИКТ. Ответ на этот непростой вопрос может быть найден в особенностях функционирования Интернета. В данном контексте особый интерес представляет спам[193]. Что касается международно-правового регулирования на универсальном уровне, то не существует международно-правового акта, который устанавливает запрет спама с целью обеспечения безопасности ГИО[194]. В связи с чем практика запрета спама могла бы быть квалифицирована как международный обычай, который в дальнейшем получил свое закрепление в нормативно-правовых актах ряда государств посредством введения ограничения на спам. Примерами выступают Закон США о приличиях в области связи 1996 г.[195] и Директива 2002/58/ЕС о конфиденциальности и электронных средствах связи от 12 июля 2002 г.[196]. Положения выше обозначенных нормативно-правовых актов устанавливают запрет на отправку писем, которые скрывают личность адресанта[197]. Однако подобного запрета на спам на международном уровне нет. В дополнение к этому, существует как общегосударственная практика по борьбе со спамом, так и судебные решения, направленные на противодействие данной деятельности. Особый научный интерес представляют торговые обычаи, которые сформировались в области международной электронной коммерции, к ним могут быть отнесены обязанность онлайн-платформ поддерживать надежное шифрование всех веб-транзакций, отказать в предоставлении услуги, если веб-браузер клиента не поддерживает надежное шифрование, воздерживаться от рассылки спама и т.д.; а также

---

[193] Brown G., Poellet K. The Customary International Law of Cyberspace. Op. cit.

[194] Polanski P. Cyberspace: A new branch of international customary law? [Электронный ресурс] // Computer Law & Security Review. – 2017. – URL: https://www.researchgate.net/publication/315937970_Cyberspace_A_new_branch_of_international_customary_law (дата обращения: 10.08.2024).

[195] Иные варианты перевода: Закон о порядочности в общении, Закон о соблюдении приличий в коммуникациях. Communication Decency Act of 1996. Pub. L. No. 104–104. it. V, 110 Stat. 133 (1996).

[196] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) // Official Journal of the European Communities. – 2002, 31 July. – L 201. – P. 37–47.

[197] Лифшиц И. М. Международное финансовое право и право Европейского союза: взаимодействие и взаимовлияние [Электронный ресурс]: монография. – Москва: Юстицинформ, 2020. – 548 с. – ISBN 978-5-7205-1646-8. – Доступ из справочно-правовой системы «ГАРАНТ». – URL: https://ivo.garant.ru/#/document/76894275 (дата обращения: 10.08.2024).

международные обычаи в области безопасности данных, конфиденциальности, регулирования вредоносного контента[198].

Еще один международный обычай, который характерен для формирующейся системы международно-правовых норм, регулирующих обеспечение безопасности в сфере использования ИКТ, связан с особенностями развития современного информационного пространства, неотъемлемым элементом которого является Интернет[199]. Особенности его развития, в частности роль негосударственных субъектов ИКТ-среды в его функционировании, предопределили возникновение нормы международного обычного права, которая заключается в привлечении всех заинтересованных сторон, или «мультистейколдеров», для дискуссий, определяющих эволюцию и функционирование Интернета. Данный обычай нашел свое закрепление в заключительных актах Всемирного Саммита по вопросам информационного общества в Женеве в 2003 г. и Тунисе в 2005 г. Тем самым, данный международный обычай получил свое дополнительное оформление, однако его закрепление в универсальном международно-правовом акте является предметом разногласий и консенсуса по данному вопросу не существует. Существуют две позиции: первая, поддерживаемая США, согласно которой гражданское общество и бизнес сектор должны быть не только участниками переговорных процессов, но и участвовать наравне с государствами в процессе принятия решений; противоположный подход, которого придерживаются развивающиеся страны и Россия, ограничивается только первым параметром, обосновывая это «цифровым разрывом» и отсутствием баланса среди технологических компаний, что может привести к тому, что переговорный процесс и принятие решений станут политическим инструментом реализации интересов технологически более развитых государств. Помимо этого, согласной второму подходу, ключевая роль в принятии решений должна сохранятся за государствами.

Далее коротко рассмотрим дополнительные источники международно-правовых норм, упомянутые в статье 38 Статута Международного Суда. Общие

---

[198] Polanski P. Cyberspace: A new branch of international customary law? Op. cit.

[199] Пазюк А. В. Особенности создания и реализации международно-правовых обычных и договорных норм в сфере управления интернетом. Указ. соч.

принципы права – это правовые принципы, которые являются общими для всех правовых систем, сущность которых очевидна из самой природы права и которые основаны на принципе справедливости. К ним относятся такие принципы, как принцип равноправия, принцип гуманизма, принцип законности, принцип добросовестности, равный над равным власти не имеет, res judicata (разрешенное дело), pacta sunt servanda (соглашения должны соблюдаться), venire contra factum proprium (принцип эстоппеля) и другие[200]. Общие принципы права относительно регулирования обеспечения безопасности в сфере использования ИКТ актуальны, когда возникают споры между государствами по вопросам информационной безопасности[201]. Например, в случае если была совершена атака против информационной безопасности государства с использование ИКТ и есть веские доказательства, которые лягут в основу атрибуции, то в результате неправомерных действий, которые нарушили суверенитет другого государства и причинили ему ущерб, такое государство будет обязано возместить ущерб потерпевшему. Особую важность в контексте обеспечения безопасности в сфере использования ИКТ имеет общий принцип права, согласно которому ответственность может наступить только за вину. В этом контексте значимость общих принципом права определяется возможностью заполнить существующие правовые вакуумы в исследуемой области[202].

Статья 38 Статута Международного суда в пункте (d) определяет судебные решения государственных и международных судов, не проводя различий между их решениями, в качестве вспомогательного средства определения норм международного права. В отличие от правовых систем государств, принадлежащим к семье общего права, в международном праве нет доктрины обязательного прецедента[203]. Статья 59 Статута Международного суда прямо предусматривает,

---

[200] Schmitt M. N., Vihul L. The Nature of International Law Cyber Norms [Электронный ресурс] // International Cyber Norms: Legal, Policy & Industry Perspectives / A.-M. Osula, H. Rõigas (Eds.). – Tallinn: NATO CCD COE Publications, 2016. – URL: https://www.ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch2.pdf (дата обращения: 10.08.2024).
[201] Ibid.
[202] Grossman C. M. ILC Report on Prevention and Punishment of Crimes Against Humanity and Enforced Disappearance. Op. cit.
[203] Greenwood C. Sources of International Law: An Introduction [Электронный ресурс]. – URL: https://legal.un.org/avl/ls/Greenwood_IL.html (дата обращения: 10.08.2024).

что решение Суда не является обязательным ни для кого, кроме сторон дела, по которому выносится это решение, и даже тогда только в отношении этого конкретного дела, однако практика Международного суда показывает, что он часто ссылается на свои прошлые решения[204]. В дополнение к этому международные трибуналы также используют ранее рассмотренные дела в качестве руководства по определению норм международного права и их содержания. Что касается международно-правового регулирования обеспечения безопасности в сфере использования ИКТ, то важно отметить, что судебные решения как источники международно-правовых норм особенно развиты с точки зрения международного права в области прав человека. Так, например, «решения международных судебных учреждений по защите свободы мнений и их выражения, принятые Европейской Комиссией и Европейским Судом по правам человека, Межамериканской комиссией и судом по правам человека, Африканского суда по правам человека и народов, в значительной мере содействовали развитию международного информационного права»[205] в целом и международно-правовому регулированию обеспечения безопасности в сфере использования ИКТ в частности.

«Судопроизводство в отношении ИКТ уже существует, но в рамках национальных правовых систем, а не глобального механизма»[206]. «Однако в виду наличия противоречий и отсутствия четкой системы международного-правового регулирования обеспечения безопасности в сфере использования ИКТ»[207], создание подобного механизма на текущий момент преждевременно.

В статье 38 также упоминаются труды специалистов по публичному праву в качестве дополнительного средства определения норм международного права по

[204] Greenwood C. Sources of International Law: An Introduction [Электронный ресурс]. – URL: https://legal.un.org/avl/ls/Greenwood_IL.html (дата обращения: 10.08.2024).
[205] Пазюк А. В. Международное информационное право. Общая часть. Международное информационное право – отрасль современного международного права. Указ. соч.
[206] Мартиросян А. Ж. Формирование системы обеспечения безопасности киберпространства: монография / отв. ред. И.О. Анисимов. – М.: Дипломатическая академия МИД России, 2021. – С. 125.
[207] Мартиросян А. Ж. Создание международного трибунала по киберпреступности // Актуальные проблемы мировой политики. IX Ежегодная международная научная конференция молодых ученых, Москва, 6–7 декабря 2022 г. (сборник тезисов) / отв. ред. О. А. Тимакова. – Москва: Дипломатическая академия МИД России, 2023. – 345 с. URL: https://pureportal.spbu.ru/files/102589388/_2022.pdf (дата обращения: 10.08.2024).

конкретному вопросу[208]. Труды юристов-международников также могут быть убедительным руководством к содержанию международного права, но сами по себе они не выполняют нормотворческой функции. Чаще всего носят толковательную и информативную значимость[209]. Доктрина как источник международно-правового регулирования обеспечения безопасности в области применения ИКТ наиболее ярко прослеживается в региональном аспекте формирования нормативной базы и подходов к ней, например, в работе ученых Международной группы экспертов, подготовившей Таллиннское руководство и Таллинн 2.0[210]. Еще одним примером может выступить совместная попытка американского и российского академического сообщества способствовать международному переговорному процессу[211] в исследуемой области посредством выработки согласованных определений, а именно общий труд Института «Восток-Запад» и Института проблем информационной безопасности МГУ им. М. В. Ломоносова[212]. Весомый вклад также сносят российские правоведы из НАМИБ, МГИМО (У) МИД России, Дипломатической академии МИД России и многие другие образовательные организации высшего образования и научно-исследовательские институты.

Список источников международного права, закреплённый в ст. 38 Статута Международного Суда, часто становится объектом научной дискуссии и критики в виду своей неполноты. Так, в нем нет упоминаний об актах международных организаций и институтов семьи ООН. Резолюции ГА ООН не имеют обязательной юридической силы, но оказывают важное влияние на дальнейших процесс

---

[208] Устав Организации Объединенных Наций [Текст]: принят в г. Сан-Франциско 26.06.1945 // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. XII. – М., 1956. – С. 14–47.

[209] Костенко Н. И. Право международной информационной безопасности (становление, тенденции и проблемы развития): монография. Указ. соч. С. 76.

[210] Данные «эксперты отвергли характеристику киберпространства как отдельной сферы регулирования, требующей новой институциональной структуры, и пришли к единодушному выводу, что общие принципы международного права должны также применяться и к киберпространству», что является объектом разногласий между отечественной и западной школами права. Источник: Берман А. М., Шинкарецкая Г. Г. Кибератаки – противоправное использование цифровых технологий // Международное право. – 2022. – № 1. – С. 42.

[211] Мартиросян А. Ж. Международная информационная безопасность: некоторые итоги 2021 г. и политический контекст 2022 г. Указ. соч.

[212] Godwin III J. B., Kulpin A., Rauscher K. F., Yaschenko V. Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2. Op. cit.

нормотворчества в международном праве. Иногда положения резолюций, которые не обладают юридически обязательной силы, могут быть преобразованы международным сообществом в юридически обязательные путем их закрепления в резолюциях Совета Безопасности или международно-правовых актах. Резолюции ГА ООН внесли весомый вклад в формирование международно-правового регулирования обеспечения безопасности в сфере использования ИКТ[213], подтверждением этому является разработка и принятие на постоянной основе резолюций по данной проблематике с 1998 г. Помимо этого, резолюции ГА ООН выступают фундаментом для выработки договоров в сфере информбезопасности[214].

Особый интерес представляет анализ кодексов поведения, которые не являются по своей юридической природе международными договорами. Подобные документы закрепляют намерения государств, а также могут иметь толковательную и оценочную функции относительного соответствующего договора. В 2016 г. на площадке ГА ООН был одобрен 119 государствами кодекс ответственного поведения государств в Интернете, инициатором которого выступила Российская Федерация. Кодекс включает 13 принципов, раскрывающих правила поведения в ИКТ-среде. Хотя документ носит рекомендательный характер, он важен с точки зрения возможного использования его положений при выработке общепризнанных юридически обязательных норм в глобальном информационном пространстве и его составляющей – ИКТ-среде.

В связи с разногласиями государств к обеспечению безопасности в области применения ИКТ и выходящего из этого факта отсутствия универсального международно-правового акта на данный момент развития международного права большинство документов, разработанных и принятых на региональном и универсальном уровнях сотрудничества, носят рекомендательный характер, являясь примерами норм «мягкого права». Тем не менее, рассматриваемые нормы

---

[213] Полякова Т. А., Смирнов А. А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы. Указ. соч.

[214] Штодина Д. Д. Международное сотрудничество государств-участников СНГ в области обеспечения информационной безопасности // Вестник ученых-международников. – 2021. – № 3 (17). – С. 105.

имеют важное значение с точки зрения их перспективного использования в качестве юридического фундамента для международного соглашения по обеспечению безопасности в сфере использования ИКТ[215].

Особую роль нормы мягкого права играют в интеграционных объединениях. Например, коммунитарный метод Монне – Шумана в рамках права Европейского союза преобразует «мягкие нормы» в юридически обязательные[216]. Интересна идея С. Ю. Кашкина, согласно которому в европейском правовой системе существует «полужесткое право»[217]. Данный нормотворческий подход возможен к использованию как ad hoc инструмента, который будет обеспечивать стабильность и безопасность международной системы, в то числе ГИО, до достижения консенсуса по вопросам разработки соответствующего международно-правового акта. Рассматриваемый подход применительно к международно-правовой регламентации использования ИКТ в контексте международной безопасности может быть Наиболее эффективен при реализации на региональном уровне с постепенным переходом на глобальный.

Помимо этого, в связи с особенностями развития современного информационного пространства большую роль в международно-правовом регулировании обеспечения безопасности в сфере использования ИКТ имеют технические стандарты, регламенты, руководящие принципы, также относящиеся к нормам «мягкого права». Среди них в сфере использования ИКТ выделяют три основных категории: стандарты кибербезопасности (технологические аспекты), стандарты безопасности ИКТ, стандарты управления рисками. Существует ряд организаций, которые занимаются стандартизацией. «Региональные организации стандартизации, например, европейские механизмы, занимающиеся стандартизацией. К ним относятся Европейский комитет по стандартизации (Comité Européen de Normalisation, CEN), Европейский комитет электротехнической стандартизации (European Committee for Electrotechnical

[215] Сборник докладов участников XVI международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Москва, 19–21 сентября 2022 г. Op. cit.
[216] Кашкин С. Ю., Алтухов А. В. В поисках концепции правового регулирования искусственного интеллекта: платформенные правовые модели // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2020. – № 4. – С. 26–40.
[217] Там же.

Standardization, CENELEC), Европейский институт телекоммуникационных стандартов (European Telecommunication Standards Institute, ETSI)[218], являющийся членом Группы сертификации кибербезопасности Европейской комиссии. К международным организациям глобального уровня, занимающимся стандартизацией, относят ИСО, МЭК и МСЭ»[219].

В рамках процесса разработки норм «мягкого права» научный интерес также представляет разрабатываемый Глобальный цифровой договор (ГЦД), который планируется к принятию как приложение Пакта во имя будущего на Саммите будущего в сентябре 2024 г.[220] «Нулевой проект» ГЦД был представлен в апреле 2024 г.[221], а его первая отредактированная версия в мае 2024 г.[222] Договор включает такие разделы, как цели, принципы, последующая деятельность и обсуждение ГЦД, а также шаги и обязательства по таким аспектам, как преодоление цифрового разрыва и ускорение прогресса в достижении ЦУР; расширение участия в цифровой экономике; создание инклюзивного, открытого, безопасного цифрового пространства; продвижение справедливого международного управления данными; управление новыми технологиями, включая искусственный интеллект, в интересах человечества. Договор, как заявляется, призван установить основы сотрудничества в цифровой сфере с целью обеспечения равных возможностей и безопасности для всего мирового сообщества. Проект документа охватывает широкий спектр вопросов, связанных с ИКТ-средой, в частности, цифровую грамотность, управление новыми технологиями, включая искусственный интеллект, а также обеспечение доступности и устойчивости цифровой инфраструктуры. Как

---

[218] European Telecommunication Standards Institute [Электронный ресурс]. – URL: https://www.etsi.org/ (дата обращения: 10.08.2024).

[219] Мартиросян А. Ж. Формирование системы обеспечения безопасности киберпространства: монография / отв. ред. И.О. Анисимов. – М.: Дипломатическая академия МИД России, 2021. – С.33.

[220] В рамках технологического трека с участием всех заинтересованных сторон: правительств, системы ООН, частного сектора (включая технологические компании), гражданского общества, научных кругов и отдельных лиц». Источник: Размышления Школы МИБ о Глобальном цифровом договоре [Электронный ресурс] / отв. ред. А. Ж. Мартиросян. – URL: https://t.me/iis_mib_school/376/ (дата обращения: 10.08.2024).

[221] Global Digital Compact: zero draft [Электронный ресурс] // Office of the Secretary-General's Envoy on Technology. – 1 April 2024. URL: www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Zero_Draft.pdf (дата обращения: 10.08.2024).

[222] Global Digital Compact: rev. 1 [Электронный ресурс] // Office of the Secretary-General's Envoy on Technology. – 15 May 2024. – URL: www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Rev_1.pdf (дата обращения: 10.08.2024).

заявлялось, ГЦД должен будет изложить общие принципы открытого, свободного и безопасного цифрового будущего для всех. Тем не менее, проект договора содержит в себе недостатки, рассмотрим некоторые из них, которые имеют прямое отношение к обеспечению безопасности в области использования ИКТ. Терминологическая составляющая документа требует существенной доработки, так, например, не ясно, что подразумевается под понятием «цифровой общественной инфраструктуры» (digital public infrastructure). Смещен акцент на «гуманитарную» составляющую, без решения насущных правовых проблем. Документ не содержит принципов ответственного поведения государств в ИКТ-среде, необходимо внести их с учетом вероятного принятия ГЦД и возможности их продвижения в очередном юридически необязательном документе ООН. Помимо этого, пункт 8 требует дополнения следующими принципами: принцип государственного суверенитета в информационном пространстве, принцип недискриминации государств, принцип мирного использования новых технологий, принцип ответственности, принцип атрибуции, принцип антропоцентричности при разработке и использовании новых технологий. Пункт 18 необходимо дополнить в части, касающейся доступа к новым технологиям, целесообразным видится запрет деятельности, направленной на ограничения доступа к технологиям и дискриминации государств по данному вопросу на основе их политического и/или экономического пути развития. В целом запрет на дискриминацию государств по политическому и экономическому пути развития является важным шагом для обеспечения равенства доступа к технологиям и предотвращения ограничений, которые могут быть направлены на определенные государства или группы государств. По всему тексту акцент сделан на обществе, а не государстве, что отражает попытки смещения роли первичного субъекта международного права с целью расширения возможностей частного сектора и гражданского общества в принятии решений. ГЦД не определяет обязанности частного сектора «заземляться», то есть соблюдать нормы законодательства того государства, на

территории которого они осуществляют деятельность[223], а напротив предлагает введение блокировки контента на основе пользовательских соглашений, что может нарушать международные нормы, закрепленные в статье 19 Международного пакта о гражданских и политических правах[224]. В целом в документе отсутствуют положения, четко определяющие организационно-правовой характер «международной структуры или механизма», в чьей мандат войдет контроль за исполнением ГЦД. Однако в пункте 24 обозначена поддержка предложения Генсека ООН о создании Цифровой консультативной службы ООН по правам человека (UN Digital Human Rights Advisory Service), в пункте 53 инициируется идея учреждения Международной научной группы по ИИ и новым технологиям (International Scientific Panel on AI and Emerging Technologies) и Международной контактной группы по управлению ИИ (International Contact Group on AI Governance), в пункте 70 – Управления Секретариата по координации цифровых и нарождающихся технологий, в пункте 76 – совещания высокого уровня «Обзор Глобального цифрового договора на высоком уровне» (high-level meeting High-Level Review of the GlobalDigital Compact). По факту в рамках разработки ГЦД в обход деятельности специализированных структур предпринимается попытка сформировать совершенно новую систему управления ИКТ-средой[225], что приведет к созданию очередных «механизмов» без соответствующего мандата и соблюдения требований к прозрачному обсуждению. Необходимо закрепить условия обсуждения целесообразности создания упомянутых механизмов с ключевой ролью в принятии решений за государствами. Также существует риск того, что обсуждение ГЦД станет еще одним шагом в сторону политизации ИКТ-повестки. Так, ГЦД может размыть международные переговоры по информационной безопасности в связи с тем, что он создает дублирование

[223] Мельникова О. А. Глобальный цифровой договор: на грани фола [Электронный ресурс] // Международная жизнь. – 2024. – № 3. – URL: https://interaffairs.ru/jauthor/material/2962 (дата обращения: 10.08.2024).

[224] Статья 19 гарантирует свободу выражения мнений, но позволяет ограничивать ее только при условии принятия соответствующих национальных законов. Введение блокировки на основе пользовательских соглашений может быть противоречивым и нарушать международные стандарты защиты свободы выражения.

[225] Выступление представителя Российской Федерации Б. А. Мещанова на презентации «нулевого проекта» Глобального цифрового договора ООН [Электронный ресурс] // Постоянное представительство Российской Федерации. – URL: https://russiaun.ru/ru/news/7120424 (дата обращения: 10.08.2024).

функций уже используемых площадок, в рамках которых предпринимаются попытки выработать не декларативные принципы использования ИКТ, а именно юридически обязывающие нормы, что идет вразрез с потребностями ГИО. Положения ГЦД весьма, вероятно, будут носить декларативный характер и существенно не смогут повлиять на цифровую монополию отдельных стран и крупных корпораций, которые активно выдвигают предложения к ГЦД[226]. Несмотря на достаточно противоречивую природу ГЦД, процесс его разработки в очередной раз подтверждает необходимость четко выстроенного институционального механизма (организационно-правовой основы) управления безопасностью в области использования ИКТ, а также разработки и принятия соответствующего универсального международно-правового акта.

На основе анализа формирующейся международно-правовой системы норм, регулирующих обеспечения безопасности в сфере использования ИКТ, можно сделать вывод, что ее структура базируется на основных и дополнительных источниках международно-правовых норм общего международного права, при этом их разработка происходит с учетом специфики развития ИКТ и ГИО. Доминирующее место среди них занимают международные договоры двустороннего или регионального характера. Помимо этого, источниковая база не ограничивается традиционными источниками международного права, их дополняют акты международных организаций, стандарты, регламенты, рекомендации, разработанные с целью обеспечения безопасности в сфере использования ИКТ, а также кодексы. Формирование международно-правовой системы норм, регулирующих обеспечение безопасности в сфере использования ИКТ отличается преобладающей ролью норм «мягкого права», что обусловлено сложностями в международном переговорном процессе, а также особенностями возникновения и развития ИКТ. Нормы «мягкого права» носят субсидиарный

[226] Как верно отмечают Зиновьева Е., Исаева Т., по своей природе рассматриваемый документ «продолжает практику глобальных договоров ООН, которые не являются договорами в юридическом смысле данного термина, а представляют собой набор общих принципов, призванных регулировать деятельность различных акторов мировой политики». Источник: Зиновьева Е., Исаева Т. Глобальный цифровой договор ООН: возможна ли прикладная реализация? [Электронный ресурс] // Международная жизнь. – 28.10.2022. – URL: https://interaffairs.ru/news/show/37601 (дата обращения: 10.08.2024).

характер регулирования и не имеют потенциала заменить юридически обязательные[227]. В этом контексте необходимость выработки юридически обязательного универсального международно-правового акта не вызывает сомнений в связи с активным использование ИКТ и исходящей из этого возрастающей потребности их нормативно-правового регулирования на международном уровне с целью обеспечения безопасности в сфере использования ИКТ. При этом, разработанные нормы «мягкого права» могут стать комплементарным механизмом, который не должен заменять универсальный международно-правовой акт с юридически обязательными к исполнению нормами, а должен отражать лишь перспективные направления развития правового регулирования обеспечения безопасности в сфере использования ИКТ на универсальном уровне.

Исследование международно-правовой основы регулирования обеспечения безопасности в сфере использования ИКТ и организационно-правовой (институциональной) базы международного сотрудничества в исследуемом направлении позволяет сделать вывод о формирующейся концепции развития всеобъемлющей системы обеспечения безопасности в сфере использования ИКТ, в которой наблюдается тенденция к системному характеру без ограничения лишь технологическими аспектами информационной безопасности. Формирующаяся система международно-правового регулирования международной безопасности в области применения ИКТ включает в себя как государственные, так и негосударственные международные отношения. Ее важной характеристикой является комплексность, представленная следующими уровнями правового регулирования: национальным, и международным уровнями, который, в свою очередь, реализуется на двустороннем, региональном, универсальном механизмов взаимодействия.

В настоящее время обсуждение разработки международных норм, регулирующих международную безопасности в контексте применения ИКТ,

[227] Мартиросян А. Ж. Формирование системы обеспечения безопасности киберпространства: монография / отв. ред. И.О. Анисимов. – М.: Дипломатическая академия МИД России, 2021. – С. 79.

