НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ В СРЕДЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

КОЛЛЕКТИВНАЯ МОНОГРАФИЯ ПО ПРОБЛЕМЕ ПРИМЕНЕНИЯ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ

НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ В СРЕДЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде

Под редакцией проф. А.А. Стрельцова, проф. А.Я. Капустина,
проф. Т.А. Поляковой, проф. А.С. Маркова, Б.Н. Мирошникова

Москва — 2023

Редакционная группа

А.А. Стрельцов, вице-президент НАМИБ, доктор юридических наук, доктор технических наук, профессор, ведущий научный сотрудник факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова

А.Я. Капустин, член НАМИБ, доктор юридических наук, профессор, Президент Российской ассоциации международного права, заведующий кафедрой, руководитель международно-правового направления Института законодательства и сравнительного правоведения при Правительстве Российской Федерации

Т.А. Полякова, член НАМИБ, доктор юридических наук, профессор, главный научный сотрудник, и.о. заведующего сектором информационного права и международной безопасности Института государства и права Российской академии наук

А.С. Марков, член НАМИБ, доктор технических наук, профессор, Президент компании «Эшелон»

Б.Н. Мирошников, вице-президент НАМИБ, кандидат юридических наук

Рецензенты

Е.С. Зиновьева, доктор политических наук, профессор, заместитель директора Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России

И.В. Сурма, кандидат экономических наук, доцент, заведующий кафедрой Дипломатической академии МИД России

От авторов

Авторы выражают глубокую признательность Президенту Национальной Ассоциации международной информационной безопасности, член-корреспонденту Академии криптографии Российской Федерации, советнику Секретаря Совета Безопасности Российской Федерации Шерстюку Владиславу Петровичу за содействие и большое внимание, проявленные к авторскому коллективу, ценные советы и рекомендации по направлениям исследования и содержания монографии, а также личное участие в обсуждении полученных результатов.

Авторы выражают благодарность рецензентам монографии — заместителю директора Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России, доктору политических наук, профессору Зиновьевой Елене Сергеевне и заведующему кафедрой Дипломатической академии МИД России, кандидату экономических наук, доценту Сурме Ивану Викторовичу за замечания и предложения, которые были учтены при подготовке монографии к печати.

Список сокращений

АСЕАН — Ассоциация государств Юго-Восточной Азии

БРИКС — межгосударственное объединение Федеративной Республики Бразилии, Российской Федерации, Республики Индии, Китайской Народной Республики и Южно-Африканской Республики

ГосСОПКА — Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

ГПЭ — Группа правительственных экспертов

ГРИИБ — Группа реагирования на инциденты информационной безопасности (англ. CSIRT)

ГРКИ — Группа реагирования на компьютерные инциденты (англ. CERT)

ЕАЭС — Евразийский экономический союз

ЕС — Европейский Союз

ИКТ — информационные и коммуникационные технологии

ЛАГ — Лига арабских государств

МГС СНГ — Межгосударственный совет по стандартизации, метрологии и сертификации Содружества Независимых Государств

МИБ — международная информационная безопасность

НИР — Научно-исследовательская работа

НКЦКИ — Национальный координационный центр по компьютерным инцидентам

ОДКБ — Организация Договора о коллективной безопасности

ООН — Организация Объединенных Наций

РГОС — Рабочая группа ООН открытого состава

СММИБ — система менеджмента международной информационной безопасности

СНГ — Содружество Независимых Государств

СОМИБ — система обеспечения международной информационной безопасности государства

УПК — Уголовно-процессуальный кодекс Российской Федерации

ЦРКИ — Национальный центр реагирования на компьютерные инциденты

ШОС — Шанхайская Организация Сотрудничества

CENELEC — Европейский комитет электротехнической стандартизации, отвечающий за европейские стандарты в области электротехники

EuroDIG — Европейский диалог по управлению Интернетом

Содержание

Сведения об авторах

1. Стрельцов Анатолий Александрович — вице-президент НАМИБ, дюн, дтн, проф., ведущий научный сотрудник факультета вычислительной математики и кибернетики Московского государственного университета имени М.В.Ломоносова, руководитель работы
2. Капустин Анатолий Яковлевич — член НАМИБ, дюн, проф., Президент Российской ассоциации международного права, заведующий кафедрой, руководитель международно-правового направления Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, руководитель временной творческой группы
3. Полякова Татьяна Анатольевна — член НАМИБ, дюн, проф., Институт государства и права Российской академии наук, руководитель временной творческой группы
4. Смирнов Александр Александрович — член НАМИБ, дюн, доцент, Институт государства и права Российской академии наук
5. Касёнова Мадина Балташевна — дюн, проф., МГИМО МИД России
6. Русинова Вера Николаевна — дюн, проф., Высшая школа экономики (НИУ ВШЭ)
7. Шинкарецкая Галина Георгиевна — дюн, проф., Институт государства и права Российской академии наук
8. Жарова Анна Константиновна — дюн, доцент, Институт государства и права Российской академии наук
9. Пилюгин Павел Львович — член НАМИБ, ктн, доцент, Московского государственного университета имени М.В.Ломоносова
10. Калицев Александр Евгеньевич — член НАМИБ
11. Горжалцан Владимир Ахиллович — Координационный центр домена «.RU»
12. Герасимов Андрей Васильевич — член НАМИБ, компания «Лаборатория Касперского»
13. Марков Алексей Сергеевич — член НАМИБ, дтн, проф., Группа компаний «Эшелон», руководитель временной творческой группы
14. Милославская Наталья Георгиевна — дтн, проф., Национальный исследовательский ядерный университет МИФИ
15. Мирошников Борис Николаевич — вице-президент НАМИБ, кюн, член Президиума НАМИБ, Группа компаний «Цитадель», руководитель временной творческой группы

16. Панин Александр Вячеславович — Автономная некоммерческая организация «Центр правовых исследований и международных коммуникаций»
17. Коротков Сергей Васильевич — член НАМИБ, квн, начальник отдела НАМИБ
18. Бойко Константин Сергеевич — член НАМИБ, эксперт НАМИБ
19. Волкова Светлана Геннадьевна — член НАМИБ, эксперт НАМИБ

Резюме

Цель научно-исследовательской работы (НИР) «Проблема применения норм ответственного поведения государств в ИКТ-среде», выполненной в 2022 г. временным творческим коллективом по заказу Национальной Ассоциации международной информационной безопасности, заключалась в подготовке научно обоснованных рекомендаций по вопросам международного сотрудничества в области безопасного использования информационно-коммуникационных технологий (ИКТ) в формирующемся глобальном информационном обществе.

Исследование было направлено на «содействие выработке с учетом специфики информационно-коммуникационных технологий новых принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве»[1] в целях «установления международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий»[2].

Фактическую основу исследования составили «нормы, правила и принципы ответственного поведения государств в ИКТ-среде», применение которых может «снизить риск нарушения международного мира, безопасности и стабильности»[3], сформулированные с учетом предложений Китая, России, Таджикистана и Узбекистана[4] и представленные в докладах Групп правительственных экспертов ООН (2015, 2021)[5].

Методологическую основу составили теоретические положения, обоснованные в результате выполнения исследовательского проекта «Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды» (2018–2020) [1]. Проект был реализован при поддержке Национальной Ассоциации международной информационной безопасности. В нем принимали участие эксперты Московского государственного университета имени М.В. Ломоносова

1 Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»

2 Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»

3 Резолюция Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности / A/RES/76/240 от 31 декабря 2020 года

4 Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при ООН на имя Генерального секретаря ООН / A/66/359, 12 сентября 2011 года

5 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности / A/70/174, 22 июля 2015 года
Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности / A/76/135, 14 июля 2021 года

(Россия), Института Восток-Запад (США), Института киберполитики (Эстония, Финляндия), Фонда «ИКТ для мира» (Швейцария).

В рамках выполнения НИР показано, что для практического применения норм ответственного поведения государств в ИКТ-среде необходимо решение проблем делимитации и демаркации зон ответственного поведения государств в ИКТ-среде, имплементации норм в национальное законодательство, а также развитие механизмов мирного разрешения споров, возникающих в связи с инцидентами в ИКТ-среде.

Научно-обоснованные рекомендации учтены при подготовке представленных в монографии предложений в проект позиции Российской Федерации по вопросам применения норм ответственного поведения государств в ИКТ-среде (Приложение 1); проекта универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде (Приложение 2); предложений по проекту международного стандарта технического регулирования в области менеджмента международной информационной безопасности (Приложение 3).

Результаты НИР доложены и одобрены на Международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности (г. Москва, 19–21 сентября 2022 г.), Международной конференции «Киберстабильность» (г. Москва, 11 декабря 2022 г.). Реферат по результатам исследования[6] представлен Председателю Рабочей группы ООН открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ 2021–2025 (г. Нью-Йорк, США, август 2022 г.).

Материалы монографии могут быть использованы представителями НАМИБ и заинтересованных федеральных органов государственной власти в процессе участия в деятельности РГОС и на других международных площадках по проблематике международной информационной безопасности.

6 Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество: Реферат по результатам исследования — М. 2022 // URL: https://namib.online/wp-content/uploads/2020/07/Brochure_IKT_rus_view.pdf

Предисловие

Одним из важных направлений поддержания международного мира и безопасности в условиях активного развития глобального информационного общества и формирования многополярного мира является обеспечение безопасного использования ИКТ и устойчивого функционирования ИКТ-среды.

Особую актуальность этому вопросу придает усиливающееся информационное противоборство, недобросовестная конкуренция и кибератаки со стороны недружественных государств на объекты информационной инфраструктуры Российской Федерации, что существенным образом меняет ситуацию на международной арене [2–6].

Как отметил Президент Российской Федерации на заседании Совета Безопасности Российской Федерации 26 марта 2021 г.: «Бурное развитие информационных технологий обеспечило невиданные ранее возможности во многих сферах, но принесло с собой и серьезные риски… Считаем необходимым заключить универсальные международно-правовые договоренности, направленные на предупреждение конфликтов и выстраивание взаимовыгодного партнерства в мировом информационном пространстве»[7].

Национальная Ассоциация международной информационной безопасности предпринимает усилия по использованию потенциала российских и зарубежных экспертов для проработки научно-обоснованных предложений по подготовке таких международно-правовых договоренностей.

В рамках решения этой задачи НАМИБ организовала выполнение научно-исследовательской работы по изучению проблемы практического использования норм ответственного поведения государств в ИКТ-среде, сформулированных в докладах Групп правительственных экспертов (2015, 2021)[8].

Применение указанных норм, по мнению участников 76-й сессии Генеральной Ассамблеи ООН, могло бы способствовать «снижению риска нарушения международного мира, безопасности и стабильности». Проработка вопросов применения этих норм и их имплементации в национальное законодательство включена в мандат Рабочей группы ООН открытого состава по вопросам безопасности использования ИКТ и самих ИКТ 2021–2025 [1–10].

---

7 URL: https://www.kremlin.ru/events/president/news/65231

8 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности A/70/174 от 22 июля 2015 года // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement; Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности A/76/135 от 14 июля 2021 года // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/88/PDF/N2107588.pdf?OpenElement

Участниками научно-исследовательской работы впервые проведено комплексное изучение проблем практического применения норм ответственного поведения государств в ИКТ-среде и сформулированы предложения по совершенствованию международно-правовых механизмов регулирования сотрудничества в области использования ИКТ в целях решения выявленных проблем. В работе принимали участие ведущие российские специалисты в области международного права и обеспечения информационной безопасности в ИКТ-среде.

Представленные в настоящей монографии рекомендации призваны также внести вклад в подготовку переговорных позиций уполномоченных органов государственной власти по вопросам продвижения российских инициатив, направленных на обеспечение безопасности в сфере использования ИКТ. Полученные результаты могли бы стать основой для предметных дискуссий на заседаниях Рабочей группы ООН открытого состава и других международных площадках.

Вниманию читателя предлагается коллективная монография, посвященная изучению проблемы практического применения норм ответственного поведения государств в ИКТ-среде.

Продолжение исследований в области практического применения норм ответственного поведения государств в ИКТ-среде на основе международного сотрудничества ученых и специалистов могло бы способствовать формированию системы международной информационной безопасности на основе равноправного сотрудничества суверенных государств — членов ООН.

Президент Национальной Ассоциации международной информационной безопасности **В.П. Шерстюк**

1. Проблемы международного сотрудничества в области безопасного использования ИКТ-среды

Мирошников Б.Н., Герасимов А.В., Коротков С.В., Стрельцов А.А.

1. Одной из наиболее актуальных задач обеспечения национальной безопасности Российской Федерации является укрепление суверенитета в информационном пространстве и, в частности, «установление международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий»[9].

По инициативе Российской Федерации вопрос о достижениях в сфере информатизации и коммуникаций в контексте международной безопасности уже более 20 лет находится в центре внимания участников сессий Генеральной Ассамблеи ООН.

Актуальность изучения этого вопроса и, прежде всего, проблем международного сотрудничества в области использования информационно-коммуникационных технологий (ИКТ), как отмечено в документах стратегического планирования Российской Федерации, сохраняется.

Так, в Стратегии национальной безопасности Российской Федерации отмечено, что одной из задач государственной политики в области информационной безопасности является «укрепление сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности, в том числе в целях установления международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий»[10].

В Доктрине информационной безопасности Российской Федерации среди основных направлений обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства выделено в качестве самостоятельного направления «создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования международных конфликтов в информационном пространстве» [11].

В Основах государственной политики Российской Федерации в области международной информационной безопасности поставлена задача «содействия выработке с учетом специфики информационно-коммуникационных технологий

9 Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»

10 Там же

новых принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве»[11].

Практическое применение норм и принципов международного права к отношениям в области использования ИКТ сталкивается с рядом серьезных трудностей, обусловленных новизной этих отношений и недостаточной изученностью проблемы в целом[12].

Впервые предложение о необходимости подготовки международного нормативного акта, направленного на регулирование отношений в ИКТ-среде, было представлено Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым осенью 2011 года на II Международной встрече высоких представителей, курирующих вопросы безопасности (г. Екатеринбург), в виде концепции конвенции об обеспечении международной информационной безопасности[13].

В том же году Китай, Россия, Таджикистан и Узбекистан представили Генеральной ассамблее ООН предложения по правилам поведения в области обеспечения международной информационной безопасности[14], к которым впоследствии в качестве соавторов присоединились Казахстан и Кыргызстан, и предложили рассмотреть эти правила с целью выработки консенсуса в отношении международных норм и правил, регулирующих действия государств в информационном пространстве[15].

Это способствовало включению в доклад Группы правительственных экспертов ООН (ГПЭ, 2015) добровольных и необязательных норм ответственного поведения государств в ИКТ-среде[16].

В докладе ГПЭ было отмечено, что «при рассмотрении вопроса о применимости норм международного права к использованию ИКТ государствами

---

11 Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»

12 Стрельцов А.А. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству. Digital report / 02.09.2015 // URL: https://digital.report/pravo-cyber-konfliktov/; Стрельцов А.А. О проблемах адаптации международного права к информационным конфликтам. Digital report./ 24.07.2015 // URL: https://digital.report/problemyi-adaptatsii-mezhdunarodnogo-prava-k-informatsionnyim-konfliktam/;
Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности A/76/135 от 14.07.2021 // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/88/PDF/N2107588.pdf?OpenElement

13 Конвенция об обеспечении международной информационной безопасности (концепция) 22.09.2011 // URL: https://www.mid.ru/ru/foreign_policy/official_documents/1698725/

14 Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при ООН от 12 сентября 2011 года на имя Генерального секретаря (A/66/359) // URL: https://digitallibrary.un.org/record/710973?ln=ru

15 Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при ООН от 9 января 2015 года на имя Генерального секретаря (A /69/723) // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/04/PDF/N1501404.pdf?OpenElement

16 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/70/174) 22.07.2015 // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement

определила, что важнейшее значение имеют обязанности государств в соответствии со следующими принципами Устава ООН и другими нормами международного права: суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями Организации Объединенных Наций; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств».

ГПЭ (2021) предложила новое понимание этих норм[17], которое принципиально не изменило общий подход предыдущей ГПЭ (2015) к регулированию международных отношений в ИКТ-среде.

В то же время, ГПЭ (2021), отметив, что нормы ответственного поведения государств в ИКТ-среде «сосуществуют с нормами и принципами международного права», по существу, признала наличие принципиальных отличий между механизмами применения этих двух нормативных механизмов регулирования международных отношений.

По резолюции 76-й сессии Генеральной Ассамблеи ООН[18] «продолжение в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств и путей их имплементации, а также при необходимости, внесения в них изменений или формулирования дополнительных правил поведения» стало составной частью мандата Рабочей группы ООН открытого состава (РГОС) по вопросам безопасности использования ИКТ и самих ИКТ 2021–2025.

Активная работа делегации Российской Федерации на заседаниях РГОС позволила сохранить этот очень важный орган ООН как перспективную площадку обсуждения путей решения проблем безопасного использования ИКТ-среды, действующую «на основе принципов универсальности, открытости, транспарентности и демократичности, а также ориентированности на достижение практических результатов»[19].

Председатель РГОС в своем резюме отметил, что, по мнению государств, «добровольные, не имеющие обязательной силы нормы ответственного поведения государств не изменяют и не заменяют собой нормы международного права, а скорее должны рассматриваться как согласующиеся с целями и прин-

17 Доклад ГПЭ (A/76/135), 14.07.2015

18 Резолюция ГА ООН Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности / A/RES/75/240 / 31.12.2022// URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement

19 Резолюции ГА ООН A/RES/73/27; A/RES/77/36

ципами ООН». Однако единое понимание механизма их согласования пока не сформировано.

Таким образом, разработка предложений по созданию таких условий, при которых оба выделенных способа нормативного регулирования международных отношений оказывают эффективное содействие поддержанию международного мира и безопасности, является важной задачей международного сотрудничества в области формирования системы международной информационной безопасности (МИБ).

2. В рамках осуществления уставной деятельности по «проработке в упреждающем режиме проблемных вопросов обеспечения МИБ в интересах формирования переговорных позиций государственных органов» Национальная Ассоциация международной и информационной безопасности в 2022 году выполнила НИР.

При проведении НИР учитывались результаты реализации международного исследовательского проекта по теме «Методологические вопросы применения норм, правил и принципов ответственного поведения государств в ИКТ-среде, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды» (2018–2020). В этом проекте приняли участие специалисты МГУ имени М.В. Ломоносова (Россия), Института Восток-Запад (США), Института киберполитики (Эстония, Финляндия) и Фонда «ИКТ для мира» (Швейцария). Предметом изучения явились три наиболее сложные нормы ответственного поведения из одиннадцати, предложенных в докладе ГПЭ (2015).

Однако, при общем понимании существования проблемы применения норм ответственного поведения государств в ИКТ-среде были выявлены разногласия фундаментального характера между российскими и западными участниками проекта по политическим и методологическим вопросам применения норм ответственного поведения[20]. Эти разногласия были вызваны, прежде всего, различиями в оценке политической целесообразности решения проблемы нормативного правового регулирования отношений в ИКТ-среде в условиях однополярного мира. Формирование многополярного мира придает особую актуальность поиску взаимоприемлемого способа преодоления существующих разногласий.

В НИР впервые проведено комплексное изучение проблемы совместного применения норм и принципов международного права, а также норм ответственного поведения государств в ИКТ-среде.

Можно выделить два основных аспекта проблемы практического применения норм ответственного поведения государств в ИКТ-среде в условиях применения норм и принципов международного права.

---

20 Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество. Реферат по результатам исследования. Москва. 2022 // URL: https://namib.online/wp-content/uploads/2020/07/Brochure_IKT_rus_view.pdf

Первым аспектом проблемы является неопределенность механизма применения норм и принципов международного права в ИКТ-среде.

Международное право, по мнению специалистов, представляет собой «систему обязательных норм, выраженных в признанных субъектами этого права источниках, являющихся обязательным критерием правомерно дозволенного и юридически недозволенного и через которые (нормы) осуществляется управление международным сотрудничеством в соответствующих областях или принуждение к соблюдению норм этого права»[21].

Субъектами международного права признаются лица:

- участвующие в международных отношениях и являющиеся носителями субъективных юридических прав и обязанностей;
- обладающие свойствами субъектов в силу норм международного права;
- обладающие правоспособностью, дееспособностью и деликтоспособностью.

Речь идет, в первую очередь, о государствах, существование которых в юридическом смысле связано с обладанием определенной территорией, т.е. «находящейся в рамках государственных границ сухопутной и водной поверхностью, воздушным пространством над ней (до границы с космосом) и недрами»[22].

ИКТ-среда представляет собой юридическую фикцию, заключающуюся в том, что совокупность специальным образом организованных и взаимосвязанных технических средств рассматривается в качестве аналога территории государства. Эта юридическая фикция позволяет распространить принципы и нормы международного права и ответственного поведения, регулирующие отношения между государствами, юрисдикция которых распространяется на суверенную территорию и на отношения по поводу использования ИКТ-среды.

В физическом смысле ИКТ-среда представляет собой совокупность технических средств (вычислительных машин, коммуникационных устройств и средств передачи данных) и программ, обеспечивающих обработку и передачу цифровых данных между вычислительными устройствами (машинами) в целях поддержания социального взаимодействия или управления техническими средствами. Объективно передача и обработка цифровых данных в ИКТ-среде характеризуются уникальным цифровым адресом их расположения в глобальном пространстве коммуникаций, вычислительных машин и систем (цифровой адрес).

Другими словами, ИКТ-среда не обладает свойствами территории и применение к ней норм и принципов международного права возможно лишь при условии принятия «системы обязательных норм, выраженных в признанных субъектами этого права источниках».

---

21 Международное публичное право. Учебник. Под ред К.А.Бекяшева. М, Проспект, 2004, С. 16

22 Там же. С. 528

Следует также отметить, что в ИКТ-среде не установлены признанные международным сообществом границы суверенных государств, что делает весьма затруднительным применение норм и принципов международного права к отношениям в этой среде. Это обстоятельство принципиально отличает ИКТ-среду от территории.

Национальный сегмент ИКТ-среды является составной частью глобальной ИКТ-среды, техническую основу которой составляют глобальные сети связи и глобальная информационно-коммуникационная сеть Интернет.

При этом национальный сегмент ИКТ-среды является материальной основой информационной инфраструктуры Российской Федерации. Безопасность использования национального сегмента ИКТ-среды и устойчивость функционирования национальной информационной инфраструктуры оказывают существенное влияние на национальную безопасность Российской Федерации.

ИКТ-среда обеспечивает автоматизацию информационной деятельности человека, т.е. деятельности по поиску, получению, передаче, производству и распространению информации в форме цифровых данных. При этом цифровые данные имеют «виртуальный» (нематериальный) характер и являются результатом деятельности субъекта информационной сферы (физического или юридического лица) либо функционирования созданных им средств автоматизации обработки информации.

Следует отметить также, что человек обладает особым правовым статусом, который характеризуется определенной свободой информационной деятельности, предоставленной ему конституционными законами[23] многих государств мира и международными договорами[24]. При этом человек может являться одним из субъектов, порождающих угрозы международной информационной безопасности.

Это обстоятельство обусловливает необходимость определения особого правового механизма регулирования общественных отношений, связанных с информационной деятельностью.

Наконец, важной особенностью ИКТ-среды как пространства реализации общественных отношений на национальном уровне и отношений на уровне международного сотрудничества является то, что данная среда не обладает абсолютной надежностью.

Ненадежность ИКТ-среды обусловлена уязвимостью компонентов этой среды, допускающих в определенных обстоятельствах возможность противоправного внедрения третьими лицами «вредоносных» программ как для осуществления различных правонарушений и преступлений, так и «враждебной» деятельности,

23 Конституция Российской Федерации. ст. 29.п.4

24 Конвенция о правах человека и основных свободах. Рим. 1950 г. ст. 10 (пп.1 и 2). Конвенция подписана Российской Федерацией 28 февраля 1996 года, вступила в силу для Российской Федерации 5 мая 1998 года

направленной на нанесение вреда национальному сегменту ИКТ-среды противостоящего государства.

В свою очередь, «виртуальный» характер цифровых данных, программ, цифровых адресов в существенной степени затрудняет применение в ИКТ-среде принуждения к правомерному поведению в рамках как национального, так и международного права.

Злонамеренная и вредоносная деятельность некоторых государств и иных субъектов международного сотрудничества, осуществляемая в военных, террористических и преступных целях на национальном, региональном и глобальном уровнях становятся все более серьезной проблемой.

Особую озабоченность вызывает злонамеренная и вредоносная деятельность в сфере использования ИКТ, затрагивающая критическую информационную инфраструктуру, т.к. данная инфраструктура используется для предоставления основных услуг населению, для обеспечения общей доступности и целостности сети Интернет, организаций экономической, социальной, политической и культурной жизни общества, органов управления государством.

По данным статистики, если количество преступлений в области компьютерной информации в России в 2006 году составило около 20 тыс., то в 2021 году — уже 517 тыс. В 2022 году каждое четвертое преступление совершалось с использованием ИКТ-среды. Возросла и социальная опасность этих преступлений.

Как отметил Президент Российской Федерации на расширенной коллегии МВД России 15 февраля 2023 года: «Количество преступлений в этой сфере ежегодно растёт. В результате действий кибермошенников урон несут отечественные компании. И, что вызывает особую остроту общественной реакции, с потерями средств и накоплений, с невосполнимым моральным ущербом сталкиваются наши граждане во всё большем и большем количестве»[25]. По данным Следственного комитета Российской Федерации, «в России за последние семь лет уровень киберпреступности поднялся в 20 раз. Действия злоумышленников в этой сфере становятся все агрессивнее»[26].

В обозримой перспективе значение противодействия угрозам обеспечения безопасности использования ИКТ и устойчивости функционирования информационной инфраструктуры, как факторов обеспечения национальной и международной безопасности, будет увеличиваться [12, 13].

Не случайно международное сотрудничество в области противодействия киберпреступности реализуется, прежде всего, между дружественными государствами. Например, к Будапештской конвенции по киберпреступности (2001)[27],

25 URL: http://www.kremlin.ru/events/president/news/67795

26 URL: https://www.rbc.ru/rbcfreenews/6000f7b39a7947863c0244d2?from=article_body

27 Конвенция о преступности в сфере компьютерной информации. ETS № 185, Будапешт, 23 ноября 2001 г.

рассматриваемой некоторыми государствами как образец регулирования международных отношений в ИКТ-среде, не присоединились более половины государств мира[28].

Вторым аспектом проблемы практического применения норм ответственного поведения государств в ИКТ-среде совместно с нормами и принципами международного права являются особенности этих норм.

Добровольные, необязательные нормы ответственного поведения государств в ИКТ-среде, являясь средством нормативного регулирования международных отношений, представляют собой рекомендательные, юридически необязательные (моральные) правила поведения государств как субъектов международного права.

Необходимость применения норм ответственного поведения государств в ИКТ-среде не вытекает непосредственно из существующих норм и принципов международного права, но является способом уточнения толкования этих норм и принципов применительно к отношениям в ИКТ-среде. Вследствие этого для применения норм ответственного поведения государств в ИКТ-среде необходимо создание соответствующей международной правовой или политической основы, с одной стороны, закрепляющей их в качестве элементов нормативной международной системы, а с другой — создающей основание для их регулирующего воздействия на международные отношения. Эта основа необходима также для имплементации норм ответственного поведения государств в национальное законодательство.

Важно отметить, что отсутствует согласованное мнение государств– членов ООН по поводу толкования содержания принципа уважения суверенитета, артикулированного некоторыми государствами в качестве императивной нормы, при применении норм ответственного поведения в ИКТ-среде. Представления государств о границах зон ответственного поведения государств в ИКТ-среде существенно различаются. Одни государства исходят из доктринального толкования этих границ как границ территорий государств, на которых расположены объекты национального сегмента ИКТ-среды (именно к этой категории можно отнести обе редакции «Таллиннского руководства»[29]), в то время как другие государства полагают, что этот вопрос необходимо решать посредством закрепления в международных соглашениях.

---

28 Конвенция ратифицирована (по состоянию на март 2023 года) следующими государствами, не являющимися членами Совета Европы: Австралия, Аргентина, Бразилия, Гана, Доминиканская Республика, Израиль, Кабо-Верде, Канада, Колумбия, Коста-Рика, Маврикий, Маврикий, Марокко, Нигерия, Панама, Парагвай, Перу, Сенегал, США, Тонга, Филиппины, Чили, Шри-Ланка Япония, еще 19 государств подписали Конвенцию или приглашены к присоединению // URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

29 Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual). M.Schmitt et al. eds. Cambridge University Press, forthcoming 2013.

Кроме того, необходимо отметить отсутствие общепринятых процессуальных механизмов обмена объективной информацией по предметам международных споров и ситуаций в ИКТ-среде. Это приводит к тому, что объявление о существовании инцидента, связанного с «вредоносным» воздействием на объекты национального сегмента ИКТ-среды, практически никогда не сопровождается заявлением какого-либо государства о его ответственности за этот инцидент. Отсутствие второй стороны не позволяет перевести ситуацию в рамки международного спора и применить к ней предусмотренный Уставом ООН механизм мирного разрешения споров[30].

Применение норм и принципов международного права суверенными государствами в отсутствие договоренности по этому вопросу приводит к усилению международной напряженности и не позволяет достичь целей ООН[31].

Таким образом, проблема практического применения норм ответственного поведения государств в ИКТ-среде во взаимодействии с нормами и принципами международного права во многом обусловлена двойственным характером ИКТ-среды, которая, с одной стороны, становится важным пространством международного сотрудничества, а с другой — обладает свойствами сложной программно-технической системы, существование которой базируется на деятельности коммерческих организаций, оказывающих коммуникационные и вычислительные услуги в глобальном пространстве уникальных цифровых адресов размещения этих программ и технических устройств.

3. Проведенные исследования позволяют сформулировать приоритетные направления международного сотрудничества в области решения выделенных проблем применения добровольных, необязательных норм ответственного поведения государств в ИКТ-среде.

Во-первых, сотрудничество в области формирования общего понимания содержания норм ответственного поведения государств в ИКТ-среде, а также процессуальных механизмов их применения, включая вопросы сотрудничества в установлении и поддержании международного правового режима безопасности объектов критической информационной инфраструктуры, применение мирных средств разрешения спорных ситуаций в ИКТ-среде.

Приоритетом в этой области могло бы стать расширение исследований в экспертном сообществе дружественных государств (Союзное государство, ОДКБ, ШОС, БРИКС, ЕАЭС и другие региональные объединения) проблем практического применения норм ответственного поведения государств в ИКТ-среде [14, 15].

Цель сотрудничества заключается в подготовке предложений по подходу к позиционированию этих норм в системе международного нормативного ре-

30 Устав ООН. Ст. 33

31 Устав ООН. Ст.1

гулирования, к определению потенциала регулирующего воздействия норм ответственного поведения государств в ИКТ-среде на международные отношения и, прежде всего, в области обеспечения международного мира и безопасности, и механизмов реализации этого потенциала.

Приоритетным вопросом для сотрудничества является поиск путей решения проблемы взаимодействия норм ответственного поведения государств в ИКТ-среде с нормами и принципами международного публичного права, а также с нормами и принципами международного частного права, регулирующими деятельность провайдеров информационных и коммуникационных услуг в глобальной сети Интернет в целях дальнейшего формирования международного информационного права.

Самостоятельным предметом дискуссий мог бы стать механизм взаимодействия норм ответственного поведения государств в ИКТ-среде с нормами и принципами национального законодательства, регулирующими отношения в области создания, развития и использования ИКТ, национальных сетей и систем связи, и коммуникации.

Проведение международных исследований по этому направлению могло бы содействовать интенсификации продвижения концепции конвенции об обеспечении международной информационной безопасности на российских и международных дискуссионных площадках.

Во-вторых, сотрудничество в изучении подходов к решению проблемы делимитации и демаркации границ зон ответственного поведения государств в ИКТ-среде. Определение границ зон ответственности государств в глобальном адресном пространстве информационной деятельности является необходимым условием согласованной деятельности государств, принявших решение соблюдать нормы ответственного поведения и сотрудничать в применении норм для создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

В рамках этого направления сотрудничества целесообразно исследовать проблемы реализации субъектами международного права «цифрового» суверенитета, а также международных обязательств США в области обеспечения устойчивости функционирования глобальной системы управления пространством IP-адресов и доменов верхнего уровня глобальной коммуникационной сети Интернет [16, 17].

Длительное время экспертное сообщество предполагало, что развитие Интернета может быть организовано, прежде всего, на основе самоуправления, и, что участие государств в этой деятельности должно носить достаточно ограниченный характер[32]. В настоящее время международное сообщество согласилось с предложением ГПЭ (2015) о том, что «государства несут главную ответствен-

32 Тунисская программа для информационного общества. Всемирная встреча на высшем уровне по информационному обществу. Второй этап. Тунис. 18 ноября 2005 г., п. 35

ность за обеспечение государственной безопасности и безопасности своих граждан, в том числе в ИКТ-среде»[33].

Суверенная власть государства заключается в его праве на независимость в реализации юрисдикции над территорией и над всеми людьми и вещами, находящимися в ее пределах, на выбор формы государственного управления, на сотрудничество с другими государствами, а также право быть субъектом международного права. Государственная граница «устанавливает пространственные пределы осуществления суверенной власти, отделяя территорию государства от территорий других государств и от международных пространств»[34].

Ответственность государств за обеспечение «государственной безопасности и безопасности своих граждан» в ИКТ-среде предполагает существование в ИКТ-среде, как пространстве международного сотрудничества, аналогичных границ, признанных международным сообществом, — границ зон ответственности государств в ИКТ-среде.

В соответствии с международным правом границы государств устанавливаются в договорном порядке путем делимитации и демаркации линий, устанавливающих пределы государственной территории.

Государства не являются обладателями адресного пространства национального сегмента ИКТ-среды. Использование сегмента адресного пространства осуществляется на основе частно-правовых договоров о выделении этого сегмента некоммерческой организацией «Корпорация по присвоению адресации и нумерации Интернета» (Internet Corporation for Assigned Names and Numbers, ICANN) (США) негосударственным организациям для коммерческого использования посредством выделения IP-адресов Интернет-провайдерам [17].

Делимитация зон ответственности государств в этой среде проводится в форме определения на основе договора общего подхода к определению части глобального адресного пространства, правовой режим использования которого определяется суверенным государством, а также определение международного правового режима поддержания устойчивости функционирования глобального адресного пространства в целом.

Демаркация зон ответственности государств в ИКТ-среде проводится в форме закрепления глобальных цифровых адресов объектов ее национального сегмента, которые находятся под особым международным правовым режимом безопасности (объекты критической информационной инфраструктуры).

Выработка научно обоснованных рекомендаций по практическому осуществлению делимитации и демаркации в ИКТ-среде может внести суще-

33 Доклад ГПЭ A/70/174, п.19.

34 Международное право. Учебник. МГЮА, М, Статут, 2004, С. 538.

ственный вклад в формирование системы международной информационной безопасности [18, 19].

В-третьих, важным направлением международного сотрудничества целесообразно определить разработку предложений по решению проблемы имплементации норм ответственного поведения государств в ИКТ-среде в национальное законодательство.

Особенностью процесса имплементации является то, что каждое государство в рамках реализации суверенитета формирует свою систему норм и принципов права, регулирующих общественные отношения в области информационной деятельности граждан, организаций и государства, а том числе в ИКТ-среде.

В Российской Федерации нормы и принципы регулирования общественных отношений по поводу информационных объектов (сведения, сообщения, данные)[35] составляют предмет информационного права как самостоятельной отрасли правовой системы.

Совокупность правовых норм, регулирующих общественные отношения, объектами которых являются цифровые данные и ИКТ, а также объекты ИКТ-среды нередко объединяют в так называемое «цифровое право» или Интернет-право, которое рассматривается как «совокупность правовых норм и институтов, регулирующих крайне многообразные отношения, так или иначе связанные с внедрением и использованием цифровых технологий, но эти нормы относятся к различным отраслям права и не объединены ни единым предметом, ни методом регулирования» [20–22].

Имплементация норм ответственного поведения государств в ИКТ-среде в национальное законодательство может потребовать внесения дополнений и изменений в значительное число нормативных правовых актов. Подготовка научно обоснованных рекомендаций по решению этой задачи сможет предотвратить нарушение функционирования уже сложившихся правовых механизмов регулирования соответствующих отношений, а также снизить ущерб от их нарушения.

Еще одним направлением международного сотрудничества в области применения норм и принципов ответственного поведения государств в ИКТ-среде является организация обмена информацией и оказание взаимопомощи, а также преследование лиц, виновных в террористическом и преступном использовании ИКТ, на основе развития системы контактных пунктов, обеспечивающих взаимодействие координаторов, на политическом, дипломатическом и техническом уровнях. Решение этой проблемы имеет ключевое значение для принятия эффективных мер в области применения средств мирного разрешения споров к отношениям, связанным с инцидентами в ИКТ-среде.

---

35 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

Идея создания института контактных пунктов, координирующих деятельность государств по применению норм ответственного поведения государств в ИКТ-среде, отражена в докладе ГПЭ (2021)[36]. По мнению правительственных экспертов, «назначение компетентных контактных пунктов на политическом и техническом уровнях может способствовать обеспечению надежной и прямой связи между государствами в целях предотвращения и урегулирования серьезных инцидентов в сфере использования ИКТ и ослабления напряженности в кризисных ситуациях».

Для обеспечения целенаправленной деятельности контактных пунктов необходимо осуществить ее регламентирование стандартом международного менеджмента информационной безопасности, имеющим статус норм международного права.

Прототипом такого стандарта могут служить стандарты менеджмента информационной безопасности[37], имеющие статус технических регламентов и регулирующие поведение должностных лиц в системе обеспечения защиты информации и аудита информационной безопасности объектов ИКТ-среды.

Взаимодействие между контактными пунктами, организованное на основе документа, регламентирующего их деятельность, может «помочь снизить напряженность и предотвратить недопонимание и неверное толкование, которые могут возникнуть в результате инцидентов в сфере использования ИКТ, в том числе затрагивающих критически важную инфраструктуру».

Включение стандарта менеджмента международной информационной безопасности в систему источников международного права может в определенной мере способствовать адаптации нового пространства международного нормативного регулирования к особенностям ИКТ-среды.

Эффективной деятельности контактных пунктов могло бы способствовать:

а) уточнение обязательств государств в области применения норм ответственного поведения государств, регулирующее воздействие которых направлено на запрещение:

- использования своей территории для совершения противоправных деяний, распространения злонамеренных программных и технических средств в ИКТ-среде, а также средств, обладающих скрытыми вредоносными функциями;
- деятельности, противоречащей обязательствам по международному праву, а также деятельности, призванной нанести ущерб информаци-

36 Доклад ГПЭ A/76/135

37 ИСО/МЭК 27000, ИСО/МЭК 27001, ИСО/МЭК 27002, ИСО/МЭК 27003, ИСО/МЭК 27004 и ИСО/МЭК 27005

онным системам уполномоченных групп экстренного реагирования на компьютерные инциденты другого государства;

б) проработка процессуальных вопросов обследования объектов ИКТ-среды и сбора информации, необходимой для мирных средств разрешения международных спорных ситуаций, связанных с инцидентами в ИКТ-среде, в том числе на объектах критической информационной инфраструктуры.

Реализация подготовленных в рамках НИР рекомендаций может содействовать «установлению международно-правового режима обеспечения безопасности в сфере использования ИКТ»[38] на основе применения «суверенитета государств и международных норм и принципов, проистекающих из суверенитета, к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях»[39].

Аккредитация Национальной Ассоциации международной информационной безопасности при РГОС создала дополнительные возможности для продвижения российской позиции по вопросам формирования системы международной информационной безопасности. Аккредитация также расширила возможности Ассоциации на этой площадке по продвижению в рамках дискуссий новых подходов к решению проблемы применения норм ответственного поведения государств в ИКТ-среде.

Таким образом, международное сотрудничество в области разработки взаимоприемлемых путей решения проблем практического применения норм ответственного поведения государств в ИКТ-среде могло бы способствовать достижению целей создания системы международной информационной безопасности, сформулированных в документах стратегического планирования Российской Федерации. Включение вопросов организации международного сотрудничества в области изучения проблем применения норм ответственного поведения государств в ИКТ-среде в позицию Российской Федерации на субстантивных сессиях РГОС способствовало бы интенсификации процесса формирования системы международной информационной безопасности.

38 Указ Президента Российской Федерации от 2 июля 2021 г. № 400

39 Доклады ГПЭ A/70/174, A/76/135

2. Проблемы международного сотрудничества в области применения добровольных, необязательных норм ответственного поведения государств в ИКТ-среде и предложения по их решению

Капустин А.Я., Русинова В.Н., Шинкарецкая Г.Г., Касёнова М.Б.

1. Роль ИКТ-среды как нового пространства международного сотрудничества. В самом общем смысле международное сотрудничество в той или иной сфере общественных отношений de facto и de jure нацелено на решение двуединой задачи: формирование регуляторных нормативных основ, организационное развитие которых осуществляется на соответствующей институциональной базе. Решение обозначенной задачи реализуется разнообразным инструментарием международного права на уровне ООН, регионального и двустороннего взаимодействия. Объективными факторами, обусловливающими параметры международного сотрудничества, выступают как специфические характеристики и особенности конкретной сферы отношений, так и историко-политический контекст, определяющий политико-правовое понимание ситуации субъектами международного публичного права, вовлеченными в решение обозначенной двуединой задачи, — государствами, международными межправительственными организациями.

Будучи самостоятельной системой права, международное право отличается от национального прежде всего кругом субъектов, а также применимыми средствами и методами регулирования. В этой связи важно обратить внимание на то, что международное сотрудничество в плане формирования нормативных основ не всегда сопрягается с установлением конвенциональных правовых (т.е. юридически обязывающих) норм, и предпочтение отдается формальным способам регулирования, осуществляемых посредством норм «мягкого» международного права, закрепляемых в соответствующих международных документах и актах.

Сложности создания юридически обязательных международных норм обусловлены среди прочего необходимостью: выработки общих концептуальных подходов; нивелирования существующих разногласий и расхождений в отношении применимого понятийно-терминологического аппарата и его содержательного объема; согласования позиций о способах и средствах обеспечения практической реализации принимаемых международных правовых норм.

В организационном плане институциональная база международного сотрудничества может быть вариативной: либо исчерпываться существующим международным механизмом, охватывающим систему международных межправительственных и неправительственных организаций, либо развивать и дополнять

инструментарий функционирующего международного механизма, базируясь на соответствующих международных мандатах (временного и постоянного характера), либо идти по пути создания нового международного органа со специальной компетенцией.

Постановка вопроса об ИКТ-среде как новом пространстве международного сотрудничества представляется правомерной при непременном условии учета комплексной природы ИКТ, центральным элементом которой является сеть Интернет, а также широкие технологические возможности трансграничного использования этих технологий в различных юрисдикциях.

Именно комплексная природа ИКТ-среды объективирует, с одной стороны, сложности определения глобального международного регуляторного формата в контексте согласования соответствующих публичных интересов государств и, с другой стороны, объясняет тот факт, что более чем за два десятилетия нынешнего века попытки регламентации соответствующих отношений в рамках всеобъемлющего международного договора, равно как и предложения ряда государств о необходимости создания новой специализированной международной межправительственной организации, которые были инициированы рядом государств-членов ООН, — не увенчались успехом.

Комплексная природа ИКТ-среды выявила предметную многоаспектность регулирования этих международных отношений, а юрисдикционные параметры определяющим образом повлияли на специфику формирования международных регуляторных нормативных и институциональных основ ИКТ-среды. Формирование регуляторных нормативных и институциональных основ обеспечения международной информационной безопасности, решение которых осуществляется через призму обозначенной выше задачи, реализуется разнообразным инструментарием международного права в рамках ООН, региональных организаций и двусторонних соглашений.

Международное сотрудничество в области обеспечения международной информационной безопасности ИКТ-среды развивается преимущественно в рамках регионального и двустороннего сотрудничества, значимость которого как в нормативно-правовом, так и в институциональном контекстах имеет существенное значение.

Это связано с тем, что сотрудничество на этих уровнях предоставляет больше возможностей для конвенционального согласования политико-правовых позиций государств и общих принципов регулирования отношений, а также закрепления соответствующего понятийно-терминологического аппарата, что принципиально важно для сферы международных отношений.

Региональное международное сотрудничество в области обеспечения международной информационной безопасности, институционально обеспечивае-

мое рамками соответствующих международных межправительственных и неправительственных организаций (Союзное государство, ЕС, ЕАЭС, ШОС, СНГ, EuroDIG, БРИКС и др.), равно как и двустороннее сотрудничество, несомненно, способствует формированию общих международно-правовых позиций и подходов регулирования в рассматриваемой сфере отношений, а также способно содействовать созданию соответствующих норм на универсальном уровне [14, 15].

Комплексная природа ИКТ-среды, разность понимания сущностных свойств сети Интернет как сложного технологического и социального ресурса, диверсифицирующего совершенствование и формат применения ИКТ, различие в уровнях развития ИКТ в конкретных государствах, а также политико-правовых приоритетов их деятельности, обусловливают регуляторный плюрализм в подходах к обеспечению международной информационной безопасности и пониманию этой деятельности в рамках международного права [7, 20, 23][40].

2. Основные принципы международного права и применение добровольных, необязательных норм ответственного поведения государств в ИКТ-среде. Доктрина информационной безопасности Российской Федерации, стратегической целью государства указывает «формирование системы международной информационной безопасности»[41].

Создание целостной системы может обеспечить применение эффективных и плодотворных мер в противодействии злонамеренному использованию информационно-коммуникационных технологий. Такая система включает в себя все средства правового воздействия на международные отношения в ИКТ-среде: заключение универсальных международных договоров, использование существующих региональных соглашений и международных рекомендательных норм, обладающих большим моральным авторитетом.

Указанные правовые средства должны основываться на общепризнанных принципах и нормах общего международного права и иметь целью продвижение тенденций создания глобальной системы международной информационной безопасности, соответствующей национальным интересам Российской Федерации.

Важнейшими элементами системы международной информационной безопасности будут основные и специальные нормы ответственного поведения государств в ИКТ-среде, меры реагирования государств на нарушения добровольных, необязательных норм ответственного поведения государств в ИКТ-среде, а также механизм ответственности всех участников деятельности в ИКТ-среде

40 Например, Россия и ряд иных государств рассматривают обеспечение международной информационной безопасности как интеграционное измерение национальной безопасности в целом. См. об этом, в частности, Указ Президента Российской Федерации от 2 июля 2021 г. №400; Указ Президента Российской Федерации от 12 апреля 2021 г. №213.

41 Указ Президента Российской Федерации от 5 декабря 2016 г. № 646.

за нарушение добровольных, необязательных норм ответственного поведения государств в ИКТ-среде.

Установлено, что в целях применения норм ответственного поведения государств в ИКТ-среде государства должны осуществлять самое широкое сотрудничество в соответствии с Уставом ООН, другими международными договорами о международном сотрудничестве в ИКТ-среде.

Результаты анализа резолюций Генеральной ассамблеи ООН, итоговых докладов рабочих групп правительственных экспертов по достижениям в области информации и телекоммуникаций в контексте международной безопасности и других документов ООН позволяют с учетом специфики ИКТ-среды, как пространства международного сотрудничества, выделить основные принципы сотрудничества государств по соблюдению норм ответственного поведения государств в ИКТ-среде. К таковым можно отнести следующие принципы: добросовестного соблюдения норм ответственного поведения государств в ИКТ-среде, реагирования на нарушение норм ответственного поведения государств в ИКТ-среде, ответственности за нарушение норм ответственного поведения государств в ИКТ-среде.

Принцип добросовестного соблюдения норм ответственного поведения государств в ИКТ-среде является реализацией более общей нормы международного права — принципа добросовестного выполнения международных обязательств, принимаемых в соответствии с Уставом ООН, который относится к категории основных принципов международного права и императивных норм (норм Jus cogens) общего международного права [24–26].

Необходимость установления конвенционного принципа соблюдения норм ответственного поведения государств в ИКТ-среде определяется тем, что в случае разработки проекта универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде его положения будут иметь обязательную юридическую силу. Логическим следствием обязательного характера международно-правового акта является закрепление в нем нормативного требования о добросовестном соблюдении норм ответственного поведения государств в ИКТ-среде как основного принципа сотрудничества государств в ИКТ-среде.

Из содержания данного принципа следует, что каждое государство в рамках своей юрисдикции не будет допускать видов деятельности, которые относятся к «злонамеренным», «заведомо противоречащим международному праву» или «наносящими преднамеренный ущерб критически важной инфраструктуре». Соответствующие определения указанных деяний нужно будет закрепить в проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде, предусмотрев в нем при необходимости

закрепление обязательства государства принимать надлежащее законодательство с целью пресечения или недопущения таких видов деятельности.

Государства в проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде должны наделяться правом принятия мер реагирования на нарушения норм ответственного поведения государств в ИКТ-среде. В этих целях следует предусмотреть, что государство, которое будет фиксировать нарушение норм ответственного поведения государств в ИКТ-среде, прежде всего должно определить разновидность нарушенного правила поведения.

В случае нарушения норм заинтересованное государство в зависимости от характера нарушения и его последствий использует либо традиционные дипломатические средства реагирования (ноты, протесты и т.д.), либо иные согласованные каналы взаимодействия с целью уведомления государства-нарушителя о своем требовании в этом случае.

Кроме того, государство может потребовать прекратить нарушение норм ответственного поведения государств в ИКТ-среде, если это нарушение продолжает осуществляться. Заинтересованное государство может выдвигать и иные требования в рамках международного права и конвенционного режима, установленного универсальным международным соглашением о применении норм ответственного поведения государств в ИКТ-среде.

Если же в результате нарушения норм ответственного поведения государств в ИКТ-среде причиняется ущерб государству, его юридическим или физическим лицам, то в этом случае государству-нарушителю может быть предъявлена претензия о возмещении причиненного ущерба. В случае отказа государства-нарушителя удовлетворить требования заинтересованного государства последнее может прибегнуть к использованию процедур мирного урегулирования возникших разногласий по договоренности с государством-нарушителем или иным допустимым международным правом способом.

Сфера применения обязанностей государств в случае совершения «серьёзного нарушения обязательства, вытекающего из императивной нормы общего международного права» включает в себя обязанность всех государств (а не только непосредственно потерпевшего), во-первых, сотрудничать с целью положить конец этому серьёзному нарушению; во-вторых, не признавать правомерным положение, сложившееся в результате нарушения, не оказывать помощи или содействия в сохранении такого положения[42]. Соответственно, эти обязанности действуют экстерриториально, вне зависимости от места совершения серьёзного нарушения нормы *jus cogens*.

42 Статьи об ответственности государств за международно-противоправные деяния, ст. 40–41; ICJ. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory. Advisory Opinion, 2004, I.C.J. Rep. 2004 (July 9). § 159.

С учетом специфики предмета регулирования универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде, ответственность государств может пониматься в позитивном смысле, то есть как долг, обязанность следовать принятым на себя международным обязательствам, а не как ответственность в негативном смысле, то есть наступающая вследствие нарушения обязательства, вытекающего из императивной нормы общего международного права.

Соответственно, применение ответственности к государству будет означать принятие индивидуальных или коллективных (специально созданных конвенционных органов, а в их отсутствие — органов ad hoc, созываемых по предложению государства или группы государств) мер воздействия на нарушителя норм ответственного поведения государств в ИКТ-среде, механизм действия которого следует предусмотреть в проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде.

Например, в необходимых случаях могут проводиться технологические экспертизы для выявления нарушения норм ответственного поведения государств в ИКТ-среде и оценки возможного причинения ущерба другим государствам-участникам универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде.

3. Закрепление зон ответственного поведения государств в ИКТ-среде. Для достижения целей обеспечения реализации положений проекта универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде следует предусмотреть международно-правовое закрепление зон ответственного поведения государств в ИКТ-среде.

Границы зон ответственного поведения государств в ИКТ-среде будут определять область действия согласованных норм ответственного поведения, в рамках которой применяются юридически обязательные принципы и нормы международного права. Применение норм ответственного поведения распространяется на действия, совершаемые из национального сегмента ИКТ-среды.

В этих целях необходимо предусмотреть закрепление границ зон ответственного поведения государств в проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде, опираясь на принципы учета определения юрисдикции государства в информационном пространстве, установленные в национальном законодательстве.

Под юрисдикцию государства будет подпадать совокупность объектов информационной инфраструктуры, отнесенных к зоне ответственности государства в ИКТ-среде и расположенных на его территории, а также на территориях, находящихся под его юрисдикцией или используемых на основании международных договоров государства.

Государства, учитывая особенности ИКТ-среды как глобальной составляющей информационной сферы, включающей взаимосвязанные объекты информационной инфраструктуры, должны предусмотреть в проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде обязательство провести делимитацию зоны ответственного поведения государств в ИКТ-среде путем закрепления в приложении к указанному проекту соглашения уникальных цифровых идентификаторов объектов ИКТ-среды, обеспечение безопасности использования которых будет осуществляться на основе государственного суверенитета.

В целях демаркации границы зоны ответственного поведения государств в ИКТ-среде государства оснастят объекты национальной зоны ответственного поведения специальным программным обеспечением и техническим оборудованием, применение которого создаст условия для поддержания установленного правового режима безопасности объектов информационной инфраструктуры, оказывающих влияние на функционирование критически важной инфраструктуры.

В проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде государства должны предусмотреть установление международного нормативного режима безопасности объектов критической информационной инфраструктуры.

В этих целях государства в рамках правового режима зоны ответственного поведения государств установят нормативный механизм соблюдения обязательств по нормативно-техническому регулированию отношений в области предупреждения и пресечения, вытекающих из норм ответственного поведения государств в ИКТ-среде.