находится в активной фазе, что обусловлено актуальностью необходимости обеспечения информационной безопасности. Однако принятие универсального международного нормативно-правового акта усложняется геополитической конъюнктурой современных международных отношений. Последнее, в свою очередь, определяет наличие разрозненных инициативы для решения актуальных проблем безопасности в сфере использования ИКТ[228], что в определенной степени отражает тенденцию фрагментации международного права.

Помимо этого, проведенный анализ в данной главе позволил сделать вывод, что структура системы международно-правового регулирования обеспечения безопасности в сфере использования ИКТ строится на основных источниках общего международного права с учетом специфики развития ГИО и ИКТ. Ее дополняют отраслевые нормы мягкого права, представленные актами международных организаций, стандартами, регламентами, рекомендациями, кодексы и иные источники, разработанные с целью обеспечения безопасности в сфере использования ИКТ. Источниковая база отличается преобладающей ролью норм мягкого права. При этом непрерывный рост угроз в ИКТ-среде обуславливает необходимость выработки юридически обязательных норм, регулирующих обеспечение безопасности в сфере использования ИКТ на глобальном уровне.

[228] Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции. Указ. соч.

ГЛАВА 3. МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ОТДЕЛЬНЫХ НАПРАВЛЕНИЯХ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В данной главе диссертационного исследования выявлены тенденции, проблемы и перспективы, существующие в исследуемых автором отраслях международного публичного права относительно регулирования использования ИКТ в контексте международной безопасности. С целью содействия совершенствования и кодификации международного права и в дополнение к инициативам по принятию универсального международно-правового акта по регулированию ИКТ-среды автором диссертационного исследования проведен анализ отдельных отраслей международного права – международного морского права и международного космического права – с точки зрения регулирования ИКТ и предложены практические и теоретические рекомендации, а также возможности выработки специализированных международных механизмов, регулирующих соответствующие правовые отношения. Выбор данных отраслей международного права обусловлен рядом причин. На сегодняшний день космическое и морское пространство выступают одним из инновационных сфер, в которых наблюдается значительное внедрение и использование ИКТ[229], что сопровождается ростом вызовов и угроз космическим и морским ИКТ-систем. Постановка вопроса о необходимости международно-правового регулирования обеспечения безопасности использования ИКТ в данных отраслях международного права, а также недостаточное исследование рассматриваемой проблематики, обуславливает интерес доктрины международного права к изучению правовой природы использования информационно-коммуникационных инноваций в них.

[229] Например, в области международного судоходства наблюдается рост обработки и использования цифровыми платформами больших данных для отслеживания судов и грузов, что привело к тому, что новые технологии стали незаменимым инструментом для процветания в эпоху цифровых услуг. В частности, широкий ИКТ спектр применения на морском транспорте можно обнаружить в электронной навигации, управлении грузами и портами, связи и передачи данных, безопасности, управлении охраной окружающей среды и др. Что касается космического пространства, то здесь наблюдается «острая потребность» в международно-правовых нормах, которые могли бы эффективно управлять растущими возможностями космических технологий, а также наблюдается возрастание влияния высоких технологий на космическое пространство.

Фокусирование на указанных отраслях международного права обусловлено также необходимостью «обеспечения интересов Российской Федерации в Мировом океане, космическом пространстве», в качестве стратегического национального приоритета России во внешнеполитической деятельности, определенного КВП 2023 г. (пункт 16, подпункт 10).

3.1. Международно-правовые основы использования информационно-коммуникационных технологий в морской сфере

Международное морское судоходство становится все более зависимым от ИКТ, которые как открывают новые возможности, так и новые уязвимости и угрозы, требующие более комплексного изучения, оперативного ответа и правового регулирования. Многие технологии, которые в настоящее время разрабатываются, оказывают положительное воздействие на океаны и деятельность в них. Например, опыт, накопленный в прокладке волоконно-оптических подводных кабелей; разработка морских дронов, пригодных для разминирования; спутники играют важную роль в борьбе с незаконным промыслом в удаленных исключительных экономических зонах. Что касается деструктивного воздействия, то атаки против ИКТ-систем морского сектора представляют собой дополнительную угрозу наряду с традиционными морскими угрозами[230]. На фоне цифровизации отрасли возникают многочисленные угрозы безопасности в сфере использования ИКТ в рамках международного морского судоходства, в том числе проникновение на судно и захват его управления теперь вполне возможны через взломы ИКТ-систем. Также увеличивается число случаев подделки сертификатов Глобальной навигационной спутниковой системы (GNSS)[231] и Автоматической

[230] Таких как пиратство, незаконная деятельность, морской терроризм, несчастные случаи на море и др.

[231] Global Navigation Satellite System (GNSS). ГМССБ призвана улучшить поисково-спасательные работы на море. Она основана на методах радиосвязи, позволяющих осуществлять двустороннюю связь между кораблем и сушей, независимо от положения судна, и в основном состоит из сети аварийной автоматической связи для судов в море. Она вступила в силу 1 февраля 1999 г. и применяется во всем мире ко всем судам, находящимся в море, и океанским грузовым судам с водоизмещением или более 300 тонн; эти суда должны быть оснащены радиоэлектронным оборудованием, отвечающим международным стандартам, установленным в рамках этой системы. Она требует установки на борту судов приемника Navtex, который позволяет получать информацию о безопасности на море, специальные метеорологические отчеты и все, что касается безопасности судоходства. Navtex – это система со средним портом, которая работает с помощью прямого телеграфа и использует фиксированную частоту 518 кГц.

системы идентификации (AIS)[232], а также проникновений в ИКТ-инфраструктуру и атаки против программного обеспечения[233] судоходных компаний и портов.

По оценкам ЮНКТАД, на отрасль морского судоходства приходится более 80% мировых перевозок, но только 33% из числа респондентов, участвовавших в опросе по информационной безопасности на море от 2020 г. среди членов Балтийский и Международный Морской Совет (БИМКО)[234], указали, что их организации используют решения для противодействия атакам против их ИКТ-систем. Учитывая значительные недостатки, которые были выявлены в безопасности ИКТ-систем, используемых для навигации в море, международные организации начали уделять данному вопросу существенное внимание. Так, ИМО выпустила в 2017 г. резолюцию, согласно которой судовладельцам до января 2021 г. необходимо включить планы управления информационными рисками в общие протоколы безопасности судов. Как справедливо отмечается в Обзоре морского транспорта ЮНКДАТ за 2021 г., главная задача, которая сегодня стоит перед международным морским судоходством – это обеспечение безопасного судоходства с соответствующей правовой базой[235], в том числе с учетом специфики ИКТ-систем и цифровизации отрасли. Действительно, в связи с подключением морской инфраструктуры к ИКТ-системам требуется соответствующее правовое регулирование и усиление мер, направленных на обеспечение безопасности международного морского судоходства в сфере использования ИКТ.

Основной угрозой международного судоходства в данном направлении выступают угрозы информационной безопасности[236], которая может быть определена, согласно исследователям из Ланкастерского университета, как безопасность в морской области, которая включает защиту критически важной информационной инфраструктуры сектора, защиту от кибератак и/или других непреднамеренных действий, которые могут вывести из строя, разрушить и/или

---

[232] Automatic Identification System (AIS).

[233] Кибератаки на морскую инфраструктуру включают также атаки вымогателей, примером которой является NotPetya 2017 г. на Maersk.

[234] The Baltic and International Maritime Council.

[235] Review of Maritime Transport 2021. UNCTAD/RMT/2021. – Geneva: United Nations, 2021. – P. 177.

[236] В секторе страхования судоходства термин, используемый для описания морской кибербезопасности судна, называется «кибер-мореходность» (cyber seaworthiness).

взять под контроль ее ИКТ-инфраструктуру[237]. Данные инфраструктуры в рамках международного морского судоходства классифицируют на следующие направления:

1) системы в общей среде (например, GNSS, AIS);

2) системы на борту судов (например, балластные системы, управление движением);

3) системы на берегу (например, системы мониторинга и обработки грузов и портовых операций).

Кроме того, ЮНКТАД выявила иные примеры кибератак и уязвимостей[238], включая массовые атаки против глобальной системы позиционирования, связь кибератак и пиратства[239]. В своей совокупности они подчеркивают важность обеспечения безопасности международного морского судоходства и управления новыми рисками, вызванными использованием ИКТ[240]. Рост количества инцидентов, связанных с безопасностью международного морского судоходства в сфере использования ИКТ, подтверждает необходимость правового регулирования исследуемой проблематики как на национальном, так и на международном уровне.

Перейдем к краткому анализу регулирования обеспечения безопасности ИКТ в морской деятельности. По предмету регулирования можно классифицировать международно-правовые основы обеспечения морской безопасности по двум направлениям – нормы, содержащие уголовные санкции и нормы, направленные на регулирование как таковое. Уголовно-правовой комплекс в основном определяет преступления в морском пространстве, а нормативно-регулирующий определяет

---

[237] Fitton O., Prince D., Germond B., Lacy M. The Future of Maritime Cyber Security [Электронный ресурс] // Lancaster University. – 2015. – URL: https://eprints.lancs.ac.uk/id/eprint/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf (дата обращения: 10.08.2024).

[238] Речь идет о навигационных и других системах на борту судов и в портах, включая вмешательство в автоматические системы идентификации и электронные системы отображения карт и информации, глушение глобальных систем позиционирования и манипулирование грузом и другими корабельными и портовыми системами, в том числе путем внедрения вредоносных программ, программ-вымогателей и вирусов. Источник: Review of Maritime Transport 2018 [Электронный ресурс]. – UNCTAD/RMT/2018. – New York; Geneva: United Nations, 2018. – P. 127. – URL: https://unctad.org/system/files/official-document/rmt2018_ru.pdf (дата обращения: 10.08.2024).

[239] Ducruet C. Maritime Networks: Spatial structures and time dynamics (Routledge Studies in Transport Analysis). – 1st Edition. – London, United Kingdom: Taylor & Francis Ltd, 2016. – P. 196.

[240] Boutet A., Chauvin C., Morel G., Tirilly G. Pêche et TIC. Marsouin [Электронный ресурс]. – URL: https://www.marsouin.org/IMG/pdf/Rapport_final___Peche_et_TIC.pdf (дата обращения: 10.08.2024).

меры, которые должны быть приняты для предотвращения инцидентов, связанных с безопасностью на море. Конвенции ООН по морскому праву 1982 г. (КМП) и Конвенции о борьбе с незаконными актами, направленными против безопасности морского судоходства 1988 г.[241] относятся к первой группе норм, а СОЛАС[242] и Международный кодекс по охране судов и портовых средств[243] – ко второй[244].

Помимо этого, различные аспекты обеспечения безопасности ИКТ в морской деятельности регулируются на международном уровне следующим образом:

1) «юрисдикционными» нормами;
2) техническими правилами;
3) нормами частного права[245].

В международной правовой доктрине существует следующая классификация требований к обеспечению безопасности международного морского судоходства: технические требования, связанные с проектированием, конструкцией и оборудованием; навигационные требования, связанные с организацией плавания судна; квалификационные и медицинские требования, связанные с экипажем судна; требования к системе управления безопасностью; требования, связанные с угрозами пиратства и терроризма[246]. Однако важно отметить, что с учетом

[241] Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства (Рим, 10 марта 1988 г.) [Текст] // Собрание законодательства Российской Федерации. – 26.11.2001. – № 48, ст. 4469.
[242] International Convention for the Safety of Life at Sea. Concluded at London, 1 November 1974 // United Nations Treaty Series. Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. – Vol. 1184, I-18961. – New York, 1987. – P. 458.
[243] ISPS-Code International code for the security of ships and of port facilities (MSC.196(80)) [Электронный ресурс]. – 12 December 2002. – URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC.196(80).pdf (дата обращения: 10.08.2024).
[244] Mejia M. Criminal and Regulatory law in the international legal framework for maritime security. Law and ergonomics in maritime security. Published doctoral thesis. – Lund: Department of Design Sciences, Lund University, 2007.
[245] Согласно ЮНКДАТ, «юрисдикционные» нормы определяют права и обязанности государств в отношении судов в различных морских районах, включая принципы и правила, касающиеся юрисдикции флага, порта и прибрежных государств, которые в основном охватываются принятой в результате работы Третьей Конференции ООН по морскому праву Конвенцией ООН по морскому праву 1982 г. Технические правила касаются, в частности, охраны, безопасности и окружающей среды, вопросов профессиональной подготовки и стандартов несения вахты, которые налагают на государства флага обязательства по принятию национального законодательства, отражающего согласованные на международном уровне стандарты, разработанные и принятые ИМО. Нормы частного права могут охватывать ответственность, в том числе за телесные повреждения, загрязнение окружающей среды, потери груза и столкновения судов, которые в некоторых случаях подпадают под действие соответствующих международно-правовых документов, но могут также подпадать и под действие национального законодательства.
[246] Kapilidis C. Cybersecurity challenges for the maritime industry, 30 July 2019 [Электронный ресурс]. – URL: https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/ (дата обращения: 10.08.2024); Al Ali N.A.R., Chebotareva A.A., Chebotarev V.E. Cyber security in marine transport: opportunities and legal challenges [Электронный ресурс] // Scientific Journal of Maritime Research. – 2021. – Vol. 35. – P. 248–255. – URL: https://hrcak.srce.hr/file/387886 (дата обращения: 10.08.2024).

исторического контекста выработки и принятие упомянутых источников, роль ИКТ в обеспечении безопасности международного морского судоходства в сфере использования ИКТ в них недостаточно отражена, что обуславливает необходимость принятия изменений к действующей правовой базе международного морского права с учетом особенностей ИКТ и их внедрения в международное морское судоходство.

На международном уровне в рамках ИМО Комитетом по безопасности на море (КМБ) было разработано несколько документов, которые регулируют обеспечение безопасности в сфере использования ИКТ, включая отдельные рекомендации по управлению киберрисками в морской отрасли и кибербезопасности на судах. Значительной в данном контексте является 96-я сессия КМБ с 11 по 20 мая 2016 г., по итогу которой были приняты предварительные руководящие принципы кибербезопасности (MSC.1/Circa.1526)[247]. Кроме того, в июне 2017 г. состоялось принятие резолюции MSC.428(98)[248] об управлении рисками в области обеспечения информационной безопасности (киберрисками) на море в системах управления безопасностью[249], в рамках которой ИМО поощряет судоходные компании учитывать управление киберрисками в соответствии с руководящими принципами, обнародованными ИМО, и включать предпринятые компаниями инициативы в общие системы управления безопасностью судов. Данная резолюция в настоящее время является единственным официальным документом на международном уровне, требующим от государств-членов ИМО обеспечения учета киберрисков в системах управления безопасностью судов.

---

[247] Interim guidelines on guidelines on maritime cyber risk management [Электронный ресурс] (MSC.1/Circ.1526). – 2016, June. – URL: https://www.imorules.com/MSCCIRC_1526.html (дата обращения: 10.08.2024).

[248] Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems [Электронный ресурс]. – 2017, 16 June. – URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (дата обращения: 10.08.2024).

[249] Согласно резолюции, утвержденная система управления безопасностью полетов должна учитывать управление кибер-рисками в соответствии с целями и функциональными требованиями Международного кодекса управления безопасностью полетов. Резолюция призывает государства флага обеспечить, чтобы киберриски надлежащим образом учитывались в системах управления безопасностью полетов не позднее первой ежегодной проверки документа компании о соответствии требованиям после 1 января 2021 г.

В следующем месяце, 5 июля 2017 г., были также опубликованы Руководящие принципы MSC-FAL.1/Circ.3 по управлению киберрисками на море. В документе представлены общие элементы и принципы, которые каждая судоходная компания может включить в свою практику. Данные руководящие принципы вводят несколько функциональных элементов для судоходных компаний в борьбе с киберугрозами: идентификация, защита, обнаружение, реагирование и восстановление. Упомянутые в руководстве факторы уязвимости могут быть объектом злонамеренных действий, таких как взлом или внедрение вредоносных программ. Данная формулировка является важной для определения на международном уровне рисков, связанных с кибератаками. До сих пор это первая попытка ИМО четко сформулировать такие риски.

Кроме того, в Стратегическом плане ИМО на шестилетний период (2018-2023 гг.)[250] признается необходимость интеграции ИКТ в нормативную базу международного морского судоходства[251]. Также в актуальном Стратегическом плане на 2024-2029 гг., принятом на 33-й сессии ИМО (27 ноября – 6 ноября 2023 г.), среди восьми стратегических направлений числится «интеграция новых, формирующихся и прогрессивных технологий в нормативно-правовую базу»[252]. Так, в документе отмечается, стремление к выработке актуального нормативного фундамента, который учитывал бы особенности ИКТ[253]. На основе этого можно сделать вывод о существующей тенденции: международное морское судоходство принимает упреждающий подход к включению управления информационным пространством в свою культуру безопасности, в том числе, чтобы предотвратить возникновение каких-либо серьезных инцидентов в ИКТ-среде.

---

[250] International Maritime Organization Strategic Plan for the six-year period 2018 to 2023 [Электронный ресурс]. – Resolution A.1110(30). Adopted on 6 December 2017. – URL: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.1110(30).pdf (дата обращения: 10.08.2024).

[251] Review of Maritime Transport 2018. – UNCTAD. UNCTAD/RMT/2018. Op. cit.

[252] IMO 33rd Assembly adopted resolutions, including on budget, strategic plan and appointment of Secretary-General [Электронный ресурс]. – URL: https://www.imo.org/en/MediaCentre/PressBriefings/pages/IMO-Assembly-adopts-budget,-strategic-plan.aspx (дата обращения: 10.08.2024).

[253] International Maritime Organization Strategic plan for the Organization for the six-year period 2024 to 2029 [Электронный ресурс]. Resolution A 33/Res.1173. Adopted on 6 December 2023. Assembly, 33rd session, Agenda item 8(a). – URL: https://wwwcdn.imo.org/localresources/en/About/strategy/Documents/A%2033-Res.1173.pdf (дата обращения: 10.08.2024).

ИСО также рассмотрела этот вопрос и опубликовала ряд стандартов, касающихся кибербезопасности. ИСО/МЭК 27001 (ISO/IEC 27000)[254] является частью системы стандартов, и они предназначены для того, чтобы помочь организациям управлять безопасностью активов, таких как финансовая информация, интеллектуальная собственность, сведения о сотрудниках или информация, доверенная третьими лицами. ISO/IEC 27001 устанавливает требования к системе управления информационной безопасностью.

Данный факт говорит о необходимости пересмотра роли норм «мягкого права» с целью обеспечения безопасности международного морского судоходства в сфере использования ИКТ, обязав государства выполнять определенные положения вместо того, чтобы оставлять их в качестве руководства. Альтернативный вариант – это передавать наиболее важные из них на рассмотрение международных органов, которые обязуют государства выполнять их в обязательном порядке, например, Совета Безопасности ООН.

КБМ ИМО в ходе своей 100-й сессии в декабре 2018 г. продолжил исследования, направленные на оценку потенциального применения инструментов ИМО к судам с различными степенями автономии (корабль с автоматизированными процессами и поддержкой принятия решений; дистанционно управляемый корабль с моряками на борту; дистанционно управляемый корабль без экипажа на борту; полностью автономный корабль). Комитет утвердил рамочную основу для проведения учений по регулированию использования морских автономных надводных кораблей.

Кроме того, КМБ ИМО в ходе 100-й и 101-й сессий отметил необходимость разработки руководящих принципов проведения испытаний автономных судов. Юридический комитет ИМО на своей 106-й сессии в марте 2019 г. начал работу по регулированию сферы применения международно-правовых документов, находящихся в его ведении. Целью было проведение оценки степени, в которой

[254] ISO/IEC 27001 Системы обеспечения информационной безопасности [Электронный ресурс]. – URL: https://www.iso.org/ru/standard/27001 (дата обращения: 10.08.2024).

существующая нормативная база может нуждаться в корректировке для решения вопросов, связанных с эксплуатацией автономных надводных кораблей[255].

В рамках института ответственности роль удаленного оператора при автономном судоходстве также должна быть рассмотрена Юридическим комитетом на определенном этапе[256]. Кроме того, ИМО приняла решение проводить исследования с целью определения того, в какой степени нормативная база международного морского судоходства должна быть изменена для интеграции новых ИКТ в целом.

Еще одной важной составляющей международной безопасности в контексте применения ИКТ, связанной с морской отраслью, является безопасность физической инфраструктуры, лежащей в основе ИКТ-среды, а именно безопасность подводной волоконно-оптической сети. Глобальная подводная сеть совместно со спутниковой является одним из физических фундаментов функционирования Интернета, а по мере развития и повсеместного внедрения ИКТ применение подводных волоконно-оптических кабелей продолжает набирать обороты. Несмотря на их статус критически важной инфраструктуры связи, подводные кабельные системы остаются уязвимыми для множества возникающих проблем обеспечения безопасности в сфере использования ИКТ[257]. Они подразумевают под собой, например, такие угрозы, как преднамеренное

---

[255] К числу международно-правовых документов, находящихся в ведении Юридического комитета ИМО, подлежащих рассмотрению, относятся следующие: Международная конвенция о гражданской ответственности за ущерб от загрязнения нефтью 2001 г., Международная Конвенция о гражданской ответственности за ущерб от загрязнения нефтью 1969 г., Конвенция о борьбе с незаконными актами, направленными на обеспечение безопасности морского судоходства 1988 г., Протокол 1988 г. о борьбе с незаконными актами, направленными против безопасности стационарных платформ, расположенных на континентальном шельфе, Протокол 2005 г. к Конвенции о пресечении незаконных актов, направленных против безопасности морского судоходства, Международная Конвенция о спасании 1989 г., Найробийская Международная конвенция об удалении затонувших судов 2007 г., Протокол 2010 г. к Международной конвенции об ответственности и компенсации за ущерб, связанный с морской перевозкой опасных и ядовитых веществ 1996 г.

[256] Эксплуатация автономных судов тесно связана с ролями капитана и экипажа на борту, что влияет на весь спектр применимых морских законов и правил. Нормативные рамки, регулирующие морскую отрасль, должны были адаптироваться на протяжении многих лет, чтобы приспособиться к новым технологиям, но они не учитывают эксплуатацию судов без экипажа. Поэтому традиционные роли капитана и экипажа на борту, а также ИИ и берегового персонала, контролирующего дистанционно управляемые или автономные суда, будут пересмотрены ИМО. Источник: Review of Maritime Transport 2019 [Электронный ресурс]. – UNCTAD/RMT/2019/Corr.1. – Geneva: United Nations, 2020. – P. 132. – URL: https://unctad.org/system/files/official-document/rmt2019_en.pdf (дата обращения: 10.08.2024).

[257] Davenport T. Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis [Электронный ресурс] // Catholic University Journal of Law and Technology. – 2015. – Vol. 24, Issue 1, Article 4. – URL: https://scholarship.law.edu/jlt/vol24/iss1/4/ (дата обращения: 10.08.2024).

повреждение подводных кабелей, проложенных на морском дне, кабельных посадочных станций, а также атаки на виртуальные части подводных кабельных систем при взломах систем управления[258], использование подводных кабелей в качестве инструментов для шпионажа и сбора разведданных.

Подводные кабели с самого начала их эксплуатации были признаны общественным благом, которое следует защищать и регулировать в рамках международного права – только с 1863 по 1913 гг. защита подводных кабелей фигурировала в повестке дня семи международных конференций[259]. Кроме того, в принятой 7 декабря 2010 г. Генеральной Ассамблеи ООН резолюции 65/37 «Мировой океан и морское право» признается роль подводных кабелей связи как критически важной инфраструктуры связи как на глобальном, так и национальном уровне[260].

Подводные кабели для военных, энергетических и научных целей имеют различное применение и различаются по конструкции и строительству, однако согласно международному праву, они пользуются регулируются теми же нормами международного права, что и кабели для телекоммуникаций[261]. Наряду с этим, эксплуатация и защита кабелей упорядочена нормами международного права в связи с влиянием данной подводной инфраструктуры на международную безопасность, в том числе и обеспечение безопасности в сфере использования ИКТ.

Что касается их международного-правового регулирования, то со второй половины XIX в. по вторую половину XX в. международное сообщество приняло несколько документов, предметом которых стали подводные кабели и которые

---

[258] Burnett D. R. Submarine Cable Security and International Law [Электронный ресурс] // International Law Studies, Stockton Center for International Law. – 2021. – Vol. 97. – URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2992&context=ils/ (дата обращения: 10.08.2024).

[259] United Nations Documents on the Development and Codification of International Law // Supplement to American Journal of International Law. – 1947. – Vol. 41, No. 4. – P. 127.

[260] Они передают большую часть мировых данных и средств связи и, следовательно, жизненно важны для глобальной экономики и национальной безопасности всех государств. Источник: United Nations General Assembly Resolution 65/37. Oceans and the law of the sea [Электронный ресурс]. Adopted by the General Assembly on 7 December 2010, A/RES/65/37. Resolutions and Decisions adopted by the General Assembly during its 65th session. – Volume I, 14 September – 24 December 2010. – General Assembly Official Records, 65th session, Supplement No. 49 (A/65/49 Vol. I). – New York: United Nations, 2010. – P. 53–76. – URL: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_65_37.pdf (дата обращения: 10.08.2024).