В частности, не допускать:

- «международно-противоправных деяний с использованием ИКТ» и «вредоносного использования ИКТ, способного создать условия для нарушения международного мира и безопасности, террористического и преступного использования ИКТ»;
- противоправной деятельности в ИКТ-среде с учетом положений морского, воздушного и космического права, «заведомо противоречащей международному праву» и «наносящей преднамеренный ущерб критически важной инфраструктуре».

В проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде необходимо предусмотреть обязательство государств установить нормативный механизм оказания помощи государствам, критическая информационная инфраструктура которых становится объектом злонамеренных действий и другой деятельности, не способствующей поддержанию международного мира и безопасности.

4. Оказание помощи государствам, пострадавшим от злонамеренного и вредоносного использования ИКТ. Эффективной мерой реализации норм ответственного поведения государств в ИКТ-среде является разработка механизма применения мер оказания помощи государствам, пострадавшим от злонамеренного и вредоносного использования ИКТ.

В проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде следует установить принципы взаимодействия государств друг с другом и с соответствующими международными и региональными организациями в разработке и осуществлении мер по оказанию помощи государствам, пострадавшим от злонамеренного и вредоносного использования ИКТ, в соответствии с основополагающими принципами своих правовых систем.

Каждое государство должно принять меры к созданию и надлежащему оснащению каналов приема информации о фактах нанесения ущерба иностранному государству или его частным организациям от злонамеренного и вредоносного использования ИКТ. Государства также принимают необходимые меры по созданию и поддержанию в надлежащем состоянии дополнительных мощностей для оказания плановых или чрезвычайных мер помощи иностранному государству или его частным организациям от злонамеренного и вредоносного использования ИКТ. Они будут содействовать тому, чтобы каждая частная организация (или их объединение), предоставляющая информационно-телекоммуникационные услуги, находящаяся на территории одного из государств, была готова к принятию действенных мер в целях оказания помощи иностранному государству или его частным организациям, пострадавшим от злонамеренного и вредоносного использования ИКТ.

Кроме того, государства должны сообщать Генеральному секретарю ООН наименование и адрес органа или органов, которые могут оказывать другим государствам содействие в разработке и осуществлении конкретных мер по предупреждению преступлений и иных противоправных деяний в сфере использования информационно-коммуникационных технологий. Меры помощи иностранному государству или его частным организациям, пострадавшим от злонамеренного и вредоносного использования ИКТ, могут включать как сферу использования ИКТ, так и меры за пределами сферы ИКТ.

Государства могут обращаться к другим государствам за взаимной помощью в кратчайшие сроки, если они считают, что существует чрезвычайная ситуация. Запрос должен включать, помимо прочего необходимого содержания, описание фактов, свидетельствующих о том, что существует чрезвычайная ситуация, и для ее ликвидации необходима запрашиваемая помощь. Запрашиваемое государство может принимать такой запрос в электронной форме. Одна-

ко оно может потребовать обеспечить соответствующий уровень безопасности и аутентификации, прежде чем принимать запрос. Запрашиваемое государство может в кратчайшие сроки запросить дополнительную информацию для оценки запроса. Запрашивающее государство предоставляет такую дополнительную информацию в возможно кратчайшие сроки. Убедившись в наличии чрезвычайной ситуации и удовлетворении других требований, необходимых для оказания взаимной помощи, запрашиваемое государство отвечает на запрос в возможно кратчайшие сроки.

Необходимо предусмотреть, что каждое государство должно обеспечить, чтобы должностное лицо его компетентного органа, отвечающее на запросы о взаимной помощи, было доступно 24 часа в сутки и 7 дней в неделю для целей реагирования на запрос, направленный в соответствии с данной статьей.

Компетентные органы, отвечающие за взаимную помощь, запрашивающего и запрашиваемого государств могут договориться о том, чтобы результаты выполнения запроса или их предварительная копия могли быть предоставлены запрашивающему государству через альтернативный канал связи, отличный от обычно используемого для направления запроса об оказании правовой помощи.

В проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде предусмотрено право государств-участников при подписании Соглашения или при сдаче на хранение ратификационной грамоты или документа о принятии, утверждении или присоединении к Соглашению сообщить Генеральному секретарю ООН, что в целях эффективности запросы, поданные в соответствии с настоящим пунктом, должны направляться только в уполномоченный орган.

Государства могут с соблюдением норм своего национального законодательства направить без предварительного запроса другого государства информацию, которая бы способствовала предотвращению нарушения норм ответственного поведения государств в ИКТ-среде.

5. Разрешение споров и ситуаций в области соблюдения норм ответственного поведения государств в ИКТ-среде. Принцип мирного урегулирования международных споров, закрепленный в Уставе ООН и других международно-правовых актах, предусматривает обязательство государств урегулировать споры между ними путем переговоров и других исключительно мирных средств.

С учетом особенностей сотрудничества государств в ИКТ-среде, требующих незамедлительных действий для предотвращения угрозы ухудшения отношений между ними, вплоть до формирования угрозы международной информационной безопасности, предусматривается особая процедура ускоренного рассмотрения споров относительно толкования или применения норм об ответственном поведении государств в ИКТ-среде.

Если любой спор между двумя или более государствами не может быть урегулирован путем переговоров в течение разумного периода времени, он будет передаваться по просьбе одного из государств на арбитражное разбирательство. Если в течение шести месяцев со дня обращения с просьбой об арбитраже спорящие государства не смогут договориться о его организации и проведении разбирательства, они могут, по взаимной договоренности, передать спор в любой международный суд по своему выбору.

При разработке проекта универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде следует предусмотреть, что каждое государство-участник может при подписании, ратификации, принятии или утверждении данного Соглашения или при присоединении к нему заявить в отношении государств, которые сделают такие же заявления, о том, что любые споры и ситуации о толковании Соглашения или его применения могут быть переданы в одностороннем порядке в какой-либо специальный международный судебный орган (например, специальный международный арбитражный суд).

В случае достижения взаимопонимания государства-участники Соглашения могут разработать дополнительное международное соглашение о создании специального международного судебного органа для урегулирования споров и ситуаций в ИКТ-среде.

Суммируя вышеизложенное, можно сделать несколько обобщающих заключений.

Во-первых, международное сотрудничество в ИКТ-среде в общем плане решает двуединую задачу, заключающуюся в следующем:

- формирование регуляторных нормативных основ, организационное развитие которых осуществляется на базе существующих международных механизмов,
- формирование международной системы организаций, действующих на основании международных договоров.

Во-вторых, международное сотрудничество в ИКТ-среде реализуется на уровне ООН, региональных международных организаций и двустороннего сотрудничества с учетом комплексной природы ИКТ-среды.

В-третьих, характер ИКТ-среды, как нового пространства международного сотрудничества, характеризуется глобальным охватом и воздействием на все государства мира, что предопределяет необходимость и безальтернативность универсального подхода к определению и регулированию сотрудничества государств по применению норм ответственного поведения государств в ИКТ-среде. Принятие юридически обязательного международного соглашения в сфере применения норм ответственного поведения государств

в ИКТ-среде является надежной юридической гарантией обеспечения соблюдения данных норм государствами.

Специфика действующего нормативного регулятора ответственного поведения государств в ИКТ-среде предопределила также структуру обязательств государств и содержание проекта международно-правового соглашения. В частности, опираясь на общепризнанные принципы и нормы Устава ООН и общего международного права, предлагается разработать как общие принципы сотрудничества государств в ИКТ-среде, так и специальные принципы, включающие меры реагирования государств на нарушения норм ответственного поведения государств в ИКТ-среде.

Предложена инновационная модель установления и реализации позитивной ответственности государств за нарушение норм ответственного поведения государств в ИКТ-среде, базирующаяся на уважении суверенитета государств в ИКТ-среде.

Таким образом, закрепление в проекте Соглашения предложенных механизмов международно-правового закрепления границ зон ответственного поведения государств, оказания помощи государствам, потерпевшим от злонамеренных действий в ИКТ-среде, а также конвенционного механизма урегулирования споров будет способствовать практической реализации норм ответственного поведения государств в ИКТ-среде.

3. Проблемы имплементации норм ответственного поведения государств в ИКТ-среде и предложения по их решению

Полякова Т.А., Смирнов А.А., Панин А.В., Бойко К.С.

1. Проблемы формирования системы правового регулирования международной информационной безопасности. Проблемы формирования системы правового регулирования международной информационной безопасности (МИБ) имеют междисциплинарный характер и включают в себя «блок теоретико-методологических правовых вопросов применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды» [9, 27]. Как подчеркивал Министр иностранных дел России С.В. Лавров, «в отсутствие универсального «кодекса поведения» в киберпространстве устойчивое социально-экономическое и научно-техническое развитие всех без исключения стран становится уязвимым. Человечество рискует быть втянутым в опасную масштабную конфронтацию в онлайн-пространстве, которую невозможно будет удержать в локальных рамках в силу трансграничности современных средств коммуникаций и взаимозависимости национальных экономик» [2].

Целью государственной политики России в области МИБ является «содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности» (п. 9)[43].

Достижение данной цели осуществляется путем решения задач развития международного сотрудничества России на глобальном, региональном, многостороннем и двустороннем уровнях по вопросам формирования системы обеспечения МИБ, а также противодействия основным угрозам МИБ. Ключевое значение имеет системное развитие правового обеспечения МИБ, включая такие приоритетные направления, как содействие принятию государствами-участниками ООН Конвенции об обеспечении МИБ и выработке новых принципов и норм международного права, регламентирующих поведение государств в глобальном информационном пространстве, а также заключение и реализация международно-правовых и иных договоренностей между Россией и иностранными государствами о сотрудничестве в сфере МИБ.

43 Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности». п.9

По мнению А.В. Минбалеева, в современную цифровую эпоху методы правового регулирования должны быть достаточно гибкими и обеспечивать оперативную выработку системы способов и средств реагирования на новые угрозы и вызовы [26]. Данные выводы особенно актуальны для правового регулирования сферы МИБ, где традиционные правовые источники регулирования в виде международных договоров пока недостаточно развиты. В этой ситуации важное значение имеет принятие и реализация иных международных актов в данной сфере, включая политико-декларативные документы и акты «мягкого» права. Нормы «мягкого» права создают практический задел для «последующего процесса нормообразования, их дальнейшего развития и отражения в универсальном международном юридически обязывающем документе в области ИКТ, а в перспективе — и формирования, возможно, отдельной отрасли международного информационного права либо подотрасли права международной безопасности» [2, 28].

Одним из перспективных источников нормативного регулирования в сфере международной информационной безопасности, по мнению ГПЭ (2015) и ГПЭ (2021) могут стать добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде[44], рекомендованные 76-й сессией Генеральной Ассамблеи ООН для рассмотрения государствами[45].

Правовая природа добровольных и необязательных норм ответственного поведения государств в ИКТ-среде раскрыта в докладах ГПЭ (2015, 2021). Согласно положениям этих докладов, добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде не предусматривают ограничения или запрета действий, согласующихся с нормами международного права, то есть эти нормы не устанавливают новых правовых ограничений для государств.

При этом следует отметить, что в Докладе ГПЭ (2021) закреплено, что «нормы и существующее международное право существуют параллельно». Однако данное утверждение представляется дискуссионным, поскольку добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде направлены на детализацию и толкование общепризнанных принципов и норм международного права относительно ИКТ-среды.

Вместе с тем в докладах ГПЭ обозначается возможность разработки в перспективе дополнительных норм и отдельно отмечается возможность, что при необходимости возможна разработка в будущем «дополнительных твердых обязательств», т.е. юридически обязывающих международно-правовых норм.

---

44 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности / A/70/174, 22 июля 2015 года
Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности / A/76/135, 14 июля 2021 года

45 Резолюция Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности / A/RES/76/240 от 31 декабря 2020 года

Российская Федерация много лет выступает с инициативой о принятии универсального международного договора в сфере международной информационной безопасности, закрепляющего такие нормы.

Также в докладах ГПЭ отмечается, что нормы ответственного поведения государств в ИКТ-среде отражают ожидания международного сообщества, определяют стандарты ответственного поведения и позволяют международному сообществу давать оценку действиям и намерениям государств. Таким образом, несмотря на отсутствие обязательной юридической силы, данные нормы могут рассматриваться в качестве определенных стандартов, позволяющих давать политико-правовую оценку действий государств в ИКТ-среде. Более того, в западных экспертных кругах при оценке норм ответственного поведения государств в ИКТ-среде делается акцент именно на механизмах принуждения к соблюдению данных норм и принятия мер воздействия в отношении государства в случае их нарушения[46].

Признавая прогрессивный характер норм ответственного поведения государств в ИКТ-среде, следует подчеркнуть отсутствие выработанного механизма их имплементации государствами. Это обусловлено прежде всего особенностями их правовой природы, признаками добровольности и необязательности. Такое положение может порождать широкий комплекс проблем, начиная от прямого отказа государств руководствоваться данными нормами в своей политической практике и заканчивая попытками присвоения отдельными державами функций принудительного контроля за выполнением данных норм другими государствами-участниками.

В этой связи оптимальным способом обеспечения реализации норм ответственного поведения государств является придание им обязательной юридической силы путем закрепления в отдельном международном соглашении (проект подобного соглашения представлен в Приложении 2). Это позволило бы использовать отработанные в государствах-участниках механизмы имплементации международных договоров применительно к нормам ответственного поведения государств в ИКТ-среде. Кроме того, данное соглашение позволило бы закрепить процедурные и институциональные механизмы имплементации данных норм.

В существующих же в настоящее время условиях имплементация норм ответственного поведения государств в ИКТ-среде, имеющих добровольный и необязательный характер, будет затруднена вследствие отсутствия в большинстве государствах-участников алгоритмов применения таких норм.

Рассмотрим общие принципы имплементации норм ответственного поведения государств в ИКТ-среде. Государства-участники осуществляют имплемен-

46 Lewis, James Andrew. Creating Accountability for Global Cyber Norms // Center for Strategic and International Studies. February 23, 2022 // URL: https://www.csis.org/analysis/creating-accountability-global-cyber-norms.

тацию норм ответственного поведения государств в ИКТ-среде самостоятельно в соответствии с принципами: государственного суверенитета: суверенного равенства государств; разрешения международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность, и справедливость; отказа в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями ООН; уважения прав человека и основных свобод; невмешательства во внутренние дела других государств. При этом государства принимают во внимание рекомендации по имплементации норм ответственного поведения государств в ИКТ-среде, содержащиеся в резолюциях Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», докладах Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Также предполагается, что государства-участники должны воздерживаться от использования ИКТ, не соответствующего нормам ответственного поведения государств в ИКТ-среде.

В практическом плане имплементация предполагает реализацию государствами-участниками комплекса законодательных и иных мер, которые необходимы для выполнения норм ответственного поведения государств в ИКТ-среде. В частности, данные нормы должны учитываться при разработке и корректировке национальных стратегий (доктрин, концепций) обеспечения безопасности в ИКТ-среде, законодательных и иных правовых актов, при подготовке и заключении двусторонних и многосторонних международных соглашений (договоров) в области обеспечения безопасности в ИКТ-среде.

В целях придания системности проводимой работе на уровне государств представляется целесообразным определение национального координатора по применению норм ответственного поведения государств в ИКТ-среде.

Учитывая важную роль негосударственных структур в ИКТ-среде, в целях содействия имплементации норм ответственного поведения государств в ИКТ-среде государства должны осуществлять диалог с частным сектором, научными и техническими кругами, а также гражданским обществом. Не менее значимым представляется развитие международного сотрудничества и обмена опытом по вопросам применения норм ответственного поведения государств в ИКТ-среде.

Далее проанализированы возможные механизмы имплементации норм ответственного поведения государств в ИКТ-среде в Российской Федерации, которые бы соответствовали требованиям национального законодательства и отвечали национальным интересам России. Еще одной задачей проведенного анализа являлось выявление готовности национальной правовой системы Российской Федерации к выполнению норм ответственного поведения государств.

2. Правовые основы имплементации норм ответственного поведения государств в ИКТ-среде в Российской Федерации. Основы правового режима национального сегмента применения международно-правовых норм регламентированы Конституцией Российской Федерации. Общепризнанные принципы и нормы международного права, а также международные договоры Российской Федерации являются составной частью ее правовой системы[47]. В случае, если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора. Однако, в соответствии с Конституцией Российской Федерации, решения межгосударственных органов, принятые на основании положений международных договоров Российской Федерации в их истолковании, противоречащем Конституции Российской Федерации, не подлежат исполнению в Российской Федерации (ст. 79).

Международные отношения и международные договоры отнесены к предметам ведения Российской Федерации (п. «к» ст. 71 Конституции Российской Федерации). По предметам ведения Российской Федерации принимаются федеральные конституционные законы и федеральные законы, имеющие прямое действие на всей территории Российской Федерации (ч. 1 ст. 76 Конституции Российской Федерации).

Базовым законодательным актом, регламентирующим порядок заключения, выполнения и прекращения международных договоров Российской Федерации, является Федеральный закон от 15 июля 1995 г. № 101-ФЗ «О международных договорах Российской Федерации» (далее — Закон о международных договорах). Однако очевидно, что доклады ГПЭ (2015, 2021), предусматривающие добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде, не являются международными договорами. Представляется, что в перспективе возможна постановка вопроса о закреплении данных норм в специальной резолюции Генеральной Ассамблеи ООН или ином международном акте, однако пока такого юридического оформления они не имеют.

Вместе с тем, как показывают результаты анализа российского законодательства, порядок имплементации норм добровольных и необязательных норм

47 Конституция Российской Федерации. Ч. 4 ст. 15.

в настоящее время не урегулирован. В связи с этим до придания данным нормам императивного характера Россией могут быть осуществлены предварительные меры, направленные на подготовку национальной правовой системы к имплементации норм ответственного поведения государств в ИКТ-среде.

При этом представляется возможным руководствоваться основными положениями статей 31–34 Закона о международных договорах, регламентирующих выполнение международных договоров Российской Федерации, с определенными оговорками. В частности, в отношении норм ответственного поведения государств в ИКТ-среде может применяться принцип добросовестного выполнения за исключением тех положений, которые противоречат национальным интересам Российской Федерации.

Согласно ч. 3 ст. 31 Закона о международных договорах, международный договор подлежит выполнению Российской Федерацией с момента вступления его в силу для Российской Федерации. Однако, учитывая тот факт, что добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде не являются нормами международного договора, принятие решения о согласии Российской Федерации на обязательность данных норм в формах, предусмотренных ч. 1 ст. 6 Закона о международных договорах (подписания, ратификации и др.), не требуется. Российская Федерация выразила свою поддержку указанным принципам при принятии резолюции Генеральной Ассамблеи A/RES/70/237 и докладов ГПЭ (2015, 2021). При необходимости приверженность России применению добровольных и необязательных норм ответственного поведения государств в ИКТ-среде может быть выражена в политических заявлениях от имени Российской Федерации, в которых будет определен порядок международного сотрудничества в этой области.

Принятие мер, направленных на обеспечение выполнения добровольных и необязательных норм ответственного поведения государств в ИКТ-среде, может быть осуществлено Президентом Российской Федерации и Правительством Российской Федерации посредством принятия соответствующих нормативных правовых и (или) организационно-распорядительных актов. Непосредственная реализация данных норм может быть возложена на уполномоченные федеральные органы исполнительной власти (ФОИВ) в соответствии с их компетенцией, к числу которых, по нашему мнению, следует отнести: МИД России, МВД России, Минобороны России, Минцифры России, Минюст России, ФСБ России, ФСТЭК России, ФСО России, а также иные уполномоченные организации.

Учитывая участие широкого круга органов публичной власти в соблюдении (реализации) добровольных и необязательных норм ответственного поведения государств в ИКТ-среде, требуется определение федерального координатора данной деятельности.

3. Проблемы согласования норм национального законодательства и норм ответственного поведения государств в ИКТ-среде. Важным фактором (показателем), свидетельствующим о готовности Российской Федерации к выполнению норм ответственного поведения государств в ИКТ-среде, является состояние национального законодательства в данной сфере. Изучение содержания 11 указанных норм, закрепленных в докладах ГПЭ, показывает, что они касаются различных сфер российского законодательства: конституционного, административного, информационного, уголовно-процессуального и др. Результаты дифференцированного анализа вопросов имплементации каждой из одиннадцати норм ответственного поведения государств в ИКТ-среде показали следующее.

Норма 13 а). В соответствии с целями Устава Организации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности.

В Докладе ГПЭ (2021) в целях реализации данной нормы государствам рекомендуется создать или укрепить существующие механизмы, структуры и процедуры на национальном уровне, такие как соответствующие директивные и законодательные меры и обзорные процессы; механизмы управления кризисными ситуациями и инцидентами; механизмы сотрудничества и партнерства с участием всего правительства; механизмы сотрудничества и диалога с частным сектором, научными и техническими кругами и гражданским обществом. Государствам также рекомендуется собирать и упорядочивать представляемую ими информацию об осуществлении норм, в том числе путем проведения добровольного обзора ведущейся на национальном уровне работы и обмена опытом.

В Стратегии национальной безопасности Российской Федерации и иных документах стратегического планирования закреплена приверженность России идее поддержания международного мира и безопасности и развития международного сотрудничества в данной сфере. Стратегическая стабильность и взаимовыгодное международное сотрудничество выделены в Стратегии национальной безопасности Российской Федерации в качестве стратегического национального приоритета [2, 29]. Концепция внешней политики Российской Федерации (2016) в числе задач внешнеполитической деятельности государства закрепляет дальнейшее продвижение курса на укрепление международного мира, обеспечение всеобщей безопасности и стабильности в целях утверждения справедливой демократической международной системы, основанной на коллективных началах в решении международных проблем, на верховенстве международного права, прежде всего на положениях Устава ООН, а также на равноправных и партнер-

ских отношениях между государствами при центральной координирующей роли Организации Объединенных Наций как основной организации, регулирующей международные отношения.

В Основах государственной политики Российской Федерации в области международной информационной безопасности (2021) в качестве цели государственной политики определено содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности. При этом отмечено, что достижение цели государственной политики в области международной информационной безопасности осуществляется путем решения задач по развитию на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации с иностранными государствами по вопросам формирования системы обеспечения международной информационной безопасности, а также противодействия основным угрозам международной информационной безопасности.

Федеральный закон «О безопасности»[48] закрепляет, что международное сотрудничество Российской Федерации в области обеспечения безопасности осуществляется на основе общепризнанных принципов и норм международного права и международных договоров Российской Федерации.

Представляется, что реализация рассматриваемой нормы о сотрудничестве государств в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения противоправных действий в сфере ИКТ не потребует внесения изменений в законодательство Российской Федерации, поскольку указанная норма носит весьма общий характер. Вместе с тем при разработке новых редакций документов стратегического планирования Российской Федерации в данной области в них могут быть включены положения, направленные на осуществление указанных норм и отвечающие национальным интересам России.

В целях сбора и упорядочивания информации об применении норм ответственного поведения государств в ИКТ-среде для внутреннего использования при формировании официальной позиции государства может быть применен механизм мониторинга в данной сфере с участием аппарата Совета Безопасности Российской Федерации и профильных органов публичной власти.

Норма 13 b). В случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст

48 Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности». Ч. 1 ст. 7.

события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий.

В Докладе ГПЭ (2021) для введения этой нормы в действие на национальном уровне, содействия расследованию и урегулированию инцидентов в сфере ИКТ с участием других стран государствам рекомендуется создавать или усиливать соответствующие национальные структуры, информационно-коммуникационные стратегии, процессы, законодательные рамки, координационные механизмы, а также партнерства и другие формы взаимодействия с соответствующими заинтересованными сторонами, с тем, чтобы оценить опасность и возможность повторения того или иного инцидента в сфере ИКТ.

В России в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации»[49] функционирует государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее — государственная система, ГосСОПКА). Координацию деятельности субъектов критической информационной инфраструктуры Российской Федерации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты обеспечивает Национальный координационный центр по компьютерным инцидентам (далее — НКЦКИ) [30, 31].

В рамках деятельности указанной государственной системы обеспечивается получение и обмен информацией между НКЦКИ и субъектами критической инфраструктуры, осуществляются сбор, накопление, систематизация и анализ информации, которая поступает в данную систему через средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также информации, которая может представляться иными, не являющимися субъектами критической информационной инфраструктуры, органами и организациями, в том числе иностранными и международными. НКЦКИ имеет право направлять уведомления и запросы субъектам критической информационной инфраструктуры, а также другим органам и организациям, в том числе иностранным и международным, по вопросам, связанным с обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагированием на компьютерные инциденты.

Предоставленное НКЦКИ право заключать соглашения о сотрудничестве со своими прямыми контрагентами в иностранных государствах несомненно позволит повысить эффективность обмена и получения всесторонней информации о компьютерных инцидентах и компьютерных атаках.

---

49 Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Основы государственной политики Российской Федерации в области международной информационной безопасности ориентируют на «развитие сотрудничества с иностранными государствами, международными, международными неправительственными организациями и организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, в целях выработки механизма обмена информацией о таких инцидентах и повышения эффективности взаимодействия уполномоченных органов»[50]. Также указанный документ предусматривает совершенствование профильного взаимодействия между НКЦКИ и «уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на компьютерные инциденты»[51].

Полагаем, что нормами Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и основанными на нем подзаконными нормативными правовыми актами, включая приказы федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА (ФСБ России), определены надлежащие алгоритмы, позволяющие Российской Федерации в случае компьютерных инцидентов изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы вменения ответственности за противоправные действия в ИКТ-среде, а также характер и масштабы последствий компьютерных атак.

Следует также отметить, что серьезные компьютерные инциденты в большинстве случаев будут квалифицироваться как преступления. Соответственно по каждому преступлению будет проводиться расследование, включающее комплекс следственных и иных процессуальных действий, направленных на установление всех обстоятельств совершенного противоправного деяния и виновных в его совершении лиц, а также направление при необходимости официальных запросов о правовой помощи. Данная деятельность регламентирована УПК[52], иными законодательными и подзаконными нормативными правовыми актами, международными договорами Российской Федерации о правовой помощи по уголовным делам.

Норма 13 с). Государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ.

---

50 Указ Президента Российской Федерации от 12 апреля 2021 № 213 (пп.«а» п. 16).

51 Там же, (пп.«д» п. 16).

52 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ

В Докладе ГПЭ (2021) не содержатся рекомендации по имплементации данной нормы, хотя закреплены некоторые ожидания в отношении поведения государств, вытекающие из содержания нормы, включая:

a) принятие государством разумных и посильных действий, с тем, чтобы положить конец деятельности, происходящей на их территории, используя соразмерные, надлежащие и эффективные средства и методы таким образом, чтобы это соответствовало международному праву и внутреннему законодательству;
b) возможность обращения за помощью к другим государствам или представителям частного сектора в соответствии с положениями международного права и внутреннего законодательства;
c) уведомление затронутым государством страны, с территории которой исходит эта деятельность;
d) отсутствие автоматического возложения вины на государство, территория которого используется для совершения противоправного деяния.

Содержание рассматриваемой нормы предполагает осуществление контроля государства за национальным информационным пространством и принятие активных мер, направленных на пресечение противоправных форм его использования. В Российской Федерации преследуются преступления и иные правонарушения, связанные с деструктивным использованием ИКТ, за которые установлена уголовная или административная ответственность. При получении первичной информации о таком правонарушении начинается ее проверка в порядке, предусмотренном законодательством, после чего принимаются соответствующие решения и меры реагирования.