[261] Davenport T. Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. Op. cit.

определяют права и обязанности государств в их отношении: Конвенция о защите подводных телеграфных кабелей 1884 г.[262], Женевские конвенции об открытом море и о континентальном шельфе 1958 г., Конвенция о Международных правилах предупреждения столкновений судов в море от 1972 г., и, наконец, КМП 1982 г.[263] Таким образом, основу международно-правового регулирования кабелей составляют положения вышеупомянутых международных договоров и обычное международное право.

Международная конвенция по охранению подводных телеграфных кабелей от 14 марта 1884 г.[264] представляет собой один из первых в мире международных договоров по морскому праву. Она стала результатом переговоров, проходивших в Париже в 1882 и 1884 гг., и представляет собой основу современного международного права в отношении подводных кабелей, как это отражено в КМП 1982 г. и Конвенции о Международных правилах предупреждения столкновений судов в море 1972 г.

Международно-правовые нормы предусматривают ряд способов предотвращения потенциальных сбоев в работе подводных кабелей. Во-первых, в соответствии со статьей 1 Международной конвенции по охранению подводных телеграфных кабелей от 1884 г. и статьями 87 и 112 КМП 1982 г. все государства и их граждане пользуются свободой прокладывать и ремонтировать кабели за пределами территориального моря, а именно по дну открытого моря за пределами континентального шельфа. Во-вторых, статьи 2, 8-12 Международной конвенции по охранению подводных телеграфных кабелей 1884 г. и статья 113 КМП 1982 г. гласят, что суда, повредившие подводный кабель из-за преднамеренных действий или преступной халатности, подлежат уголовному наказанию в виде штрафов и тюремного заключения без ущерба для права владельца кабеля на возмещение гражданского ущерба. Данный контекст касается как преднамеренных, так

[262] Основная цель конвенции состояла в том, чтобы потребовать принятия государством законодательства, защищающего кабели, проложенные за пределами территориальных вод.
[263] Регулирует права и обязанности государств как в отношении защиты подводных кабелей, так и свободы прокладки, ремонта и обслуживания таких кабелей.
[264] Международная конвенция по охранению подводных телеграфных кабелей (Париж, 14 марта 1884 г.), с Декларацией (Париж, 1 декабря 1886 г.) и Заключительным Протоколом (Париж, 7 июля 1887 г.) [Текст] // Собрание законов СССР. – 1926. – Отд. II, № 31. – Ст. 190.

небрежных действий за исключением случаев разрывов или повреждений подводных кабелей «с целью спасения своей жизни или своих судов, после принятия всех мер предосторожности для избежания таких разрывов или повреждений»[265]. Иными словами, согласно положениям конвенций, существует освобождение от уголовных и гражданских исков, если капитан повредил трос с целью спасения судна и его пассажиров. В-третьих, исходя из статьи 7 Международной конвенции по охранению подводных телеграфных кабелей от 1884 г. и статьи 115 КМП 1982 г., если судно не по своей вине зацепляет кабель своим рыболовным снаряжением или якорем, судно должно пожертвовать своим снаряжением или якорем, чтобы избежать повреждения кабеля, впоследствии владелец кабеля обязан возместить владельцу судну ущерб за это. Значение данного положения сводится к предотвращению большего вреда от нарушения связи в результате повреждения кабеля[266]. В-четвертых, согласно ст. 4 Международной конвенции по охранению подводных телеграфных кабелей 1884 г. и ст. 114 КМП 1982 г. на государства накладывается обязательство выработать и принять национальное законодательство, которое будет предусматривать ответственность «находящихся под его юрисдикцией лиц, которым принадлежит подводный кабель или трубопровод в открытом море»[267], в случае, если они «причиняют при прокладке или ремонте этого кабеля или трубопровода разрыв или повреждение другого кабеля или трубопровода»[268], в частности в виде финансовых издержек по починке. В-пятых, на основе статей 5 и 6 Международной конвенции по охранению подводных телеграфных кабелей 1884 г. и правилам 18 и 27 Конвенции о Международных правилах предупреждения столкновений судов в море 1972 г., если на судне отображаются сигналы, указывающие на то, что оно занято укладкой или ремонтом подводного кабеля, другие суда должны либо удалиться, либо находиться на расстоянии одной морской мили от судна и в четверти мили от любого бакена, установленного для ремонта кабеля, и должно

[265] Конвенция Организации Объединенных Наций по морскому праву от 10 декабря 1982 г. [Электронный ресурс]. – URL: www.un.org/depts/los/convention_agreements/texts/unclos/unclos_r.pdf (дата обращения: 10.08.2024).
[266] Burnett D. R. Submarine Cable Security and International Law. Op. cit.
[267] Конвенция Организации Объединенных Наций по морскому праву от 10 декабря 1982 г. Указ. соч.
[268] Там же.

избегать действий, которые мешают укладке или ремонту кабеля. С целью предотвращения чрезмерного и неуместного вмешательства в свободу судоходства право подниматься на борт судов в районах за пределами территориального моря строго регулируется КМП 1982 г. и допускается только в определенных случаях. Что касается статьи 10 Международной конвенции по охранению подводных телеграфных кабелей 1884 г., то она допускает, что экипаж военного судна может подняться на борт невоенного судна, подозреваемого в преднамеренном повреждении подводного кабеля, для требования предъявить официальные документы, удостоверяющие национальность этого судна, и составления протокола[269].

Некоторые ученые, среди которых известный юрист-международник Р. Ч. Бекман, утверждают, что преднамеренное повреждение кабелей может подпадать под определение пиратства в соответствии со ст.101 КМП 1982 г. В этом смысле преднамеренное повреждение кабеля стало бы подпадать под универсальную юрисдикцию и дало бы военным кораблям право высаживаться на борт и арестовывать подозреваемое судно. Однако действие КМП 1982 г. распространяется только на ту часть кабеля, которая проложена по морскому дну, а не к местам прокладки кабелей. В данном контексте важно отметить, что МСЭ издал некоторые правила и стандарты, которые могут применяться к кибератакам, использующим электромагнитный спектр или международные телекоммуникационные сети, но ни одно из них напрямую не подразумевает защиту кабельных систем от преднамеренного повреждения[270].

В резолюции Генеральной Ассамблеи ООН 65/37 А «Мировой океан и морское право», принятой 7 декабря 2010 г., отмечается подтверждение того факта, «что кабели подвержены непреднамеренному и случайному повреждению в результате судоходства и других видов деятельности, а также подчеркивается необходимость принятия государствами национальных законов и нормативных

[269] Международная конвенция по охранению подводных телеграфных кабелей (Париж, 14 марта 1884 г.), с Декларацией (Париж, 1 декабря 1886 г.) и Заключительным Протоколом (Париж, 7 июля 1887 г.) [Текст] // Собр. Зак. СССР. – 1926. – Отд. II, № 31, ст. 190.
[270] Davenport T. Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. Op. cit.

актов для защиты подводных кабелей и предотвращения их умышленного повреждения или повреждения в результате преступной халатности, наказуемых преступлений» [271]. В связи с этим ООН призвала государства принять меры для защиты волоконно-оптических подводных кабелей и в полной мере решить проблемы, связанные с этими кабелями, в соответствии с нормами международного права, как это отражено в КМП 1982 г., а также выступила «за расширение диалога и сотрудничества между государствами и соответствующими международными организациями в целях повышения безопасности такой критически важной инфраструктуры связи»[272], отметив внимание, уделяемое этому вопросу в Окинавской декларации VII Совещания министров Азиатско-Тихоокеанского экономического сотрудничества по телекоммуникациям и информационной индустрии, состоявшегося на Окинаве, Япония, 30 и 31 октября 2010 г.[273]

Данные предложения также можно рассмотреть с точки зрения необходимости доработки действующей системы международного права из-за наличия некоторых правовых пробелов. Так, отсутствуют нормы, регулирующие защиту подводных кабелей от преднамеренных действий, совершаемых за пределами территориальных морей, например, от террористических атак: Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства 1988 г.[274] и Конвенция о борьбе с незаконными актами, направленными против безопасности гражданской авиации 1971 г.[275] охватывают воздушные суда, морские суда, морские платформы и навигационные средства, однако не содержат норм, регулирующих кабели, что обуславливает необходимость принятие поправок к Международной конвенции по охранению

[271] United Nations General Assembly 65/37. Oceans and the law of the sea. – A/RES/65/37, adopted by the General Assembly on 7 December 2010. Op. cit.
[272] Resolutions adopted by the General Assembly at its 65th session [Электронный ресурс]. – URL: https://research.un.org/en/docs/ga/quick/regular/65 (дата обращения: 10.08.2024).
[273] United Nations General Assembly 65/37. Oceans and the law of the sea. – A/RES/65/37, adopted by the General Assembly on 7 December 2010. Op. cit.
[274] Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства (Рим, 10 марта 1988 г.). Указ. соч.
[275] Конвенция о борьбе с незаконными актами, направленными против безопасности гражданской авиации (Монреаль, 23 сентября 1971 г.) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. 29. – М., 1975. – С. 90–95.

подводных телеграфных кабелей 1884 г. и КМП 1982 г. Однако, учитывая разногласия государств в целях обеспечения международной безопасности в контексте применения ИКТ, реализация данной идеи в ближайшей перспективе представляется маловероятной.

Кроме того, в рамках международного гуманитарного права кабельные суда пользуются защитой в мирное время от навигационных помех при прокладке и ремонте кабелей. В военное время для кабельных судов могут быть разработаны дополнительные методы защиты, подобные тем, которые применяются к госпитальным суднам[276] в соответствии с положениями Женевской конвенции об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море 1949 г.[277]

Также встает вопрос о применимости международного морского права для обеспечения информационной безопасности подводных кабелей, в частности в случае кибератак. Отдельные нормы могут быть использованы, однако они носят фрагментарный характер и не могут решать системные проблемы обеспечения безопасности в области применения информтехнологий, возникающие в результате кибератак[278].

В связи с большими рисками, исходящими от противоправного использования ИКТ, видится целесообразным дать короткую характеристику институту страхования. ИКТ-системы, на базе которых в настоящее время функционирует международное морское судоходство, были разработаны для удовлетворения потребностей XX в., но они не оснащены для предотвращения угроз XXI в. и борьбы с ними. Морское страхование, которое охватывает суда, верфи и грузовые погрузочно-разгрузочные сооружения, за последние годы реализуется с учетом клаузулы об исключении рисков, связанных с компьютерной преступностью (CL 380) 10/11/2003 Института лондонский страховщиков, чьи

[276] Burnett D. R. Submarine Cable Security and International Law. Op. cit.
[277] II Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea (Geneva, 1949, August 12). – Geneva International Committee of the Red Cross, 1960. – 327 p.
[278] Hathaway O., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J. The Law of Cyber-Attack [Электронный ресурс] // California Law Review. – 2011. – URL: https://openyls.law.yale.edu/handle/20.500.13051/3283 (дата обращения: 10.08.2024).

оговорки в практике страхования международных грузоперевозок считаются основными условиями договора морского страхования. CL 380 – это «первостепенная оговорка» о кибератаках. Страхование не покрывает ущерб или расходы, прямо или косвенно вызванные использованием или эксплуатацией в качестве средства для причинения вреда любого компьютера, компьютерной системы, компьютерной программы, вредоносного кода, компьютерного вируса или процесса или любой другой электронной системы[279]. Пункт 1.2 устанавливает, что эта клаузула одобрена в отношении политики, охватывающей риски международной войны, гражданской войны, революции, мятежа, восстания или гражданских беспорядков, возникших в результате этого, или любого враждебного акта со стороны воюющей державы или против нее, или терроризма, или любого лица, действующего по политическим мотивам. То есть в перечисленных условия пункт 1.1. не распространяется на потери (которые в противном случае были бы покрыты), возникающие в результате использования любого компьютера, компьютерной системы или компьютерной программы или любой другой электронной системы в системе запуска и/или наведения и/или механизме наведения любого оружия или ракеты. Хотя в отрасли нет предложений о том, что эта оговорка будет снята в ближайшее время, небольшое число крупных страховщиков готовы рассмотреть возможность предоставления значительных возможностей для покрытия рисков, которые были исключены с 2003 г.[280]

Проведя анализ международно-правовой основы, регулирующей обеспечение безопасности в сфере использования ИКТ в рамках морской деятельности государств, можно сделать вывод, что определенно существуют механизмы, направленные на формирование международно-правовой регламентации, однако они не представляют собой единый комплекс мер, способный обеспечить безопасность ИКТ-систем морской отрасли. До сих пор не

[279] Institute Cyber Attack Exclusion Clause [Электронный ресурс]. – Cl.380. (2003). – URL: https://www.modernaforsakringar.se/siteassets/documents/foretag--industri/villkorsbanken/foretagsforsakring/allmanna-villkor/transport/institute-cyber-attack-exclusion-clause---cl-380-vst-24-1-.pdf (дата обращения: 10.08.2024).

[280] The risk of cyber-attack to the maritime sector [Электронный ресурс] // MARSH. – Global Marine Practice. – 2014, July. – URL: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/The%20Risk%20of%20Cyber-Attack%20to%20the%20Maritime%20Sector-07-2014.pdf (дата обращения: 10.08.2024).

существует надлежащего международно-правового акта[281], предметом которого является регулирование обеспечения безопасности в сфере использования ИКТ в рамках международного морского судоходства из-за отсутствия универсального подхода в рамках международного сотрудничества в этой области. Последнее, в свою очередь, должно строиться на основе «мультискейкхолдерного» подхода, который наиболее эффективен для отношений, в которые вовлечены главным образом не только государственные субъекты, но также представители частного сектора, для комплексного решения возникающих правовых вопросов (при этом принятие решений должно оставаться за государствами как первичными субъектами международного права).

Автор убежден, что международному сообществу необходимо включить данный вопрос в повестку специальных органов ООН, которые занимаются ИКТ-проблематикой, с конечной целью разработать и принять отраслевой международно-правовой акт, способный упорядочить безопасность в сфере использования морских ИКТ, с учетом их важности для мировой экономики, а также безопасности. Данный документ должен стать основополагающим источник международного морского права в части защиты ИКТ-инфраструктуры морской отрасли, что ставит долгосрочную задачу перед мировым сообществом, так как защита ИКТ-инфраструктуры морской отрасли включает в себя виртуальные, наземные, морские и даже космические элементы. Он сможет обеспечить эффективное регулирование вопросов обеспечения информационной безопасности международного морского судоходства и борьбы против угроз, стоящих перед ней. Организационно-правовая реализация может быть осуществлена, во-первых, посредством создания новой международной специализированной межправительственной организации в рамках системы ООН, которая будет отвечать за обеспечение безопасности ИКТ-систем морской отрасли. Во-вторых, возможно рассмотрение МСЭ, однако необходимо пересмотреть его мандат с

[281] Ogundare B., Akinwande G. International Maritime Organisation Framework on Cyber Risk Management a Case for a Comprehensive Legal Framework [Электронный ресурс] // Maritime Safety and Security Law Journal. – URL: https://www.marsafelawjournal.org/wp-content/uploads/2021/12/MarSafeLaw-Journal_Issue-9_2021-1.pdf (дата обращения: 10.08.2024).

обязательным включением вопросов, которые составляют правовой вакуум в международном морском праве, как регулирование подводных кабелей и др. В-третьих, это может быть реализовано благодаря расширению роли ИМО в вопросах морской ИКТ-безопасности путем разработки и принятия необходимых мер, стандартов, правил и руководящих принципов для борьбы с угрозами, которые могут быть сформулированы и реализованы с целью защиты уязвимых систем судов и различных типов информационных технологий, используемых в портах, морских сооружениях, судах и других элементах морской инфраструктуры[282].

Государства не должны намеренно наносить ущерб критически важной инфраструктуре друг друга с помощью ИКТ, в том числе в морской отрасли. Например, с учетом того, что международное гуманитарное право не регулирует нападение на подводные кабели, однако так как они являются критически важной инфраструктурой, которая является составляющей не только национальной, но и международной безопасности, то должен быть принят запрет на применение силы даже в случае обороны.

Международно-правовой акт должен предусматривать необходимость привлечения ответственности за совершение нападения и нанесения ущерба ИКТ-инфраструктуры морской отрасли и регулирования данных правонарушений национальным законодательством. В нем должен быть определен ряд правонарушений, которые будут включать умышленное повреждение морской ИКТ-инфраструктуры, включая любые преступление, связанные с использованием вредоносных ИКТ для получения контроля над системами управления морской ИКТ-инфраструктуры. Вопрос квалификации действий, направленных против объектов морской отрасли, как тяжкого уголовно наказуемого деяния в национальном уголовном законодательстве также весьма актуален[283]. Необходимость выработки международно-правовых норм, направленных на предотвращения правонарушений в сфере использования ИКТ в рамках международного морского судоходства не вызывает сомнения. В данном контексте

[282] Al Ali N. A. R., Chebotareva A. A., Chebotarev V. E. Cyber security in marine transport: opportunities and legal challenges. Op. cit.
[283] Ibid.

важно отметить, что в правовой доктрине также высказывались идеи о создании Международного морского трибунала, в чьей юрисдикции, помимо иных вопросов, могли бы числиться и преступления против информационной безопасности международного морского судоходства.

Иной вариант решения данного вопроса может быть найден в российской инициативе о необходимости принятия международной конвенции по противодействию использованию ИКТ в преступных целях[284], на основе которой возможна выработка универсальной международно-правовой базы сотрудничества по борьбе с преступностью в сфере использования ИКТ с учетом особенностей и международного морского судоходства.

Наряду с этим стоит подчеркнуть, что международно-правовой акт должен быть направлен на международное сотрудничество и гармонизацию правовых систем и их законодательств посредством создания специального научного комитета, который будет изучать соответствующие вопросы и будет способствовать оказанию правовой помощи государствам-подписантам.

Повсеместное внедрение ИКТ-систем, в том числе в международное морское судоходство, и неопределенность в отношении полного спектра их потенциальной уязвимости[285], выдвигает новую неотложную задачу перед международным сообществом: поддержание безопасности ИКТ-систем морской отрасли[286]. По мере технического прогресса должна происходить адаптация международно-правового регулирования как на национальном, так и на международном уровнях. Исходя из анализа норм, регулирующих использование ИКТ в международном морском праве, можно сделать вывод, что международному сообществу необходимо выработать нормы, которые будут регулировать обеспечением безопасности в сфере использования ИКТ для морской отрасли. Наиболее эффективным видится разработка международно-правовых норм, регулирующих данные угрозы на

[284] Российский проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях [Электронный ресурс]. – 2021, 29 июля. – URL: www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 10.08.2024).

[285] Review of Maritime Transport 2019. UNCTAD. Op. cit.

[286] Karlsson J. The future of maritime cybersecurity. Secure State Cyber [Электронный ресурс]. – URL: https://www.securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/ (дата обращения: 10.08.2024).

трехэтапной основе: во-первых, на двустороннем уровне посредством заключения договоров между отдельными государствами; во-вторых, на региональном уровне[287]; в-третьих, дальнейшее рассмотрение наиболее передового опыта регулирования рассматриваемой проблематики на глобальном уровне.

3.2. Международно-правовые основы использования информационно-коммуникационных технологий в космической деятельности

В настоящее время выгоды от использования космических ресурсов имеют важнейшее значение для нашей повседневной жизни[288]. Космическая эра знаменовала свое начало с запуска Советским Союзом Социалистических Республик первого в мире искусственного спутника «Спутник» 4 октября 1957 г. Важной вехой в истории становления международного космического права стало 14 ноября 1957 г., день принятия Генеральной Ассамблеей ООН резолюции 1149(XII)289 в ходе своей 12-ой сессии, что стало отправной точкой формирования новой на тот момент отрасли международного права – международного космического права. Позднее искусственные спутники стали использоваться как средства обеспечивающее телекоммуникации: пассивный спутник Echo 1 был запущен в 1960 г. США, далее последовал в 1962 г. запуск Telstar 1 (совместный проект Франции, Великобритании и США), первый спутник связи[290]. Далее благодаря научным исследованиям была реализована идея геостационарного спутника связи, впервые предложенная писателем А. К. Кларком в 1945 г., в 1964 г., после экспериментов с геосинхронными спутниками, был запущен первый

[287] В рамках которого, например, страны, расположенные вдоль побережья, могут выступить с подобной инициативой, например, в ходе встречи министров обороны стран АСЕАН в 2021 г. по данной проблематике было утверждено создание Центра передового опыта в области кибербезопасности и информации, базирующегося в Сингапуре.

[288] Transparency and Confidence-Building Measures in Outer Space Activities to Enhance Stability in Outer Space. – Report A/68/189 of the Group of Governmental Experts, 29 July 2013. – New York: United Nations, 2013. – P. 106.

[289] United Nations General Assembly Resolution 1149(XII), Collective action to inform and enlighten the peoples of the world as to the dangers of the armaments race, and particularly as to the destructive effects of modern weapons. – A/RES/1149(XII). – 14 November 1957. – Resolutions adopted by the General Assembly during its 12th session, 17 September-14 December 1957 // General Assembly Official Records, 12th Session. – Supplement No. 18 (A/3805). – New York: United Nations, 1958. – P. 4.

[290] De Gouyon Matignon L. The International Telecommunication Union [Электронный ресурс]. – 2019, 21 February. – URL: www.spacelegalissues.com/space-law-the-international-telecommunication-union/ (дата обращения: 10.08.2024).

геостационарный спутник[291]. В связи с тем, что радиочастотный спектр и геостационарная орбита вокруг Земли считаются иссекаемым природным ресурсом, встал вопрос о необходимости регулирования их использования и распределения. Так, в 1963 г. МСЭ провел Чрезвычайную Административную конференцию по космической связи, на которой были распределены частоты между различными службами[292], а в 1992 г. МСЭ впервые выделил спектр для удовлетворения потребностей Глобальной мобильной персональной спутниковой связи[293]. Постоянно растущее число развертываемых спутников и увеличение их роли в жизни человечества сделало вопрос безопасности ИКТ-инфраструктуры космического пространства одним из актуальных: стало необходимо защищать как сами устройства, так и все этапы передачи данных через них. Считается, что «слабое шифрование и старое ИКТ-оборудование являются одними из ключевых уязвимостей спутниковых сетей, которые являются главной целью для использования» злоумышленниками против безопасности в сфере использования ИКТ в космическом пространстве[294].

Выделяют три ключевых точки доступа для потенциальной атаки против космической инфраструктуры[295]:

1) уязвимости в физическом наземном сегменте;

2) уязвимости в космическом сегменте[296];

3) уязвимости каналов передачи данных и цепочка поставок космической инфраструктуры.

---

[291] De Gouyon Matignon L. The International Telecommunication Union [Электронный ресурс]. – 2019, 21 February. – URL: www.spacelegalissues.com/space-law-the-international-telecommunication-union/ (дата обращения: 10.08.2024).

[292] Помимо соединения систем вещания и проводной телефонной связи и предоставления навигационных услуг, спутники также используются в мобильной связи. Спутниковые телефоны, например, могут быть жизненно важны в чрезвычайных ситуациях или в районах, где нет доступа к альтернативным сетям.

[293] Global Mobile Personal Communications, GMPC.

[294] Stremlau T. The vulnerability of satellite communications [Электронный ресурс]. – 2021, April 19. – URL: www.securitymagazine.com/articles/94689-the-vulnerability-of-satellite-communications/ (дата обращения: 10.08.2024).

[295] Shadbolt L. Technical Study Satellite Cyber attacks and Security [Электронный ресурс]. – HDI Global Specialty SE. – 2021, July. – URL: www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite_Cyberattack_whitepaper.pdf/ (дата обращения: 10.08.2024).

[296] Военные космические инфраструктуры (спутники), как правило, менее уязвимы для подобных атак, чем их гражданские аналоги, поскольку на их области информационную безопасность затрачивается больше усилий, например, при использовании передовых методов шифрования и обеспечении защиты физической инфраструктуры.

Космическая инфраструктура обычно классифицируется на три вышеупомянутых технологических и операционных сегмента, которые отвечают за различные функции и поэтому подвержены различным угрозам с точки зрения информационной безопасности: наземный сегмент, космический сегмент и сегмент связи. С целью изучения данного вопроса необходимо обратиться к коллективному исследованию экспертов Университета Тель-Авива г. Барам и О. Векслер[297]. Наземный сегмент состоит из всех наземных элементов космических систем и позволяет осуществлять командование, контроль и управление самим спутником и данными. Большинство атак против ИКТ-инфраструктуры наземного сегмента осуществляются через веб-уязвимости и посредством вредоносных программ и троянов на компьютеры наземных станций. Основная причина в таких атаках – попытки завладеть каналами передачи данных и самими данными. Впоследствии проникновение в сеть наземного сегмента может привести к захвату доступа к самому спутнику. Космический сегмент представляет собой непосредственно инфраструктуру, которая находится в космическом пространстве, – спутники. Согласно экспертам, серьезные пробелы в безопасности архитектуры спутников существуют как в старых, так и в новых спутниках: первые имеют устаревшую неприспособленную к нынешним информационным угрозам систему безопасности, вторые производятся с приоритетом экономической выгоды, а не безопасности. Угрозы в сфере использования ИКТ космических сегментов обычно возникают из-за уязвимостей в наземных станциях, в сетевых компонентах и в приемниках, которые получают данные со спутника, что позволяет злоумышленнику проникать в сеть и оставаться незамеченным. Другая угроза может быть связана с внедрением вредоносного программного обеспечения в аппаратном обеспечении спутника в цепочке поставок, чтобы на более позднем этапе скомпрометировать наземные устройства. Кроме того, в связи с уязвимостями в рамках систем связи и передачи данных в данном контексте

[297] Baram G., Wechsler O. Cyber Threats to Space Systems [Электронный ресурс]. – URL: https://www.researchgate.net/publication/342666394_Cyber_Threats_to_Space_Systems_-_Current_Risks_and_the_Role_of_NATO (дата обращения: 10.08.2024).