Учитывая международный аспект применения нормы 13 c), необходимо принимать во внимание получившую широкое распространение практику необоснованных политизированных обвинений России в потворствовании совершению компьютерных атак с ее территории без предоставления какой-либо фактической информации по установленным каналам межгосударственного сотрудничества. Общеизвестна проблема атрибуции компьютерных атак и возможности их совершения «под чужим флагом» [29, 32–35]. В этих условиях согласие Российской Федерации на применение данной нормы должно сопровождаться официальными разъяснениями относительно невозможности полного контроля над национальным сегментом ИКТ-среды и недопустимости возложения на государство вины за совершение компьютерных атак с его территории до установления всех фактических обстоятельств. В данном контексте целесообразно содействовать продвижению инициативы России о деанонимизации информационного пространства, что будет, в частности, способствовать исключению возможности использования территории государств для совершения международно-противоправных деяний с использованием ИКТ.

При этом следует подчеркнуть готовность России к оперативному рассмотрению запросов иностранных государств относительно фактов совершения международно-противоправных деяний с использованием ИКТ с российской территории и запросов о правовой помощи по соответствующим уголовным делам. Политические обвинения в отсутствие указанных официальных запросов, содержащих факты совершения международно-противоправных деяний и имеющиеся доказательства, должны признаваться несостоятельными и юридически ничтожными и подвергаться всеобщему осуждению.

Представляется, что реализация нормы 13 с) в процедурном плане предполагает наличие регламентированных национальными правовыми нормами алгоритмов получения от иностранных государств информации относительно использования территории государства для совершения противоправного деяния и реагирования на такую информацию. В настоящий момент такие алгоритмы наиболее развиты в сфере уголовного судопроизводства. Уголовно-процессуальный кодекс Российской Федерации[53] детально регулирует порядок международного сотрудничества в сфере уголовного судопроизводства и, по нашему мнению, нормы данной части УПК Российской Федерации вполне применимы для значительной части «международно-противоправных деяний с использованием ИКТ», о которых речь идет в рассматриваемой норме.

Однако оперативное реагирование государства на компьютерные инциденты может потребоваться раньше начала полноценного уголовного судопроизводства. Полагаем, что на обсуждение с заинтересованными государственными органами может быть вынесен вопрос о возможности дополнения Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» отдельной статьей, регламентирующей порядок международного сотрудничества в сфере безопасности критической информационной инфраструктуры. Реализация данного предложения может иметь важное значение и в контексте имплементации других норм ответственного поведения государств в ИКТ-среде.

Следует отметить, что в настоящее время порядок обмена информацией о компьютерных инцидентах с иностранными государствами регламентирован приказом ФСБ России[54].

---

53 Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. №174-ФЗ. Ч. 5.

54 Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».

Норма 13 d). Государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. Государствам, возможно, потребуется рассмотреть вопрос о разработке новых мер в этой сфере.

Доклад ГПЭ (2021) указывает, что соблюдение данной нормы подразумевает наличие национальной политики, законодательства, структур и механизмов, способствующих трансграничному сотрудничеству по техническим, правоохранительным, правовым и дипломатическим вопросам, имеющим отношение к борьбе с использованием ИКТ в преступных и террористических целях. Для реализации данной нормы государствам рекомендуется укреплять и далее развивать механизмы, которые могут способствовать обмену информацией и оказанию помощи между соответствующими национальными, региональными и международными организациями для повышения осведомленности государств о безопасности ИКТ и уменьшения оперативной зоны онлайновой террористической и преступной деятельности. Государствам также рекомендуется разработать соответствующие протоколы и процедуры для сбора, обработки, хранения и использования в онлайновом режиме доказательств, имеющих отношение к преступному и террористическому использованию ИКТ, и своевременно оказывать помощь в проведении расследований, обеспечивая принятие таких мер в соответствии с обязательствами государства по международному праву. Кроме того, для содействия обмену информацией и оказанию помощи в борьбе с использованием ИКТ в преступной и террористической деятельности государства могут использовать существующие процессы и инициативы, другие правовые инструменты, а также рассмотреть возможность использования дополнительных процедур или каналов связи.

Также государствам рекомендуется продолжать наращивать усилия, предпринимаемые в ООН и на региональном уровне, по реагированию на использование сети Интернет и ИКТ в преступных и террористических целях, и развивать с этой целью партнерские отношения для сотрудничества с международными организациями, промышленными и научными кругами и гражданским обществом.

Согласно Федеральному закону «О противодействии терроризму»[55] Российская Федерация в соответствии с международными договорами Российской Федерации сотрудничает в области противодействия терроризму с иностранными государствами, их правоохранительными органами и специальными службами, а также с международными организациями. Россия является активным субъектом международного сотрудничества в данной области, которое осуществляется

55 Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму». Ст. 4.

в рамках ООН, региональных международных организаций (Союзное государство, СНГ, ОДКБ, ШОС, БРИКС, ЕАЭС) и на двусторонней основе.

Порядок обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, регламентированы нормами УПК и других федерльных законов[56]. Таким образом, готовность национальной правовой системы к выполнению рассматриваемой нормы может оцениваться как высокая. Вместе с тем это не исключает потенциальной потребности разработки новых мер в этой сфере, в частности, в отношении организации сбора, обработки и хранения в онлайновом режиме доказательств, имеющих отношение к преступному и террористическому использованию ИКТ, а также закрепления правового статуса электронных доказательств и норм, обеспечивающих оперативный и защищенный обмен ими.

Кроме того, в Российской Федерации ведется активная межведомственная работа по подготовке проектов протоколов, направленных на совершенствование положений двусторонних и многосторонних договоров Российской Федерации о взаимной правовой помощи по уголовным делам в целях противодействия и расследования преступлений в сфере ИКТ, а также разработка национальных нормативных правовых актов, направленных на совершенствование и повышение эффективности межведомственного взаимодействия в данной области.

В контексте практической реализации данной нормы могут быть рассмотрены основные направления реализации государственной политики в области международной информационной безопасности, связанные с содействием разработке на межгосударственном уровне комплекса мер в указанных целях, с совершенствованием на глобальном, региональном, многостороннем и двустороннем уровнях механизма обмена информацией о фактах использования ИКТ в террористических целях, а также с повышением эффективности взаимодействия уполномоченных государственных органов[57].

Норма 13 е). В процессе обеспечения безопасного использования ИКТ государства должны соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение.

В Докладе ГПЭ (2021) отмечается, что исполнение государствами данной нормы относительно уважения и защиты прав человека и основных свобод в Интернете и реальной жизни должно осуществляться в соответствии с нормами

56 Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»

57 Указ Президента Российской Федерации от12 апреля 2021 № 213(пп. «б» и «в» п. 13)

основополагающих международных актов о правах человека и конкретными указаниями, содержащимися в указанных резолюциях. Подчеркивается, что усилия государств по поощрению уважения и соблюдения прав человека и обеспечения безопасного использования ИКТ должны носить взаимодополняющий, взаимоукрепляющий и взаимосвязанный характер. Также содержится рекомендация об инвестировании в разработку технических и правовых мер, призванных направлять развитие и использование ИКТ в более инклюзивном и доступном ключе, без негативного воздействия на членов отдельных общин или групп, а также об ускорении такой разработки.

В Российской Федерации признаются и гарантируются права и свободы человека и гражданина согласно общепризнанным принципам и нормам международного права и в соответствии с Конституцией Российской Федерации. В частности, в ст. 29 Конституции Российской Федерации гарантируется право человека на свободу выражения мнения. Свобода поиска, получения, передачи, производства и распространения информации любым законным способом закреплена в качестве одного из базовых принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации[58].

Конституция Российской Федерации в целях обеспечения баланса между правами личности и интересами обеспечения национальной безопасности предусматривает возможность ограничения основных прав и свобод в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (ч. 3 ст. 55).

Критерии допустимости ограничения основных прав соответствуют международно-правовым стандартам, в частности нормам Конвенции о защите прав человека и основных свобод (1950), в пункте 3 статьи 19 которого указывается, что реализация прав на свободу выражения мнения, поиска, получения и распространения информации налагает особые обязанности и особую ответственность.

Следовательно, такое право может быть сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми для уважения прав и репутации других лиц, а также для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

Федеральным законом «Об информации, информационных технологиях и о защите информации», Законом Российской Федерации «О средствах массовой информации» и другими законодательными актами Российской Федерации предусмотрены определенные ограничения права на неприкосновенность част-

58 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Ст.3.

ной жизни, личную и семейную тайну, свободы слова, права свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Данные ограничения соответствуют конституционным критериям допустимости, применяются в строго установленном законом порядке и подлежат судебному обжалованию. Вместе с тем следует исходить из того, что любые ограничения, вводимые федеральными законами, направлены на защиту интересов и прав граждан, а также на обеспечение их безопасности.

Приоритетное значение в плане обеспечения неприкосновенности частной жизни в условиях цифровой среды имеет Федеральный закон «О персональных данных»[59], закрепляющий правовые гарантии защиты прав личности в связи с обработкой персональных данных органами публичной власти, юридическими и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях. Кроме того, в Российской Федерации принят Федеральный закон «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации»[60], устанавливающий организационно-правовые основы формирования и ведения единого федерального информационного регистра, содержащего сведения о населении Российской Федерации.

В целом законодательство Российской Федерации обеспечивает выполнение требований рассматриваемой нормы о поощрении, защите и осуществлении прав человека в условиях современной цифровой среды. Вместе с тем необходимо учитывать, что наша страна постоянно подвергается критике со стороны недружественных государств и международных организаций якобы за нарушение прав человека в ИКТ-среде. Поэтому норма 13 е), несомненно, может использоваться враждебными иностранными государствами в информационных кампаниях против России, в связи с чем данной норме следует уделить особое внимание.

Норма 13 f). Государство не должно осуществлять или заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения.

В Докладе ГПЭ (2021) содержатся пояснения о значимости данной нормы в связи с основополагающим значением критически важной инфраструктуры как национального достояния и серьезными последствиями, которые может вызвать ее повреждение. В плане имплементации государствам рекомендуется при-

59 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

60 Федеральный закон от 8 июня 2020 г. № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации».

нять соответствующие директивные и законодательные меры на национальном уровне для обеспечения того, чтобы деятельность в области использования ИКТ, осуществляемая или поддерживаемая государством, которая может повлиять на критическую информационную инфраструктуру, используемую для оказания основных услуг населению другого государства, согласовывалась с этой нормой, использовалась в соответствии с его международно-правовыми обязательствами и подлежала всеобъемлющему обзору и надзору.

Национальное законодательство Российской Федерации в целом соответствует международно-правовым стандартам в части закрепления правовых запретов и криминализации деструктивной деятельности с использованием ИКТ. В частности, глава 28 Уголовного кодекса Российской Федерации закрепляет основные составы преступлений в сфере компьютерной информации, включая неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1). Кроме того, в Уголовном кодексе Российской Федерации закреплена уголовная ответственность за использование ИКТ в террористических и экстремистских целях (ст. 205-207, 280-282.3), а также для совершения преступлений против мира и безопасности человечества (ст. 354, 354.1, 361). Как уже отмечалось, в России действует отдельный Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», который детально регламентирует организацию защиты такой инфраструктуры с позиций национальных интересов.

Вместе с тем рассматриваемая норма касается и прямых действий государств по совершению компьютерных атак на критическую информационную инфраструктуру иностранных государств. Известно, что такие действия являются одним из направлений кибервойн (информационных войн). В этой связи требуется обсуждение вопроса о том, необходимо ли закрепление в документах стратегического планирования и (или) нормативных правовых актах возможности применения Россией методов воздействия на критическую инфраструктуру иностранных государств в качестве ответной или превентивной меры в рамках реализации права на самооборону. Данный вопрос также может быть отражен в специальной оговорке относительно применения нормы 13 f).

Норма 13 g). Государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции.

В Докладе ГПЭ (2021) в качестве мер по выполнению данной нормы указаны отнесение государством инфраструктур или секторов к категории критически важных, а также определение структурных, технических, организационных, за-

конодательных и нормативных мер, необходимых для их защиты и восстановления функциональности в случае возникновения инцидента. В докладе содержится отсылка к резолюции A/RES/58/199 Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур». Также рекомендуется поощрение мер по обеспечению безопасности и защищенности продуктов ИКТ на протяжении всего их жизненного цикла или классификации инцидентов в сфере ИКТ с точки зрения их масштаба и серьезности.

В России указанные вопросы достаточно полно урегулированы нормами Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и принимаемыми в соответствии с ним подзаконными нормативными правовыми актами. Элементы для защиты важнейших информационных инфраструктур, закрепленные в приложении к резолюции A/RES/58/199 Генеральной Ассамблеи ООН, в нашей стране реализованы. В частности, успешно функционирует ГосСОПКА.

Также Указом Президента Российской Федерации от 14 апреля 2022 г. № 203[61] в Российской Федерации учреждена Межведомственная комиссия Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации [7, 9, 35–39]. Данная комиссия создана в целях выполнения возложенных на Совет Безопасности Российской Федерации задач по выработке мер, направленных на обеспечение безопасности критической информационной инфраструктуры Российской Федерации, а также по координации деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, органов местного самоуправления и организаций при реализации мероприятий по обеспечению технологической независимости объектов критической информационной инфраструктуры, оснащению таких объектов отечественной радиоэлектронной продукцией, техническим оборудованием, программно-аппаратными комплексами, включая программное и информационное обеспечение.

Кроме того, комплекс значимых мер по обеспечению безопасности критической информационной инфраструктуры Российской Федерации предусмотрен нормативным правовым актом Президента Российской Федерации[62].

В соответствии с ним на руководителей федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов

61 Указ Президента Российской Федерации от 14 апреля 2022 г. № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации».

62 Указ Президента Российской Федерации «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 1 мая 2022 г. № 250

Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации, возложена персональная ответственность за обеспечение информационной безопасности соответствующих органов (организаций). На заместителя руководителя органа (организации) должны быть возложены полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. Для непосредственного осуществления данной функции предписано создать в органе (организации) специальное структурное подразделение. Комплекс этих и других мер, предусмотренных данным нормативным правовым актом, несомненно, послужит укреплению состояния защищенности критической информационной инфраструктуры Российской Федерации, в том числе в контексте реализации рассматриваемой нормы 13 g).

Норма 13 h). Государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета.

В Докладе ГПЭ (2021) отмечается, что при получении просьбы об оказании помощи государствам следует предлагать любую помощь в рамках имеющихся у них возможностей и ресурсов с учетом имеющихся у них разумных возможностей и в соответствии с обстоятельствами, включая обращения за помощью к международным структурам или частному сектору. Эффективность осуществления этой нормы обеспечивается с помощью соответствующих национальных структур и механизмов обнаружения и смягчения последствий инцидентов в сфере ИКТ, потенциально угрожающих международному миру и безопасности. Такие механизмы дополняют существующие механизмы повседневной обработки и урегулирования инцидентов в сфере ИКТ. В докладе подчеркивается значимость единых и транспарентных процессов и процедур обращения за помощью к другому государству и реагирования на такие просьбы, что предполагает разработку типовых форм подобных запросов и ответов на них.

Как отмечалось ранее, Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» непосредственно

не определяет порядок обмена информацией о компьютерных инцидентах на межгосударственном уровне и выполнения запросов об оказании помощи, поступающие от других государств. В настоящее время порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, а также между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, урегулирован ведомственным нормативным актом[63].

В соответствии с ним обмен информацией о компьютерных инцидентах осуществляется субъектами критической информационной инфраструктуры путем взаимного направления уведомлений, а также запросов, уточняющих представляемую информацию. Направление уведомлений и запросов иностранными и международными органами и организациями осуществляется посредством использования технической инфраструктуры НКЦКИ. По общему правилу обмен информацией о компьютерных инцидентах с иностранными (международными) организациями осуществляется НКЦКИ, за исключением случаев, когда обмен субъекта критической информационной инфраструктуры такой информацией напрямую с иностранной (международной) организацией предусмотрен международным договором Российской Федерации. Направление информации в иностранную (международную) организацию осуществляется НКЦКИ в соответствии с установленными в ГосСОПКА форматами представления информации о компьютерных инцидентах и составом технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, и определенными НКЦКИ.

Таким образом, приказ ФСБ России достаточно четко регламентирует механизмы взаимодействия с иностранными государствами, связанные с вопросами компьютерных инцидентов. Вместе с тем в рамках имплементации рассматриваемой нормы 13 h) считаем целесообразным рассмотрение вопроса о возможном дополнении Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» нормой общего характера, регламентирующей базовые принципы взаимодействия Российской Федерации с иностранными государствами по вопросам компьютерных инцидентов.

Кроме того, в рамках развития механизмов государственно-частного партнерства в сфере обеспечения безопасности использования ИКТ представляется целесообразной разработка концепции взаимодействия государственных

63 Приказ ФСБ России от 24 июля 2018 г. № 368.

органов и организаций с частным сектором по вопросам компьютерных инцидентов.

В контексте практической реализации данной нормы могут быть рассмотрены основные направления реализации государственной политики в области международной информационной безопасности, связанные с содействием созданию на глобальном, региональном, многостороннем и двустороннем уровнях эффективного механизма межгосударственного взаимодействия, направленного на предотвращение компьютерных атак на критическую информационную инфраструктуру[64], а также с содействием выработке на указанных уровнях порядка обмена информацией о передовых практиках обнаружения, предупреждения и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру[65].

Норма 13 i). Государства должны принимать разумные меры для обеспечения целостности каналов поставки, 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.

В Докладе ГПЭ (2021) содержится широкий перечень рекомендаций относительно имплементации данной нормы, включая принятие следующих мер, направленных на снижение уязвимости каналов поставок:

a) создание на национальном уровне всеобъемлющих, транспарентных, объективных и беспристрастных рамок и механизмов для управления рисками в отношении каналов поставки в соответствии с международными обязательствами государств;

b) разработка стратегий и программ, направленных на поощрение внедрения поставщиками оборудования и систем ИКТ передовых методов в целях укрепления международного доверия к целостности и безопасности информационно-коммуникационных продуктов и услуг, повышения качества и содействия выбору;

c) обращение повышенного внимания в национальной политике и в диалоге с государствами и соответствующими участниками в ООН и на других площадках вопросу о том, как обеспечить всем государствам возможность равноправно конкурировать и внедрять инновации, с тем чтобы создать условия для полной реализации ИКТ в целях ускорения глобального социального и экономического развития и содействия поддержанию международного мира и безопасности при одновременном обеспечении национальной безопасности и учете общественных интересов;

64 Указ Президента Российской Федерации от12 апреля 2021 г. № 213, пп. «в» пункта 16.

65 Там же, пп. «г» пункта 16.

d) совместные меры, такие как обмен передовым опытом на двустороннем, региональном и многостороннем уровнях по управлению рисками в отношении каналов поставки; разработка и внедрение глобально совместимых общих правил и стандартов безопасности каналов поставок.

Отдельный блок рекомендаций касается разработки и внедрения на национальном уровне следующих средств борьбы с распространением злонамеренных программных и технических инструментов в сфере ИКТ и использованием скрытых вредоносных функций, включая закладки:

a) меры по повышению целостности каналов поставок, включая требования к поставщикам ИКТ учитывать вопросы безопасности и защиты информационно-коммуникационных продуктов при их проектировании и разработке, а также на протяжении всего их жизненного цикла. В этих целях государства могут также рассмотреть вопрос о создании независимых и беспристрастных процессов сертификации;
b) законодательные и другие гарантии, повышающие уровень защиты данных и конфиденциальности;
c) меры, запрещающие внедрение вредных скрытых функций и использование уязвимостей в продуктах ИКТ, которые могут поставить под угрозу конфиденциальность, целостность и доступность систем и сетей, в том числе в критической информационной инфраструктуре.

Еще одна рекомендация касается участия частного сектора и гражданского общества в укреплении безопасности ИКТ и процессов их использования. В контексте практической реализации данной нормы может быть рассмотрено одно из основных направлений реализации государственной политики в области международной информационной безопасности, связанное с повышением эффективности государственно-частного партнерства в сфере информационной безопасности, с содействием участию национальных коммерческих организаций-производителей товаров и услуг в указанной сфере в международном сотрудничестве в интересах укрепления информационной безопасности Российской Федерации и формирования системы обеспечения международной информационной безопасности[66].

В Российской Федерации вопросы обеспечения безопасности продуктов ИКТ относятся преимущественно к сфере технического регулирования[67]. Сегодня действует значительное количество технических стандартов в данной сфере[68].

66 Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, п. 17 «ж».

67 Федеральный закон «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ

68 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель; ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасно-

Одним из основных способов обеспечения безопасности продуктов ИКТ, в частности, средств защиты информации, выступает сертификация, которая осуществляется ФСБ России и ФСТЭК России в порядке, установленном ведомственными правовыми актами [40, 41].

Вопрос готовности Российской Федерации к исполнению обязательств, предусмотренных нормой 13 i), требует дополнительных консультаций со специалистами в области обеспечения информационной безопасности.

Вместе с тем совместно с ответственными органами государственной власти целесообразна проработка вопроса о дополнении профильных государственных программ Российской Федерации положениями об обеспечении целостности каналов поставки. Более того, на рассмотрение коллегиальных органов Союзного государства и ЕАЭС может быть вынесен вопрос о принятии модельных законов в данной сфере.

Норма 13 j). Государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры.

В Докладе ГПЭ (2021) отмечается необходимость создания беспристрастных правовых рамок, стратегий и программ, которыми можно было бы руководствоваться при принятии решений по устранению факторов уязвимости ИКТ и ограничить их коммерческое распространение. Также рекомендуется рассмотреть вопрос о введении правовой защиты для исследователей и специалистов по тестированию на проникновение. Еще один блок рекомендаций по имплементации касается разработки руководящих принципов и стимулирующих мер, которые касаются ответственной координации работы с уязвимостями и составления соответствующей отчетности, а также соответствующих ролей и обязанностей различных заинтересованных сторон в процессе представления отчетности; типов технической информации, подлежащих раскрытию или публичному распространению; способов работы с конфиденциальными данными и обеспечения безопасности и конфиденциальности информации.

Полагаем, что реализация рассматриваемой нормы частично охватывается организацией обмена информацией о компьютерных инцидентах с иностранными (международными) организациями, порядок которого был проанализирован нами выше. Однако данная норма затрагивает и более широкий пласт вопросов,

---

сти. Безопасность сетей. Часть 1. Обзор и концепции; ГОСТ Р 50.1.031-2001 Информационные технологии поддержки жизненного цикла продукции. Терминологический словарь. Часть 1. Стадии жизненного цикла продукции; ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть1. Общие положения и др.

связанных с предоставлением информации о факторах уязвимости в сфере ИКТ и о существующих методах борьбы с ними. ФСТЭК России утверждена Методика оценки угроз безопасности информации[69] и Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России[70].

В соответствии с данными документами предусматривается, что в данном банке угроз должны содержаться общедоступные сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов. Представляется, что обмен информацией с зарубежными партнерами может осуществляться ФСТЭК России в рамках международного сотрудничества, включая мероприятия по международному информационному обмену[71].

При характеристике правовых основ данной деятельности необходимо отметить, что ранее в России действовал федеральный закон[72], в котором были закреплены общие правовые основания участия России в международном информационном обмене в рамках единого мирового информационного пространства, защиты публичных и частных интересов при международном информационном обмене. В настоящее время эти отношения федеральным законодательством не регулируются. В этой связи возможно выдвижение инициативы о дополнении базового Федерального закона «Об информации, информационных технологиях и о защите информации» соответствующими нормами. Другим возможным вариантом, требующим обсуждения, может стать разработка и принятие федерального закона «Об информационной безопасности Российской Федерации», отдельный раздел которого был бы посвящен международному сотрудничеству в области обеспечения информационной безопасности. В данном разделе можно было бы нормативно закрепить положения, позволяющие успешно имплементировать пункты 13 a), 13 d), 13 h), 13 j) добровольных, необязательных норм ответственного поведения государств в ИКТ-среде.

Отдельного внимания в контексте имплементации рассматриваемой нормы имеет вопрос правовой защиты для исследователей и специалистов по тестированию на проникновение, на что обращено внимание в Докладе ГПЭ (2021). В Российской Федерации с 2021 года во исполнение постановления Правительства Российской Федерации от 12 октября 2019 г. № 1320 и в рамках Национальной программы «Цифровая экономика России» действует киберполигон для

69 Утверждена ФСТЭК России 5 февраля 2021 г.

70 Утвержден ФСТЭК России 26 июня 2018 г.

71 Указ Президента Российской Федерации от 16 августа 2004 г. № 1085. Положение о Федеральной службе по техническому и экспортному контролю. п. 8

72 Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене»

отработки практических навыков руководителей и специалистов по отражению компьютерных атак. В то же время правовой статус специалистов, проводящих оценку реальной защищенности системы путем теста на проникновение, в Российской Федерации законодательно не определен.

Представляется целесообразной проработка вопроса о дополнении Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» нормами, закрепляющими основы правового статуса исследователей и специалистов по тестированию на проникновение, а также порядок их привлечения к тестовым мероприятиям субъектами критической информационной инфраструктуры и уполномоченными органами. Также следует рассмотреть вопрос о дополнении статей главы 28 Уголовного кодекса Российской Федерации (ст. 272-274.1) примечаниями, предусматривающими освобождение от уголовной ответственности лиц, привлекаемых владельцами информационной инфраструктуры или уполномоченными государствами органами и организациями для проведения тестов на проникновение.

Норма 13 k). Государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

В Докладе ГПЭ (2021) в качестве основного способа имплементации данной нормы указано публичное объявление государством или принятие им мер, подтверждающих, что они не будут использовать уполномоченные группы экстренного реагирования для участия в злонамеренной международной деятельности. При этом государства будут признавать и уважать сферы деятельности и этические принципы, которыми руководствуются в своей работе уполномоченные группы экстренного реагирования.

В качестве еще одной меры определено создание национальной системы обработки инцидентов в сфере ИКТ с определенными функциями и обязанностями, в том числе для национальных групп реагирования на компьютерные инциденты (ГРКИ) / групп реагирования на инциденты информационной безопасности (ГРИИБ)[73] для упрощения сотрудничества и координации между такими группами и другими соответствующими органами по вопросам безопасности и техническими органами на национальном, региональном и международном уровнях.

73 Англ. CERT/CSIRT

Такая система может включать в себя политику, нормативные меры или процедуры, которые более точно определяют статус, полномочия и мандаты ГРКИ/ГРИИБ и отделяют уникальные функции таких групп от других функций управления.

В Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» для обозначения национальных групп реагирования на компьютерные инциденты (ГРКИ) используется термин «силы, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (ч. 2 ст. 5). К ним относятся:

1) подразделения и должностные лица ФСБ России;
2) НКЦКИ;
3) подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

Порядок их деятельности регламентирован нормами названного федерального закона и подзаконными нормативными правовыми актами ФСБ России. Соответствующие положения могут включаться в правовые акты, устанавливающие кодекс этики сотрудников.