наиболее распространенной физической угрозой являются помехи GPS и спуфинг[298], в результате которых происходят манипуляции с нарушением или изменением частотной сигнализации, а также возможен перехват незашифрованного спутникового трафика.

Еще одна проблема заключается в том, что сегодня благодаря повсеместному внедрению ИКТ и доступности знаний и необходимых для этого оборудования, такие возможности противоправного и злонамеренного использования ИКТ растут, в связи с чем проблема атрибуции подобных атак набирает свою актуальность, т.к. злонамеренные действия против спутников способны привести к катастрофическим последствиям. Спутниковые системы уязвимы для вредоносных атак, таких как взлом, спуфинг, захват контроля и др.[299] Как отмечает Л.Шадболт[300] в своем исследовании о безопасности спутниковых систем, предположительные доказательства атак на космические системы в открытом доступе имеют ограниченное распространение; существует только несколько случаев, когда были публично раскрыты кибератаки, которые непосредственно затрагивали космические системы, и даже их описание не является полным[301]. Одним из таких негативных примеров может служить инцидент, произошедший со спутникном дистанционного зондирования Земли Landsat 7. 20 октября 2007 г. Landsat 7, совместно управляемый NASA и Геологической службой США, испытал 12 минут помех из-за прямой атаки на спутниковую связь C2. Вмешательство было обнаружено только после аналогичного события, имевшегося место 23 июля 2008 г. Считается, что обе атаки предположительно связаны с Китаем[302].

Кроме того, рассматриваемая проблема усугубляется тенденцией милитаризации космического пространства и появлением широких технических возможностей, которые могут быть использованы злоумышленниками, в том числе

---

[298] Поддмена сигналов путем передачи неверных сигналов GPS, структурированных так, чтобы они походили на подлинные.

[299] Alshaer M. Cyber attacks on satellites: Review and solutions [Электронный ресурс]. – URL: www.academia.edu/18156391/Cyber_attacks_on_satellites_Review_and_solutions/ (дата обращения: 10.08.2024).

[300] Инженер по космическим системам и консультант по страхованию в HDI Global Specialty.

[301] Shadbolt L. Technical Study Satellite Cyber attacks and Security. Op. cit.

[302] Weeden B., Samson V. Global Counterspace Capabilities: An Open Source Assessment [Электронный ресурс] // Secure World Foundation. – April 2018. – URL: https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf (дата обращения: 10.08.2024).

террористами, для целей, не совместимых с целями и принципами Устава ООН, что обуславливает возникновение очередных угроз и вызовов для обеспечения безопасности космических ИКТ-систем. В связи с выше обозначенными угрозами обеспечение безопасности космических ИКТ-систем, как и для любых других ИКТ-систем, поддерживающих критическую инфраструктуру представляется особо важным вопросом, что актуализирует необходимость выработки норм, регулирующих обеспечение безопасности в сфере использования ИКТ относительно космического пространства как на национальном, так и международных уровнях.

Как справедливо отмечает Г. Г. Шинкарецкая, начало 1980-х гг. ознаменовало периодом, когда процесс формирования договорной базы международного космического права остановился[303]. На данный момент отсутствует единый подход и всеобъемлющий механизм, направленный на международно-правовое регулирование обеспечения безопасности в сфере использования ИКТ как в целом, так и относительно космического пространства, что обуславливает актуальность исследования данного вопроса. Данный факт также можно отследить в Руководящих принципах обеспечения долгосрочной устойчивости космической деятельности Комитета по использованию космического пространства в мирных целях (КОПУОС)[304]. Кроме того, в них отмечается важность сотрудничества международного сообщества с целью обеспечения безопасности в области применения информтехнологий, в том числе в части обеспечения защиты «важных национальных, иностранных и международных информационных инфраструктур, которые могут быть непосредственно связаны с обеспечением надежного и безопасного

[303] Шинкарецкая Г. Г. Общие принципы права в регулировании космической деятельности // Государство и право. – 2023. – № 2. – С. 131.

[304] В принципах установлена необходимость государств «принимать разумные меры для обеспечения целостности каналов поставок, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций». Источник: Руководящие принципы обеспечения долгосрочной устойчивости космической деятельности Комитета по использованию космического пространства в мирных целях [Электронный ресурс] / Научно-технический подкомитет. – 18 октября 2016 г. – A/AC.105/C.1/L.354/Rev.1 – URL: https://www.unoosa.org/res/oosadoc/data/documents/2017/aac_105c_1l/aac_105c_1l_354rev_1_0_html/V1609035.pdf (дата обращения: 10.08.2024).

функционирования орбитальных систем» и соответствующей наземной инфраструктуры[305]. Помимо этого, 25 января 2018 г. КОПУОС опубликовал Повестку дня «Космос-2030» и глобальное управление космической деятельностью[306], в которой отмечается, что «рассмотрение вопросов, связанных с важнейшими объектами инфраструктуры, включая изучение вопросов кибербезопасности, имеющих отношение к космической деятельности» заслуживает отдельного внимания»[307].

Международно-правовые нормы, обеспечивающие безопасность космического пространства, содержатся в отраслевых источниках[308]. Наиболее значимые из универсальных источников международного космического права – это Договор о запрещении испытаний ядерного оружия в атмосфере, в космическом пространстве и под водой 1963 г., Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела 1967 г. (Договор по космосу), Соглашение о спасании космонавтов, возвращении космонавтов и возвращении объектов, запущенных в космическое пространство 1968 г., Конвенция о международной ответственности за ущерб, причиненный космическим объектами 1972 г., Конвенция о регистрации объектов, запускаемых в космическое пространство 1975 г., Соглашение о деятельности государств на Луне и других небесных телах 1979 г.

При рассмотрении эволюции международного космического права, важно отметить, что Соглашение о деятельности государств на Луне и других небесных телах 1979 г. было ратифицировано наименьшим числом государств, включая несколько космических держав, и ознаменовало конец развития международного

---

[305] Руководящие принципы обеспечения долгосрочной устойчивости космической деятельности Комитета по использованию космического пространства в мирных целях [Электронный ресурс] / Научно-технический подкомитет. – 18 октября 2016 г. – A/AC.105/C.1/L.354/Rev.1 – URL: https://www.unoosa.org/res/oosadoc/data/documents/2017/aac_105c_1l/aac_105c_1l_354rev_1_0_html/V1609035.pdf (дата обращения: 10.08.2024).

[306] Черных И.А. Международно-правовые аспекты обеспечения устойчивости космической деятельности [Электронный ресурс]. Диссертация на соискание степени кандидата юридических наук. – URL: http://dissovet.rudn.ru/web-local/prep/rj/index.php?id=37&mod=dis&dis_id=2156 (дата обращения: 10.08.2024).

[307] Note by the Secretariat. The «Space2030» agenda and the global governance of outer space activities [Электронный ресурс]. – A/AC.105/1166. – Committee on the Peaceful Uses of Outer Space. – 13 December 2017 – URL: https://www.unoosa.org/oosa/oosadoc/data/documents/2018/aac.105/aac.1051166_0.html (дата обращения: 10.08.2024).

[308] Борьба за мирный космос: Правовые вопросы / Ю. М. Колосов, С. Г. Сташевский. – 2-е изд., стер. – М.: Статут, 2014. – С. 3.

космического права посредством выработки и принятия обязательных к исполнению международных договоров[309]. С тех пор международное космическое право развивалось благодаря норм «мягкого права», закрепленным в резолюциях Генеральной Ассамблеи ООН. Кроме того, они дополняются многосторонними и двусторонними источниками, а также международным обычаем[310].

Статья 3 Договора по космосу 1967 г. устанавливает, что деятельность по исследованию и использованию космического пространства должна осуществляться в соответствии с международным правом в интересах поддержания международного мира и безопасности. Соответственно с учетом данной статьи можно заключить, что какая-либо операция против космической ИКТ-инфраструктуры, угрожающая международному миру и безопасности[311], может считаться нарушением общего запрета на деятельность в космическом пространстве, которая не предназначена для мирных целей, даже если она не будет нарушать другие нормы международного права. Помимо данного запрета рассматриваемый договор не предусматривает регламентации ответственности за осуществление атак на космическую ИКТ-инфраструктуру и ее любые сегменты и компоненты.

В дополнение к универсальным источникам международного космического права существует ряд документов, определяющих принципы деятельности в космическом пространстве, которые классифицируются как содержащие нормы «мягкого права»[312].

Важно упомянуть также Устав и Конвенции МСЭ, действующая редакция которых была принята в 1992 г. и в соответствии с которыми основная функция

---

[309] Morozova E., Vasyanin Y. International Space Law and Satellite Telecommunications [Электронный ресурс]. – 23 December 2019. – URL: https://archive.org/details/acrefore-9780190647926-e-75 (дата обращения: 10.08.2024).

[310] Обычай представлен в данной отрасли права положениями резолюций Генеральной Ассамблеи ООН, принятыми единогласно и выражающими согласованные позиции государств, и другими общепризнанными и систематически применяемыми правилами при осуществлении космической деятельности.

[311] Lotrionte C. Expanding the Mandate of the ITU? [Электронный ресурс] // 2013 World Cyberspace Cooperation Summit IV (WCC4). – Silicon Valley, CA, USA, 2013. – P. 1–7. – URL: https://ieeexplore.ieee.org/document/7050501 (дата обращения: 10.08.2024).

[312] Декларация правовых принципов, регулирующих деятельность государств по исследованию и использованию космического пространства от 1963 г.; Принципы, регулирующие использование государствами искусственных спутников Земли для международного прямого телевизионного вещания 1982 г.; Принципы, касающиеся дистанционного зондирования Земли из Космоса 1986 г.; Принципы, касающиеся использования ядерных источников энергии в космическом пространстве 1992 г. и другие разработанные в рамках системы ООН документы.

МСЭ заключается в предотвращении помех при использовании радиочастотного спектра путем распределения и назначения сегментов спектра различным службам. Учредительная конвенция МСЭ, Устав и Конвенции МСЭ, хотя и не представляют собой источники международного права, предметом которых непосредственно выступает космос, они все же являются регулирующими документами для всех радиочастот, относящихся к космическим ресурсам и, таким образом, считаются основополагающими для космической деятельности.

МСЭ играет важную роль в борьбе с киберпреступностью. Так, в 2007 г. МСЭ учредила Группу экспертов высокого уровня по кибербезопасности в качестве консультационной платформы для экспертов по информационной безопасности с участием многих заинтересованных сторон, обладающих консультативными полномочиями, из различных областей и регионов для того, чтобы «обеспечить рамки, в которых все заинтересованные стороны могут координировать международные меры реагирования на растущие вызовы в области кибербезопасности» и «укреплять доверие и безопасность в информационном обществе»[313]. МСЭ как специализированное учреждение ООН в области ИКТ внес значительный вклад в формировании системы обеспечения безопасности в сфере использования ИКТ посредством своей деятельности. В контексте космического пространства МСЭ сосредоточил свою работу в направлении выработки и принятия норм в виде резолюций, регламентов, руководящих принципов и т.д., оставив без внимания вопрос создания института обязательств для государств в космическом пространстве с учетом развития ИКТ. Например, МСЭ не регулирует вопрос нападения на космические инфраструктуры и не осуществляет контроля за соответствующими действиями.

Многосторонние соглашения имеют чрезвычайно важное значение в регулировании использования ИКТ и формировании режима обеспечения безопасности космического пространства относительно использования ИКТ.

Что касается двусторонних соглашений по сотрудничеству в сфере использования ИКТ, то они рассматриваются как наиболее эффективный

[313] ITU Global Cybersecurity Agenda (GCA). Framework for International Cooperation in Cybersecurity. – ITU, 2007. – P. 13.

инструмент, на базе которого в дальнейшем может строиться как региональная, так и глобальная нормативная база. Примечательным является сотрудничество России и Китая в данной области, которое постоянно эволюционирует с момента подписания соглашения в области обеспечения МИБ от 8 мая 2015 г.[314] Стороны обязались не совершать операции против информационных пространств друг друга, проводить двусторонний диалог на постоянной основе, а также реагировать на технологии, которые, по их мнению, могут оказать дестабилизирующее воздействие на политическую и социально-экономические области или которые могут нарушать принцип суверенитета государств.

Также принимаются инициативы на региональном уровне – политика ЕС в данной области предстает положительной моделью регионального сотрудничества. В рамках союза в 2003 г. была утверждена Европейская стратегия безопасности[315], в которой числятся также угрозы в информационном пространстве. Что касается обеспечения безопасности ИКТ-инфраструктуры космического пространства, то ЕС определяет в качестве приоритета два основных направления деятельности, которые направлены на защиту космической инфраструктуры – это меры по борьбе с кибератаками, включая киберпреступность, и меры по поддержке защиты критически важной инфраструктуры и сетевой безопасности. В 2016 г. была утверждена Глобальная стратегия внешней политики и политики безопасности Европейского Союза, которая представляет собой обновленную доктрину Европейского Союза по повышению эффективности обороны и безопасности Союза и его государств-членов, защите гражданского населения, сотрудничеству между вооруженными силами государств-членов, управлению иммиграцией, кризисами и т.д., которая заменяет Европейскую стратегию безопасности 2003 г.[316]

---

[314] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. (вступило в силу 10 августа 2016 г.) [Электронный ресурс] // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1/ (дата обращения: 10.08.2024).

[315] Report on the Implementation of the European Security Strategy – Providing Security in a Changing World [Электронный ресурс]. – Brussels, 11 December 2008. – S407/08. – URL: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf (дата обращения: 10.08.2024).

[316] Shared Vision, Common Action: a Stronger Europe. A Global Strategy for the European Union’s Foreign and Security Policy [Электронный ресурс]. –2016, 29 June. – URL: https://www.iss.europa.eu/content/global-strategy-european-union’s-foreign-and-security-policy/ (дата обращения: 10.08.2024).

В Глобальной стратегии внешней политики и политики безопасности Европейского Союза отмечается, что ЕС будет уделять больше внимания кибербезопасности[317]. Анализируя данный документ, можно сказать, что ЕС рассматривает обеспечение безопасности в сфере использования ИКТ приоритетным направлением во всех областях, том числе и в рамках космической деятельности, где функционируют критически важные инфраструктуры. Также была принята Директива Европейского Совета об определении и определении европейских критических инфраструктур и оценке необходимости улучшения их защиты 2008/114[318]. Директива является одним из столпов Европейской программы защиты критической инфраструктуры, которая определяет общий политический подход и рамки деятельности ЕС в данном направлении[319].

Меры обеспечения безопасности дополняют систему норм международного космического права и были одобрены в результате деятельности таких механизмов, как ГПЭ ООН и РГОС ООН, а также Группы правительственных экспертов по мерам транспарентности и укрепления доверия в космосе. Последняя в своих докладах подтверждает ответственность государств за санкционирование деятельности в космическом пространстве и реализацию контроля за ней, примат международного сотрудничества, направленный на исследование и использование космического пространства на благо и в интересах всего человечества[320]. Группа правительственных экспертов по мерам транспарентности и укрепления доверия в космосе классифицирует два типа мер по обеспечению транспарентности и укрепления доверия «те, которые касаются потенциала, и те, которые касаются поведения», относя к ним меры «по повышению доступности информации о

---

[317] «Оснащая ЕС и помогая государствам-членам защищать себя от киберугроз, сохраняя при этом открытое, свободное и безопасное киберпространство, что влечет за собой укрепление технологических возможностей, направленных на смягчение угроз и повышение устойчивости критически важной инфраструктуры, сетей и услуг, а также сокращение киберпреступности. Это означает развитие инновационных систем ИКТ, которые гарантируют доступность и целостность данных, обеспечивая при этом безопасность в европейском цифровом пространстве».

[318] Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Executive summary. – European Union, 2019. – 99 p.

[319] Этот документ также примечателен тем, что впервые на региональном уровне ЕС сослался на защиту критической инфраструктуры для обеспечения безопасности информационного пространства в целом, а в частности Интернета, признав протоколы и ключевые услуги Интернета частью защиты гражданской критической инфраструктуры.

[320] Transparency and Confidence-Building Measures in Outer Space Activities to Enhance Stability in Outer Space. – Report A/68/189 of the Group of Governmental Experts, 29 July 2013. Op. cit.

космической деятельности, обмен информацией о программах разработки новых космических систем действующих системах космического базирования, изложение принятых государствами принципов и целей, касающихся осуществляемой ими деятельности по исследованию и использованию космического пространства в мирных целях, меры, касающиеся определения норм поведения в отношении повышения безопасности космических полетов», уведомления о рисках, а также меры, которые связаны с реализацией принципа международного сотрудничества в космическом пространстве. Они представляют собой «добровольные меры, относящиеся к нормам «мягкого права», которые в своей совокупности наряду с другими механизмами формирует систему норм, обеспечивающих безопасность космоса.

Группа правительственных экспертов по дальнейшим практическим мерам по предотвращению гонки вооружений в космическом пространстве в 2019 г. представила рекомендации по разработке соответствующего международного юридически обязательного документа[321], в процессе обсуждений были проанализированы различные возможные угрозы космической деятельности как традиционные, так и новые, в том числе угрозы безопасности ИКТ-инфраструктуры космического пространства[322]. Также было заключено, что в данном контексте наиболее применимым многосторонним регулирующим документом является Договор по космосу 1967 г., однако в нем нет специальных положений, которые бы учитывали использование ИКТ и были направлены на защиту космической инфраструктуры.

В связи с отсутствием в системе международного права специализированных норм, которые направлены на регулирование обеспечения безопасности ИКТ-инфраструктуры космического пространства, в правовой доктрине используются

---

[321] Белокрылова Е. А., Кологерманская Е. М., Бевзюк Е. А. Комментарий к Федеральному закону от 28 декабря 2010 г. N 390-ФЗ «О безопасности» [Электронный ресурс]. – Доступ из справочно-правовой системы «ГАРАНТ». – URL: https://ivo.garant.ru/#/document/57469858 (дата обращения: 10.08.2024).

[322] Они связаны с «(i) радиоэлектронной борьбой, включая помехи и спуфинг радиопередач; (ii) кибератаками, в том числе непосредственно на космические объекты, а также на наземную инфраструктуру, и коммерческие операции, связанные с космосом». Источник: Report by the Chair of the Group of governmental experts on further practical measures for the prevention of an arms race in outer space [Электронный ресурс]. – New York, 31 January 2019. – URL: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/oral-report-chair-gge-paros-2019-01-31.pdf (дата обращения: 10.08.2024).

стандартный подход толкования более общих норм применительно к конкретным правовым отношениям. Так, запрет применения силы распространяется на все виды деятельности, в том числе в космосе, однако космическое пространство демилитаризировано лишь частично.

Что касается действующих стандартов и норм, применимых к космической ИКТ-инфраструктуре, то МСЭ регулирует частоты спутниковой связи для предотвращения помех связи и регистрирует орбиты спутников, а за пределами этих областей в настоящее время существует несколько стандартов. В 2007 г. МСЭ создал «Глобальную повестку дня в области кибербезопасности»[323] – механизм, который не продемонстрировал своей эффективности до настоящего момента[324]. Можно сказать, что сегодня не функционируют международные специализированные институты, ограничивающие использование спутников, и нет всеобъемлющего руководящего органа, который контролировал бы конкретное использование спутников. Однако существуют подобные инициативы в частном секторе, одним из примеров является NIST Cybersecurity Framework – проект документа, опубликованный Национальным институтом стандартов и технологий США[325] в июне 2021 г., «Введение в кибербезопасность для коммерческих спутниковых операций», предназначен для внедрения в коммерческие космические предприятия набора руководящих принципов по снижению рисков кибербезопасности организации на основе существующих стандартов, руководств и практик.

В контексте международного космического права все спутники являются космическими объектами, независимо от их технических характеристик, общего назначения и других возможных особенностей. В этом отношении на них распространяются правила и требования, которые международное космическое право выдвигает к космическим объектам, включая, среди прочего, обязательство

[323] Задуманную как «основу для международного сотрудничества, направленного на укрепление доверия и безопасности в информационном обществе. Источник: Global Cybersecurity Agenda (GCA) [Электронный ресурс]. – URL: www.itu.int/en/action/cybersecurity/Pages/gca.aspx/ (дата обращения: 10.08.2024).
[324] Последний доклад датируется 2008 г.
[325] Национальный институт стандартов и технологий США (The National Institute of Standards and Technology, NIST).

по их регистрации[326], реализацию институтов юрисдикции и ответственности, права собственности, процедуры возврата в случае запланированной или непреднамеренной посадки. Международно-правовое регулирование спутниковой связи основывается на общепринятых для международного космического права нормах. Космическое пространство считается свободным для исследования и использования всеми государствами. При этом развертывание спутниковых систем не считается присвоением, которое в космическом пространстве запрещено, и должно осуществляться на основе правового режима, установленного нормами международного космического права, а также на основе национального законодательства и требований МСЭ.

Международно-правовое регулирование спутниковых систем, в частности телекоммуникационных, и принципов их вещания было сформировано в период идеологического противоборства социалистического и капиталистического блока государств. В нем существует также правовой пробел, который связан с обеспечением информационной безопасности спутниковых систем: в рамках разработанных на национальных и региональных уровнях программных документах в области космической деятельности и информационной безопасности отсутствуют меры, направленные на обеспечение безопасности спутниковых систем. Так, представляется возможным обратиться к анализу Директивы ЕС по сетевой и информационной безопасности[327], которая является частью стратегии информационной (кибер) безопасности ЕС и представляет собой первый нормативно-правовой акт, распространяющийся на все географическое пространство ЕС, в области кибербезопасности; была предложена Европейском комиссией и принята в 2016 г. В ней отсутствует упоминание спутниковых систем и регулирование их информационной безопасности. Проведя анализ, можно сделать вывод, что существует фрагментированное регулирование использования ИКТ применительно к отдельным аспектам безопасности космического

[326] Morozova E., Vasyanin Y. International Space Law and Satellite Telecommunications. Op. cit.
[327] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. – L 194, 19.7.2016. – P. 1-30.

пространства и важность ее обеспечения не вызывает сомнения. Тем не менее, на данный момент не учреждено специализированной организации, деятельность которой была бы сосредоточена вокруг выработки комплексной международно-правовой базы, регулирующей безопасность ИКТ-систем, связанных с космосом.

Международно-правовое регулирование обеспечения безопасности в сфере использования ИКТ в рамках космического пространства должно строиться на основополагающих принципах международного публичного и специализированных принципах международного космического права, а также иметь своей ключевой целью осуществление деятельности в космическом пространстве в интересах поддержания мира и безопасности и содействия международного сотрудничеству. В этой связи международному сообществу нужно будет прийти к консенсусу насчет того, будет ли военная космическая деятельность, включая военную спутниковую связь, противоречить использованию космического пространства в мирных целях, а также решить вопрос, возникающий в связи с тем, что небесные тела, определение которых может включать орбиты вокруг них, должны использоваться исключительно в мирных целях, что ставит под сомнение возможность использования ИКТ, основанных на спутнике, вращающемся вокруг Луны, в военных целях, что не запрещено в случае, если речь идет о земных орбитах[328].

Космическая деятельность осуществляется посредством использования единого информационного пространства и его основополагающего элемента на современном этапе развития – глобальной сети Интернет и связанных с ним ИКТ, что обуславливает заинтересованность всего международного сообщества в обеспечении безопасности ИКТ-инфраструктуры космического пространства. Международное сотрудничество в данном направлении, в свою очередь, должно стать основополагающим принципом для создания «структурированной, эффективной и гибкой структуры для противодействия» информационной угрозам

[328] Morozova E., Vasyanin Y. International Space Law and Satellite Telecommunications. Op. cit.

космических ИКТ-систем[329]. Само международное сотрудничество, связанное с любым аспектом обеспечения безопасности в сфере использования ИКТ, должно учитывать особенности развития ИКТ-среды, основываться на «мультистейкхолдерном» подходе с ключевой ролью государств как первичных субъектов международного права и при обеспечении равенства государств в ИКТ-среде. Международно-правовое регулирование ИКТ с целью обеспечения безопасности космического пространства должно строиться на основе мирного, устойчивого, транспарентного использования. В данном контексте особенно важно обеспечивать эффективное функционирование системы международного космического права, а также создание новых международно-правовых норм, которые будут способствовать обеспечению безопасности всего космического пространства.

Космическая деятельность неразрывно связана с информационными технологиями, соответственно, безопасность ИКТ-инфраструктуры в данной сфере должна стать одним из ключевых направлений международной безопасности[330]. Проведенный автором анализ приводит к выявлению правовых пробелом и необходимости со стороны международного сообщества предпринять соответствующие инициативы, направленные на их устранение. На текущий момент не существует международного органа, занимающегося вопросами безопасности ИКТ-инфраструктур в космосе, в том числе по причине медленного прогресса в ООН по обеспечению безопасности в области применения информтехнологий. Учреждение подобного отраслевого института с участием многих заинтересованных сторон с ключевой ролью государств в принятии решений с целью оценки рисков и продвижения передовой практики будет способствовать формированию международно-правовых основ обеспечения безопасности в сфере использования ИКТ в рамках космического пространства и всех его сегментов, начиная от наземного и заканчивая каналами передачи данных

[329] Mendonça H. C. Cyberspace in Outer Space: New Challenges, New Responses Cyberspace in Outer Space. [Электронный ресурс]. – 2016, 16 December. – URL: https://interactive.satellitetoday.com/via/january-2017/cyberspace-in-outer-space-new-challenges-new-responses/ (дата обращения: 10.08.2024).

[330] Белокрылова Е. А., Кологерманская Е. М., Бевзюк Е. А. Комментарий к Федеральному закону от 28 декабря 2010 г. № 390-ФЗ «О безопасности». Указ. соч.

от «любых действий, которые могли бы нанести ущерб или негативно повлиять на функционирование наземных и информационных инфраструктур»[331]. Кроме учреждения нового института также представляется возможным расширение манданта Комитета ООН по мирному использованию космического пространства.

Регулирование вопросов обеспечения безопасности ИКТ-инфраструктуры космического пространства, в свою очередь, станет катализатором для усовершенствования международного регулирования использования ИКТ в целом, а также для кодификации международного права и его прогрессивного развития относительно ИКТ.

Резюмируя третью главу диссертационного исследования, отметим основные вывод по каждому параграфу. Относительно международного морского судоходства важно подчеркнуть, что вследствие постоянного прогресса в области ИКТ и их внедрения в отрасль, вызовы и угрозы, которые стоят перед ней, становятся более комплексными. Анализ международно-правовой базы, регулирующей обеспечение безопасности в области применения информтехнологий в рамках международного морского судоходства позволил сделать вывод, что определенно существуют механизмы, направленные на формирование международно-правовых основ обеспечения безопасности ИКТ-инфраструктуры морской отрасли, тем не менее, они не являются системой мер, способной обеспечить безопасность ИКТ-систем международного морского судоходства, а представляют собой фрагментированные правовые механизмы, основная часть которых была выработана и принята задолго до цифровизации морской отрасли. В связи с чем перед современным международным сообществом стоит задача разработки комплекса международно-правовых норм, которые будут надлежащим образом обеспечивать безопасность международного морского судоходства, в особенности в ее ИКТ-аспекте. Среди прочего, автором предложены отдельные положения, которые могли бы упорядочить регулирование и

[331] Draft guidelines for the long-term sustainability of outerspace activities [Электронный ресурс]. Conference room paper by the Chair of the Working Group on the Long-term Sustainability of Outer Space Activities, 27 June 2018. – A/AC.105/2018/CRP.21. – URL: https://www.unoosa.org/res/oosadoc/data/documents/2018/aac_1052018crp/aac_1052018crp_21_0_html/AC105_2018_CRP21E.pdf (дата обращения: 10.08.2024).

обеспечение безопасности международного морского судоходства относительно ИКТ. Также предложено выработать их в формате специализированного международно-правового акта, который дополнит источниковую базу международного морского права, что станет важным вкладом в прогрессивное развитие международного права и дальнейшую кодификацию международно-правовых норм в области обеспечения всей системы международной безопасности в целом и обеспечения безопасности в области использования ИКТ в частности. Кроме того, важно активизировать усилия государств в данном направлении как на международном, так и региональном уровнях.

В ходе исследования международно-правового регулирования использования ИКТ в космической деятельности автором был проведен анализ существующих угроз космической ИКТ-инфраструктуры в отношении наземного сегмента, космического сегмента, а также передачи данных и цепочек поставок космической инфраструктуры. Также были рассмотрены действующие на международном и региональном уровне правовые механизмы и инициативы, направленные на снижение рисков в области информбезопасности космоса. Текущий период развития международного права характеризуется отсутствием единого подхода, а также всеобъемлющего механизма, который бы упорядочил обеспечение безопасности в области использования информтехнологий как в целом, так и относительно космического пространства. Это является одним из основных факторов, которые обусловливают актуальность исследования настоящего вопроса. В основном распространены нормы международного космического права общего характера, которые применяется сейчас ко всем видам деятельности в космическом пространстве, а что касается специальных мер, связанных с обеспечением безопасности ИКТ-систем, связанных с космосом, то они ограничены в части предмета регулирования и в основном носят узкоспециализированный характер.

На данный момент международно-правовой фундамент, обеспечивающий безопасность космического пространства, зиждется на источниках международного космического права, среди которых универсальные

международные договоры, международные договоры регионального и двустороннего характера, иные документы, содержащие те или иные нормы, определяющие деятельность в космическом пространстве. Однако они не адаптированы под существующие уязвимости ИКТ и угрозы, исходящих от ИКТ-среды, что обуславливает необходимость выработки норм, которые будут регулировать непосредственно обеспечение безопасности ИКТ-инфраструктуры космического пространства. Автором также предложено рассмотрение возможности учреждения специализированного органа или расширения полномочий уже существующих институтов, в чей мандат входил бы данный вопрос.

ЗАКЛЮЧЕНИЕ

В ходе исследования автором сформировано новое юридическое знание и разработана совокупность теоретических положений о международно-правовом регулировании обеспечения безопасности в сфере использования ИКТ.

Первая глава посвящена выявлению различных подходов к терминологическому аппарату относительно регулирования обеспечения безопасности в сфере использования ИКТ и определение их особенностей. Актуальность данного аспекта исследования была обоснована тем, что международно-правовое регулирование обеспечения безопасности в сфере использования ИКТ влияет на процесс формирования самой системы ее обеспечения, в том числе с точки зрения лингвистики и герменевтики. Посредством проведения анализа использования и эволюции терминологии в различных сферах использования ИКТ, было установлено, что в научном дискурсе не существует общепринятого определения ИКТ в связи с их комплексных характером и разнообразием подходов, поскольку в различных исследованиях используется разные определения ИКТ. Предложено определение ИКТ в широком смысле, в рамках которого ИКТ определяется как совокупность методов, процессов и средств, используемых для сбора, обработки, хранения и распространения графической, звуковой, текстовой и числовой информации с помощью электронно-вычислительных устройств, а также телекоммуникационных аппаратных и программных средств

Также было отмечено, что термин ИКТ охватывает широкий спектр процессов обработки информации и недавно стал использоваться в качестве собирательного термина для всего спектра технологий, обеспечивающих способы и средства получения, хранения, передачи, извлечения и обработки информации. В работе проводится исследование влияния ИКТ на развитие международной безопасности, при этом выявлено, что развитие и широкое использование ИКТ принесли неоспоримые положительные выгоды, однако зависимость от ИКТ и их повсеместный характер создали новые уязвимости, которые приобрели

международный характер, тем самым став частью повестки международной безопасности, что, в свою очередь, определяет необходимость выработки четкой системы международно-правовых норм, регулирующих межгосударственные отношения в ИКТ-среде, включая обеспечение безопасности в сфере использования ИКТ.

Автором сформулированы концептуальные подходы к информационно-коммуникационным технологиям и регулированию обеспечения безопасности в сфере их использования в доктрине международного права. С этой целью был проведен сравнительно-правовой анализ евроатлантического и российского подхода к определению безопасности ИКТ. Автором был сделан вывод, что подход Российской Федерации на обеспечения безопасности в сфере использования ИКТ, который продвигается ею на двустороннем и многостороннем уровнях сотрудничества, демонстрирует целостный взгляд на обеспечение информационной безопасности, согласно которому, в отличии от позиции коллективного Запада, кибербезопасность является одним из ее компонентов наряду с другими. С точки зрения юридической лингвистики и герменевтики важно отметить особенность российской терминологии, которая формируется вне рамок «западного понимания и трактовок» и стремится к более широким смыслам. Это прослеживается не только на теоретическом уровне отечественной юридической доктрины, но и практическом в части деятельности Российской Федерации на внешнеполитическом направлении. В данном контексте инициативы Российской Федерации, направленные на выработку чёткого нормативного механизма регулирования использования ИКТ, отражают современные реалии развития ГИО и ИКТ. Что касается «кибертерминологии», то под ней умышленно скрывается не только понимание «кибербезопасности» с точки зрения обеспечения защиты, но легализация реализации наступательных операций, в том числе с применением информационного оружия, из-за правового вакуума в действующем международном праве в части отсутствия ограничение на проведение информационных операций. Существующая разница между евроатлантическим взглядом на безопасность ИКТ и подходами России и ее единомышленниками

приводит к относительно медленному переговорному процессу по формированию комплексной системы международно-правового регулирования обеспечения безопасности в сфере использования ИКТ. Автор полагает, что Российская Федерации должна продолжать свою линию и ей необходимо и дальше придерживаться ИКТ-терминологии, не допуская признания на глобальном уровне «кибертерминологии», которая в своей перспективе имеет конфликтогенный потенциал и представляет собой наибольший терминологический вызов в контексте. Таким образом, автор приходит к заключению, что сегодняшний этап формирования комплексной системы международно-правового регулирования обеспечения безопасности в сфере использования ИКТ с точки зрения теоретического развития встречается с проблемой отсутствия взаимоприемлемого понятийного аппарата, что обуславливает наличие сложностей для достижения общности взглядов на международное управление и регулирование ИКТ. В данном контексте автор диссертационного исследования отмечает, что в доктрине международного права существуют такие термины, которые могут стать основой для конструктивных переговоров. Таким термином может выступить обеспечение безопасности в сфере использования ИКТ. В этой связи обосновывается необходимость его использования в рамках дальнейшего процесса международного нормотворчества. Помимо этого, целесообразно продвигать инициативы, направленные на гармонизацию терминологических подходов. Данная идея может способствовать согласованию различных концепций понимания обеспечения безопасности в сфере использования ИКТ, гармонизации национальных законодательств, достижению прогресса в переговорах по ИКТ-проблематике и, наконец, приведет к их конечной цели – разработки универсального международно-правового акта, направленного на регулирование ИКТ и обеспечения безопасности в сфере их использования.

В работе также проведен анализ отечественной и зарубежной доктрины международного права с точки зрения исследования ИКТ как предмета международного права относительно выделения новой отрасли, объектом которой являются межгосударственные отношения в информационной области.

Формирование новой отрасли международного права определяется необходимостью регулирования ИКТ и идентификации целей, задач, принципов и основ выстраивания отношений в области информационной безопасности. Автор отмечает, что вопрос о наличии достаточных свойств для признания за совокупностью международно-правовых норм в информационной сфере статуса отрасли международного права не находит однозначного ответа в доктрине международного права. Наблюдается отсутствие единого теоретического подхода к определению и содержанию новой отрасли международного права. Отмечается, что разнообразие подходов выделения новой отрасли права связано с особенностями развития межгосударственных отношений в информационной области. Автор обосновывает тезис о том, что различные подходы к определению и содержанию новой отрасли права имеют общую черту: они направлены на изучение информационной области в целом или ее составных элементов в частности. В связи с чем автор полагает целесообразным выделение новой отрасли права – международного информационного права – и обосновывает выбор наиболее комплексным подходом к изучению информационной области и ее составных элементов. На фоне нормотворческого процесса с целью обеспечения безопасности в сфере использования ИКТ, который наблюдается в последнее время на международном уровне, и в связи с тем, что данная отрасль начинает получать более четкие контуры, оправданно говорить о ней, несмотря на то, что ее формирование все еще продолжается. Автор дополняет определение международного информационного права и предлагает его следующее содержание: международное информационное право – это совокупность специальных международных принципов и норм, определяющих права и обязанности субъектов международного права в информационном пространстве. Дана характеристика объекта, предмета, субъекта, принципов, институтов, источников международного информационного права как отрасли международного права. В диссертационном исследовании установлено, что исторический контекст разработки и принятия норм международного права, а также особенности информационной области вызывают дискуссии в части

применимости действующих норм к ИКТ: выделяют две основные позиции по данному вопросу. Подход России, Китая и других ее приверженцев сводится к необходимости выработки новых норм международного права, которые будут применимы непосредственно к ИКТ и будут соответствовать особенностям их продолжающейся эволюции; вторая позиция отражает евроатлантическое видение ИКТ-проблематики и подразумевает возможность применения действующих норм к ИКТ. Автор также отмечает, что отсутствие единства по рассматриваемому вопросу предопределяет переменный успех переговорного процесса в рамках ООН.

Помимо этого, обобщены, систематизированы и раскрыты нормативно-правовые и концептуальные основы регулирования обеспечения безопасности в сфере использования ИКТ в законодательстве Российской Федерации. Проведенные систематизация и анализ позволили заключить, что законодательство, регулирующее обеспечение безопасности в сфере использования ИКТ, сравнительно ново и имеет связь с непрерывным развитием ИКТ, требующих постоянной адаптации нормативно-правовой базы и выступающих импульсом для развития информационного законодательства в целом и его подотрасли – законодательства об обеспечении информационной безопасности – в частности. Исследование регулирования обеспечения безопасности в сфере использования ИКТ позволило сделать вывод о том, что российский подход отличается преемственностью и прозрачностью, отвечает современным потребностям системы международных отношений и научно-технологического прогресса, а также специфике развития ИКТ. В результате исследования российского законодательства установлено, что достижение безопасности в сфере использования ИКТ рассматривается Российской Федерацией посредством формирования системы международно-правового обеспечения безопасности в сфере использования ИКТ, в основу которой должны лечь закрепленные в международном-правовом акте юридически обязательные к исполнению нормы.

Во второй главе автор выявил перспективы развития системы правового обеспечения безопасности в сфере использования ИКТ с точки зрения

международно-правовой, а также организационно-правовой (механизмов международного сотрудничества) основы регулирования исследуемой области.

Сделан вывод о том, что формирующееся международное информационное право базируется на основных источниках международно-правовых норм общего международного права. Они дополняются специализированными источниками в виде актов международных организаций, стандартов, регламентов, рекомендаций, кодексов, разработанных с целью обеспечения международной безопасности с учетом особенностей развития глобального информационного пространства и ИКТ. На примере регулирования ИКТ-среды дана оценка роли международного обычного права. Автором также обзорно рассмотрены дополнительные источники международно-правовых норм относительно обеспечения безопасности в сфере использования ИКТ, упомянутые в статье 38 Статута Международного Суда, – общие принципы права, судебные решения государственных международных судов, труды наиболее квалифицированных специалистов по публичному праву. На основе проведенного анализа источниковой базы международно-правового регулирования обеспечения безопасности в сфере использования ИКТ, доказано, что преобладающей формой регламентации в исследуемой области являются нормы «мягкого права». Научно обосновано, что на фоне роста угроз в ИКТ-среде отчетливо прослеживается необходимость нормативно-правового регулирования обеспечения безопасности в сфере использования ИКТ на международном уровне в виде универсального международно-правового акта с обязательными к исполнению нормами, который должен стать юридическим фундаментом комплексной системы обеспечения безопасности в сфере использования ИКТ.

Проведена оценка роли как международных правительственных и неправительственных механизмов в формировании международно-правовой системы обеспечения безопасности в области использования ИКТ. Установлено, что разнообразие механизмов сотрудничества обусловлено тем, что отсутствует четко выстроенная институциональная система (организационно-правовая основа регулирования) и тем, что угрозы, исходящие от ИКТ, приобретают все большее значение для международной безопасности и стабильности, занимая важное место

в деятельности международных правительственных и неправительственных механизмов как глобального, так и регионального уровня. Проанализирована эволюция ИКТ-проблематики в рамках системы ООН, при это отмечается, что наиболее важными переговорными механизмами в рамках ООН являются ГПЭ ООН и РГОС ООН. Их деятельность также стала предметом исследования во второй главе работы.

Автором выявлено более эффективное правовое регулирование обеспечения безопасности в сфере использования ИКТ на региональном уровне по сравнению с универсальным (в условиях торможения развития международного права в части обеспечения безопасности в сфере использования ИКТ из-за существующих противоречий государств). В связи с чем предлагается при разработке международно-правовых норм универсального характера использовать наиболее передовой и прогрессивный опыт регионального нормотворчества в рассматриваемой области. Автор выступает с рекомендацией продолжать налаживать стратегические партнерские отношения со странами и региональными объединениями-единомышленниками, которые разделяют стремления Российской Федерации выработать международно-правовое регулирование обеспечения безопасности в сфере использования ИКТ. В диссертационном исследовании также изучены международные инициативы вне системы ООН и доказано, что они также выступают важными механизмами сотрудничества с целью обеспечения безопасности в сфере использования ИКТ. Автором также разработаны рекомендации по совершенствованию международного сотрудничества в изучаемой области в рамках системы ООН. Основополагающее место среди данных рекомендаций занимает необходимость консолидация площадок ООН, занимающихся ИКТ и информационным пространством: автором рассматривается целесообразным учреждение специализированной Организации ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ, в мандат которой вошли бы разработка и принятие универсального международно-правового акта по обеспечению безопасности в сфере использования ИКТ и самих ИКТ, в связи с чем предлагается соответствующий проект конвенции. При этом она должна будет

также осуществлять роль координационного центра ООН по ИКТ-среде с постоянно действующими органами и механизмами сотрудничества с региональными и субрегиональными организациями[332].

В дополнение к этому дана оценка российских инициатив, направленных на обеспечение безопасности в сфере использования ИКТ, при этом автор подчеркивает, что инициативы и усилия, предлагаемые и предпринимаемые Российской Федерации, имеют своей целью поддержание инклюзивного диалога, равного международного сотрудничества с сохранением ключевой роли государств в принятии решений и центральной роли ООН как центральной переговорной площадки по вопросам обеспечения безопасности в сфере использования ИКТ, а также выработку юридического фундамента, регулирующего ИКТ.

В третьей главе диссертационного исследования раскрыты и обоснованы особенности и перспективы отраслевого регулирования обеспечения безопасности в сфере использования ИКТ в контексте международного морского и космического права. Общий анализ международно-правовой основы, регулирующей обеспечение безопасности в сфере использования ИКТ в международном праве и его отдельных отраслях лег в основу вывода о том, что существуют разрозненные специализированные механизмы, направленные на формирование международно-правовых основ регулирования безопасности ИКТ в конкретных областях, но, несмотря на это, они не представляют собой единый комплекс мер, способный обеспечить международную безопасность. В связи с чем для содействия прогрессивному развитию международного права и его кодификации и в дополнение к рекомендациям по международно-правовому акту, регулирующему обеспечение безопасности ИКТ-среды, автором диссертационного исследования проведен анализ отдельных отраслей международного права с точки зрения регулирования ИКТ и предложены практические и теоретические рекомендации, а также рассмотрены возможности выработки специализированных международных организаций, в мандат которых могут входить общественные отношения,

[332] Данное предложение соотносится с инициативой России, Беларуси и Никарагуа о создании постоянного органа, мандат которого должен включать весь спектр вопросов, связанных с безопасностью ИКТ, в том числе разработку юридически обязательного международного документа по международной информационной безопасности.

складывающиеся в процессе обеспечения безопасности в сфере использования ИКТ в таких отраслях международного права, как международное морское право и международное космическое право, или расширение мандата уже существующих организаций.

Автором выявлены отдельные проблемы и перспективы регулирования обеспечения безопасности в сфере использования ИКТ в контексте международного морского судоходства. Доказано, что международное морское судоходство становится все более зависимым от ИКТ, которые как открывают новые возможности, так и новые угрозы, требующие более комплексного изучения и оперативного юридического ответа. Классифицированы ИКТ-инфраструктуры международного морского судоходства, которые требуют международно-правовых усилий для обеспечения информационной безопасности: системы в общей среде, системы на борту судов, системы на берегу. Помимо этого, установлено, что перед международным сообществом стоит долгосрочная задача, так как защита ИКТ-инфраструктуры морской отрасли включает в себя виртуальные, наземные, морские и даже космические элементы. Проанализированы некоторые инциденты международного морского судоходства, связанные с уязвимостями в сфере использования ИКТ. Они подтверждают необходимость разработки и принятия надлежащего правового механизма, предметом которого является регулирование обеспечения безопасности ИКТ-инфраструктуры международного морского судоходства. На основе анализа правовой основы международного морского права, предметом которой является обеспечение безопасности международного морского судоходства относительно использования ИКТ, было заключено, что она опирается на универсальные источники международного морского права. Тем не менее фактор ИКТ в обеспечении безопасности международного морского судоходства в них не полностью отражен с учетом исторического контекста их выработки и принятия. Автор выдвигает тезис, согласно которому по мере технического прогресса должна происходить адаптация существующих правовых норм как на национальном, так и на международном уровнях. Научно обосновывается необходимость принятия

изменений к действующей правовой основе международного морского права с учетом специфики ИКТ и их внедрения в международное морское судоходство. Выявлено, что существуют механизмы, направленные на формирование международно-правовых основ регулирования обеспечения безопасности морской ИКТ-инфраструктуры, тем не менее, они не являются системой мер, способной обеспечить безопасность ИКТ-систем международного морского судоходства, а представляют собой фрагментированные правовые механизмы, основная часть которых была выработана и принята задолго до цифровизации морской отрасли. Автор доказывает необходимость разработки системы норм, которые будут регулировать информационную безопасность морской отрасли во всех ее аспектах, что должно быть реализовано в рамках многоуровневой структуры: на межгосударственном уровне, региональном уровне, который станет подготовительным переговорным этапом для дальнейшего рассмотрение наиболее передового опыта в изучаемой области на универсальном уровне. Выработаны предложения по формированию международно-правовых основ, способных обеспечить безопасность ИКТ-систем морской отрасли посредством разработки и принятия специализированного международно-правового акта, который станет отраслевым источником международного морского права и предметом которого станет отраслевое регулирование обеспечения безопасности в сфере использования ИКТ. Он может стать основополагающим источник международного морского права в части защиты ИКТ-инфраструктуры морской отрасли. Его разработка и принятие также внесут вклад в прогрессивное развитие международного права и дальнейшую кодификации международно-правовых норм в области обеспечения всей системы международно-правового регулирования обеспечения безопасности в сфере использования ИКТ. Отраслевой международно-правовой акт должен предусматривать регулирование правонарушений в информационной области и необходимость привлечения ответственности за их совершение в национальном законодательстве, определять правонарушения, нарушающие обеспечения информационной безопасности морской отрасли. С целью формирования комплексной системы обеспечения безопасности морской отрасли поддержана

идея принятия международной конвенции по противодействию использованию ИКТ в преступных целях с учетом особенностей и международного морского судоходства. Предлагается системное регулирование проблем обеспечения безопасности в сфере использования ИКТ, возникающих в результате кибератак против морской ИКТ-инфраструктуры, а также совершенствование института морского страхования с учетом угроз, исходящих от прямого или косвенного использования в качестве средства для причинения вреда ИКТ. Также с целью гармонизации правовых систем и их законодательств предложено учреждение специального научного комитета, мандат которого будет распространяться на изучение соответствующих вопросов, и который, как полагает автор, будет способствовать оказанию правовой помощи государствам-участникам будущей конвенции. Помимо этого, выдвинуто предложение о направлении данного вопроса на рассмотрение специальных органов ООН, которые занимаются ИКТ-проблематикой. Сделан вывод, что вопрос регулирования обеспечения безопасности в сфере использования ИКТ в контексте международного морского судоходства вызывает потребность ее закрепления за конкретным механизмом, что может быть реализовано посредством нескольких опций: создания новой международной специализированной межправительственной организации в рамках системы ООН, расширения мандата МСЭ или ИМО.

В ходе исследования международно-правовых аспектов использования ИКТ в космической деятельности государств автором были выявлены существующие и потенциальные угрозы космической отрасли в исследуемой области относительно наземного сегмента, космического сегмента, а также передачи данных и цепочек поставок космической инфраструктуры. Установлено, что космическая деятельность осуществляется посредством использования единого информационного пространства и его основополагающего элемента Интернета и связанных с ним ИКТ, что обуславливает заинтересованность всего международного сообщества в обеспечении безопасности ИКТ-инфраструктур космического пространства. Была исследована также деятельность отраслевых универсальных и региональных механизмов сотрудничества и инициатив,

направленных на снижение рисков в данной области. Изучена международно-правовая основа, обеспечивающая безопасность космического пространства, которая имеет своим фундаментом универсальные международные акты, международные договоры регионального и двустороннего характера, иные документы, содержащие те или иные нормы, определяющие деятельность в космическом пространстве. Исследование взаимосвязи ИКТ и космического пространства, а также международно-правовых норм, регулирующих безопасность в сфере использования ИКТ в космическом пространстве, позволило прийти к заключению о том, что существуют правовые пробелы и необходимо предпринять соответствующие инициативы для их заполнения. Установлено, что текущее состояние регулирования ИКТ в космической отрасли характеризуется отсутствием единого подхода и всеобъемлющего механизма, направленного на международно-правовое регулирование обеспечения безопасности ИКТ-инфраструктуры как в целом, так и относительно космического пространства, что обуславливает актуальность исследования данного вопроса. Выявлено, что в основном распространены нормы международного космического права общего характера, которые применяются сейчас ко всем видам деятельности в космическом пространстве, а что касается специальных мер, связанных с обеспечением безопасности ИКТ-систем, связанных с космосом, то они ограничены в части предмета регулирования и в основном носят узкоспециализированный характер. Научно обосновано, что существующее фрагментированное регулирование отдельных аспектов безопасности ИКТ-инфраструктуры космического пространства обуславливает необходимость учреждения специализированного института, деятельность которого была бы сосредоточена вокруг выработки комплексной правовой основы, регулирующей безопасность ИКТ-систем, связанных с космосом, или расширения полномочий уже существующих институтов, в чьей мандат входили бы данные вопросы. Это будет способствовать формированию комплексного режима обеспечения безопасности в области использования ИКТ. В результате исследования автором предлагается включить в объект международно-правового регулирования

обеспечения безопасности в сфере использования ИКТ космическую деятельность с целью минимизации рисков потенциальной атаки против космической ИКТ-инфраструктуры – физического наземного сегмента, космического сегмента, каналов передачи данных и цепочек поставок космической инфраструктуры. Разработаны рекомендации для совершенствования системы международного космического права с точки зрения обеспечения безопасности ИКТ-инфраструктуры. Она должна строиться на основополагающих принципах международного права и специализированных принципах международного космического права, в частности осуществлении деятельности в космическом пространства в интересах поддержания мира и безопасности и содействия международного сотрудничеству. При этом международное сотрудничество с целью обеспечения безопасности ИКТ-инфраструктуры космического пространства должно учитывать особенности развития ИКТ-среды. Помимо этого, оно должно основываться на мультистейхолдерном подходе с акцентом на определяющую роль государств как первичного субъекта международного права посредством разработки международного режима с участием многих заинтересованных сторон, который включал бы правительственные и неправительственные организации, научное и экспертное сообщество, гражданское общества в виду особенностей развития ИКТ и космической деятельности.