Что касается рекомендации относительно «публичного объявления государством или принятия им мер, подтверждающих, что они не будут использовать уполномоченные группы чрезвычайного реагирования для участия в злонамеренной международной деятельности», то ее реализация может быть осуществлена путем выступлений официальных должностных лиц Российской Федерации, выпуска заявлений и комментариев. Однако закрепление подобного положения в документах стратегического планирования представляется нецелесообразным.

Таким образом, проведенное исследование показало, что законодательством Российской Федерации не определен порядок имплементации норм ответственного поведения государств в ИКТ-среде, поскольку они не являются нормами международного договора. В этой связи требует продвижения обоснованная в НИР инициатива о придании нормам ответственного поведения государств в ИКТ-среде императивного характера посредством закрепления его в универсальном международном соглашении (международном договоре).

До принятия подобного соглашения могут быть осуществлены предварительные меры, направленные на подготовку национальной правовой системы к имплементации норм ответственного поведения государств в ИКТ-среде. Приверженность к их исполнению может быть выражена в политических заявлениях от имени Российской Федерации. В отношении норм ответственного поведения государств в ИКТ-среде может применяться принцип добросовестного

выполнения за исключением тех положений, которые противоречат национальным интересам Российской Федерации. В организационно-правовом плане это потребует нормативного закрепления порядка обеспечения выполнения норм ответственного поведения государств в ИКТ-среде, включая назначение ответственных федеральных органов исполнительных властей и координатора их деятельности.

Сравнительно-правовой анализ содержания одиннадцати норм ответственного поведения государств в ИКТ-среде и норм российского законодательства позволил прийти к выводу, что национальная правовая система Российской Федерации в целом позволяет обеспечивать их выполнение. Ключевое значение в рассматриваемой сфере имеет федеральные законодательство по вопросу о безопасности критической информационной инфраструктуры[74]. Вместе с тем по ряду позиций в российском законодательстве имеются правовые лакуны, требующие устранения. Также нормы действующих законодательных и подзаконных нормативных правовых актов Российской Федерации должны быть адаптированы с целью обеспечения надлежащего выполнения норм ответственного поведения государств в ИКТ-среде.

Важным фактором совершенствования процедур имплементации норм ответственного поведения государств в ИКТ-среде является активное международное сотрудничество по вопросам обмена информацией, синхронизации принимаемых мер и гармонизации национального законодательства.

Кроме глобальных форматов обсуждения вопросов практического применения норм ответственного поведения государств в ИКТ-среде (РГОС, ГПЭ), требует дальнейшего развития деятельность Группы экспертов государств-членов ШОС по международной информационной безопасности и Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ, а также проведение мероприятий в целях координации и выработки единых подходов со странами АСЕАН, ЛАГ и Африканского союза. Отдельного внимания на данном направлении заслуживает развитие и укрепление сотрудничества государств-участников ОДКБ.

Требуется активное подключение научного сообщества к обсуждению вопросов имплементации норм ответственного поведения государств в ИКТ-среде. Представляется необходимой организация в России серии научно-практических конференций, семинаров и круглых столов по данной тематике с привлечением экспертов из иностранных государств, а также представителей ИКТ-индустрии и институтов гражданского общества. Возможно проведение совместных научно-исследовательских работ учеными Союзного государства, стран СНГ, ШОС, ОДКБ, БРИКС по вопросам имплементации рассматриваемых норм.

74 Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

4. Проблемы международного сотрудничества в области мирного разрешения споров, связанных с инцидентами в ИКТ-среде

Марков А.С., Волкова С.Г., Горжалцан В.А., Жарова А.К., Калицев А.Е., Милославская Н.Г., Пилюгин П.Л., Стрельцов А.А.

4.1. Международное регулирование отношений в области мирного разрешения споров в ИКТ-среде. Одной из наиболее актуальных проблем практического применения норм ответственного поведения государств в ИКТ-среде является разрешение споров по поводу инцидентов в ИКТ-среде.

Международный спор предполагает наличие взаимных претензий между сторонами. Спор существует, если одна сторона выдвигает жалобу против другой стороны, а другая сторона, в свою очередь, отвергает жалобу [42, 43]. Обычно международный спор обладает следующими характеристиками: конкретные участники, достаточно четкие взаимные претензии, определенный предмет спора.

Особенностью споров в ИКТ-среде является то, что в них, как правило, не бывает второй стороны. Имеется только сторона, считающая себя жертвой злонамеренного использования ИКТ[75], при этом даже существование фактов, подтверждающих нанесение ущерба этой стороне вследствие инцидента в ИКТ-среде, не является очевидным. Государство-жертва, как правило, имеет общие предположения относительно стороны, которая является виновной в злонамеренном использовании ИКТ против объектов ее информационной инфраструктуры, и не может представить соответствующие доказательства.

В связи с этим ключевой проблемой разрешения спора (спорной ситуации), связанных со злонамеренным использованием ИКТ против объектов критической информационной инфраструктуры, находящейся под государственным суверенитетом, посредством установленных международным правом средств (обследование, добрые услуги и посредничество, примирение, арбитраж, судебное разбирательство), является следующее:

- установление второй стороны спора;
- получение фактических данных об инциденте и подтверждение фактов нанесения ущерба;
- установление причин возникновения инцидента (ИКТ, с помощью которых было осуществлено вмешательство в функционирование объек-

75 Самые громкие кибератаки на критические инфраструктуры. PandasecurityRus. / 30.11.2016 г. // URL: https://habr.com/ru/company/panda/blog/316500/

та критической информационной инфраструктуры, способа осуществления такого вмешательства);
- оценка возможных негативных последствий, которые проявятся в будущем;
- определение мер, которые обеспечили бы невозможность возникновения подобных инцидентов в будущем.

Отдельной проблемой является придание юридической значимости тем фактическим данным, которые в определенных обстоятельствах может представить государство-жертва злонамеренного применения ИКТ в глобальной информационной инфраструктуре. Это обусловлено особенностями функционирования ИКТ-среды, в которой осуществление операций приема, передачи, хранения, обработки и распространения информации носит виртуальный (невидимый возможным свидетелям) характер.

Не менее важной проблемой при разрешении споров относительно инцидентов, связанных со злонамеренным использованием ИКТ, является вопрос о толковании и применении норм ответственного поведения государств в ИКТ-среде, которые образуют основу нового нормативного механизма регулирования международных отношений.

Так, например, в Конвенции ООН по морскому праву, применение норм которого имеет весьма длительную историю, закреплён специальный механизм урегулирования споров, в рамках которого может быть достигнуто решение в сложных ситуациях.

Данный механизм предоставляет с одной стороны возможность прибегнуть, по выбору сторон, к процедуре урегулирования спора с привлечением третьей стороны, при этом достигнутое решение является обязательным, а с другой — возможность прибегнуть к согласительной процедуре, результаты которой не являются обязательными для сторон.

Кроме того, определенная категория споров прямо исключается из предусмотренных Конвенцией процедур или государство имеет право исключить их из сферы применения соответствующих процедур [42].

Представляет интерес для разработки подхода к решению проблем мирного разрешения споров, связанных с инцидентами в ИКТ-среде, опыт применения Общего арбитража для разрешения споров, касающихся толкования или применения Конвенции по морскому праву, а также специального арбитража — для рассмотрения только определенной категории дел в некоторых специальных и технических областях отношений между государствам[76]. Опыт его применения мог бы быть полезен для разрешения международного спора в глобальной информационной инфраструктуре [44, 45].

76 Конвенция ООН по морскому праву. Монтего-Бей, 10.12.1982 г. Приложение VII. Арбитраж, Приложение VIII. Специальный арбитраж.

Специальный арбитраж в соответствии с Конвенцией 1982 г. носит обязательный порядок и установлен для строго определенной категории споров (рыболовство, защита и сохранение морской среды, научные исследования, судоходство)[77]. Однако он обладает более широкой компетенцией, выходящей за рамки традиционных арбитражных функций. Он имеет право по просьбе сторон производить расследования, устанавливать факты, вызвавшие спор. По просьбе всех сторон в споре специальный арбитраж может сформулировать рекомендации, которые, не имея силы решения, образуют лишь основу для рассмотрения сторонами вопросов, вызвавших спор[78]. Обязательным условием вынесения рекомендаций должно быть наличие соответствующей просьбы всех спорящих сторон. В противном случае установление фактов специальным арбитражем рассматривается как окончательное для сторон [44].

Подобные меры разрешения международных споров можно было бы применять и для разрешения споров в глобальной информационной инфраструктуре.

В то же время необходимо учитывать, что эффективность применения таких средств разрешения споров как «переговоры, обследование, посредничество, примирение, арбитраж, судебное разбирательство, обращение к региональным органам или соглашениям… по своему выбору»[79] для разрешения международного спора в глобальной информационной инфраструктуре ввиду неопределенности его субъективной и объективной составляющих существенно ограничена.

С учетом изложенного, под международным спором в глобальной информационной инфраструктуре можно было бы понимать объективно существующее столкновение интересов (разногласия в позициях) между субъектами международного права. Это столкновение возникает в связи с жалобой одного из субъектов международного права о злонамеренном вмешательстве в его деятельность по обеспечению безопасного использования ИКТ и устойчивого функционирования национального сегмента глобальной информационной инфраструктуры.

В силу особенностей этой инфраструктуры для содействия применению специального арбитража в отношении международных споров в глобальной информационной инфраструктуре целесообразно было бы создать специальный орган по международному сотрудничеству в области менеджмента международной информационной безопасности. Деятельность такого органа могла бы базироваться на системе центров обеспечения международной информационной безопасности национальных сегментов ИКТ-среды (контактных пунктов), осуществляемой в целях сотрудничества государств по вопросам применения норм ответственного поведения государств в ИКТ-среде.

77 Приложения VIII к Конвенции 1982 г., ст. 1. Возбуждение дела.
78 Там же., ст. 5. Процедура.
79 Устав ООН. Ст. 33.

В качестве предварительного шага в направлении создания специального арбитража по вопросам разрешения споров в ИКТ-среде в настоящей работе предлагается рассматривать следующие меры:

- создание системы международного сотрудничества в области менеджмента международной информационной безопасности;
- принятие международного стандарта технического регулирования в области менеджмента международной информационной безопасности.

4.2. Система международного сотрудничества в области менеджмента международной информационной безопасности. Важным направлением международного сотрудничества в области предотвращения и урегулирования инцидентов в ИКТ-среде и ослабления напряженности в кризисных ситуациях, по мнению Группы правительственных экспертов[80] является создание системы контактных пунктов на политическом и техническом уровнях.

Предлагаемая система менеджмента международной информационной безопасности (СММИБ) должна была бы базироваться на взаимодействии государственных и коммерческих организаций, обладающих объектами национальных сегментов ИКТ-среды.

В основу данной системы можно было бы положить опыт сотрудничества государственных и коммерческих организаций, приобретенный в процессе создания и применения ГосСОПКА.

В рамках деятельности данной системы обеспечивается получение и обмен информацией между НКЦКИ и субъектами критической информационной инфраструктуры, осуществляются сбор, накопление, систематизация и анализ информации, которая поступает в данную систему через средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также информации, которая может предоставляться иными, не являющимися субъектами критической информационной инфраструктуры, органами и организациями, в том числе и международными [30].

Использование этого опыта при создании СММИБ на основе национальных центров реагирования на компьютерные инциденты (ЦРКИ) можно было бы реализовать через существующие региональные и глобальные организации и сети по реагированию на чрезвычайные ситуации.

Формы и направления международного сотрудничества и стандартизации в сфере информационной безопасности имеют известную и сложившуюся практику. Наиболее распространенной формой современного межгосударственного сотрудничества является деятельность международных организаций, созданных на основе двухсторонних, многосторонних соглашений. Аппарат такой между-

80 Доклад ГПЭ A/76/135, Глава 5, С. 23–26.

народной организации обеспечивает межсессионное сотрудничество на непрерывной основе. Состав Аппарата формируется и действует на основе принципов:

- взаимодействия уполномоченных государствами-участниками компетентных координаторов на политическом и техническом уровнях в рамках единой координационной сети;
- партнерства государств-участников и заинтересованных представителей бизнеса и экспертного сообщества.

Следует отметить, что ключевую роль в развитии стандартов для ИКТ-среды играют международные отраслевые органы стандартизации, объединяющие разработчиков коммуникационных и информационных технологий, представителей технического и исследовательского сообщества, общественных организаций. Необходимо учитывать, что возможности регулирования отношений в области системы международного менеджмента международной информационный безопасности ограничены тремя международными системами стандартизации: ИСО, МЭК и МСЭ (табл. 1).

Таблица 1.

Международные профессиональные объединения в сфере нормативно-технического регулирования ИКТ-среды

Сокращение	**Наименование**	**Описание**
ACM	Association for Computing Machinery	Ассоциация вычислительной техники
ICSA	International Computer Security Association	Международная ассоциация компьютерной безопасности
IEC	International Electrotechnical Commission	Международная электротехническая комиссия
IEEE	Institute of Electrical and Electronics Engineers	Институт инженеров по электротехнике и электронике
IETF	Internet Engineering Task Force	Инженерный совет по Интернету
ISA	Internet Security Alliance	Альянс по безопасности Интернета
ISACA	Information Systems Audit and Control Association	Ассоциация аудита и контроля информационных систем
ISO	International Organization for Standardization	Международная организация по стандартизации
ISSA	Information Systems Security Association	Ассоциация по безопасности информационных систем
ITU	International Telecommunication Union	Международный союз электросвязи
UNCCT	UN Counter-Terrorism Centre	Контртеррористический центр ООН, который содействует международному сотрудничеству в области борьбы с терроризмом и оказания поддержки государствам-членам
W3C	World Wide Web Consortium	Международное сообщество, которое разрабатывает открытые стандарты для обеспечения долгосрочного развития интернет

Определенный опыт международного сотрудничества в области менеджмента информационный безопасности накоплен региональными и межгосударственными органами стандартизации. К числу таких органов относятся, например, Европейский комитет электротехнической стандартизации, отвечающий за европейские стандарты в области электротехники (CENELEC) и МГС СНГ, которые дополняют международную систему стандартизации в этой сфере.

Требования, предъявляемые международными техническими стандартами к ИКТ, напрямую затрагивают обязательства государств, т.к. определяют технологические особенности ИКТ-среды, в том числе, как пространства международного сотрудничества в области международной безопасности и мира. Развитие системы международных технических стандартов является необходимым условием для применения норм, правил и принципов ответственного поведения государств в ИКТ-среде, для выработки нормативно-технических механизмов управления рисками международной информационной безопасности, для обеспечения международной системы мониторинга соблюдения норм, правил и принципов ответственного поведения государств в ИКТ-среде, создающей условия для сбора цифровых данных, необходимых для применения мирных средств разрешения споров об инцидентах в ИКТ-среде.

4.3. Международный стандарт менеджмента международной информационной безопасности. Целью разработки нормативно-технического регулирования в сфере менеджмента международной информационной безопасности является согласование единой методологии управления рисками и создание организационной и технологической базы для практического выполнения государствами обязательств по применению норм, правил и принципов ответственного поведения государств в ИКТ-среде.

Запрос на это существует. Государства-члены международного сообщества все более четко формулируют потребность институализации системы обеспечения международной информационной безопасности и выработки общих методологических подходов к ее функционированию. Постепенно происходит трансформация политик различных региональных и международных объединений в части защиты критических информационных инфраструктур и управления цифровыми рисками. В частности, Организация экономического сотрудничества и развития (ОЭСР) констатировала, что несоответствие политик различных государств увеличивает сложность управления цифровой безопасностью взаимозависимых критических информационных инфраструктур, трансграничных сервисов и услуг. В связи с чем она считает, что международное сотрудничество является наиболее результативным для сокращения указанных несоответствий и повышения общей эффективности внутренней политики.

В 2019 г. ОЭСР выработала согласованные рекомендации по формированию правовых инструментов обеспечения цифровой безопасности критически важных видов деятельности[81], которые могут рассматриваться как политические ориентиры формирования СММИБ.

Примеры создания международных систем менеджмента безопасности организаций существуют в сферах контроля вооружений, распространения опасных заболеваний, защиты окружающей среды. Такие системы являются основой практической реализации международных договоров и построены на регламентах (протоколах/стандартах) взаимодействия уполномоченных государственных органов и национальных систем управления соответствующей деятельностью.

Для формирования каркаса СММИБ могут быть применены наилучшие практики реализации указанных международных систем менеджмента и технические стандарты в области обеспечения информационной безопасности и управления рисками[82]. Выработка конкретных предложений по созданию, функционированию и развитию СММИБ является важной научно-технической и практической задачей. Она будет решаться в ходе разработки заинтересованными государствами Универсального международного соглашения о применении норм, правил и принципов ответственного поведения государств в ИКТ-среде, что будет способствовать сохранению «открытости, безопасности, стабильности, доступности и мирности» глобальной ИКТ-среды.

Условием присоединения к сотрудничеству в рамках СММИБ будет являться добровольное согласие государства и имплементация им норм, правил и принципов ответственного поведения государств в ИКТ-среде в национальное законодательство.

Для преодоления выявленных в ходе работы проблем имплементации норм, правил и принципов ответственного поведения государств в ИКТ-среде СММИБ должна соответствовать общими принципами имплементации указанных норм[83] и реализовывать две наиболее важные функции.

1. Функция координации деятельности государств-участников СММИБ в целях:

- установления политики деятельности СММИБ, включая цели функционирования системы и условий их достижения;
- определения порядка взаимодействия государств внутри СММИБ и с внешними сторонами для реализации ими обязательств, обусловленных применением норм ответственного поведения в ИКТ-среде;

81 Recommendation of the Council on OECD Legal Instruments Digital Security of Critical Activities / / OECD, Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456.

82 В том числе с принципами и общими рекомендациями, представленными в ИСО/МЭК 31000 и ИСО/МЭК 27005.

83 Приложение 2. Проект универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде. Статья 5

- развития системы компетентных координаторов на политическом и техническом уровнях в качестве уполномоченных от государств по вопросам мониторинга соблюдения норм ответственного поведения государств в ИКТ-среде, а также вовлечения координаторов в координационную сеть в рамках международной системы мониторинга;
- эффективного обмена информацией, необходимой для поддержания СММИБ в актуальном состоянии;
- согласования перечня угроз международной информационной безопасности;
- оценки рисков нарушения международной информационной безопасности, а также рисков возникновения инцидентов в ИКТ-среде, связанных с нарушением правового режима безопасности объектов национального сегмента ИКТ-среды (риски возникновения инцидентов МИБ);
- выработки согласованных требований по обработке указанных рисков;
- реагирования на нарушения норм, правил и принципов ответственного поведения государств в ИКТ-среде;
- обеспечения эффективного контроля процессов, необходимых для соответствия требованиям СММИБ и для осуществления действий, а также достижения целей СММИБ.

2. Функция создания организационной и технологической основы функционирования СММИБ в целях:

- разграничения границ зон ответственного поведения государств в ИКТ-среде;
- обеспечения надлежащей защиты объектов критической информационной инфраструктуры путем выработки принципов единого системного подхода к организации и ведению деятельности по управлению инцидентами безопасности в ИКТ-среде и описания системы управления инцидентами безопасности объектов критической в рамках, например, общепринятой циклической модели Деминга (PDCA[84]);
- мониторинга соблюдения норм, правил и принципов ответственного поведения государств в ИКТ-среде;
- выявления и преследования лиц, виновных в террористическом и преступном использовании ИКТ;
- унификации процедур взаимодействия национальных групп реагирования, в том числе гармонизации процедур сбора, хранения и предоставления согласованной и одинаково понимаемой информации об инцидентах в ИКТ-среде, которые создают риск нарушения выполнения

84 Англ: Модель Plan-Do-Check-Act — «планируй–выполняй–проверяй–действуй». Выбор конкретной модели менеджмента может быть определен спецификой организации согласно ИСО/МЭК 27001.

государствами обязательств по применению норм, правил и принципов ответственного поведения государств в ИКТ-среде;

- оказания (по запросу) помощи пострадавшим от нарушения выполнения государствами обязательств по применению норм, правил и принципов ответственного поведения государств в ИКТ-среде;
- унификации процедур сбора, хранения и предоставления суверенными государствами информации об инцидентах нарушения международной информационной безопасности и мирных средств разрешения споров и ситуаций.

Для поддержания международного мира и безопасности особую значимость имеет содействие предупреждению нарушения обязательств, обусловленных применением норм ответственного поведения в ИКТ-среде. Разрешение таких ситуаций наиболее сложная функция СММИБ, которая требует задействование практически всех возможностей системы. В связи с этим, в рамках работы сформулированы предложения по менеджменту международной информационной безопасности, как неотъемлемой части проекта универсального международного соглашения в области мирного разрешения споров, связанных с инцидентами в ИКТ-среде.

За основу СММИБ предлагается взять скоординировано действующую совокупность центров обеспечения международной информационной безопасности национальных сегментов ИКТ-среды (контактных центров), обеспечивающих сотрудничество государств по вопросам применения норм ответственного поведения в ИКТ-среде.

В свою очередь каждый национальный контактный центр является компонентом национальной системы обеспечения международной информационной безопасности (СОМИБ), обеспечивающей общенациональный подход к решению задач системы международного менеджмента.

Государства организуют деятельность СОМИБ в рамках своей юрисдикции, в том числе в соответствии с национальными нормативно-правовыми актами в области информационной безопасности и имеющимися силами, и средствами. В собственной зоне ответственного поведения государства обеспечивают реализацию функций СММИБ и имплементацию норм ответственного поведения государств в ИКТ-среде в национальное законодательство.

Определенная база для формирования СММИБ уже существует. Большинством государств внедрены национальные системы менеджмента информационной безопасности. Так, выработана необходимая нормативная и правовая база, действуют государственные органы управления системой защиты национальных сегментов ИКТ-среды, функционируют национальные группы реагирования на компьютерные инциденты.

На основании рекомендации Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[85] определены надлежащие контактные «центры на политическом и техническом уровнях для рассмотрения серьезных инцидентов в сфере ИКТ и создание перечня таких центров», тем самым создана сеть уполномоченных организаций для трансграничного обмена информацией и взаимодействия в случае серьезных компьютерных инцидентов.

Кроме того, накоплен опыт международного сотрудничества по обеспечению безопасности критических информационных инфраструктур и противодействия киберпреступности. Кроме того, разработана база международных стандартов менеджмента информационной безопасности (серия ISO/IEC 27000), менеджмента непрерывности бизнеса (ИСО/МЭК 22301 и ГОСТ Р 53647.4-2011), менеджмента ИТ-сервисов (серия ИСО/МЭК 20000), менеджмента инцидентов информационной безопасности (ИСО/МЭК 27035 и ГОСТ Р ИСО/МЭК ТО 18044-2007) и др.

Разработка стандарта (регламента/протокола) СММИБ будет осуществляться на основе открытого и транспарентного сотрудничества всех заинтересованных сторон, в ходе которого цели и задачи системы международного менеджмента могут быть уточнены и дополнены.

Таким образом, закрепление стандарта СММИБ универсальным международным соглашением позволит создать на единых методологических принципах правовую, организационную и технологическую основу международного сотрудничества по практической реализации норм ответственного поведения государств в ИКТ-среде [18, 46], прежде всего в сфере предупреждения и разрешения инцидентов международной информационной безопасности.

85 Доклад ГПЭ A/70/174, раздел 16 a).

Литература

1. Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды / Под ред. А.Стрельцова и Э.Тикк. — Исследовательский проект международного исследовательского консорциума информационной безопасности — М.: МИКИБ, 2020, 34 с.
2. Международная информационная безопасность: теория и практика / Крутских А.В., Бирюков А.В., Бойко С.М., Волкова С.Г., Зиновьева Е.С., Зинченко А.В., Матюхин Д.В., Смирнов А.И. Учебник для вузов: в 3-х томах / Под общ. ред. А.В. Крутских. — М.: МГИМО, 2021. — Том 1 (2-е изд., доп.) — 384 с.
3. Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество / Стрельцов А.А. и др.; Предисловие В.Шерстюк — М.: НАМИБ, 2022. — 32 с.
4. Стрельцов А.А., Шерстюк В.П. Ключевые проблемы правового обеспечения международной информационной безопасности // В сборнике: Сборник докладов участников Четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». 2020. С. 48–52.
5. Шерстюк В.П. Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности. безопасность и устойчивость ИКТ-среды ради стабильности и процветания. // В сб: докладов участников Пятнадцатого международного форума. — М.: НАМИБ, 2021. С. 12–15.
6. Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. 2014. № 11. С. 20–34.
7. Международная информационная безопасность. Новая геополитическая реальность / М. Б. Алборова и др.; ред.: Е. С. Зиновьева, М. Б. Алборова. — М.: Аспект Пресс, 2021. 112 с.
8. Стрельцов А.А. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству Право и государство: теория и практика. 2014. № 3 (111). С. 75–88.
9. 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. 138–142.

10. Voluntary, non-binding norms for responsible state behaviour in the use of information and communications technology. / By ed. E.Tikk -NY.: UNODA, 2017. — 296 p.
11. Стрельцов А.А. Новая доктрина информационной безопасности Российской Федерации: информационно-правовые основы обеспечения безопасности информационных угроз // Труды по интеллектуальной собственности. 2017. Т. 28. № 1. С. 116–123.
12. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под. ред. Зегжды Д.П., Москва, 2021. М.: Горячая линия — Телеком, 2021. — 560 с.
13. Мирошников Б.Н. Перспективы международного сотрудничества в рамках Конвенции о киберпреступности // Национальные интересы: приоритеты и безопасность. 2007. Т. 3. № 6 (15). С. 46–48.
14. Бойко С.М., Дылевский И.Н., Комов С.А. и др. Возможные направления реализации военной политики Российской Федерации в области международной информационной безопасности в современных условиях // Военная мысль. 2009. № 4. С. 10–15.
15. Полякова Т.А. Формирование единого научно-технологического пространства союзного государства: правовые проблемы, перспективы и инновации // Государство и право. 2018. № 4. С. 81–90.
16. Зиновьева Е.С. Киберсдерживание и цифровая дилемма безопасности в американском экспертном дискурсе // Международные процессы. 2019. Т. 17. № 3 (58). С. 51–65.
17. Касенова М.Б. Корпорация интернета по распределению имен и адресов в механизме управления интернетом // Юрист. 2013. № 24. С. 35–37.
18. Стрельцов А.А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. — 2017. — № 2. — С. 87–106.
19. Стрельцов А.А., Пилюгин П.Л. К вопросу о цифровом суверенитете // Информатизация и связь. 2016. № 2. С. 25–30.
20. Рожкова М.А. Категории «цифровое право», «цифровые права» и «цифровая валюта» в российском праве // Право цифровой экономики — 2021 (17): Ежегодник-антология / Рук. и науч. ред. М. А. Рожкова. М.: Статут, 2021. С. 10–68.
21. Рожкова М.А. Цифровые права: публично-правовая концепция и понятие в российском гражданском праве // Хозяйство и право. 2020. № 10 (525). С. 3–12.
22. Стрельцов А.А. О предмете и методе информационного права // Информационное право. — 2019. — № 4. — С. 4–11.

23. Кефели И.Ф., Мальмберг С. Информационный потенциал государства как основа информационного суверенитета. // Управленческое консультирование. № 1. 2019 С. 29–39;
24. Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 6 (67). С. 44–51.
25. Полякова Т.А. Цифровизация и синергия правового обеспечения информационной безопасности // Информационное право. 2019. № 2. С. 4.
26. Цифровая трансформация: вызовы праву и векторы научных исследований: монография / Под общ. ред. А.Н. Савенкова; отв. ред. Т.А. Полякова, А.В. Минбалеев. М.: РГ-Пресс, 2021. С. 62.
27. Полякова Т.А., Смирнов А.А. Международной информационной безопасности: проблемы и перспективы // Российский юридический журнал. 2022. № 3 (144). С. 7–15.
28. Ясносокирский Ю.А. К вопросу о применимости международного права в информационной сфере // Международная жизнь. 2021. № 7. С. 12–17.
29. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. М.: ИМЭМО РАН, 2020. 98с. DOI: 10.20542/978-5-9535-0581-9.
30. Месенгисер Я.Я., Малахов М.А., Милославская Н.Г. Центры управления сетевой безопасностью как силы ГосСОПКА // Безопасность информационных технологий. 2022. Т. 29. № 1. С. 94–107.
31. Сурма И.В. КиберНАТО и угрозы цифровому суверенитету России. В сборнике: Прогнозируемые вызовы и угрозы национальной безопасности Российской Федерации и направления их нейтрализации. Сборник материалов круглого стола. Москва, 2021. С. 562–577.
32. Жарова А.К. Обеспечение защиты государства от компьютерных атак в ИКТ-сфере // Труды Института государства и права Российской академии наук. 2022. Т. 17. № 4. С. 100–125.
33. Марков А.С., Ромашкина Н.П. Проблема выявления источника (атрибуции) кибератак — фактор международной безопасности // Мировая экономика и международные отношения. 2022. Т. 66. № 12. С. 58–68.
34. Смирнов А.И. Проблема атрибуции кибератаки в контексте международной информационной безопасности. В кн.: Международная информационная безопасность: Новая геополитическая реальность. / Алборова М.Б. и др. / Под ред. Е.С.Зиновьевой, М.Б.Алборовой. — М.: Аспект Пресс, 2021. С. 61–66.

35. Сурма И.В. Кибербезопасность и современные формы межгосударственного противоборства // Дипломатическая служба. 2021. № 2. С. 199–206.
36. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. М.: «Горячая линия-Телеком», 2021. 240 с.
37. Жарова А.К. Обеспечение информационного суверенитета Российской Федерации // Юрист. 2021. № 11. С. 28–33.
38. Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО Университета. 2011. № 4 (19). С. 154–162.
39. Петренко С.А. О решении проблемы раннего предупреждения компьютерного нападения на критическую информационную инфраструктуру российской // Методы и технические средства обеспечения безопасности информации. 2019. № 28. С. 15–19.
40. Марков А. С., Шеремет И. А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник академии военных наук. — 2019. — № 2. — С. 82–90.
41. Барабанов А.В., Марков А.С., Цирлов В.Л. Международная сертификация в области информационной безопасности // Стандарты и качество. 2016. № 7. С. 30–33.
42. Абашидзе А.Х, Солнцев А.М. Международное право. Мирное разрешение споров. М.: Юрайт, 2021. С. 30.
43. Кэрон Д.Д., Шинкарецкая Г.Г. Мирное разрешение споров посредством права. Вне конфронтации. Международное право в период после холодной войны: сб. статей. М., Спарк, 1996. С. 323
44. Брехова Н.А. Современные арбитражные средства разрешения морских споров. // Право и политика. 2003. 7. С. 66–74.
45. Вельяминов Г.М., Крылов Н.Б., Шинкарецкая Г.Г. Судьба конвенции ООН по морскому праву // Труды Института государства и права Российской академии наук. 2022. Т. 17. № 5. С. 128–148.
46. Стрельцов А.А. Международное нормативное регулирование безопасности в среде информационно-коммуникационных технологий. В кн.: Проблемы развития права и правоприменения в условиях социально-экономических преобразований на современном этапе. Монография. / Под. общ.ред. В.Н.Синюкова и М.А.Егоровой. — М.: Приоритет 2030, 2023. С. 281–294.

Приложение 1

Предложения в проект позиции Российской Федерации по вопросам применения норм ответственного поведения государств в ИКТ-среде

Настоящие предложения отражают мнение экспертов, выполнявших НИР, по проблеме применения норм ответственного поведения государств в ИКТ-среде, являющихся частью системы международных нормативных механизмов регулирования сотрудничества в области обеспечения международной информационной безопасности. Кроме того, в предложениях сформулированы подходы к решению этой проблемы.

Реализация предложений будет способствовать «развитию сотрудничества с иностранными государствами, международными, международными неправительственными организациями и организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, в целях выработки механизма обмена информацией о таких инцидентах и повышения эффективности взаимодействия уполномоченных органов»[86].

Предложения могут быть использованы при подготовке позиции Российской Федерации по проблемам формирования системы международной информационной безопасности в рамках участия российских экспертов в работе:

- Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (РГОС)[87];
- тематических подгрупп межгосударственного обмена мнениями по отдельным вопросам, связанным с мандатом РГОС;
- рабочих органов других региональных организаций.

Предложения могут также составить предмет обсуждения представителей государственных органов власти, бизнеса, неправительственных организаций и научно-экспертного сообщества при выборе приоритетных направлений сотрудничества в области формирования системы международной информационной безопасности.

Нормы ответственного поведения государств в ИКТ-среде рекомендованы к рассмотрению государствам резолюциями 70-й и 76-й сессий Генеральной Ассамблеи ООН по докладам Групп правительственных экспертов ООН[88].

---

86 Указ Президента Российской Федерации от 12 апреля 2021 г. №213. Основы государственной политики Российской Федерации в области международной информационной безопасности.

87 Группа созвана Генеральным Секретарем ООН в соответствии с Резолюцией Генеральной Ассамблеи ООН A/RES/75/240 от 31 января 2021 г.

88 Доклады ГПЭ A/70/174 от 22 июля 2015 г., A/76/135 от 14 июля 2021 г.

I. Исходные положения

1.1. Среда информационно-коммуникационных технологий (ИКТ-среда), образуемая совокупностью объектов информационной инфраструктуры (цифровых данных, расположенных на электронно-вычислительных устройствах; цифровых ИКТ обработки информации; коммуникационных сетей и сетей связи) и пользователей, использующих эту инфраструктуру для участия в разнообразных общественных отношениях, является важным фактором развития общества и государства.

Информационная инфраструктура обеспечивает функционирование национального сегмента ИКТ-среды и одновременно является одной из ключевых составляющих инфраструктуры Российской Федерации.

Безопасность использования национального сегмента ИКТ-среды и устойчивость функционирования национальной информационной инфраструктуры оказывают существенное влияние на национальную безопасность Российской Федерации.

1.2. Национальный сегмент ИКТ-среды является составной частью глобальной ИКТ-среды, техническую основу которой составляют распределенные сети вычислительных машин, глобальные сети связи и глобальная информационно-коммуникационная сеть Интернет.

Злонамеренная и вредоносная деятельность некоторых государств и иных субъектов международного сотрудничества, осуществляемая в военных, террористических и преступных целях на национальном, региональном и глобальном уровнях становится все более серьезной проблемой.

Особую озабоченность вызывает злонамеренная и вредоносная деятельность в сфере использования ИКТ, затрагивающая объекты критической информационной инфраструктуры, т.к. объекты данной инфраструктуры используются для предоставления основных услуг населению, для обеспечения общей доступности и целостности сети Интернет, организаций экономической, социальной, политической и культурной жизни общества, органов управления государством.

В обозримой перспективе значение противодействия угрозам обеспечения безопасности использования ИКТ и устойчивости функционирования объектов критической информационной инфраструктуры как факторов обеспечения национальной и международной безопасности будет увеличиваться.

1.3. ИКТ-среда как пространство международного сотрудничества обладает свойствами, принципиальным образом отличающими ее от традиционных пространств реализации территориального суверенитета государств и международного сотрудничества (суша, водное, воздушное и космическое пространство, недра), к которым относятся: особый характер общественных отношений, реали-

зуемых с использованием этого пространства; особые свойства информации как объекта обработки с использованием ИКТ; особый характер способов поддержания функционирования ИКТ-среды как пространства осуществления информационной деятельности человека; особый правовой статус человека как субъекта информационной деятельности, в том числе и в ИКТ-среде.

1.4. Добровольные, необязательные нормы ответственного поведения государств в ИКТ-среде, являясь средством нормативного регулирования международных отношений, представляют собой рекомендательные, юридически необязательные правила поведения государств как субъектов международного права, перечисленные в докладах групп правительственных экспертов ООН и рекомендованные для изучения резолюциями Генеральной Ассамблеи ООН.

Эти правила поведения государств дополняют нормы международного и национального права и нормы, закрепленные в международных политических договорённостях, а также нормы поведения, вытекающие из общих принципов общественной морали.

Добровольные, необязательные нормы ответственного поведения государств могут при определённых обстоятельствах в будущем учитываться при толковании действующих международно-правовых норм, использоваться при формировании новых международных обычаев и составить основу нормативного правового механизма, регулирующего международные отношения в области использования ИКТ-среды.

1.5. Применение норм ответственного поведения государств в ИКТ-среде является одной из форм реализации (в форме действия или бездействия государств и уполномоченных органов государственной власти в конкретных ситуациях), с учетом норм международного и национального права, положений международных политических договорённостей и этических норм, распространяющихся на данное государство.

II. Проблема применения добровольных, необязательных норм ответственного поведения государств в ИКТ-среде

2.1. Применение добровольных, необязательных норм ответственного поведения государств в ИКТ-среде для регулирования международных отношений и общественных отношений в рамках национальной юрисдикции сталкивается с рядом сложностей, имеющих фундаментальный характер.

2.2. Во-первых, нормы ответственного поведения государств в ИКТ-среде не вытекают непосредственно из существующих норм международного права, т.е. не являются положениями lex lata (закон в том виде, в каком он существует) международного публичного права. Эти нормы направлены на уточнение толко-

вания существующих норм международного права применительно к отношениям в ИКТ-среде, а также на расширение состава международной нормативной системы, регулирующей деятельность в области использования ИКТ.

Вследствие этого для применения норм ответственного поведения государств в ИКТ-среде необходимо создание соответствующей международной правовой или политической основы, с одной стороны, закрепляющей их в качестве элементов нормативной международной правовой или международной политической системы, а с другой — создающей определенные основания для их регулирующего воздействия как на международные отношения, так и на общественные отношения, регулируемые национальным законодательством.

2.3. Во-вторых, добровольность и необязательность норм ответственного поведения государств в ИКТ-среде, а также отсутствие их непосредственной взаимосвязи с существующими нормами международного права, создают дополнительные препятствия на пути их непосредственной имплементации в национальное законодательство.

2.4. В-третьих, отношение государств к соблюдению принципов Устава ООН и других норм международного права отличается дихотомией между теми видами использования ИКТ, которые государства не хотят допускать в отношении себя, и теми видами использования ИКТ, которые они хотели бы иметь возможность использовать в отношении других.

2.5. В-четвертых, многообразие подходов к толкованию содержания принципа уважения суверенитета, артикулированного некоторыми государствами в качестве императивной нормы, в конечном счёте свидетельствует об отсутствии самого правила, которое могло бы применяться в отношении ИКТ. Полифоничность позиций государств не позволяет предположить возможность достижения консенсуса по этому вопросу в процессе практического применения норм ответственного поведения государств в ИКТ-среде.

2.6. В-пятых, юридически обязательные нормы международного права, на которых частично базируются нормы ответственного поведения (принцип суверенного равенства государств и вытекающий из него принцип невмешательства во внутренние дела, принцип неприменения силы и угрозы силой, принцип надлежащей осмотрительности, нормы международного гуманитарного права и международного права прав человека, а также нормы международной ответственности) имеют частично несовпадающие сферы применения в пространстве ИКТ-среды.

Вследствие этого обязательства государств, вытекающие из утверждения о применимости принципов международного права к регулируемым нормами ответственного поведения в области ИКТ-среды отношениям, требуют обоснования применительно к каждой норме отдельно.

2.7. В-шестых, представления государств о границах зон ответственного поведения государств в ИКТ-среде существенно различаются. Одни государства исходят из доктринального толкования этих границ как границ территорий государств, на которых расположены объекты национального сегмента ИКТ-среды (именно к этой категории можно отнести так называемое «Таллиннское руководство»[89]), в то время как другие — полагают необходимым консенсуальный подход к решению этого вопроса.

Вследствие этого трудно предположить возможность достижения согласия по данному вопросу в процессе применения норм ответственного поведения государств в ИКТ-среде.

2.8. В-седьмых, применению норм ответственного поведения государств в ИКТ-среде в форме имплементации препятствует также их терминологическая несогласованность с нормами национального законодательства, а также отсутствие правовых оснований для их реализации в системе российского права.

2.9. В-восьмых, особой проблемой применения норм ответственного поведения государств в ИКТ-среде является отсутствие поддержки процесса их применения со стороны международного нормативного технического регулирования, обусловливающего возможность сбора объективной информации по предметам международных споров и ситуаций в ИКТ-среде.

Исходя из изложенного, применение норм ответственного поведения государств в ИКТ-среде может осуществляться только на основе соответствующего международного соглашения.

III. Предложения по решению проблем применения норм ответственного поведения государств в ИКТ-среде

3.1. Решение проблемы применения норм ответственного поведения в ИКТ-среде предлагается осуществлять посредством последовательного решения следующих задач.

3.2. Адаптация норм и принципов международного права к регулированию отношений в области применения ИКТ и функционирования глобальной информационной инфраструктуры в рамках ИКТ-среды как нового пространства международного сотрудничества.

3.2.1. Адаптация норм и принципов международного права должна способствовать, с одной стороны, достижению устойчивого развития национальных обществ на основе реализации потенциала ИКТ во всех сферах жизнедеятельности человека, а с другой — поддержанию международного мира и безопасности в ус-

89 Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual). M.Schmitt et al. eds. Cambridge University Press, forthcoming 2013.

ловиях возникновения инцидентов в ИКТ-среде. Такие инциденты возникают вследствие злонамеренной и вредоносной деятельности некоторых государств и иных субъектов международного сотрудничества, направленной на достижения военных, террористических и преступных целей, на национальном, региональном и глобальном уровнях.

3.2.2. В рамках адаптации норм и принципов международного права к применению в ИКТ-среде необходимо осуществить следующее:

- международное правовое закрепление границ зон ответственного поведения государств в ИКТ-среде;
- уточнение международных обязательств государств в отношении сотрудничества в ИКТ-среде;
- уточнение обязательств государств в области обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ;
- создание системы координаторов на политическом и техническом уровнях и определение порядка их взаимодействия в рамках единой координационной сети, обеспечивающей безопасное использование и устойчивое функционирование ИКТ-среды.

Международные обязательства государств по сотрудничеству в области использования ИКТ-среды вытекают из принципов международного права, и, в частности, из принципа мирного разрешения международных споров. В то же время такие обязательства не возникают в связи с применением норм ответственного поведения государств в ИКТ-среде, регулирующих отношения в области обеспечения безопасности критической информационной инфраструктуры.

3.3. Развитие на основе соглашений государств и международных организаций системы норм международного права, закрепляющих обязательства государств по вопросам применения норм ответственного поведения в ИКТ-среде, по процедуре их имплементации в национальное законодательство.

Кроме того, закрепление в данной системе норм международного права обязательств государств по сотрудничеству в области согласования правовых механизмов регулирования соответствующих групп общественных отношений с учетом различия терминологии, используемой для описания этих отношений.

3.4. Организация международного сотрудничества по вопросам развития системы технических стандартов, применение которых создает условия для сбора суверенными государствами информации об инцидентах в ИКТ-среде. Такое сотрудничество призвано обеспечить соблюдение обязательств государств, вытекающих из принципа международного права по разрешению мирными средствами международных споров и спорных ситуаций в ИКТ-среде.

IV. Основные направления международного сотрудничества в целях применения норм ответственного поведения государств в ИКТ-среде

4.1. Применение норм ответственного поведения государств в ИКТ-среде имеет целью сохранение на основе сотрудничества государств открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, имеющей важное значение для устойчивого развития современного общества.

4.2. Выделяются следующие основные направления международного сотрудничества в области применения норм ответственного поведения государств в ИКТ-среде:

- формирование общего понимания содержания норм ответственного поведения государств в ИКТ-среде, а также процессуальных механизмов их реализации, включая вопросы сотрудничества в установлении и поддержании международного правового режима безопасности объектов критической информационной инфраструктуры, применение мирных средств разрешения спорных ситуаций в ИКТ-среде;
- делимитация и демаркация границ зон ответственного поведения государств в ИКТ-среде;
- имплементация норм ответственного поведения государств в ИКТ-среде в национальное законодательство;
- обмен информацией, оказание взаимопомощи, преследование лиц, виновных в террористическом и преступном использовании ИКТ;
- развитие системы координаторов на политическом и техническом уровнях и вовлечение координаторов в координационную сеть.

4.4. Сотрудничество в области формирования общего понимания содержания норм ответственного поведения государств в ИКТ-среде имеет целью предупреждение спорных ситуаций, связанных с толкованием регулируемых норм и регулируемых отношений и, соответственно, с толкованием содержания принимаемых государствами соответствующих обязательств.

К числу понятий, используемых в нормах ответственного поведения государств в ИКТ-среде и не имеющих однозначного толкования, относятся следующие: «международно-противоправные деяния с использованием ИКТ»; «вредоносное использование ИКТ»; «террористическое и преступное использование ИКТ», «злонамеренные программные и технические средства ИКТ», «скрытые вредоносные функции».

Добросовестному применению норм будет способствовать уточнение видов деятельности государств в сфере ИКТ, относимых к «злонамеренным», «заведомо противоречащим международному праву», «наносящим преднамеренный ущерб критически важной инфраструктуре», а также достижение договорен-

ности по вопросам классификации «надлежащих» мер, принимаемых государством для защиты своей критически важной инфраструктуры, а также критериев «разумности» мер обеспечения целостности каналов поставки.

4.5. Предупреждению возникновения спорных ситуаций будет способствовать также уточнение обязательств государств в области установления запрета следующих действий:

- использование своей территории для совершения противоправных деяний, распространения злонамеренных программных и технических средств в сфере ИКТ, а также средств, обладающих скрытыми вредоносными функциями;
- осуществление деятельности, противоречащей обязательствам по международному праву, а также деятельности, призванной нанести ущерб информационным системам уполномоченных групп экстренного реагирования на компьютерные инциденты другого государства.

Достижению этой цели будет способствовать уточнение процессуальных вопросов реализации норм ответственного поведения государств в ИКТ-среде, связанных с обследованием объектов ИКТ-среды, в том числе объектов критической информационной инфраструктуры, и сбором информации, необходимой для применения мирных средств разрешения международных спорных ситуаций в ИКТ-среде.

4.6. Сотрудничество в области согласования процедур и механизмов осуществления демаркации и делимитации границ зон ответственного поведения государств в ИКТ-среде является одним из условий применимости средств мирного разрешения международных споров к отношениям в этой области, а также равноправного сотрудничества по вопросам применения норм ответственного поведения государств, основанного на «суверенитете государств, международных нормах и принципах, проистекающих из суверенитета»[90].

4.6.1. С учетом особенностей ИКТ-среды как глобальной составляющей информационной сферы, включающей взаимосвязанные сети объектов информационной инфраструктуры, делимитация могла бы заключаться в закреплении в международном договоре цифровых идентификаторов объектов ИКТ-среды, находящихся под суверенитетом государства.

4.6.2. Демаркация границы зоны ответственного поведения государства в ИКТ-среде могла бы заключаться в оснащении объектов национальной зоны ответственного поведения специальным программным обеспечением и техническим оборудованием, применение которого создаст условия для поддержания правового режима границы, а также международного правового режима безопасности объектов критической информационной инфраструктуры.

90 Доклад ГПЭ A/70/174, п.27.

4.6.3. В рамках правового режима зоны ответственного поведения государства следует определить механизм обеспечения соблюдения обязательств, вытекающих из норм ответственного поведения государств в ИКТ-среде. Такие обязательства включают обязательства по нормативно-техническому регулированию отношений в области:

- предупреждения и пресечения противоправной деятельности в ИКТ-среде с учетом положений морского, воздушного и космического права;
- деятельности «заведомо противоречащей международному праву» и «наносящей преднамеренный ущерб критически важной инфраструктуре»;
- совершения «международно-противоправных деяний с использованием ИКТ» и «вредоносного использования ИКТ, способного создать условия для нарушения международного мира и безопасности», «террористического и преступного использования ИКТ»;
- оказания помощи государствам, критически важная инфраструктура которых становится объектом злонамеренных действий и другой деятельности, не способствующей поддержанию международного мира и безопасности.

4.7. Сотрудничество в области имплементации в национальное законодательство норм ответственного поведения государств в ИКТ-среде имеет целью создание условий для гармонизации этих норм и норм национального права, регулирующих отношения в области осуществления информационной деятельности в различных сферах общественной жизни.

Это сотрудничество базируется, с одной стороны, на принципе добровольности выполнения международных обязательств[91], а с другой — на императивной норме международного права, устанавливающей для государств «невозможность ссылаться на положения своего внутреннего права в качестве оправдания для невыполнения им договора»[92].

4.8. Сотрудничество в области обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, является относительно новым направлением взаимодействия государств и других субъектов международного права.

В настоящее время это сотрудничество целесообразно сосредоточить на содействии продвижению на заседаниях Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности российского проекта конвенции ООН о противодействии использованию ИКТ в преступных целях.

---

91 Венская конвенция о праве международных договоров. 1969 г., Ст. 6.

92 Там же. Ст. 27.

4.9. Сотрудничество в области развития системы координаторов на политическом и техническом уровнях и вовлечение координаторов в координационную сеть имеет целью обеспечение надёжной и прямой связи между государствами в целях предотвращения и урегулирования серьезных инцидентов в сфере использования ИКТ и ослабления напряженности в кризисных ситуациях.

Коммуникация между контактными пунктами, осуществляемая под эгидой уполномоченной международной организации (например, Международный союз электросвязи) могла бы помочь снизить напряженность и предотвратить недопонимание, которые могут возникнуть в результате инцидентов в сфере использования ИКТ, в том числе затрагивающих объекты критической информационной инфраструктуры и имеющих национальное, региональное или глобальное значение.

Государства могли бы расширить использование контактных пунктов для обмена информацией и оказания помощи в эффективном управлении инцидентами в сфере использования ИКТ, а также в содействии урегулированию таких инцидентов[93].

По существу, речь может идти о создании специализированного механизма (платформы доверия) практического взаимодействия государств по политическим, нормативным и техническим вопросам применения мирных средств разрешения спорных ситуаций в ИКТ-среде таким образом, чтобы «не подвергать угрозе международный мир, безопасность и справедливость»[94].

93 Доклад ГПЭ A/76/135, п. 76.
94 Ст. 2 п. 3 Устава ООН.

Приложение 2

Универсальное международное соглашение о применении норм ответственного поведения государств в ИКТ-среде

(проект)

Преамбула

Государства — участники настоящего Соглашения,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств коммуникации,

осознавая, что информационно-коммуникационные технологии (ИКТ) могут использоваться как в законных, так и в злонамеренных целях, и что доказательства совершения таких деяний могут храниться в этих сетях и передаваться по ним,

подчеркивая, что все государства заинтересованы в использовании ИКТ в мирных целях в интересах всего человечества для создания информационного общества и дальнейшего устойчивого развития всех стран,

выражая озабоченность по поводу возможности включения в ИКТ скрытых вредоносных функций, которые угрожают безопасности использования ИКТ, а также подрывают доверие между участниками систем производства и сбыта продуктов ИКТ, предоставления услуг в области использования ИКТ,

считая необходимым предотвратить использование информационных ресурсов или технологий для причинения ущерба национальной безопасности, а также для осуществления преступных или террористических деяний,

отмечая, что ООН должна играть ведущую роль в формировании среди государств-членов общего понимания условий безопасного использования ИКТ, а также порядка применения международного права и норм ответственного поведения государств в этой сфере,

напоминая содержащийся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/70/174, 2015) вывод о важнейшем значении следующих принципов Устава ООН и прочих норм международного права: суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в международных отношениях от применения силы или угрозы силой как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями ООН; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств,

подтверждая содержащийся в докладах Группы правительственных экспертов 2013, 2015 и 2021 годов вывод, о том, что международное право, и в частности Устав ООН, применяются к отношениям в ИКТ-среде и имеют важное значение для создания открытой, безопасной, стабильной, доступной и мирной информационной среды, а также вывод о том, что применение норм, правил и принципов ответственного поведения государств в сфере использования ИКТ может снизить риск нарушения международного мира, безопасности и стабильности,

будучи убеждены в необходимости выработки в приоритетном порядке общей политики по адаптации международного права к применению в ИКТ-среде, в том числе посредством развития международного технического регулирования,

подтверждая, что суверенитет государств, международные нормы и принципы, проистекающие из суверенитета, применяются к деятельности государств в ИКТ-среде и к их юрисдикции над расположенной на их территории ИКТ-инфраструктурой,

вновь подтверждая право и обязанность государств бороться, в рамках своих конституционных полномочий, против распространения фальшивых сообщений, которые могут рассматриваться как вмешательство во внутренние дела других государств, наносящие ущерб укреплению мира, сотрудничества и дружественных отношений между государствами и нациями,

осознавая обязанность государств воздерживаться от применения оскорбительной или враждебной пропаганды и злонамеренных информационных кампаний для вмешательства во внутренние дела других государств,

подчеркивая, что государства несут главную ответственность за поддержание безопасной и мирной ИКТ-среды и признают необходимость вовлечения в диалог частного сектора, научных кругов и гражданского общества, а также сотрудничества между государствами и частным сектором в борьбе против злонамеренного и вредоносного использования ИКТ,

полагая, что для эффективной борьбы против компьютерных преступлений требуется более широкое, оперативное и хорошо отлаженное международное сотрудничество в области применения норм ответственного поведения государств в ИКТ-среде,

будучи убеждены в том, что настоящее соглашение необходимо для сдерживания действий, направленных против целостности и доступности цифровых данных, а также против безопасности использования компьютерных систем и сетей,

выражая надежду, что настоящее соглашение будет способствовать поддержанию безопасной и мирной ИКТ-среды посредством: предоставления государствам достаточных полномочий для эффективной борьбы с вредоносным

использованием ИКТ, а также содействия выявлению и расследованию ситуаций такого использования ИКТ, выявлению совершающих такие деяния государств; разработки механизмов оперативного и надежного международного взаимодействия государств по вопросам противодействия такому использованию ИКТ,

подчеркивая важность уважения прав человека и основных свобод в сфере использования ИКТ,

памятуя о необходимости обеспечения должного баланса между интересами поддержания правопорядка и уважения основополагающих прав человека, как это предусмотрено Конвенцией Совета Европы о защите прав человека и основных свобод от 1950 года, Международным пактом ООН о гражданских и политических правах от 1966 года и другими применимыми международными договорами о правах человека, в которых подтверждается право каждого независимо от государственных границ беспрепятственно придерживаться своего мнения, право на свободное выражение своего мнения, включая свободу искать, получать и распространять всякого рода информацию и идеи, право на невмешательство в личную жизнь,

согласились о нижеследующем:

Глава I. Общие положения

Статья 1. Употребление терминов

В целях настоящего соглашения:

«Информационно-коммуникационные технологии (ИКТ)» означает совокупность процессов, способов и методов поиска, сбора, хранения, обработки, представления и распространения цифровых данных пользователям (информационные технологии), а также процессов, способов и методов передачи цифровых данных по каналам и сетям связи, а также коммуникационным сетям (коммуникационные технологии).