Вторая и третья главы диссертационного исследования взаимодополняют рекомендации, прописанные в каждой из них. В частности, на основе проведенного исследования в рамках деятельности по учреждению постоянного институционального диалога по ИКТ-проблематике можно сделать вывод, что существует необходимость выработки специальных норм в отношении существующих отраслей международного права, помимо общего регулирования обеспечения безопасности в сфере использования ИКТ. Иными словами, автор предлагает:

1) создать отдельный экспертный механизм, который бы занимался исследованием данного вопроса на основе отраслевого принципа; либо

2) создать научно-экспертный центр, в чьи полномочия войдут рассматриваемые вопросы, в рамках будущей постоянно действующей организации по ИКТ с целью более комплексного изучения международно-правовых аспектов регулирования ИКТ и избегания риска «фрагментации» переговорного, правового и исследовательского процесса.

Таким образом, изучив некоторые аспекты теоретико-правовых основ и подходов к определению ИКТ, выявив международно-правовые основы регулирования обеспечения безопасности в сфере использования ИКТ и сотрудничества в данной области, а также их тенденции и перспективы на примере отдельных отраслей права, автором проведена попытка представить комплексный анализ международно-правового регулирования обеспечения безопасности в области применения ИКТ с целью формирования нового юридического знания, разработки теоретических положений об исследуемой проблематике, а также выработки рекомендаций для международного нормотворческого процесса.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АТЭС – Азиатско-Тихоокеанское экономическое сотрудничество

БИМКО – Балтийский и Международный Морской Совет

ВАСЭ – Всемирная ассамблея по стандартизации электросвязи

ВВИУО – Всемирная встреча на высшем уровне по вопросам информационного общества

ВМО – Всемирная метеорологическая организация

ИИ – искусственный интеллект

ИКТ – информационно-коммуникационные технологии

ИМО – Международная морская организация

ИС – информационные системы

ИСО – Международная организация по стандартизации

КОПУОС – Комитет по использованию космического пространства в мирных целях

МАРПОЛ – Международная конвенция по предотвращению загрязнения с судов

МГП – международное гуманитарное право

МСЭ – Международный союз электросвязи

МТС – Международный телеграфный союз

НАТО – Организация Североатлантического договора

ОАГ – Организация Американских Государств

ОБСЕ – Организация по безопасности и сотрудничеству в Европе

ООН – Организация Объединенных Наций

ОЭСР – Организация экономического сотрудничества и развития

ЦУР – цели устойчивого развития

ЭСКАТО – Экономическая и социальная комиссия для Азии и Тихого океана

ЮНЕСКО – Организация Объединенных Наций по вопросам образования, науки и культуры

ЮНКТАД – Конференции Организации Объединенных Наций по торговле и развитию

ЮНСИТРАЛ – Комиссия Организации Объединенных Наций по праву международной торговли

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Международно-правовые акты и официальные документы

1. Венская конвенция о праве международных договоров (Вена, 23 мая 1969 г.) // Ведомости ВС СССР. – 1986, 10 сентября. – № 37. – Ст. 772.

2. Всестороннее исследование проблемы киберпреступности. Проект, февраль 2013 года. – Текст : электронный // Управление Организации Объединенных Наций по наркотикам и преступности. – URL: www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 10.08.2024).

3. Доклад, подготовленный Секретариатом // Восьмой Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, Гавана, 27 августа – 7 сентября 1990 г. – A/CONF.144/28/Rev.1. – Нью-Йорк : ООН, 1991. – 307 с.

4. Конвенция о борьбе с незаконными актами, направленными против безопасности гражданской авиации (Монреаль, 23 сентября 1971 г.) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. 29. – М., 1975. – С. 90–95.

5. Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства (Рим, 10 марта 1988 г.). – Текст : непосредственный // Собрание законодательства Российской Федерации. – 2001. – № 48, ст. 4469.

6. Конвенция Организации Объединенных Наций по морскому праву (Монтего-Бей, 10 декабря 1982 г.) // Собрание законодательства Российской Федерации. – 1997. – № 48, ст. 5493.

7. Международная конвенция по охранению подводных телеграфных кабелей (Париж, 14 марта 1884 г.), с Декларацией (Париж, 1 декабря 1886 г.) и Заключительным Протоколом (Париж, 7 июля 1887 г.). – Текст : непосредственный // Собрание законов СССР. – 1926. – Отд. II, № 31. – Ст. 190.

8. Обновленная концепция конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности.

Предложение Российской Федерации. – URL: www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (дата обращения: 10.08.2024). – Текст : электронный.

9. Первый доклад по теме «Формирование и доказательство существования международного обычного права», подготовленный Специальным докладчиком Майклом Вудом. Комиссия международного права. Шестьдесят пятая сессия. Женева, 6 мая – 7 июня и 8 июля – 9 августа 2013 года. – A/CN.4/663. – URL: https://legal.un.org/ilc/guide/1_13.shtml (дата обращения: 10.08.2024). – Текст : электронный.

10. Российский проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях. – URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 10.08.2024). – Дата публикации: 29.07.2021. – Текст : электронный.

11. Руководящие принципы обеспечения долгосрочной устойчивости космической деятельности Комитета по использованию космического пространства в мирных целях. Научно-технический подкомитет, 18 октября 2016 г. – A/AC.105/C.1/L.354/Rev.1. – URL: https://www.unoosa.org/res/oosadoc/data/documents/2017/aac_105c_1l/aac_105c_1l_354rev_1_0_html/V1609035.pdf (дата обращения: 10.08.2024). – Текст : электронный.

12. Устав Организации Объединенных Наций : принят в г. Сан-Франциско 26.06.1945. – Текст : непосредственный // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. XII. – М., 1956. – С. 14–47.

13. Constitution and Convention of the International Telecommunication Union (with annexes and optional protocol). Concluded at Geneva on 22 December 1992 // United Nations Treaty Series. Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. – Vol. 1825, 1-3125. – New York, 1998. – P. 506.

14. Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium. – WSIS-03/GENEVA/DOC/4, 12 December 2003. – URL: https://digitallibrary.un.org/record/533621?ln=ru (дата обращения: 10.08.2024). – Текст : электронный.

15. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. 19.7.2016. – L 194. – P. 1–30.

16. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) // Official Journal of the European Communities. –2002, July 31. – L 201. – P. 37–47.

17. Draft guidelines for the long-term sustainability of outerspace activities : Conference room paper by the Chair of the Working Group on the Long-term Sustainability of Outer Space Activities, 27 June 2018. – A/AC.105/2018/CRP.21. – URL: www.unoosa.org/res/oosadoc/data/documents/2018/aac_1052018crp/aac_1052018crp_21_0_html/AC105_2018_CRP21E.pdf (дата обращения: 10.08.2024). – Текст : электронный.

18. Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Executive summary. – European Union, 2019. – 99 p.

19. Global Digital Compact: rev. 1, 15 May 2024. – Office of the Secretary-General's Envoy on Technology. – URL: www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Rev_1.pdf (дата обращения: 10.08.2024). – Текст : электронный.

20. Global Digital Compact: zero draft. – 1 April 2024 // Office of the Secretary-General's Envoy on Technology. – URL: www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Zero_Draft.pdf (дата обращения: 10.08.2024). – Текст : электронный.

21. II Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea (Geneva, 1949, August 12). – Geneva International Committee of the Red Cross, 1960. – 327 p.

22. IMO 33rd Assembly adopted resolutions, including on budget, strategic plan and appointment of Secretary-General. – URL: https://www.imo.org/en/MediaCentre/PressBriefings/pages/IMO-Assembly-adopts-budget,-strategic-plan.aspx (дата обращения: 10.08.2024). – Текст : электронный.

23. Interim guidelines on guidelines on maritime cyber risk management (MSC.1/Circ.1526). – 2016, June. – URL: https://www.imorules.com/MSCCIRC_1526.html (дата обращения: 10.08.2024). – Текст : электронный.

24. International Convention for the Safety of Life at Sea. Concluded at London, 1 November 1974 // United Nations Treaty Series. Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. – Vol. 1184, I-18961. – New York, 1987. – P. 458.

25. International Maritime Organization Strategic plan for the Organization for the six-year period 2024 to 2029. Resolution A 33/Res.1173. Adopted on 6 December 2023. Assembly, 33rd session, Agenda item 8(a). – URL: https://wwwcdn.imo.org/localresources/en/About/strategy/Documents/A%2033-Res.1173.pdf (дата обращения: 10.08.2024). – Текст : электронный.

26. International Maritime Organization Strategic Plan for the six-year period 2018 to 2023. Resolution A.1110(30). Adopted on 6 December 2017. – URL: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.1110(30).pdf (дата обращения: 10.08.2024). – Текст : электронный.

27. ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary. – URL: http://www.iso.org/standard/73906.html/ (дата обращения: 10.08.2024). – Текст : электронный.

28. ISO/IEC 27001 Системы обеспечения информационной безопасности.– URL: https://www.iso.org/ru/standard/27001 (дата обращения: 10.08.2024). – Текст : электронный.

29. ISO/IEC 27032:2012 Information technology, Security techniques. Guidelines for cybersecurity. – URL: https://www.iso.org/ru/standard/44375.html (дата обращения: 10.08.2024). – Текст : электронный.

30. ISO/IEC 27032:2023 Cybersecurity. Guidelines for Internet security. – URL: https://www.iso.org/ru/standard/76070.html (дата обращения: 10.08.2024). – Текст : электронный.

31. ISPS-Code International code for the security of ships and of port facilities (MSC.196(80)). – 2002, December 12. – URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC.196(80).pdf (дата обращения: 10.08.2024). – Текст : электронный.

32. ITU Global Cybersecurity Agenda (GCA). Framework for International Cooperation in Cybersecurity. – ITU, 2007. – 20 p.

33. Note by the Secretariat. The «Space2030» agenda and the global – governance of outer space activities. A/AC.105/1166. Committee on the Peaceful. Uses of Outer Space. – 2017, December 13. – URL: https://www.unoosa.org/oosa/oosadoc/data/documents/2018/aac.105/aac.1051166_0.html (дата обращения: 10.08.2024). – Текст : электронный.

34. Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. – A/AC.290/2021/CRP.2. – 2021, 10 March. – URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 10.08.2024). – Текст : электронный.

35. Plan of Action of the World Summit on the Information Society. Document WSIS-03/GENEVA/DOC/5-E. – 2003, December 12. – URL: https://www.itu.int/net/wsis/docs/geneva/official/poa.html (дата обращения: 10.08.2024). – Текст : электронный.

36. Report by the Chair of the Group of governmental experts on further practical measures for the prevention of an arms race in outer space, New York, 31 January 2019. – URL: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/oral-report-chair-gge-paros-2019-01-31.pdf (дата обращения: 10.08.2024). – Текст : электронный.

37. Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security established pursuant to General Assembly resolution 73/27 of 5 December 2018, 28 April 2021. A/DEC/75/564. – URL: https://digitallibrary.un.org/record/3924426?ln=en/ (дата обращения: 10.08.2024). – Текст : электронный.

38. Report on the Implementation of the European Security Strategy. Providing Security in a Changing World. – Brussels, S407/08. – 2008, December 11. – URL: https://www.europeansources.info/record/report-on-the-implementation-of-the-european-security-strategy-providing-security-in-a-changing-world/ (дата обращения: 10.08.2024). – Текст : электронный.

39. Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems. – 2017, June 16. – URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (дата обращения: 10.08.2024). – Текст : электронный.

40. Resolutions adopted by the General Assembly at its 65th session. – URL: https://research.un.org/en/docs/ga/quick/regular/65 (дата обращения: 10.08.2024). – Текст : электронный.

41. Review of Maritime Transport 2018. UNCTAD. UNCTAD/RMT/2017. – New York ; Geneva : United Nations, 2017. – 130 p. – URL: https://unctad.org/system/files/official-document/rmt2018_ru.pdf (дата обращения: 10.08.2024). – Текст : электронный.

42. Review of Maritime Transport 2019. UNCTAD/RMT/2019/Corr.1. – Geneva : United Nations, 2020. – 132 p. – URL: https://unctad.org/system/files/official-document/rmt2019_en.pdf (дата обращения: 10.08.2024). – Текст : электронный.

43. Review of Maritime Transport 2021. UNCTAD. UNCTAD/RMT/2021. – Geneva : United Nations, 2021. – 177 p.

44. Shared Vision, Common Action: a Stronger Europe. A Global Strategy for the European Union’s Foreign and Security Policy. – 2016, June 29. – URL: https://www.iss.europa.eu/content/global-strategy-european-union’s-foreign-and-security-policy/ (дата обращения: 10.08.2024). – Текст : электронный.

45. The ASEAN Cybersecurity Cooperation Strategy 2021–2025. – URL: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf (дата обращения: 10.08.2024). – Текст : электронный.

46. Toolkit on disability for Africa. Information and communication technology (ICT) and disability / The Division for Social Policy and Development (DSPD) of the Department of Economic and Social Affairs (DESA). – 2016. – 40 p.

47. Transparency and Confidence-Building Measures in Outer Space Activities to Enhance Stability in Outer Space. Report A/68/189 of the Group of Governmental Experts, 29 July 2013. – New York : United Nations, 2013. – 106 p.

48. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bisas adopted in 1998. – United Nations Publication Sales No. E.99. – Vol. 4. – 76 p. – ISBN 92-1-133607-4.

49. United Nations Convention on the Use of Electronic Communications in International Contracts. Adopted in New York, 23 November 2005 // United Nations, Treaty Series, Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. Vol. 2898. – New York, 2018. – 411 p.

50. United Nations General Assembly Resolution 1149(XII). Collective action to inform and enlighten the peoples of the world as to the dangers of the armaments race, and particularly as to the destructive effects of modern weapons. – A/RES/1149(XII). – 14 November 1957. – Resolutions adopted by the General Assembly during its 12th session, 17 September-14 December 1957 // General Assembly Official Records, 12th Session, Supplement No. 18 (A/3805). – New York : United Nations, 1958. – 64 p.

51. United Nations General Assembly Resolution 51/162. Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law, A/RES/51/162, 30 January 1997. Resolutions and Decisions adopted by the General Assembly during its 51st session. Vol. I. 17 September – 18 December 1996 // General Assembly Official Records, 51st Session, Supplement No. 49 (A/51/49 (Vol. I). – New York : United Nations, 1997. – P. 336–340.

52. United Nations General Assembly Resolution 53/73. Role of science and technology in the context of international security and disarmament. – A/RES/53/73. – 4 January 1999. – Resolutions and Decisions adopted by the General Assembly during its 53rd session. Vol. I. Resolutions 9 September – 18 December 1998 // General Assembly Official Records, 53rd Session, Supplement No. 49 (A/53/49). – New York : United Nations, 1999. – 400 p.

53. United Nations General Assembly Resolution 58/32. Developments in the field of information and telecommunications in the context of international security, A/RES/58/32, 8 December 2003. Resolutions and Decisions adopted by the General Assembly during its 58th session. Vol. I. Resolutions 16 September – 23 December 2003 // General Assembly Official Records, 58th Session, Supplement No. 49 (A/58/49). – New York : United Nations, 2004. – 575 p.

54. United Nations General Assembly Resolution 61/54. Developments in the field of information and telecommunications in the context of international security, A/RES/61/54, 6 December 2006. Resolutions and Decisions adopted by the General Assembly during its 61st session. Vol. I. 12 September – 22 December 2006 // General Assembly Official Records, 61st session, Supplement No. 49 (A/61/49 (Vol. I). – New York : United Nations, 2007. – 546 p.

55. United Nations General Assembly Resolution 65/37, Oceans and the law of the sea, adopted by the General Assembly on 7 December 2010. – A/RES/65/37. – Resolutions and Decisions adopted by the General Assembly during its 65th session. – Vol. I, 14 September – 24 December 2010 // General Assembly Official Records, 65th session, Supplement No. 49 (A/65/49 (Vol. I). – New York : United Nations, 2010. – 666 p.

56. United Nations General Assembly Resolution 73/266. Advancing responsible State behaviour in cyberspace in the context of international security. – A/RES/73/266. – 22 December 2018. – Resolutions and Decisions adopted by the General Assembly during its 73rd session. Vol. I. 18 September – 22 December 2018 // General Assembly Official Records, 73rd session. Supplement No. 49 (A/73/49 (Vol. I). – New York : United Nations, 2019. – 1184 p.

57. United Nations General Assembly Resolution 73/27. Developments in the field of information and telecommunications in the context of international security. – A/RES/73/27. – 5 December 2018. – Resolutions and Decisions adopted by the General Assembly during its 73rd session. Vol. I. 18 September – 22 December 2018 // General Assembly Official Records, 73rd session. Supplement No. 49 (A/73/49 (Vol. I). – New York : United Nations, 2019. – 1184 p.

58. United Nations General Assembly Seventy-eighth session. Item 96 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General. Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. – A/78/265. – 2023, August 1. – URL: https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports (дата обращения: 10.08.2024). – Текст : электронный.

59. United Nations General Assembly Seventy-seventh session. Item 95 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General. Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. – A/77/275. – 2022, 8 August. – URL: https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports (дата обращения: 10.08.2024). – Текст : электронный.

60. United Nations General Assembly Sixty-eighth session. Item 94 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. – A/68/98. – 2013, June 24. – URL: https://digitallibrary.un.org/record/753055 (дата обращения: 10.08.2024). – Текст : электронный.

61. United Nations General Assembly Sixty-fifth session. Item 94 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. – A/65/201. – 2010, July 30. – URL: https://digitallibrary.un.org/record/688507?ln=ru (дата обращения: 10.08.2024). – Текст : электронный.

62. World Development Report 2006. Equity and Development. – A copublication of the World Bank and Oxford University Press. – URL: https://documents1.worldbank.org/curated/en/435331468127174418/pdf/322040 World0Development0Report02006.pdf (дата обращения: 10.08.2024). – Текст : электронный. –

63. Written Input of the International Information Security School to the United Nations Open-ended Working Group on Security of and in the Use of Information and Communications Technologies. – URL: https://documents.unoda.org/wp-content/uploads/2022/09/Written-input-of-the-IISS-to-the-UN-OEWG.pdf (дата обращения: 10.08.2024). – Текст : электронный.

64. WSIS: Tunis Agenda for the Information Society. – WSIS-05/TUNIS/DOC/6 (Rev. 1)-E. – 2005, November 18. – URL:

www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (дата обращения: 10.08.2024). – Текст : электронный.

II. Нормативные правовые акты Российской Федерации

65. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 : с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации 30 декабря 2008 года № 6-ФКЗ, от 30 декабря 2008 года № 7-ФКЗ, от 5 февраля 2014 года № 2-ФКЗ, от 21 июля 2014 года № 11-ФКЗ, от 14 марта 2020 года № 1-ФКЗ, от 4 октября 2022 года № 5-ФКЗ, от 4 октября 2022 года № 6-ФКЗ, от 4 октября 2022 года № 7-ФКЗ, от 4 октября 2022 года № 8-ФКЗ // Официальный интернет-портал правовой информации (www.pravo.gov.ru). – Ст. 0001202210060013. – Дата публикации: 06.10.2022.

66. ГОСТ Р 50922-2006. Защита информации: основные термины и определения : национальный стандарт Российской Федерации : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст : дата введения 01.02.2008. – URL: https://protect.gost.ru/document.aspx?control=7&id=129024 (дата обращения: 10.08.2024). – Текст : электронный.

67. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года : утверждены Президентом Российской Федерации 24.07.2013 № Пр-1753 // Законы, кодексы и нормативно-правовые акты Российской Федерации. – URL: http://legalacts.ru/doc/osnovy-gosudarstvennoi-politiki-rossiiskoi-federatsii-v-oblasti/ (дата обращения: 10.08.2024). – Текст : электронный.

68. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. (вступило в силу 10 августа 2016 г.) // Официальный интернет-портал правовой информации. – URL:

http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1/ (дата обращения: 10.08.2024). – Текст : электронный.

69. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 // Собрание законодательства Российской Федерации. – 2021. – № 16, ч. I, ст. 2746.

70. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации : Указ Президента Российской Федерации от 30 марта 2022 г. № 166 // Собрание законодательства Российской Федерации. – 2022. – № 14, ст. 2242.

71. Об утверждении Концепции внешней политики Российской Федерации : Указ Президента Российской Федерации от 31 марта 2023 г. № 229 // Собрание законодательства Российской Федерации. – 2023. – № 14, ст. 2406.

72. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50, сСт. 7074.

73. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. – 2017. – № 20, ст. 2901.

74. О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. – 2021. – № 27-2, ст. 5351.

75. Об утверждении Концепции внешней политики Российской Федерации : Указ Президента Российской Федерации от 30 ноября 2016 г. № 640 // Собрание законодательства Российской Федерации. – 2016. – № 49, ст. 6886.

76. О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 // Собрание законодательства Российской Федерации. – 2016. – № 1-2, ст. 212.

III. Нормативные акты иностранных государств

77. National Security Strategy. The White House, February 2015. – URL: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf (дата обращения: 10.08.2024). – Текст : электронный.

78. National Security Strategy. The White House, October 2022. – URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (дата обращения: 10.08.2024). – Текст : электронный.

79. National Cybersecurity Strategy. The White House, March 2023. – URL: www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата обращения: 10.08.2024). – Текст : электронный.

IV. Книги и статьи на русском языке

80. Белокрылова, Е. А. Комментарий к Федеральному закону от 28 декабря 2010 г. N 390-ФЗ «О безопасности» / Е. А Белокрылова, Е. М. Кологерманская, Е. А. Бевзюк. – URL: https://ivo.garant.ru/#/document/57469858 (дата обращения: 10.08.2024). – Режим доступа: справочно-правовая система «ГАРАНТ». – Текст : электронный.

81. Берман, А. М. Кибератаки – противоправное использование цифровых технологий / А. М. Берман, Г. Г. Шинкарецкая // Международное право. – 2022. – № 1. – С. 40–50.

82. Бойко, С. М. Международная информационная безопасность: Россия в ООН. Два формата диалога (2018–2021 гг.) / С. М. Бойко // Международная жизнь. – 2024. – № 3. – URL: https://interaffairs.ru/virtualread/ia_rus/32024/files/assets/downloads/publication.pdf (дата обращения: 10.08.2024). – Текст : электронный.

83. Колосов, Ю. М., Борьба за мирный космос: Правовые вопросы / Ю. М. Колосов, С. Г. Сташевский. – 2-е изд., стер. – М. : Статут, 2014. – 176 с.

84. Гуляева, Е. Е. Международно-правовые аспекты кибербезопасности / Е. Е. Гуляева, А. А. Данельян // Московский журнал международного права. – 2020. – № 1. –С. 44–53.

85. Ефремов, А. А. Информационно-правовое обеспечение технологического суверенитета / А. А. Ефремов // Информационное право. – 2022. – № 4 (74). – С. 14–20.

86. Жуков, Ю. Терминология в сфере международной информационной безопасности / Ю. Жуков, А. Кузьмин, Д. Финогенов. – Текст : электронный // BIS Journal. – 2015, 16 сентября. – № 3 (18). – URL: https://ib-bank.ru/bisjournal/post/385 (дата обращения: 10.08.2024).

87. Зиновьева, Е. Глобальный цифровой договор ООН: возможна ли прикладная реализация? / Е. Зиновьева, Т. Исаева. – Текст : электронный // Международная жизнь. – 2022, 28 октября. – URL: https://interaffairs.ru/news/show/37601 (дата обращения: 10.08.2024).