«Цифровые (компьютерные) данные» (далее — «цифровые данные», «данные») означает любое представление фактов, сведений или понятий в форме, пригодной для обработки с помощью компьютерных систем, в том числе программ, предназначенных для выполнения компьютерной системой определенных действий.

«ИКТ-продукт» означает представленное на рынке изделие (программное или техническое) промышленного производства, предназначенное для автоматизации процессов поиска, сбора, хранения, обработки и представления требуемой информации по запросам пользователей, а также для автоматизации процессов передачи информации в коммуникационных сетях и сетях связи.

«Компьютерная система» означает любое устройство или совокупность соединенных между собой или связанных устройств, одно либо более из которых осуществляет автоматическую обработку данных в соответствии с программой.

«Информационная система» означает совокупность цифровых данных, а также ИКТ-продуктов, обеспечивающих поиск, сбор, хранение, обработку и представление требуемой информации по запросам пользователей.

«Использование ИКТ» означает процессы применения ИКТ-продуктов субъектом жизнедеятельности общества для решения конкретных задач социального взаимодействия, а также для управления устройствами и механизмами.

«Критически важная инфраструктура» означает использующую информационную инфраструктуру отрасль хозяйственной деятельности государства по оказанию материальных (производство, торговля, общественное питание, жилищно-коммунальные, бытовое обслуживание, транспорт и связь) и нематериальных услуг (образование, культура, здравоохранение, спорт, государственное управление, оборона, охрана порядка) как общественного блага.

«ИКТ-среда» означает совокупность: информационных систем; коммуникационных сетей, включая сеть Интернет, и сети связи; ИКТ-продуктов, осуществляющих обработку цифровых данных для решения конкретных задач социального взаимодействия и для управления устройствами и механизмами.

«Информационная инфраструктура» («ИКТ-инфраструктура») означает систему организационных структур, подсистем, обеспечивающих функционирование и развитие ИКТ-среды.

«Национальный сегмент ИКТ-среды» означает совокупность объектов информационных инфраструктур, создание, развитие и использование которых осуществляется на основе государственного суверенитета.

«Поведение государства в ИКТ-среде» означает совокупность политических, правовых и организационных мер, направленных на упорядочение процессов создания и использования информационной инфраструктуры для решения конкретных задач социального взаимодействия, а также для управления устройствами и механизмами.

«Ответственное поведение государств в ИКТ-среде» означает совокупность политических, правовых и организационных мер, направленных на упорядочение процессов создания и использования ИКТ-инфраструктуры для решения конкретных задач социального взаимодействия, а также для управления устройствами и механизмами, осуществляемого с соблюдением международных обязательств государства.

«Злонамеренная деятельность с использованием ИКТ» означает совокупность политических, правовых и организационных мер, направленных на нане-

сение вреда безопасности использования или устойчивости функционирования составляющих информационную инфраструктуру и ИКТ-продуктов;

«Деятельность в сфере ИКТ, наносящая ущерб критически важной инфраструктуре», означает способ применения ИКТ-продуктов, нарушающий устойчивость функционирования и безопасности использования ИКТ-инфраструктуры.

«Террористическое и преступное использование ИКТ» означает использование ИКТ-продуктов для осуществления террористической и преступной деятельности.

«Действия в сфере ИКТ, признанные вредоносными или способными создать угрозу международному миру и безопасности», означает такие способы использования ИКТ-продуктов, которые признаны Советом Безопасности ООН вредоносными или способными создать угрозу международному миру и безопасности.

«Международный инцидент» (далее — инцидент) в сфере ИКТ означает событие, заключающееся в нарушении безопасности использования систем, сетей и ИКТ-продуктов, составляющих ИКТ-инфраструктуру, и приводящее к возникновению спора между государствами или к ситуации роста напряженности в международных отношениях.

«Злонамеренный инцидент в сфере ИКТ» означает инцидент в сфере ИКТ, возникший вследствие злонамеренной деятельности государств или других субъектов международного права.

«Уязвимость в операционных технологиях и взаимосвязанных вычислительных устройствах, платформах, машинах или объектах, составляющих Интернет вещей» означает особенность программного ИКТ-продукта (операционная система, информационная система) или технического ИКТ-продукта (сети вычислительных и коммуникационных устройств) системы Интернета вещей, заключающаяся в том, что данная особенность может быть использована недобросовестными субъектами для нарушения описанного в эксплуатационной документации на эти ИКТ-продукты процесса обработки цифровых данных.

«Нормы ответственного поведения государств в ИКТ-среде» означает систему международных обязательств государств в области ответственного поведения государств в ИКТ-среде, закрепленных в настоящем Соглашении.

«Норма ответственного поведения государств в ИКТ-среде» означает правило поведения, следование которому принято государством в качестве международного обязательства.

«Зона ответственного поведения государства в ИКТ-среде» означает совокупность информационных систем, коммуникационных сетей, ИКТ-продуктов, осуществляющих обработку цифровых данных для решения конкретных задач

социального взаимодействия и для управления устройствами и механизмами, входящих в состав национального сегмента ИКТ-среды.

«Оператор (поставщик) услуг в области использования ИКТ» означает:

любую государственную или частную организацию, предоставляющую своим пользователям возможность обмениваться цифровыми данными (коммуникационные услуги) посредством компьютерной системы;

любую иную организацию, которая обрабатывает или хранит цифровые данные по поручению организации, предоставляющей коммуникационные услуги, либо пользователей таких услуг.

«Данные трафика» означает любые цифровые данные, связанные с операциями по передаче данных посредством компьютерной системы, которые созданы компьютерной системой как отдельной составляющей цепочки передачи данных, и указывают на источник сообщения, его назначение, маршрут, время, дату, размер, длительность, или тип лежащей в его основе услуги;

«Целостность каналов поставки продуктов ИКТ («ИКТ-продуктов»)» означает свойство информационной инфраструктуры обеспечивать устойчивое и безопасное взаимодействие между поставщиками и потребителями ИКТ-продуктов.

«Раскрытие информации об уязвимостях в сфере ИКТ» означает публикацию в открытых или специализированных средствах массовой информации результатов сертификации ИКТ-продуктов на безопасность использования.

«Национальная группа реагирования на компьютерные инциденты (CERT) или Национальная группа реагирования на инциденты в сфере компьютерной безопасности (CSIRT)» означает группу экспертов по компьютерной безопасности, уполномоченную государством (или управомоченную законодательством) осуществлять сбор, обобщение информации об инцидентах в национальном сегменте ИКТ-среды, участвовать в ликвидации последствий возникновения инцидентов, а также обмениваться информацией об инцидентах с группами реагирования на компьютерные инциденты других государств.

«Система менеджмента международной информационной безопасности» — совокупность центров обеспечения международной информационной безопасности национальных сегментов ИКТ-среды (контактных пунктов), взаимодействующих в целях сотрудничества государств по вопросам применения норм ответственного поведения государств в ИКТ-среде.

«Менеджмент международной информационной безопасности» означает согласованную деятельность центров обеспечения международной информационной безопасности национальных сегментов ИКТ-среды (контактных пунктов), осуществляемую в целях сотрудничества государств по вопросам применения норм ответственного поведения государств в ИКТ-среде.

«Орган» означает международный орган по содействию применению норм ответственного поведения государств в ИКТ-среде.

«Деятельность государств, связанная с ИКТ», означает деятельность по развитию объектов информационной инфраструктуры, регулированию отношений в области использования ИКТ и обеспечения их безопасности.

Статья 2. Сфера применения

1. «Государство-участник» означает государство, которое согласилось на обязательность для него положений настоящего Соглашения и для которого настоящее Соглашение находится в силе.

2. Настоящее Соглашение открыто для подписания всеми государствами-членами ООН, либо государствами-членами одного из специализированных учреждений или Международного агентства по атомной энергии, либо государствами-участниками Статута Международного Суда, а также любыми другими государствами, приглашенными Генеральной Ассамблеей ООН стать участником настоящего Соглашения.

Глава II. Применение норм ответственного поведения государств в ИКТ-среде

Статья 3. Применение норм ответственного поведения в ИКТ-среде

1. Применение норм ответственного поведения в ИКТ-среде должно осуществляться государствами-участниками на основе существующих международных норм и обязательств, вытекающих из принципов Устава ООН:

суверенное равенство;

разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость;

отказ в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями ООН;

уважение прав человека и основных свобод;

невмешательство во внутренние дела других государств.

2. Применение норм ответственного поведения в ИКТ-среде должно осуществляться в том числе, в соответствующих случаях, на основе принципов гуманности, необходимости, пропорциональности и индивидуализации.

3. Существующие обязательства по международному праву применимы к использованию ИКТ государствами-участниками.

4. Государства-участники должны выполнять обязательства по международному праву, касающиеся уважения и защиты прав человека и основных свобод.

Глава III. Граница зоны ответственного поведения государства в ИКТ-среде

Статья 4. Правовой статус национального сегмента ИКТ-среды

1. Суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами-участниками деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях.

2. ИКТ-среда, расположенная на территории и находящаяся под суверенитетом государства-участника, определяется совокупностью информационных систем, коммуникационных сетей и ИКТ-продуктов, а также коммуникационных устройств сети Интернет с уникальными цифровыми идентификаторами (IP-адресами, номерами автономных систем), используемыми для коммуникации с ИКТ-инфраструктурой других государств.

3. Границы ИКТ-инфраструктуры, находящейся под суверенитетом государств-участников (национального сегмента ИКТ-среды), закрепляются международным соглашением и являются границей зоны ответственного поведения государств в ИКТ-среде.

4. Государства-участники сотрудничают в развитии системы менеджмента международной информационной безопасности (СММИБ) на базе международных стандартов технического регулирования в области информационной безопасности национальных сегментов ИКТ-среды, содействующих мирному разрешению спорных ситуаций, связанных с инцидентами в ИКТ-среде.

Глава IV. Меры, принимаемые на национальном уровне

Статья 5. Общие принципы имплементации норм ответственного поведения государств в ИКТ-среде

1. Каждая из Сторон осуществляет имплементацию норм ответственного поведения государств в ИКТ-среде самостоятельно в соответствии с принципами государственного суверенитета, суверенного равенства государств, разрешения международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость, отказа в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого

государства, так и каким-либо другим образом, несовместимым с целями ООН, уважения прав человека и основных свобод, невмешательства во внутренние дела других государств.

2. Каждая из Сторон выбирает способы и формы обеспечения имплементации норм ответственного поведения государств в ИКТ-среде с учетом рекомендаций, содержащихся в резолюциях Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», докладах Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ.

3. Каждая из Сторон воздерживается от использования ИКТ, не соответствующего нормам ответственного поведения государств в ИКТ-среде.

Статья 6. Соблюдение суверенитета государств при имплементации норм ответственного поведения государств в ИКТ-среде

1. Присоединение государств-участников к настоящему Соглашению, выбор форм и методов имплементации норм ответственного поведения государств в ИКТ-среде является их суверенным правом.

2. Каждая из Сторон в целях имплементации норм ответственного поведения государств в ИКТ-среде в пределах своей юрисдикции осуществляет определение правового режима национального сегмента ИКТ-среды, регламентацию правового статуса его субъектов, осуществляет контроль за соблюдением правовых и технических норм, а также реагирование на инциденты в сфере ИКТ.

3. Настоящее Соглашение не наделяет государств-участников правом осуществлять на территории другого государства юрисдикцию и функции, которые относятся к исключительной компетенции органов этого государства в соответствии с его внутренним правом.

Статья 7. Механизмы имплементации

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обеспечить применение норм ответственного поведения государств в ИКТ-среде во внутренней и внешней политике государства.

2. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы учитывать положения

норм ответственного поведения государств в ИКТ-среде при разработке и корректировке национальных стратегий (доктрин, концепций) обеспечения безопасности в ИКТ-среде, законодательных и иных правовых актов.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы учесть положения норм ответственного поведения государств в ИКТ-среде при разработке и заключении проектов двусторонних и многосторонних международных соглашений (договоров) в области обеспечения безопасности в ИКТ-среде.

4. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы содействовать участию частного сектора, научных и технических кругов и гражданского общества в имплементации норм ответственного поведения государств в ИКТ-среде в национальное законодательство.

4.1. Материальные нормы публичного права

Статья 8. Нормы ответственного поведения государств в ИКТ-среде

Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве такое нормативное правовое регулирование, которое будет способствовать поддержанию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, снижению риска нарушения международного мира, безопасности и стабильности и обеспечит соблюдение следующих норм ответственного поведения государств в ИКТ-среде.

1. Каждая из Сторон должна сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности в соответствии с целями Устава ООН, в том числе касающимися поддержания международного мира и безопасности.

2. Каждая из Сторон должна изучить в случае инцидентов в сфере ИКТ всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий.

3. Каждая из Сторон должна заведомо не позволять использовать ее территорию и национальный сегмент ИКТ-среды для совершения международно-противоправных деяний с использованием ИКТ.

4. Каждая из Сторон должна рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования

лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам.

5. Каждая из Сторон должна при обеспечении безопасного использования ИКТ соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий и, в частности, всестороннее уважать права человека, включая право свободно выражать свое мнение.

6. Каждая из Сторон должна не осуществлять или заведомо не поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит ее обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения.

7. Каждая из Сторон должна принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции.

8. Каждая из Сторон должна удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ, а также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с ее территории или с находящегося под его суверенитетом национального сегмента ИКТ-среды.

9. Каждая из Сторон должна принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ, а также стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций.

10. Каждая из Сторон должна способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а также по возможности и устранить возможные угрозы для ИКТ и зависящей от сегмента ИКТ-среды, находящегося под ее суверенитетом.

11. Каждая из Сторон должна не осуществлять или заведомо не поддерживать деятельность, призванную нанести ущерб информационным системам уполномо-

ченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства, а также не использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

4.2. Процессуальные нормы публичного права

4.2.1. Нормы общего характера

Статья 9. Сфера применения процессуальных норм

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для реализации механизмов, структур и процедур, необходимых для имплементации норм ответственного поведения государств в ИКТ-среде.

2. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы определить координатора по применению норм ответственного поведения государств в ИКТ-среде, осуществляющего координацию проводимой на национальном уровне работы по имплементации норм ответственного поведения государств в ИКТ-среде.

Статья 10. Условия и гарантии

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обеспечить установление, исполнение и применение полномочий и процедур, предусмотренных Соглашением, в соответствии с условиями и гарантиями, предусмотренными нормами национального законодательства и обеспечивающими надлежащую защиту прав и свобод человека, включая права, вытекающие из обязательств по Международному пакту о гражданских и политических правах от 16 декабря 1966 года и по другим применяемым в государстве международным договорам по правам человека.

2. Такие условия и гарантии с учетом характера полномочий и процедур включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничения сферы и сроков действия таких полномочий или процедур.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы в той мере, в какой это соответствует общественным интересам, в частности осуществлению правосудия, рассматривать влияние предусмотренных Соглашением полномочий и процедур на права, ответственность и законные интересы третьих лиц.

Статья 11. Сбор и систематизация информации

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обеспечить сбор, обобщение и систематизацию информации о проводимой на национальном уровне работы по имплементации норм ответственного поведения государств в ИКТ-среде.

2. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы в добровольном порядке осуществлять подготовку обзора ведущейся на национальном уровне работы по имплементации норм ответственного поведения государств в ИКТ-среде.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы оказывать необходимое содействие тому, чтобы уполномоченный Генеральной Ассамблеей ООН рабочий орган мог обеспечить обобщение поступившей в добровольном порядке от государств-участников обзорных докладов по вопросам имплементации государствами норм ответственного поведения государств в ИКТ-среде.

Статья 12. Сотрудничество и обмен опытом

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы осуществлять сотрудничество и обмен опытом по вопросам применения норм ответственного поведения государств в ИКТ-среде в форматах международных организаций и на двусторонней основе.

2. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы организовать и поощрять проведение международных форумов и конференций, в том числе с участием представителей частного сектора и гражданского общества, для обсуждения вопросов и обмена опытом применения норм ответственного поведения государств в ИКТ-среде.

4.2.2. Нормы специального характера.

Часть 1. Незамедлительное сохранение цифровых данных

Статья 13. Незамедлительное сохранение цифровых данных

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы предоставить ее компетентным органам возможность предписывать или сходным образом добиваться незамедлительного сохранения определенных цифровых данных, включая данные трафика, которые хранятся посредством компьютерной системы, особенно

в тех случаях, когда есть основания полагать, что существует опасность потери или изменения этих цифровых данных.

2. В случаях, когда Сторона приводит в действие пункт 1 посредством предписания лицу сохранить определенные цифровые данные, находящиеся во владении или под контролем этого лица, Сторона должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обязать это лицо сохранять и поддерживать целостность подобных цифровых данных в течение необходимого периода времени, который не может превышать 90 дней, чтобы позволить компетентным органам провести расследование по данному факту. Сторона может предусмотреть положение о возможности продления срока действия предписания.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обязать хранителя данных или иное лицо, обязанное сохранять цифровые данные, держать в тайне факт совершения таких процедур в течение промежутка времени, предусмотренного во внутреннем законодательстве.

4. На полномочия и процедуры, указанные в данной статье, распространяются положения статей 14 и 15.

Статья 14. Незамедлительное сохранение и частичное предоставление данных трафика.

1. В отношении данных трафика, подлежащих сохранению согласно Статье 16, каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы:

(a) гарантировать, что подобное незамедлительное сохранение данных трафика будет возможно вне зависимости от того, сколько поставщиков услуг были вовлечены в операцию по передаче данной информации — один или несколько; а также

(b) гарантировать быстрое предоставление компетентным органам Стороны или лицу, назначенному таким компетентным органом, данных трафика в объеме, достаточном для того, чтобы Сторона могла идентифицировать поставщиков услуг и маршрут, по которому производилась передача информации.

2. На полномочия и процедуры, указанные в данной статье, распространяются положения статей 15 и 16.

Часть 2. Предписание о предоставлении информации

Статья 15. Предписание о предоставлении информации

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы предоставить ее компетентным властям полномочия предписывать:

(a) лицу, находящемуся на ее территории, предоставить определенные цифровые данные, находящиеся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на носителе цифровых данных; а также

(b) поставщику услуг, предлагающему свои услуги на территории Стороны, предоставить ту информацию о подписчиках, связанную с такими услугами, которая находится во владении или под контролем поставщика услуг;

2. На полномочия и процедуры, указанные в данной статье, распространяются положения статей 14 и 15.

3. В целях настоящей статьи, «информация о подписчике» означает любую информацию в форме цифровых данных или в любой иной форме, которой обладает поставщик услуг, относительно подписчика его услуг, и отличную от данных трафика или данных содержания, с помощью которой можно установить:

(a) тип использованной коммуникационной услуги, примененные для этого технические средства и срок предоставления услуги;

(b) личность подписчика, его почтовый или географический адрес, номер телефона или иного средства доступа, информация о выставлении счетов и их оплате, доступная на основании соглашения или договора об обслуживании;

(c) любая иная информация о месте установки коммуникационного оборудования, доступная на основании соглашения или по договора об обслуживании.

Часть 3. Поиск и изъятие цифровых данных

Статья 16. Поиск и изъятие цифровых данных

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам путем произведения обыска или сходным образом получать доступ на ее территории:

(a) к компьютерной системе в целом или отдельной ее части, а также к хранящимся там цифровым данным; и

(b) к носителю цифровых данных, на котором могут храниться цифровые данные.

2. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы гарантировать, что в случаях, когда ее компетентные органы производят обыск или сходным образом получают доступ к определенной компьютерной системе или отдельной ее части в соответствии с пунктом 1(a), а также имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или какой-либо ее части на территории Стороны, и такие данные законным образом доступны из изначальной системы или же доступны ей, то такие органы должны быть в состоянии быстро

распространить сферу обыска на другую систему или сходным образом получить доступ к такой системе.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам конфисковывать или равным образом изымать цифровые данные, доступ к которым получен на основании пунктов 1 или 2. Эти меры должны включать в себя полномочия:

(a) по конфискации, или, равным образом, изъятию компьютерной системы или ее части, или же носителя цифровых данных;

(b) по изготовлению и сохранению копии таких цифровых данных;

(c) по поддержанию целостности соответствующих сохраненных цифровых данных; а также

(d) по прекращению доступа к этим цифровым данным в компьютерной системе, к которой получен доступ, или удалению их из этой системы.

4. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам предписывать любому лицу, которое обладает сведениями о функционировании компьютерной системы или применяемых в ней мерах по защите цифровых данных, предоставить, насколько это целесообразно, информацию, необходимую в целях обеспечения принятия мер, указанных в пунктах 1 и 2.

5. На полномочия и процедуры, указанные в данной статье, распространяются положения статей 14 и 15.

Часть 4. Сбор цифровых данных в режиме реального времени

Статья 17. Сбор данных трафика в режиме реального времени

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам:

(a) собирать или записывать в режиме реального времени данные трафика, связанные с определенными операциями по передаче данных на ее территории, путем применения технических средств, а также

(b) принуждать поставщика услуг, в пределах имеющихся у него технических возможностей:

(i) собирать или записывать в режиме реального времени данные трафика, связанные с определенными операциями по передаче данных на ее территории, путем применения технических средств; или

(ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные трафика, связанные с опреде-

ленными операциями по передаче данных на ее территории, осуществляемыми посредством компьютерной системы.

2. В случае если Сторона из-за установленных в ее национальном законодательстве принципов не в состоянии принять меры, указанные в пункте 1(a), она может вместо этого принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обеспечить сбор или запись в режиме реального времени данных трафика, связанных с определенными операциями по передаче данных на ее территории, осуществляемыми посредством компьютерной системы.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обязать поставщика услуг хранить в тайне факт исполнения любого из полномочий, предусмотренных в данной Статье, а также любую связанную с этим информацию.

4. На полномочия и процедуры, указанные в данной статье, распространяются положения статей 14 и 15.

Статья 18. Перехват данных содержания

1. Каждая из Сторон должна принять такие необходимые меры законодательного и иного характера в отношении ряда серьезных преступлений, определенных в соответствии с ее национальным законодательством, которые позволили бы ее компетентным органам:

(a) собирать или записывать в режиме реального времени данные содержания определенных передач информации на ее территории путем применения технических средств, и

(b) принуждать поставщика услуг, в пределах имеющихся у него технических возможностей:

(i) собирать или записывать в режиме реального времени данные содержания определенных передач информации на ее территории путем применения технических средств, или

(ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные содержания определенных передач информации на ее территории, осуществляемых посредством компьютерной системы.

2. В случае если Сторона из-за установленных в ее национальном законодательстве принципов не в состоянии принять меры, указанные в пункте 1(a), она может вместо этого принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обеспечить сбор или запись в режиме реального времени данных содержания определенных передач информации путем применения технических средств на данной территории.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обязать поставщика услуг хранить в тайне факт исполнения любого из полномочий, предусмотренных в данной Статье, а также любую связанную с этим информацию.

4. На полномочия и процедуры, указанные в данной статье, распространяются положения статей 14 и 15.

Глава V. Международное сотрудничество
Сотрудничество государств в применении норм ответственного поведения государств в ИКТ-среде (область, принципы, механизмы).

Раздел 1

5.1. Общие принципы сотрудничества

Статья 19. Общие принципы сотрудничества

1. В целях применения норм ответственного поведения государств в ИКТ-среде Стороны должны осуществлять самое широкое сотрудничество в соответствии с положениями настоящего раздела и через применение соответствующих международных договоров о международном сотрудничестве в области отграничения зон ответственности государств в ИКТ-среде и развития системы менеджмента международной информационной безопасности.

2. Основными принципами сотрудничества являются принципы добросовестности соблюдения норм ответственного поведения государств в ИКТ-среде, реагирования на нарушение норм ответственного поведения государств в ИКТ-среде, ответственности за нарушение норм ответственного поведения государств в ИКТ-среде.

3. Принцип добросовестного соблюдения норм ответственного поведения государств в ИКТ-среде является реализацией более общей нормы международного права — принципа добросовестного выполнения международных обязательств, принимаемых в соответствии с Уставом ООН, который относится к категории основных принципов международного права и императивных норм (норм Jus cogens) международного права.

Необходимость установления конвенционного принципа соблюдения норм ответственного поведения государств в ИКТ-среде определяется тем, что проект универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде предполагает придание его положениям обязательной юридической силы. Логическим следствием обязательного международно-правового акта является закрепление в нем нормативного требования о добро-

совестном соблюдении норм ответственного поведения государств в ИКТ-среде, которые будут содержаться в тексте универсального международного соглашения.

4. Государства-участники в рамках своей юрисдикции соглашаются не допускать видов деятельности, которые относятся к «злонамеренным», «заведомо противоречащим международному праву» или «наносящими преднамеренный ущерб критически важной инфраструктуре». В случае необходимости государства принимают надлежащее законодательство с целью пресечения или недопущения таких видов деятельности.

Статья 20. Реагирование на нарушение норм ответственного поведения государств в ИКТ-среде

1. Государство, фиксирующее нарушение норм ответственного поведения государств в ИКТ-среде, прежде всего, должно определить разновидность нарушенного правила поведения.

2. Если государство фиксирует нарушение норм ответственного поведения государств в ИКТ-среде, оно также в зависимости от характера нарушения и его последствий использует либо традиционные дипломатические средства реагирования (ноты, протесты и т.д.), либо иные согласованные каналы взаимодействия с целью уведомления государства-нарушителя о своем требовании.

3. Государство также может потребовать прекратить нарушение норм ответственного поведения государств в ИКТ-среде, если это нарушение продолжает осуществляться.

4. Заинтересованное государство может выдвигать и иные требования в рамках международного права и конвенционного режима, установленного универсальным международным соглашением о применении норм ответственного поведения государств в ИКТ-среде.

5. Если же в результате нарушения норм ответственного поведения государств в ИКТ-среде причиняется ущерб государству, его юридическим или физическим лицам, то в этом случае государству-нарушителю может быть выдвинута претензия о возмещении причиненного ущерба. В случае отказа государства-нарушителя удовлетворить требования заинтересованное государство может прибегнуть к использованию процедур мирного урегулирования возникших разногласий по договоренности с государством-нарушителем или иным допустимым международным правом способом.