88. Зиновьева Е. С. Анализ внешнеполитических инициатив РФ в области международной информационной безопасности / Е. С. Зиновьева. – Текст : электронный // Вестник МГИМО-Университета. – 2014. – № 6(39). – С. 47–52. – URL: https://www.vestnik.mgimo.ru/jour/article/view/240/240/ (дата обращения: 10.08.2024).

89. Иванова, К. А. Понятие киберпространства в международном праве / К. А. Иванова, М. Ж. Мылтыкбаев, Д. Д. Штодина // Правоприменение. – 2022. – Т. 6, № 4. – С. 32–44.

90. Канаев, Е. А. Большая Евразия, Индо-Тихоокеанский регион и отношения России с АСЕАН / Е. А. Канаев, А. С. Королев. – DOI 10.23932/2542-0240-2019-12-1-26-43 // Контуры глобальных трансформаций: политика, экономика, право. – 2019. – Т. 12, № 1. – С. 26–43.

91. Капустин, А. Я. Суверенитет государства в киберпространстве: международно-правовое измерение / А. Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения. – 2022. – Т. 18, № 6. – С. 100.

92. Кашкин, С. Ю. В поисках концепции правового регулирования искусственного интеллекта: платформенные правовые модели / С. Ю. Кашкин, А. В. Алтухов // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2020. – № 4. – С. 26-–0.

93. Кибербезопасность и управление интернетом : документы и материалы для российских регуляторов и экспертов / отв. ред. М. Б. Касенова ; сост. О. В. Демидов, М. Б. Касенова. – М. : Статут, 2013. – 463 с.

94. Концепция кибербезопасности разошлась с государственной стратегией. – URL: www.kommersant.ru/doc/2355154/ (дата обращения: 10.08.2024). – Дата публикации: 29.11.2013. – Текст : электронный.

95. Костенко, Н. И. Право международной информационной безопасности: (становление, тенденции и проблемы развития) : монография / Н. И. Костенко. – М. : Юрлитинформ, 2019. – 458 с.

96. Костенко, Н. И. Теоретические проблемы формирования права международной информационной безопасности : монография / Н. И. Костенко. – М. : Юрлитинформ, 2019. – 464 с.

97. Крутских, А. Международное право и проблема обеспечения международной информационной безопасности / А. Крутских, А. Стрельцов. – Текст : электронный. // Международная жизнь. – 2014. – № 11. – URL: https://interaffairs.ru/jauthor/material/1167 (дата обращения: 10.08.2024).

98. Лифшиц, И. М. Международное финансовое право и право Европейского союза: взаимодействие и взаимовлияние : монография / И. М. Лифшиц. – М. : Юстицинформ, 2020. – 548 с. – ISBN 978-5-7205-1646-8. – URL: https://ivo.garant.ru/#/document/76894275 (дата обращения: 10.08.2024). – Текст : электронный.

99. Лобанова, О. Новые тенденции формирования системы международной информационной безопасности в Азии / О. Лобанова, Е. Нархова. – Текст : электронный. // Международная жизнь. – 2021. – № 11. – URL: https://interaffairs.ru/jauthor/material/2586 (дата обращения: 10.08.2024).

100. Мартиросян, А. Ж. Международная информационная безопасность: некоторые итоги 2021 г. и политический контекст 2022 г. / А. Ж. Мартиросян. – Текст : электронный // Интернет – сегодня и завтра : сборник авторских статей к Двенадцатому российскому форуму по управлению интернетом (RIGF 2022), 28–29 сентября 2022 г. –

URL: https://cgitc.ru/upload/iblock/ff1/zzzc5u5zgad3ywxomp10xq0foe8fbss5.pdf (дата обращения: 10.08.2024).

101. Мартиросян, А. Ж. Создание международного трибунала по киберпреступности / А. Ж. Мартиросян // Актуальные проблемы мировой политики. IX Ежегодная международная научная конференция молодых ученых, 6–7 декабря 2022 г. (сборник тезисов) / отв. ред. О. А. Тимакова. – М. : Дипломатическая академия МИД России, 2023. – 345 с. – URL: https://pureportal.spbu.ru/files/102589388/_2022.pdf (дата обращения: 10.08.2024).

102. Мартиросян, А. Ж. Формирование системы обеспечения безопасности киберпространства : монография / А. Ж. Мартиросян ; отв. ред. И.О. Анисимов. – М. : Дипломатическая академия МИД России, 2021. – 154 с.

103. Мартиросян, А. Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы / А. Ж. Мартиросян. – Текст : электронный // Вестник ученых-международников. – 2022. – № 2 (20). – С. 179–187. – URL: https://elibrary.ru/item.asp?id=49808514 (дата обращения: 10.08.2024).

104. Международная безопасность в среде информационно-коммуникационных технологий: коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / под ред. проф. А. А. Стрельцова, проф. А. Я. Капустина, проф. Т. А. Поляковой, проф. А. С. Маркова, Б. Н. Мирошникова. – М. : Национальная Ассоциация международной информационной безопасности, 2023. – URL: https://namib.online/2023/03/mezhdunarodnaja-bezopasnost-v-srede-informacionno-kommunikacionnyh-tehnologij/ (дата обращения: 10.08.2024). – Текст : электронный.

105. Международная информационная безопасность: подходы России. Доклад ЦМИБ МГИМО. – 2021. – URL: https://mgimo.ru/upload/2022/03/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii.pdf (дата обращения: 10.08.2024). – Текст : электронный.

106. Мельникова, О. А. Глобальный цифровой договор: на грани фола / О. А. Мельникова – Текст : электронный. // Международная жизнь. – 2024. – № 3. – URL: https://interaffairs.ru/jauthor/material/2962 (дата обращения: 10.08.2024).

107. Мельникова, О. А. Манипуляция общественным мнением и глобальная кибербезопасность : монография / О. А. Мельникова. – М. : Гнозис, 2021. – 204 с.

108. Меньшиков, П. В. Особенности государственного регулирования информационной сферы России / П. В. Меньшиков. – Текст : электронный // Международные коммуникации. – 2018. – № 1 (6). – URL: https://intcom-mgimo.ru/2018/2018-06/state-regulation-of-russian-information-sphere (дата обращения: 10.08.2024).

109. Молчанов, Н. А. Информационный терроризм в международно-правовом контексте / Н. А. Молчанов, Е. К. Матевосова. – Текст : электронный // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2018. – № 5. – URL: https://ivo.garant.ru/#/document/77584175 (дата обращения: 10.08.2024). – Режим доступа: справочно-правовая система «ГАРАНТ».

110. Пазюк, А. В. Понятие международного информационного права как комплексной отрасли международного права / А. В. Пазюк. – Текст : электронный // Actual Problems of International Relations. – 2012. – Vol. 1, No. 111. – URL: https://www.academia.edu/4459264/Понятие_международного_информационного_ права_как_комплексной_отрасли_международного_права (дата обращения: 10.08.2024).

111. Пазюк, А. В. Международное информационное право. Общая часть. Международное информационное право – отрасль современного международного права / А. В. Пазюк. – URL: http://cyberpeace.org.ua/files/razdel-1.pdf (дата обращения: 10.08.2024). – Текст : электронный.

112. Пазюк, А. В. Особенности создания и реализации международно-правовых обычных и договорных норм в сфере управления интернетом / А. В. Пазюк. – URL: https://digital.report/upravlenie-internetom/ (дата обращения: 10.08.2024). – Дата публикации: 03.08.2024. – Текст : электронный.

113. Полякова, Т. А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы / Т. А. Полякова, А. А. Смирнов. – Текст : электронный // Российский юридический журнал. – 2022. – № 3. – URL: https://ivo.garant.ru/#/document/76906647 (дата обращения: 10.08.2024). – Режим доступа: справочно-правовая система «ГАРАНТ».

114. Полякова, Т. А. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз / Т. А. Полякова, Г. Г. Шинкарецкая // Право и государство: теория и практика. – 2020. – № 10 (190). – С. 138–142.

115. Правовые проблемы формирования межгосударственных объединений (на примере зоны свободной торговли и таможенного союза ЕВРАЗЭС) : монография / отв. ред. В. Ю. Лукьянова. – URL: https://ivo.garant.ru/#/document/57736662 (дата обращения: 10.08.2024). – Режим доступа: справочно-правовая система «ГАРАНТ». – Текст : электронный.

116. Размышления Школы МИБ о Глобальном цифровом договоре / отв. ред. А. Ж. Мартиросян. – URL: https://t.me/iis_mib_school/376/ (дата обращения: 10.08.2024). – Текст : электронный.

117. Сборник докладов участников XIII международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Москва, 22–25 апреля 2019 г. / Национальная ассоциация международной информационной безопасности. – URL: https://elibrary.ru/item.asp?id=45719883 (дата обращения: 10.08.2024). – Текст : электронный.

118. Сборник докладов участников XVI международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Москва, 19–21 сентября 2022 г. / Национальная ассоциация международной информационной безопасности. – URL: https://elibrary.ru/item.asp?id=50460981 (дата обращения: 10.08.2024). – Текст : электронный.

119. Смыслова, Т. М. Международное информационное право : методические материалы к междисциплинарному спецкурсу / сост. Т. М. Смыслова. – М. : СТЭНСИ, 2002. – 192 с.

120. Стрельцов, А. А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности / А. А. Стрельцов. – Текст : электронный // Международная жизнь. – 2017. – № 2. – URL: https://interaffairs.ru/jauthor/material/1806 (дата обращения: 10.08.2024).

121. Талимончик, В. П. Международно-правовое регулирование отношений информационного обмена / В. П. Талимончик. – СПб. : Юридический центр Пресс, 2011. – 382 с.

122. Угрозы информационной безопасности в кризисах и конфликтах XXI века / под ред. А. В. Загорского, Н. П. Ромашкиной. – М. : ИМЭМО РАН, 2015. – 151 с. – URL: www.imemo.ru/files/File/ru/publ/2015/2015_027.pdf (дата обращения: 10.08.2024). – Текст : электронный.

123. Шинкарецкая, Г. Г. Проблема выработки определения кибератаки / Г. Г. Шинкарецкая // Международное право. – 2023. – № 2. – С. 10–21.

124. Шинкарецкая, Г. Г. Общие принципы права в регулировании космической деятельности / Г. Г. Шинкарецкая // Государство и право. – 2023. – № 2. – С. 131–138.

125. Шинкарецкая, Г. Г. Роль информационно-коммуникационных технологий (ИКТ) в обеспечении устойчивого развития человеческого общества / Г. Г. Шинкарецкая // Право и управление. – 2023. – № 9. – С. 152–158.

126. Штодина, Д. Д. Международное сотрудничество государств – участников СНГ в области обеспечения информационной безопасности / Д. Д. Штодина // Вестник ученых-международников. – 2021. – № 3 (17). – С. 104–118.

127. Яковенко. А. В. Цифровой суверенитет оказался важен в условиях новой идеологической конфронтации / А. В. Яковенко // Независимая газета. – 2021.

128. Яковенко, А. В. Цифровое будущее в российской дипломатии / А. В. Яковенко // Сборник докладов участников Форума Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности. – 2021.

V. Диссертации, авторефераты диссертаций

129. Зиновьева, Е. С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции : диссертация на соискание ученой степени доктора политических наук : 23.00.04 / Зиновьева Елена Сергеевна. – Москва, 2019. – 362 с. – URL: https://mgimo.ru/upload/diss/2019/zinovieva-diss.pdf (дата обращения: 10.08.2024). – Текст : электронный.

130. Мельникова, О. А. Информационное обеспечение внешнеполитической деятельности современных государств (политологический анализ) : диссертация на соискание ученой степени кандидата политических наук : 23.00.04 / Мельникова Ольга Андреевна. – Москва, 2020. – 210 с. – URL: http://dipacademy.ru/documents/2056/Dissertatsiya_Melnikova.pdf (дата обращения: 10.08.2024). – Текст : электронный.

131. Мысина, А. И. Международно-правовое регулирование сотрудничества государств оп противодействию преступлениям в сфере информационных технологий : диссертация на соискание ученой степени кандидата юридических наук : 12.00.10 / Мысина Анастасия Ильинична. – Москва, 2021. – URL: https://viewer.rsl.ru/ru/rsl01010794479 (дата обращения: 10.08.2024). – Текст : электронный.

132. Прокофьев, К. В. Международно-правовые проблемы обеспечения международной информационной безопасности в сети Интернет : диссертация на соискание ученой степени кандидата юридических наук : 12.00.10 / Прокофьев Константин Викторович. – URL: https://www.dissercat.com/content/mezhdunarodno-pravovye-problemy-obespecheniya-mezhdunarodnoi-informatsionnoi-bezopasnosti-v- (дата обращения: 10.08.2024). – Текст : электронный.

133. Сорокин, Д. В. Проблемы правового обеспечения информационной безопасности России в условиях глобализации информационного пространства : диссертация на соискание ученой степени кандидата юридических наук : 12.00.14 / Сорокин Даниил Викторович. – Санкт-Петербург, 2006. – 223 с. – URL: https://www.dissercat.com/content/problemy-pravovogo-obespecheniya-informatsionnoi-bezopasnosti-rossii-v-usloviyakh-globalizat (дата обращения: 10.08.2024). – Текст : электронный.

134. Талимончик, В. П. Международно-правовое регулирование отношений в сфере информации : диссертация на соискание ученой степени доктора юридических наук : 12.00.10 / Талимончик Валентина Петровна. – Санкт-Петербург, 2013. – 399 с. – URL: https://www.dissercat.com/content/mezhdunarodno-pravovoe-regulirovanie-otnoshenii-v-sfere-informatsii (дата обращения: 10.08.2024). – Текст : электронный.

135. Тедеев, А. А. Теоретические основы правового регулирования информационных отношений, формирующихся в процессе использования глобальных компьютерных сетей : диссертация на соискание ученой степени доктора юридических наук : 12.00.14 / Тедеев Астамур Анатольевич. – Москва, 2007. – 507 с. – URL: https://www.dissercat.com/content/teoreticheskie-osnovy-pravovogo-regulirovaniya-informatsionnykh-otnoshenii-formiruyushchikhs (дата обращения: 10.08.2024). – Текст : электронный.

136. Федулов, В. И. Международно-правовые аспекты защиты компьютерной информации : диссертация на соискание ученой степени кандидата юридических наук : 12.00.10 / Федулов Вячеслав Ильич. – Москва, 2006. – 192 с. – URL: https://www.dissercat.com/content/mezhdunarodno-pravovye-aspekty-zashchity-kompyuternoi-informatsii (дата обращения: 10.08.2024). – Текст : электронный.

137. Черных, И. А. Международно-правовые аспекты обеспечения устойчивости космической деятельности : диссертация на соискание степени кандидата юридических наук : 12.00.10 / Черных Ирина Алексеевна. – Москва, 2018. – 257 с. – URL: http://dissovet.rudn.ru/web-

local/prep/rj/index.php?id=37&mod=dis&dis_id=2156 (дата обращения: 10.08.2024). – Текст : электронный.

138. Штодина, Д. Д. Международно-правовой режим киберпространства: позиция США : диссертация на соискание ученой степени кандидата юридических наук : 5.1.5 / Штодина Дарья Дмитриевна. – Москва, 2023. – 313 с. – URL: https://mgimo.ru/science/diss/shtodina-d-d.php?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 10.08.2024). – Текст : электронный.

139. Яникеева, И. О. Фактор международной информационной безопасности в двусторонних отношениях России и США в XXI веке : диссертация на соискание степени кандидата политических наук : 5.5.4 / Яникеева Инна Олеговна. – Москва, 2023. – 269 с. – URL: https://viewer.rsl.ru/ru/rsl01011749760 (дата обращения: 10.08.2024). – Текст : электронный.

140. Kyslytsya, I. International Cooperation in Ensuring International Information Security : Thesis for the degree of Master of Arts in International Relations / I. Kyslytsya ; Central European University Department of International Relations. – Vienna, Austria, 2021. – URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwix8uH2zob3AhXBAxAIHd9_ApQQFnoECA8QAQ&url=https%3A%2F%2Fwww.etd.ceu.edu%2F2021%2Fkyslytsya_ian.pdf&usg=AOvVaw2jaEt9GZg1Thw0CJ8SjYsV/ (дата обращения: 10.08.2024). – Текст : электронный.

141. Mejia, M. Criminal and Regulatory law in the international legal framework for maritime security. Law and ergonomics in maritime security : doctoral thesis / M. Mejia ; Department of Design Sciences, Lund University. – Lund, 2007.

VI. Книги и статьи иностранных авторов

142. Эннан, Р. Е. Формирование международного информационного права / Р. Е. Эннан // Правове життя сучасної України : матеріали Міжнар. наук. конф. проф.-викл. та аспірант. складу, м. Одеса, 16–17 травня 2013 р. / відп. за вип. В. М. Дрьомін ; НУ "ОЮА". Півд. регіон. центр НАПрН України. – Одеса : Фенікс, 2013. – Т. 2. – С. 661–664.

143. Al Ali, N. A. R. Cyber security in marine transport: opportunities and legal challenges / N. A. R. Al Ali, A. A. Chebotareva, V. E. Chebotarev. – Текст : электронный // Scientific Journal of Maritime Research. – 2021. – Vol. 35. – P. 248–255. – URL: https://hrcak.srce.hr/file/387886 (дата обращения: 10.08.2024).

144. Alshaer, M. Cyber attacks on satellites: Review and solutions / M. lshaer. – URL: https://www.academia.edu/18156391/Cyber_attacks_on_satellites_Review_and_solutions (дата обращения: 10.08.2024). – Текст : электронный.

145. Attaran, M. Information technology and business-process redesign / M. Attaran // Business Process Management Journal. – 2003. – Vol. 4. – P. 440–458.

146. Baram, G. Cyber Threats to Space Systems / G. Baram, O. Wechsler. – URL: https://www.researchgate.net/publication/342666394_Cyber_Threats_to_Space_Systems_-_Current_Risks_and_the_Role_of_NATO (дата обращения: 10.08.2024). – Текст : электронный.

147. Barlow, J. P. A Declaration of the Independence of Cyberspace / J. P. Barlow. – URL: https://www.eff.org/cyberspace-independence/ (дата обращения: 10.08.2024). – Текст : электронный.

148. Boar, B. H. Strategic Thinking for Information Technology: How to Build the IT Organization for the Information Age / B. H. Boar. – New York, NY : John Wiley and Sons, Inc., 1997. – 270 p.

149. Boutet, A. Pêche et TIC / A. Boutet, C. Chauvin, G. Morel, G. Tirilly. – Текст : электронный // Marsouin. – URL: https://www.marsouin.org/IMG/pdf/Rapport_final___Peche_et_TIC.pdf (дата обращения: 10.08.2024).

150. Brown, G. The Customary International Law of Cyberspace / G. Brown, K. Poellet. – Текст : электронный // Strategic Studies Quarterly, 2012. – Vol. 6, No. 3. – P. 126–145. – URL: https://www.jstor.org/stable/26267265 (дата обращения: 10.08.2024).

151. Burgelman, R. A. Strategic Management of Technology and Innovation / R. A. Burgelman, C. M. Christensen, S. C. Wheelwright. – 5th edition. – New York : McGraw-Hill, 2009. – 1264 p.

152. Burnett, D. R. Submarine Cable Security and International Law / D. R. Burnett. – Текст : электронный. // International Law Studies, Stockton Center for International Law. – 2021. – Vol. 97. – URL: https://digital-commons.usnwc.edu/ils/vol97/iss1/55/ (дата обращения: 10.08.2024).

153. Davenport, T. Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis / T. Davenport. – Текст : электронный // Catholic University Journal of Law and Technology. – 2015. – Vol. 24, Issue 1, Article 4. – URL: https://scholarship.law.edu/jlt/vol24/iss1/4/ (дата обращения: 10.08.2024).

154. De Gouyon Matignon, L. The International Telecommunication Union De / L. Gouyon Matignon. – URL: www.spacelegalissues.com/space-law-the-international-telecommunication-union/ (дата обращения: 10.08.2024). – Дата публикации: 21.02.2019. – Текст : электронный.

155. Ducruet, C. Maritime Networks: Spatial structures and time dynamics (Routledge Studies in Transport Analysis) / C. Ducruet. – 1st edition. – London, United Kingdom : Taylor & Francis Ltd, 2016. – 196 p.

156. Existing and potential threats. – URL: https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/existing-and-potential-threats (дата обращения: 10.08.2024). – Дата публикации: 14.12.2021. – Текст : электронный.

157. Fitton, O. The Future of Maritime Cyber Security / O. Fitton, D. Prince, B. Germond, M. Lacy. – Lancaster University, 2015. – URL: https://eprints.lancs.ac.uk/id/eprint/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf (дата обращения: 10.08.2024). – Текст : электронный.

158. Godwin III, J. B. Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2 / J. B. Godwin III, A. Kulpin, K. F. Rauscher, V. Yaschenko. – East West Institute and the Information Security Institute of Moscow State University, 2014. – URL: https://www.files.ethz.ch/isn/178418/terminology2.pdf (дата обращения: 10.08.2024). – Текст : электронный.

159. Goldsmith, J. L. Against Cyberanarchy / J. L. Goldsmith. – Текст : электронный // University of Chicago Law Review. – 1998. –Vol. 65, Iss. 4, Article 2.

– – URL: https://chicagounbound.uchicago.edu/uclrev/vol65/iss4/2/ (дата обращения: 10.08.2024).

160. Greenwood, C. Sources of International Law: An Introduction / C. Greenwood. – URL: https://legal.un.org/avl/ls/Greenwood_IL.html (дата обращения: 10.08.2024). – Текст : электронный.

161. Grossman, C. M. ILC Report on Prevention and Punishment of Crimes Against Humanity and Enforced Disappearance / C. M. Grossman ; American University Washington College of Law. – URL: https://works.bepress.com/claudio_grossman/166/ (дата обращения: 10.08.2024). – Дата публикации: 20.08.2019. – Текст : электронный.

162. Hathaway, O. The Law of Cyber-Attack / O. Hathaway, R. Crootof, P. Levitz [et al.]. – Текст : электронный // California Law Review. – 2011. – URL: https://openyls.law.yale.edu/handle/20.500.13051/3283 (дата обращения: 10.08.2024).

163. Hollander, A. Accounting, information technology, and business solutions / A. Hollander, E. Denna, J. O. Cherrington. – 2nd edition. – New York : McGraw-Hill Higher Education, 1999. – 600 p.

164. Ifeanyi, A. The impact of Information and Communication Technology (ICT) on News Processing, Reporting and Dissemination on Broadcast stations in Lagos, Nigeria / A. Ifeanyi. – 2012. – URL: http://www.researchgate.net/publication/280049026_The_impact_of_Information_and_Communication_Technology_ict_on_News_Processing_Reporting_and_Dissemination_on_Broadcast_stations_in_Lagos_Nigeria/ (дата обращения: 10.08.2024). – Текст : электронный.

165. Institute Cyber Attack Exclusion Clause – Cl.380. – 2003. – URL: https://www.modernaforsakringar.se/siteassets/documents/foretag--industri/villkorsbanken/foretagsforsakring/allmanna-villkor/transport/institute-cyber-attack-exclusion-clause---cl-380-vst-24-1-.pdf (дата обращения: 10.08.2024). – Текст : электронный.

166. Ittelson, P. What’s new with cybersecurity negotiations? UN Cyber OEWG Final Report analysis / P. Ittelson. – URL: www.diplomacy.edu/blog/whats-new-

cybersecurity-negotiations-un-cyber-oewg-final-report-analysis/ (дата обращения: 10.08.2024). – Дата публикации: 19.03.2021. – Текст : электронный.

167. Johnson, D. R. Law and Borders: The Rise of Law in Cyberspace / D. R. Johnson, D. Post. – Текст : электронный. // Stanford Law Review. – 1996. – Vol. 48, No. 5. – P. 1367–1402. – URL: https://www.researchgate.net/publication/220167912_Law_and_Borders_The_Rise_of_Law_in_Cyberspace (дата обращения: 10.08.2024).

168. Kapilidis, C. Cybersecurity challenges for the maritime industry / C. Kapilidis. – URL: https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/ (дата обращения: 10.08.2024). – Дата публикации: 30.08.2019. – Текст : электронный.

169. Karlsson, J. The future of maritime cybersecurity. Secure State Cyber / J. Karlsson. – URL: https://www.securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/ (дата обращения: 10.08.2024). – Текст : электронный.

170. Keir, G. Divided by a common language: Cyber definitions in Chinese, Russian and English / G. Keir, W. Hagestad. – Текст : электронный // 5th International Conference on Cyber Conflict, 2013. – URL: www.researchgate.net/publication/261300676_Divided_by_a_common_language_Cyber_definitions_in_Chinese_Russian_and_English/ (дата обращения: 10.08.2024).

171. Kulesza, J. International Internet Law. – Routledge Research in Information Technology and E-Commerce Law / J. Kulesza. – 1st Edition. – 2012. – 196 p.

172. Laudon, K. C. Management information systems: Organization and technology in the networked enterprise / K. C. Laudon, J. P. Laudon. – Upper Saddle River : Prentice Hall, 2000. – 588 p.

173. Lessig, L. Code and Other Laws of Cyberspace / L. Lessig. – URL: https://books.google.ru/books/about/Code.html?id=swD6jNulNYEC&redir_esc=y/ (дата обращения: 10.08.2024). – Текст : электронный.

174. Lessig, L. The Path of Cyberlaw / L. Lessig. – Текст : электронный // University of Chicago Law School Chicago Unbound Journal Articles. – 1995. – URL:

https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=11678&context=journal_articles/ (дата обращения: 10.08.2024).

175. Lilly, B. The Past, Present, and Future of Russia’s Cyber Strategy and Forces, 2020 / B. Lilly, J. Cheravitch. – Текст : электронный // 12th International Conference on Cyber Conflict (CyCon), Estonia, 2020. – P. 129–155. – URL: https://ieeexplore.ieee.org/document/9131723 (дата обращения: 10.08.2024).

176. Lotrionte, C. Expanding the Mandate of the ITU? / C. Lotrionte – Текст : электронный // 2013 World Cyberspace Cooperation Summit IV (WCC4), Silicon Valley, CA, USA, 2013. – P. 1–7. – URL: https://ieeexplore.ieee.org/document/7050501 (дата обращения: 10.08.2024).

177. Mendonça H. C. Cyberspace in Outer Space: New Challenges, New Responses / H. C. Mendonça. – URL: https://interactive.satellitetoday.com/via/january-2017/cyberspace-in-outer-space-new-challenges-new-responses/ (дата обращения: 10.08.2024).– Текст : электронный.

178. Modalities of multistakeholder participation. – URL: https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/modalities-of-multistakeholder-participation (дата обращения: 10.08.2024). – Дата публикации: 13.12.2021. – Текст : электронный.

179. Morozova, E. International Space Law and Satellite Telecommunications / E. Morozova, Y. Vasyanin. – URL: https://archive.org/details/acrefore-9780190647926-e-75 (дата обращения: 10.08.2024). – Дата публикации: 23.12.2019. – Текст : электронный.

180. Moynihan, H. The Application of International Law to State Cyberattacks. Research paper / H. Moynihan. – URL: https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/6-processes-reaching-agreement-application/ (дата обращения: 10.08.2024). – Дата публикации: 02.12.2019. – Текст : электронный.

181. O'Connor, T. As Biden Puts US on Alert, Russia Seeks Talks to Help Prevent Cyber War / T. O'Connor. – URL: https://www.newsweek.com/biden-puts-us-alert-

russia-seeks-talks-help-prevent-cyber-war-1690673/ (дата обращения: 10.08.2024). – Дата публикации: 22.03.2022. – Текст : электронный.

182. OEWG 2021-2025 – Regular institutional dialogue. – URL: https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/oewg-2021-2025-regular-institutional-dialogue (дата обращения: 10.08.2024). – Дата публикации: 01.04.2022. – Текст : электронный.

183. OEWG 2021-2025 Organisational session, 1 Jun 2021. – URL: https://dig.watch/updates/oewg-2021-2025-holds-organisational-session (дата обращения: 10.08.2024). – Текст : электронный.

184. Ogundare, B. International Maritime Organisation Framework on Cyber Risk Management – a Case for a Comprehensive Legal Framework / B. Ogundare, G. Akinwande. – Текст : электронный // Maritime Safety and Security Law Journal. – URL: https://www.marsafelawjournal.org/wp-content/uploads/2021/12/MarSafeLaw-Journal_Issue-9_2021-1.pdf (дата обращения: 10.08.2024).

185. Polanski, P. Cyberspace: A new branch of international customary law? / P. Polanski – Текст : электронный // Computer Law & Security Review. – 2017. – URL: https://www.researchgate.net/publication/315937970_Cyberspace_A_new_branch_of_international_customary_law (дата обращения: 10.08.2024).

186. Regular institutional dialogue. – URL: https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/regular-institutional-dialogue (дата обращения: 10.08.2024). – Дата публикации: 17.12.2021. – Текст : электронный.

187. Rodriguez, F. Are Poor Countries Losing the Information Revolution? MfoDev Working Paper / F. Rodriguez, E. Wilson. – Washington D.C. : World Bank, 2000. – URL: https://documents1.worldbank.org/curated/en/600361468762019045/pdf/266510WP0Scode1tries0losing0Infodev.pdf (дата обращения: 10.08.2024). – Текст : электронный.

188. Schmitt, M. N. The Nature of International Law Cyber Norms / M. N. Schmitt, L. Vihul. – Текст : электронный // International Cyber Norms: Legal, Policy & Industry Perspectives / A.-M. Osula, H. Rõigas (Eds.). – Tallinn : NATO CCD COE Publications,

2016. – URL: https://www.ccdcoe.org/uploads/2018/10/ InternationalCyberNorms_Ch2.pdf (дата обращения: 10.08.2024).

189. Shadbolt, L. Technical Study Satellite Cyber attacks and Security / L. Shadbolt. – Текст : электронный // HDI Global Specialty SE. – 2021, July. – URL: www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite_Cyberattack_whitepaper.pdf (дата обращения: 10.08.2024).

190. Significant Cyber Incidents Since 2006. – URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (дата обращения: 10.08.2024). – Текст : электронный.

191. Slaughter, A.-M. International Law and International Relations Theory: A Dual Agenda / A.-M. Slaughter. – Текст : электронный // American Journal of International Law. – 1993. – Vol. 87, Issue 2. – P. 205–239. – URL: www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/international-law-and-international-relations-theory-a-dual-agenda/04816F63C68ACF71DEF4555E1C470D27/ (дата обращения: 10.08.2024).

192. Stadnik, I. What Is an International Cybersecurity Regime and How We Can Achieve It? / I. Stadnik. – Текст : электронный. // Masaryk University Journal of Law and Technology. – 2017. – URL: https://www.researchgate.net/publication/318075735_What_Is_an_International_Cyber security_Regime_and_How_We_Can_Achieve_It (дата обращения: 10.08.2024).

193. Stremlau, T. The vulnerability of satellite communications / T. Stremlau. – URL: www.securitymagazine.com/articles/94689-the-vulnerability-of-satellite-communications/ (дата обращения: 10.08.2024). – Дата публикации: 19.04.2021. – Текст : электронный.

194. The risk of cyber-attack to the maritime sector. – – Текст : электронный // MARSH. – Global Marine Practice. – 2014, July. – URL: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/The%20Risk%20of%20Cyber-Attack%20 to%20the%20Maritime%20Sector-07-2014.pdf (дата обращения: 10.08.2024).

195. Tiirmaa-Klaar, H. The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting

Body / H. Tiirmaa-Klaar. – Текст : электронный // Cyberstability Paper Series. – 2021, December. – URL: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf (дата обращения: 10.08.2024).

196. Turban, E. Information technology for management: Transforming organizations in the digital economy / E. Turban, E. McLean, J. Wetherbe, D. Leidner. – Hoboken : John Wiley and Sons, 2004. – 784 p.

197. UN OEWG 2021–2025 – Confidence building measures. – URL: https://dig.watch/events/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-confidence-building-measures (дата обращения: 10.08.2024). – Дата публикации: 31.03.2022. – Текст : электронный.

198. UN OEWG 2021–2025 – International law. – URL: https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-international-law (дата обращения: 10.08.2024). – Дата публикации: 30.03.2022. – Текст : электронный.

199. UN OEWG 2021–2025 – Organisation of work. – URL: https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/oewg-2021-2025-organisation-of-work (дата обращения: 10.08.2024). – Дата публикации: 28.03.2022. – Текст : электронный.

200. UN OEWG 2021–2025 – Rules, norms, and principles of responsible state behaviour in cyberspace. – URL: https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-rules-norms-and-principles-of-responsible-state-behaviour-in-cyberspace (дата обращения: 10.08.2024). – Дата публикации: 30.03.2022. – Текст : электронный.

201. United Nations Documents on the Development and Codification of International Law // Supplement to American Journal of International Law. – 1947. – Vol. 41, No. 4. – P. 127.

202. US-Russia Cybersecurity Cooperation: Future Paths and Historical Perspective. – URL: https://geohistory.today/us-russia-cybersecurity-cooperation/ (дата обращения: 10.08.2024). – Дата публикации: 04.12.2021. – Текст : электронный.

203. Weeden, B. Global Counterspace Capabilities: An Open Source Assessment / B. Weeden, V. Samson. – Текст : электронный // Secure World Foundation. – 2018, April. – URL: https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf (дата обращения: 10.08.2024).

204. What’s new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted. – URL: www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/ (дата обращения: 10.08.2024). – Дата публикации: 13.08.2022. – Текст : электронный.

205. Young, O. R. The Politics of International Regime Formation: Managing Natural Resources and the Environment / O. R. Young. – Текст : электронный // International Organization. – 1989. – Vol. 43, No. 3. – P. 349–375. – URL: http://www.jstor.org/stable/2706651 (дата обращения: 10.08.2024).

VII. Интернет-ресурсы

206. Библиотека Организации Объединенных Наций. – URL: https://www.un.org/library (дата обращения: 10.08.2024). – Текст : электронный.

207. Издательство «Юридическая литература» Администрации Президента Российской Федерации. – URL: http://jurizdat.ru/index.htm (дата обращения: 10.08.2024). – Текст : электронный.

208. Информационное Агентство «АИС». – URL: https://vg-news.ru/ (дата обращения: 10.08.2024). – Текст : электронный.

209. Международный союз электросвязи. – URL: http://www.itu.int/ru/about/ (дата обращения: 10.08.2024). – Текст : электронный.

210. Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 10.08.2024). – Текст : электронный.

211. Официальный сайт МИД России. – URL: http://mid.ru (дата обращения: 10.08.2024). – Текст : электронный.

212. Сетевое издание «Коммерсантъ». – URL: https://www.kommersant.ru (дата обращения: 10.08.2024). – Текст : электронный.

213. Словари. Краткий словарь. – URL: http://slovo.yaxy.ru (дата обращения: 10.08.2024). – Текст : электронный.

214. Собрание законодательства Российской Федерации (электронные версии периодических изданий). – URL: https://www.szrf.ru (дата обращения: 10.08.2024). – Текст : электронный.

215. Справочная-правовая система «КонсультантПлюс». Версия Проф. – URL: https://www.consultant.ru (дата обращения: 10.08.2024). – Текст : электронный.

216. Цифровая библиотека Организации Объединенных Наций. – URL: https://digitallibrary.un.org/?ln=ru (дата обращения: 10.08.2024). – Текст : электронный.

217. Электронная библиотека исторических документов. – URL: https://docs.historyrussia.org/ru/nodes/1-glavnaya (дата обращения: 10.08.2024). – Текст : электронный.

218. Электронный фонд правовых и нормативно-технических документов «Техэксперт/Кодекс». – URL: https://docs.cntd.ru (дата обращения: 10.08.2024). – Текст : электронный.

219. Юридическая информационная система «Легалакт – законы, кодексы и нормативно-правовые акты Российской Федерации». – URL: https://legalacts.ru (дата обращения: 10.08.2024). – Текст : электронный.

220. Enterprise Search engine for the United Nations. – URL: https://search.un.org (дата обращения: 10.08.2024). – Текст : электронный.

221. European Telecommunication Standards Institute. – URL: https://www.etsi.org/ (дата обращения: 10.08.2024). – Текст : электронный.

222. Geneva Internet Platform Digiital Watch. – URL: https://dig.watch (дата обращения: 10.08.2024). – Текст : электронный.

223. International Organization for Standardization. – URL: http://www.iso.org/ (дата обращения: 10.08.2024). – Текст : электронный.

224. UNESCO Institute of Statistics Glossary. – URL: https://uis.unesco.org/en/home/ (дата обращения: 10.08.2024). – Текст : электронный.

225. United Nations Office for Disarmanent Affairs. – URL: https://disarmament.unoda.org (дата обращения: 10.08.2024). – Текст : электронный.

226. United Nations Office of Legal Affairs. – URL: https://www.un.org/ola/(дата обращения: 10.08.2024). – Текст : электронный.

227. United Nations Treaty Collection. – URL: https://treaties.un.org/pages/Home.aspx?clang=_en (дата обращения: 10.08.2024). – Текст : электронный.

Приложение А
(обязательное).
Проект конвенции по учреждению организации ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий

ПРОЕКТ КОНВЕНЦИИ ПО УЧРЕЖДЕНИЮ ОРГАНИЗАЦИИ ООН ПО ВОПРОСАМ БЕЗОПАСНОСТИ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И САМИХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Договаривающиеся стороны,

признавая общую заинтересованность всего мирового сообщества в развитии использования информационно-коммуникационных технологий (ИКТ) в мирных целях, за каждым Государством суверенное право регламентировать использование ИКТ на национальном уровне, необходимость прогрессивного развития международного права и адаптации как национального, так и на международного регулирования использования ИКТ с учетом их специфики на фоне технического прогресса, необходимым сохранение в Организация Объединенных Наций (ООН) единого переговорного механизма и консолидации усилий различных площадок ООН в этой сфере;

приветствуя дальнейшую разработку норм «мягкого права», выступающего комплементарным механизмом, который не должен заменить универсальный международно-правовой акт, а лишь отражать перспективные направления развития правового регулирования использования ИКТ на универсальном уровне;

осознавая, что дальнейшие разработки и использование ИКТ должны быть направлены на благо всего человечества;

полагая, что Организация Объединенных Наций должна содействовать международному сотрудничеству в сфере использования ИКТ;

желая систематизировать институциональные основы международного сотрудничества по обеспечению безопасности в сфере использования ИКТ в рамках ООН;

отмечая необходимость недопущения дублирования международных усилий, направленных на обеспечение безопасности в сфере использования ИКТ и самих ИКТ, согласились о нижеследующем:

Статья 1

Учреждение Организации

1. Настоящей Конвенцией учреждается постоянно действующая специализированная организация Организации Объединенных Наций по вопросам безопасности в сфере использования информационно-коммуникационных технологий – Международная организация по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ (далее – Организация).

Статья 2

Цели Организации

1. Организация имеет следующие цели:

a) поддержание и расширение международного сотрудничества между всеми его Государствами-Членами с целью обеспечения безопасности в сфере использования ИКТ и самих ИКТ;

b) согласование деятельности Государств-Членов и содействие плодотворному и конструктивному сотрудничеству и партнерству между Государствами-Членами;

c) содействие стабильному, безопасному и открытому информационному пространству, доступному для всех Государств;

d) создание всеобъемлющей системы обеспечения безопасности в сфере использования ИКТ и самих ИКТ;

e) разработка и принятие универсального международно-правового акта по обеспечению безопасности в сфере использования ИКТ и самих ИКТ;

Статья 3

Принципы функционирования

1. Организация будет осуществлять свою деятельность на основе следующих принципов:

a) уважение принципов Устава ООН;

b) уважение суверенитета Государств в информационном пространстве, признание их права на защиту своей критической информационной инфраструктуры и данных;

c) признание, что безопасность одного Государства не должна укрепляться за счет безопасности других;

d) продвижение использования ИКТ в целях развития и благополучия человечества, предотвращение их использования для враждебных и военных целей;

e) универсальность и инклюзивность: Организация должна обеспечивать участие всех заинтересованных сторон - Государств-Членов ООН, международных организаций, частного сектора, научного сообщества и гражданского общества;

f) гибкость и адаптивность: в связи с быстрым развитием ИКТ, Организация должна быть способна адаптироваться к новым вызовам и технологиям;

g) сбалансированность и равноправие интересов: необходимо учитывать интересы развитых и развивающихся стран, обеспечивая равный доступ к технологиям и защиту информационного пространства;

h) открытость: Организация должна обеспечивать прозрачность и доступность информации о своей деятельности.

Статья 4

Направления деятельности

1. Содействие обеспечению международной безопасности в сфере использования ИКТ и самих ИКТ и международному сотрудничеству в данной области в мирных целях.

2. Координация международной деятельности и усилий, направленных на обеспечение безопасности в сфере использования ИКТ и самих ИКТ.

3. Прогрессивное развитие международного права, а также адаптация отраслевых международно-правовых норм к специфике ИКТ в дополнение к инициативам по принятию универсального международно-правового акта по регулированию ИКТ-среды.

4. Содействие имплементации международных стандартов и рекомендаций по обеспечению безопасности ИКТ, включая защиту инфраструктуры и данных.

5. Оказание помощи странам в имплементации международных стандартов и рекомендаций на национальном уровне.

6. Отслеживание угроз безопасности в сфере использования ИКТ, анализ и распространение информации о лучших практиках и решениях.

7. Разработка и реализация образовательных программ, направленных на повышение уровня осведомленности и понимания вопросов обеспечения безопасности в сфере использования ИКТ.

Статья 5

Особенности функционирования

1. Регулярный диалог: проведение ежегодной Конференции, открытой для всех Государств-Членов и заинтересованных сторон, и тематических заседаний для обмена опытом, обсуждения прогресса и планирования будущих действий.

2. Гибкое финансирование: обеспечение устойчивого финансирования Организации через взносы Государств-Членов, а также возможные вклады от частного сектора и других источников.

3. Преемственность: входе своей работы Организация будет учитывать прогресс, достигнутый в рамках созывов Группы правительственных экспертов ООН по международной информационной безопасности и Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ.

4. Консультации: помимо заседаний в ходе официальных сессий Организации Государства-Члены смогут проводить консультации с иными структурными подразделениями Организации в рамках своих усилий.

5. Вовлеченность в региональные процессы: Организация будет координировать свою работу с региональными и субрегиональными организациями.

Статья 6

Членство

1. Любое Государство, являющееся членом Организации Объединенных Наций, которое присоединяется к настоящей Конвенции.

Статья 7

Структура

1. Организация состоит из:

a) Конференции, которая является высшим органом Организации;

b) Комитетов;

c) Секретариата.

Статья 8

Конференция

1. Конференция образуется из делегаций, представляющих Государств-Членов Организации.

2. На Конференции рассматриваются важные вопросы деятельности Организации.

3. На Конференции ежегодно каждый Комитет отчитывается о своей работе в формате доклада.

4. Конференция созывается на ежегодной основе в качестве платформы для обсуждения всеми заинтересованными сторонами различных вопросов обеспечения безопасности в сфере использования ИКТ и самих ИКТ.

5. Конференция правомочна, если на ней присутствует более половины Государств-членов Организации.

6. В период между работой Конференции руководящую деятельность осуществляет Секретариат.

7. К компетенции Конференции также относится:

a) утверждение изменений и дополнений в настоящую Конвенцию;

b) определение приоритетных направлений и задач Организации;

c) раз в три года определение основных направления деятельности каждого комитета, формирование подкомитетов, утверждение плана работ, избирание Генерального директора и Государства-Члены комитетов;

d) принятие резолюций по вопросам, относящимся к обеспечению безопасности в сфере применения ИКТ и самих ИКТ;

e) решение стратегических вопросов Организации и иных вопросов в соответствии с настоящей Конвенцией.

Статья 9

Генеральный директор

1. Организацию возглавляет Генеральный директор, который избирается Конференцией сроком на три года.

2. Генеральный директор назначает на тот же срок своих Заместителей в соответствии с количеством функционирующих комитетов, которые не могут быть гражданами одного и того же Государства.

3. Генеральный директор возглавляет Секретариат и с помощью него координирует деятельность Организации.

4. Генеральный директор раз в два года будет представлять доклады Генеральной Ассамблее Организации Объединенных Наций о проделанной работе Комитетов.

5. Генеральный директор может предлагать на рассмотрение Конференции учреждение соответствующих комитетов из представителей Государств-Членов, которые занимаются конкретными вопросами, такими как разработка юридически обязательного универсального международно-правового акта и стандартов, мониторинг угроз, инициатив по мерам укрепления доверия и т.д., и другими возложенными на него обязательствами.

Статья 10

Секретариат

1. Секретариат – выборный, постоянно действующий коллегиальный руководящий орган Организации.

2. Секретариат является административным органом Организации, организует и руководит всей деятельностью Организации и правомочно решать любые вопросы её деятельности, кроме вопросов, относящихся к исключительной компетенции Конференции.

3. Секретариат выполняет функцию координационного центра по международному сотрудничеству по вопросам обеспечения безопасности в сфере использования ИКТ и самих ИКТ.

4. Секретариат ответственен за координацию работы Организации, обеспечение связей с другими органами Организации Объединенных Наций, а также взаимодействия с другими международными организациями и объединениями, региональными инициативами и ключевыми заинтересованными сторонами.

Статья 11

Комитеты

1. Комитеты Организации подразделяются на региональные и функциональные.

2. Региональные комитеты Организации будут созданы для развития международного сотрудничества с целью обеспечения безопасности в сфере применения ИКТ и прогрессивного развития международно-правового регулирования ИКТ-проблематики с опорой на региональный опыт.

3. Функциональные Комитеты Организации подразделяются на постоянно действующие и временные.

4. Наименование, направление деятельности и план работы Комитетов утверждает Конференция.

5. Постоянно действующими комитетами Организации являются:

a) Комитет по исследованию угроз в сфере применения ИКТ и самих ИКТ;

b) Комитет по правовым вопросам (подкомитет по общим вопросам международного права, подкомитет по отраслевым вопросам международного права, подкомитет по гармонизации понимания и трактовки терминов, связанных с ИКТ);

c) Комитет по мерам укрепления доверия;

d) Комитет по содействию наращиванию потенциала.

6. При необходимости Конференцией может быть принято решение о создании дополнительных временных и/или постоянно действующих комитетах.

7. В состав каждого постоянного Комитета войдут все Государства-Члены Организации.

8. В состав каждого временного Комитета войдет 36 членов Организации, избираемых в ходе Конференции на трехгодичный срок в соответствии с принципами справедливого географического представительства.

9. Каждое Государство-Член имеет право участвовать в деятельности структурных подразделений Организации и представлять кандидатов для избрания в качестве избираемых служащих.

10. В рамках деятельности Комитетов могут привлекаться приглашенные эксперты из академического сообщества, частного сектора и гражданского общества, для учета мнения всех заинтересованных сторон на основе справедливого географического представительства.

Статья 12

Принятие решений

1. Каждое Государство-Член имеет право на один голос на всех конференциях и заседаниях структурных подразделений Организации.

2. Организация и ее структурные подразделения принимают свои решения большинством в две трети поданных голосов.

3. Голоса воздержавшихся в расчет не принимаются.

Статья 13

Языки

1. Официальными и рабочими языками являются английский, арабский, испанский, китайский, русский и французский.

2. Указанные языки используются для составления и публикации документов и текстов Комитета в эквивалентных по форме и содержанию версиях, а также при взаимном устном переводе на его мероприятиях.

Статья 14

Отношения с другими организациями

1. Организация, если это целесообразно, устанавливает рабочие отношения и сотрудничает с другими межправительственными организациями. Любое соглашение об этом, достигнутое с такими организациями, заключается Генеральным директором после одобрения Конференцией.

2. Организация может по вопросам своей компетенции проводить соответствующие мероприятия по консультациям и сотрудничеству с международными неправительственными организациями, а также с согласия заинтересованных правительств с национальными организациями, правительственными или неправительственными. Такие мероприятия проводятся Генеральным директором после одобрения Конференцией.

Статья 15

Подписание, ратификация Конвенции и присоединение к ней

1. Государства, упомянутые в статье 6, могут стать сторонами настоящей Конвенции и членами Комитета путем:

a) подписания Конвенции без оговорки о ратификации;

b) подписания с оговоркой о ратификации, после которого последует депонирование ратификационной грамоты; или

c) депонирования акта о присоединении.

2. Ратификационные грамоты или акты о присоединении депонируются у Генерального директора.

Статья 16

Вступление в силу Конвенции

1. Настоящая Конвенция вступает в силу в отношении любого Государства через три месяца после даты, на которую такое Государство предприняло действия, предусмотренные в статье 15.

Статья 17

Поправки

1. Предложения о внесении поправок в настоящую Конвенцию могут быть направлены в Секретариат любым государством-подписантом Конвенции не позднее чем за полгода до очередной Конференции для ее рассмотрения.

2. Для принятия соответствующей поправки, она должна быть одобрена на пленарном заседании по крайней мере двумя третями делегаций, аккредитованных на Конференции.

Статья 18

Денонсация

1. Любое Государство-Член имеет право денонсировать настоящую Конвенцию путем нотификации, адресованной Генеральному директору.

2. Денонсация вступает в действие по истечении шести месяцев с даты получения такой нотификации Генеральным директором.

Статья 19

Заключительные положения

1. Настоящая Конвенция сдается на хранение Генеральному директору.

2. Генеральный директор:

a) информирует все государства, подписавшие настоящую Конвенцию или присоединившиеся к ней, а также всех членов Организации о:

i) каждом новом подписании Конвенции или сдаче на хранение документа о ратификации, принятии, утверждении или присоединении с указанием их даты;

ii) дате вступления настоящей Конвенции в силу;

iii) сдаче на хранение любого документа о денонсации настоящей Конвенции с указанием даты его получения и даты вступления денонсации в силу;

iv) получении любого заявления или уведомления, сделанного в соответствии с настоящей Конвенцией;

b) направляет заверенные копии с подлинного текста настоящей Конвенции всем государствам, подписавшим Конвенцию или присоединившимся к ней.

3. Как только настоящая Конвенция вступит в силу, заверенная копия с ее подлинного текста направляется депозитарием Генеральному секретарю Организации Объединенных Наций для регистрации и опубликования в соответствии с статьей 102 Устава Организации Объединенных Наций.

4. Настоящая Конвенция подписывается в единственном экземпляре на английском, арабском, испанском, китайском, русском и французском языках, причем каждый текст равно аутентичен.