Статья 21. Ответственность за нарушение норм ответственного поведения государств в ИКТ-среде

1. С учетом специфики предмета регулирования универсального международного соглашения о применении норм ответственного поведения государств

в ИКТ-среде, ответственность государств может пониматься в позитивном смысле, то есть как долг, обязанность следовать принятым на себя международным обязательствам.

2. Призвание к ответственности государства будет означать применение индивидуальными или коллективными (специально созданными конвенционными органами, а в их отсутствие органами ad hoc, созываемыми по предложению государства или группы государств) мер воздействия на нарушителя норм ответственного поведения государств в ИКТ-среде.

3. В необходимых случаях могут проводиться технологические экспертизы, для выявления нарушения норм ответственного поведения государств в ИКТ-среде и оценки возможного причинения ущерба другим государствам-участникам универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде.

Раздел 2.

5.2. Закрепление зон ответственного поведения государств в ИКТ-среде.

Статья 22. Международное правовое закрепление границ зон ответственного поведения государств в ИКТ-среде

1. Границы зон ответственного поведения государств в ИКТ-среде определяют область действия норм ответственного поведения, в рамках которой применяются юридически обязательные принципы и нормы международного права. Применение норм ответственного поведения распространяется на действия, совершаемые из национального сегмента ИКТ-среды.

2. При закреплении границ зон ответственного поведения государств в проекте универсального международного соглашения о применении норм ответственного поведения государств в ИКТ-среде, следует учитывать принципы определения юрисдикции государства в информационном пространстве, установленные в национальном законодательстве.

3. Под юрисдикцию государства подпадает совокупность объектов информационной инфраструктуры, отнесенных к зоне ответственности государства в ИКТ-среде или используемых на основании международных договоров государства.

4. Государства-участники, учитывая особенности ИКТ-среды как глобальной составляющей информационной сферы, включающей взаимосвязанные объекты информационной инфраструктуры, соглашаются провести делимитацию зоны ответственного поведения государств в ИКТ-среде путем закрепления в приложении к настоящему Соглашению уникальных цифровых идентифика-

торов объектов ИКТ-среды, обеспечение безопасности использования которых осуществляется на основе государственного суверенитета.

5. С целью демаркации границы зоны ответственного поведения государств в ИКТ-среде государства-участники соглашаются оснастить объекты национальной зоны ответственного поведения специальным программным обеспечением и техническим оборудованием, применение которого создаст условия для поддержания установленного правового режима безопасности объектов ИКТ-инфраструктуры, оказывающих влияние на функционирование критически важной инфраструктуры.

Раздел 3

5.3. Международный режим безопасности объектов критически важной инфраструктуры

Статья 23. Содержание международного нормативного режима безопасности объектов критически важной инфраструктуры

1. Государства-участники соглашения в рамках правового режима зоны ответственного поведения государств соглашаются установить нормативный механизм соблюдения обязательств по нормативно-техническому регулированию отношений в области предупреждения и пресечения, вытекающих из норм ответственного поведения государств в ИКТ-среде, и, в частности, обязательств в области недопущения:

противоправной деятельности в ИКТ-среде с учетом положений морского, воздушного и космического права;

деятельности «заведомо противоречащей международному праву» и «наносящей преднамеренный ущерб критически важной инфраструктуре»:

«международно-противоправных деяний с использованием ИКТ» и «вредоносного использования ИКТ, способного создать условия для нарушения международного мира и безопасности, террористического и преступного использования ИКТ».

2. Государства соглашаются установить нормативный механизм оказания помощи государствам, критически важная инфраструктура которых становится объектом злонамеренных действий и другой деятельности, не способствующей поддержанию международного мира и безопасности.

Раздел 4

5.4. Оказание помощи государствам, пострадавшим от злонамеренного и вредоносного использования ИКТ

Статья 24. Принципы взаимодействия

Государства-участники, в надлежащих случаях в соответствии с основополагающими принципами своих правовых систем, взаимодействуют друг с другом и с соответствующими международными и региональными организациями в разработке и осуществлении мер по оказанию помощи государствам, пострадавшим от злонамеренного и вредоносного использования ИКТ.

Статья 25. Меры по поддержанию связи

Каждое Государство-участник принимает меры к созданию и надлежащему оснащению каналов передачи информации о фактах нанесения ущерба иностранному государству или его частным организациям от злонамеренного и вредоносного использования ИКТ.

Статья 26. Меры по планированию помощи

Каждое Государство-участник принимает меры к созданию и поддержанию в надлежащем состоянии дополнительных сил и средств для оказания плановых или чрезвычайных мер помощи иностранному государству или его частным организациям от злонамеренного и вредоносного использования ИКТ.

Статья 27. Меры по поддержанию частно-государственного партнерства

Каждое Государство-участник принимает меры к тому, чтобы каждая частная организация (или их объединение), предоставляющая информационно-телекоммуникационные услуги, находящаяся на территории Государства-участника, была готова к принятию действенных мер в целях оказания помощи иностранному государству или его частным организациям, пострадавшим от злонамеренного и вредоносного использования ИКТ.

Статья 28. Меры по взаимодействию с ООН

Каждое Государство-участник сообщает Генеральному секретарю ООН наименование и адрес уполномоченного органа или органов, которые могут оказывать другим Государствам-участникам содействие в разработке и осуществлении конкретных мер по предупреждению преступлений и иных противоправных деяний в сфере использования информационно-коммуникационных технологий.

Статья 29. Область оказания содействия

Меры помощи иностранному государству или его частным организациям, пострадавшим от злонамеренного и вредоносного использования ИКТ, могут включать как сферу использования ИКТ, так и меры за пределами сферы ИКТ.

Статья 30. Меры по оценке необходимой помощи

1. Каждое Государство-участник может обратиться к другому Государству-участнику за взаимной помощью в кратчайшие сроки, если оно считает, что существует чрезвычайная ситуация. Запрос должен включать, помимо прочего необходимого содержания:

- описание фактов, свидетельствующих о том, что существует чрезвычайная ситуация;
- описание запрашиваемой помощи для локализации данной чрезвычайной ситуации.

2. Запрашиваемое Государство-участник может принимать такой запрос в электронной форме. Однако оно может потребовать обеспечить соответствующий уровень безопасности и аутентификации, прежде чем принимать запрос.

3. Запрашиваемое Государство-участник может в кратчайшие сроки запросить дополнительную информацию для оценки запроса. Запрашивающее Государство-участник предоставляет такую дополнительную информацию в возможно кратчайшие сроки.

4. Убедившись в наличии чрезвычайной ситуации и удовлетворении других требований, необходимых для оказания взаимной помощи, запрашиваемое Государство-участник отвечает на запрос в возможно кратчайшие сроки.

5. Каждое Государство-участник обеспечивает, чтобы должностное лицо его компетентного органа, отвечающее на запросы о взаимной помощи, было доступно 24 часа в сутки и 7 дней в неделю для целей реагирования на запрос, направленный в соответствии с данной статьей.

6. Компетентные органы, отвечающие за взаимную помощь, запрашивающего и запрашиваемого Государств-участников могут договориться о том, чтобы результаты выполнения запроса или их предварительная копия могли быть предоставлены запрашивающему Государству-участнику через альтернативный канал связи, отличный от обычно используемого для направления запроса об оказании правовой помощи.

7. Каждое Государство-участник при подписании настоящего Соглашения или при сдаче на хранение ратификационной грамоты или документа о принятии, утверждении или присоединении может сообщить Генеральному секретарю ООН, что в целях эффективности запросы, поданные в соответствии с настоящим пунктом, должны направляться только в Орган по содействию применению норм ответственного поведения государств в ИКТ-среде.

Статья 31. Меры по информированию

Государство-участник может с соблюдением норм своего внутреннего законодательства направить без предварительного запроса другого Государства-участника информацию, которая бы способствовала предотвращению нарушения норм ответственного поведения государств в ИКТ-среде.

Раздел 5.

5.5. Разрешение споров и ситуаций в области соблюдения норм ответственного поведения государств в ИКТ-среде

Статья 32. Сотрудничество в разрешении споров и ситуаций

1. Государства-участники стремятся урегулировать споры и ситуации относительно толкования или применения настоящего Соглашения путем переговоров.

2. Любой спор или ситуация между двумя или более Государствами-участниками относительно толкования или применения настоящего Соглашения, который не может быть урегулирован путем переговоров в течение разумного периода времени, передается по просьбе одного из Государств-участников на арбитражное разбирательство. Если в течение шести месяцев со дня обращения с просьбой об арбитраже эти Государства-участники не смогут договориться о его организации, они могут, по договоренности, передать спор в любой международный суд по своему выбору.

3. Каждое Государство-участник может при подписании, ратификации, принятии или утверждении настоящего Соглашения или при присоединении к нему заявить в отношении государств, которые сделают такие же заявления, о том, что любые споры и ситуации о толковании настоящего Соглашения или применения настоящего Соглашения могут быть переданы в одностороннем порядке в какой-либо специальный международный судебный орган (например, специальный международный арбитражный суд).

Примечание. Вопросы создания специального международного судебного органа для урегулирования споров и ситуаций в ИКТ-среде должны быть решены в дополнительном международном соглашении.

Раздел 6.

5.6. Принципы развития международного технического регулирования в области применения норм ответственного поведения государств в ИКТ-среде

Статья 33. Цель сотрудничества

Государства-участники сотрудничают в разработке норм международного технического регулирования, обеспечивающих условия для применения норм ответственного поведения государств в ИКТ-среде.

Статья 34. Принципы сотрудничества

Сотрудничество в разработке норм международного технического регулирования обеспечивает создание системы менеджмента международной информационной безопасности, формируемой и действующей на основе принципов:

- взаимодействия уполномоченных Государствами-участниками координаторов на политическом и техническом уровнях в рамках единой координационной сети;
- партнерства Государств-участников и заинтересованных представителей бизнеса и экспертного сообщества.

2. Международное сотрудничество в области разработки норм международного технического регулирования в области безопасности использования ИКТ-среды может регулироваться отдельным соглашением Государств–участников.

Статья 35. Обмен информацией и оказание помощи в урегулировании международных инцидентов

Государства-участники в рамках системы менеджмента международной информационной безопасности действуют в направлении расширения использования центров обеспечения международной информационной безопасности национальных сегментов ИКТ-среды (контактных пунктов) для обмена информацией и оказания помощи в управлении инцидентами, а также для содействия урегулированию инцидентов на основе использования мирных средств таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость.

Статья 36. Обеспечение информационной безопасности национальных сегментов ИКТ-среды

Государства-участники организуют деятельность центров обеспечения международной информационной безопасности национальных сегментов ИКТ-среды (контактных пунктов) в соответствии с национальным законодательством.

Статья 37. Международный стандарт технического регулирования в области менеджмента международной информационной безопасности

Международный стандарт технического регулирования в области менеджмента международной информационной безопасности является неотъемлемой частью данного Соглашения.

Глава VI. Заключительные положения

Статья 38. Подписание и вступление в силу

1. Настоящее Соглашение открыто для подписания всеми государствами-членами ООН, либо государствами-членами одного из специализированных учреждений или Международного агентства по атомной энергии, либо государствами-участниками Статута Международного Суда, а также любым другим государством, приглашенным Генеральной Ассамблеей ООН стать участником настоящего Соглашения.

2. Соглашение подлежит ратификации, принятию или утверждению. Грамоты о ратификации, принятии или утверждении подлежат депонированию у Генерального Секретаря ООН.

3. Соглашение вступает в силу в первый день следующего месяца по истечении трехмесячного срока с момента, когда государства-участники выразят свое согласие на обязательность для них Соглашения в соответствии с положениями пунктов 1–2.

4. В отношении любого из государств, подписавших Соглашение, а впоследствии выразивших согласие на обязательность для них ее положений, Соглашение вступает в силу в первый день следующего месяца по истечении трехмесячного срока с момента выражения государством согласия на обязательность для них Соглашения в соответствии с положениями пунктов 1–2.

Статья 39. Присоединение к Соглашению

1. После вступления в силу настоящего Соглашения к нему могут присоединиться другие государства-члены ООН, либо государства-члены одного из специализированных учреждений или Международного агентства по атомной энергии, либо государствами-участниками Статута Международного Суда, а также любые другие государства, приглашенные Генеральной Ассамблеей ООН стать участником настоящего Соглашения, согласные на обязательность для них положений Соглашения.

2. В отношении любого из государств, присоединяющихся к настоящему Соглашению в соответствии с пунктом 1, Соглашение вступает в силу в первый день следующего месяца по истечении трехмесячного срока с момента депонирования документа о присоединении у Генерального Секретаря ООН.

Статья 40. Территориальное применение

Во время подписания или депонирования своей ратификационной грамоты или документа о принятии, утверждении или присоединении любое Государство-участник может провести делимитацию и демаркацию границ национального сегмента ИКТ-среды, на который будет распространяться действие Соглашения.

Статья 41. Оговорки

Во время подписания или депонирования своей ратификационной грамоты или документа о принятии, утверждении или присоединении любое из Государств путем подачи письменного заявления на имя Генерального секретаря ООН может объявить, что оно сделает оговорку или оговорки относительно пунктов статей Соглашения, по которым Государство участвует в сотрудничестве. Иные оговорки не допускаются.

Статья 42. Статус и снятие оговорок

1. Любая из Сторон, сделавшая оговорку на основании Статьи, может полностью или частично снять ее посредством уведомления в адрес Генерального секретаря ООН. Снятие оговорки вступает в силу с момента получения такого уведомления Генеральным секретарем. Если в уведомлении указана дата, когда снятие оговорки вступает в силу, и эта дата наступает позднее дня получения уведомления Генеральным секретарем, снятие должно вступить в силу в указанную, более позднюю дату.

2. Сторона, сделавшая оговорку в соответствии со Статьей 41, должна снять такую оговорку, полностью или частично, как только позволят обстоятельства.

3. Генеральный секретарь ООН может периодически запрашивать Стороны, сделавшие одну или более оговорок, упомянутых в Статье 41, относительно перспектив снятия ими таких оговорок.

Статья 43. Консультации между Сторонами

1. Стороны должны периодически проводить консультации с целью содействия:

(a) эффективному использованию и осуществлению настоящего Соглашения, включая определение любых возникающих, в связи с этим, проблем, а также последствий любых деклараций или оговорок, сделанных согласно настоящему Соглашению;

(b) обмену информацией относительно важных событий и разработок в юридической, политической и технологической областях, имеющих отношение к применению норм ответственного поведения государств в ИКТ-среде;

(c) рассмотрению возможных дополнений или поправок к Соглашению.

2. Генеральный Секретарь ООН должен периодически информироваться о результатах, достигнутых в ходе упомянутых в пункте 1 консультаций.

3. Секретариат ООН оказывает Сторонам помощь в выполнении ими своих функций в соответствии с настоящей Статьей.

Статья 44. Денонсация

1. Любая из Сторон может в любое время денонсировать настоящее Соглашение посредством уведомления в адрес Генерального секретаря ООН.

2. Такая денонсация вступает в силу в первый день следующего месяца по истечении трехмесячного срока после даты получения уведомления Генеральным Секретарем ООН.

Статья 45. Уведомление

Генеральный секретарь ООН уведомляет Государства-участников Соглашения о:

(a) любом подписании Соглашения;

(b) депонировании любой ратификационной грамоты или документа о принятии, утверждении или присоединении;

(c) любой дате вступления настоящего Соглашения в силу в соответствии с положениями Статьи 38;

(d) любой декларации, сделанной в соответствии со Статьей 39, или любой оговорке, сделанной в соответствии со Статьей 41;

(e) любом другом акте, уведомлении или сообщении, касающемся настоящего Соглашения.

В удостоверение чего нижеподписавшиеся, в должной форме уполномоченные на это, подписали настоящее Соглашение.

Приложение 3

Приложение к Универсальному международному соглашению о применении норм ответственного поведения государств в ИКТ-среде

Международный стандарт технического регулирования в области менеджмента международной информационной безопасности
(проект)

Международный стандарт в области менеджмента международной информационной безопасности (далее — ММИБ) подготовлен с целью установления требований по созданию, внедрению, поддержке и постоянному совершенствованию системы менеджмента международной информационной безопасности (далее — СММИБ).

Решение о внедрении СММИБ принимается Государствами-участниками Соглашения по применению норм ответственного поведения государств в ИКТ-среде (далее — Государства-участники).

Структура и функции СММИБ определяются согласованной Государствами-участниками моделью угроз нарушения международного правового режима безопасности объектов национального сегмента ИКТ-среды (далее — риски нарушения МИБ). Эти структура и функции устанавливаются положениями данного Соглашения и обязательствами государств в области ответственного поведения в ИКТ-среде в целях противодействия угрозам.

Предполагается, что угрозы нарушения международного правового режима безопасности объектов национального сегмента ИКТ-среды могут со временем изменяться.

СММИБ содействует (способствует) сохранению открытости, безопасности, стабильности, доступности и мирности глобальной ИКТ-среды посредством реализации процесса управления рисками нарушения МИБ. Это придает заинтересованным сторонам уверенность в том, что эти риски надлежащим образом учитываются.

СММИБ базируются на системах обеспечения МИБ (далее — СОМИБ), находящихся в зоне ответственного поведения Государств–участников. СОМИБ обеспечивают реализацию функций СММИБ с учетом результатов имплементации норм ответственного поведения государств в ИКТ-среде в национальное законодательство.

Процесс создания, внедрения, поддержки и постоянного совершенствования СММИБ должен быть гармонизирован с процессом имплементации норм ответственного поведения государств в ИКТ-среде в национальное законодательство.

Предполагается, что СММИБ будет адаптироваться к изменениям модели угроз нарушения МИБ.

Стандарт может быть использован заинтересованными сторонами для оценки готовности Государств-участников к применению норм ответственного поведения государств в ИКТ-среде.

Предполагается также, что СММИБ базируется на выполнении организациями Государств-участников рекомендаций международных стандартов информационной безопасности (включая ИСО/МЭК 27000, ИСО/МЭК 27001, ИСО/МЭК 27002, ИСО/МЭК 27003, ИСО/МЭК 27004 и ИСО/МЭК 27005), содержащих соответствующие термины и определения, представленные в ИСО/МЭК 27000.

Раздел 1. Область применения

1.1. Стандарт устанавливает общие требования по созданию, внедрению, поддержке и постоянному улучшению СММИБ в контексте деятельности Государств-участников.

1.2. Стандарт должен содержать требования по оценке и обработке рисков нарушения МИБ, а также рисков возникновения инцидентов в ИКТ-среде, связанных с нарушением правового режима безопасности объектов национального сегмента ИКТ-среды (далее — риски возникновения инцидентов МИБ).

1.3. Кроме того, стандарт должен содержать требования к составу функций по противодействию угрозам нарушения МИБ, включая функции противодействия угрозам безопасности информационным системам критических инфраструктур, реализуемые уполномоченными группами реагирования на компьютерные инциденты.

1.4. Изложенные в стандарте требования являются обобщенными и предназначены для применения всеми Государствами-участниками.

Раздел 2. Внешние и внутренние факторы

2.1. Государствами-участниками должны быть определены внешние и внутренние факторы, имеющие отношение к деятельности СОМИБ и оказывающие влияние на способность СОМИБ поддерживать достаточный уровень доверия к ее деятельности.

2.2. Государства-участники должны определить:

a) степень участия в международном сотрудничестве по обеспечению функционирования СОМИБ;

b) требования к участникам СОМИБ;

П р и м е ч а н и е — Требования могут включать правовые и нормативные требования, а также договорные обязательства.

Раздел 3. Сотрудничество в деятельности СММИБ

3.1. Для установления области сотрудничества в деятельности СММИБ Государства-участники должны с учетом внутренних и внешних факторов, упомянутых в п.2.1, а также требований, упомянутых в п.2.2, определить порядок взаимодействия и взаимозависимости между СОМИБ.

Описание области и порядка взаимодействия Государств-участников по содействию функционированию СММИБ должны быть доступны в виде документированной информации.

3.2. Создание, внедрение, поддержка и постоянное улучшение деятельности СММИБ в области оценки и обработки рисков нарушения МИБ, а также рисков возникновения инцидентов МИБ в ИКТ-среде, должны проводиться в соответствии с требованиями стандарта.

Раздел 4. Руководство деятельностью СММИБ

4.1. Уполномоченные лица Государств-участников должны активно участвовать в руководстве деятельностью СММИБ посредством следующего:

a) установление политики и целей сотрудничества в области деятельности СММИБ, совместимых с целями Соглашения о применении норм ответственного поведения государств в ИКТ-среде;

b) интеграция требований СММИБ в процессы сотрудничества по вопросам реализации функций СММИБ;

c) обеспечение доступности ресурсов, необходимых для СММИБ;

d) учет важности обеспечения эффективной деятельности СММИБ и важности соответствия СОМИБ государств требованиям СММИБ;

e) оценка эффективности деятельности СММИБ (оценка достижения ожидаемых результатов);

f) определение ключевых проблем применения СММИБ и поддержка лиц, способствующих повышению результативности деятельности СММИБ;

g) содействие постоянному улучшению СММИБ;

h) поддержка деятельности руководителей, организующих деятельность СММИБ в зонах ответственного поведения Государств-участников.

Раздел 5. Политика деятельности СММИБ

5.1. Уполномоченные лица Государств-участников должны устанавливать политику деятельности СММИБ, которая:

a) соответствует целям деятельности СММИБ;

b) содержит цели функционирования СММИБ и создает основу для их достижения;

c) содержит обязательства в области обеспечения выполнения требований к СОМИБ;

d) содержит обязательство содействовать совершенствованию СММИБ.

5.2. Политика деятельности СММИБ должна:

a) быть доступна в виде документированной информации;

b) быть доведена до сведения лиц, участвующих в обеспечения деятельности СММИБ;

c) быть доступна заинтересованным сторонам сотрудничества.

5.3. Уполномоченные лица Государств-участников должны:

обеспечить распределение обязанностей и полномочий между руководителями СММИБ в зонах ответственного поведения государств по видам деятельности в области выполнения функций СММИБ, и доведение информации об этих обязанностях и полномочиях до всех заинтересованных сторон;

определять обязанности и полномочия этих руководителей в области оценки степени уверенности в соответствии СММИБ требованиям стандарта, а также в области представления отчетности о функционировании СММИБ уполномоченному Органу Соглашения.

П р и м е ч а н и е — Уполномоченные лица Государств-участников могут также устанавливать обязанности и полномочия для представления отчетности о функционировании СММИБ.

Раздел 6. Планирование деятельности СММИБ, в части зон ответственного поведения Государств-участников.

6.1. Действия по рассмотрению рисков нарушения МИБ и рисков возникновения инцидентов МИБ и возможностей реагирования на эти нарушения.

6.1.1. При планировании деятельности СММИБ государства-участники Соглашения должны учитывать факторы, упомянутые в разделе 2, и требования, упомянутые в разделе 3, а также определять подлежащие рассмотрению риски нарушения МИБ и риски возникновения инцидентов МИБ, а также возможности реагирования на нарушения для следующего:

a) обеспечение уверенности в том, что СММИБ способна достичь намеченных целей;

b) предотвращение или уменьшение нежелательных последствий нарушения МИБ и возникновения инцидентов МИБ;

c) обеспечение постоянного улучшения возможностей СММИБ по реагированию на изменение рисков нарушения МИБ.

Государства-участники должны планировать:

a) действия по учету рисков нарушения МИБ и рисков возникновения инцидентов МИБ и возможностей реагирования на эти риски;

b) интегрирование и внедрение этих действий в процессы деятельности СММИБ, а также оценивание результативности этих действий (например, уровень доверия Государств-участников к результатам деятельности СММИБ).

6.1.2. Уполномоченные лица Государств-участников должны определять и внедрять в деятельность СОМИБ оценку рисков нарушения МИБ и рисков возникновения инцидентов МИБ, которая позволяет:

a) устанавливать и оценивать критерии опасности рисков нарушения МИБ и рисков возникновения инцидентов МИБ;

b) обеспечивать уверенность в том, что повторные оценки рисков нарушения МИБ и риски возникновения инцидентов МИБ дают непротиворечивые, достоверные и сопоставимые результаты;

c) идентифицировать риски нарушения МИБ и риски возникновения инцидентов МИБ;

d) проводить анализ рисков нарушения МИБ и рисков возникновения инцидентов МИБ (т.е. учитывать потенциальные последствия реализации рисков нарушения МИБ и рисков возникновения инцидентов МИБ, идентифицированных в соответствии с 6.1.2);

e) оценивать реальную вероятность реализации угроз нарушения МИБ и рисков возникновения инцидентов, идентифицированных в соответствии с 6.1.2;

d) определять уровни рисков нарушения МИБ и рисков возникновения инцидентов МИБ;

e) оценивать риски нарушения МИБ и риски возникновения инцидентов МИБ, т.е.:

1) сравнивать результаты анализа рисков с критериями опасности рисков, установленными в соответствии с 6.1.2 a);

2) определять приоритетность обработки проанализированных рисков нарушения МИБ и рисков возникновения инцидентов МИБ.

Государства-участники должны хранить документированную информацию о процессах оценки рисков нарушения МИБ и рисков возникновения инцидентов МИБ.

6.1.3. Обработка Государствами-участниками рисков нарушения МИБ и рисков возникновения инцидентов МИБ.

Государства-участники должны определять и осуществлять обработку рисков нарушения МИБ и рисков возникновения инцидентов МИБ для осуществления следующего:

a) выбор подходящих вариантов предупреждения проявления рисков, учитывая результаты оценки их опасности;

b) определение всех мер и средств, которые необходимы для реализации выбранного варианта предупреждения проявления рисков.

П р и м е ч а н и е — При необходимости Государство-участник может разрабатывать меры и средства предупреждения проявления рисков, информация о которых получена из достоверных источников;

c) сравнение мер и средств предупреждения проявления рисков, определенных в соответствии с 6.1.3 b), с определенными Государствами-участниками в дополнительном приложении, для проверки того, что никакие необходимые меры и средства не были упущены.

d) подготовка Ведомости применимости мер и средств предотвращения проявления рисков, которая содержит:

перечень необходимых мер и средств предотвращения проявления рисков (см. 6.1.3 b) и c));

обоснование необходимости их применения;

информацию о том, реализованы или нет необходимые меры и средства предупреждения проявления рисков;

обоснование неприменения мер и средств предупреждения проявления рисков, представленных в национальных перечнях сертифицированных средств;

e) разработка плана обработки рисков нарушения МИБ и рисков возникновения инцидентов МИБ;

f) согласование и (или) утверждение плана обработки рисков и принятия остаточных рисков владельцами рисков.

Государства-участники должны хранить документированную информацию о процессе обработки рисков нарушения МИБ и рисков возникновения инцидентов МИБ.

6.2. Уполномоченными лицами Государств-участников должны быть установлены цели обеспечения МИБ применительно к соответствующим функциям и уровням управления обеспечением соблюдения международного правового режима МИБ.

Цели обеспечения деятельности СММИБ должны быть:

a) согласованы с политикой деятельности СММИБ;

b) измеримыми (если это практически возможно);

c) согласованы с требованиями к СММИБ и результатами оценки и обработки рисков нарушения МИБ;

d) доведены до сведения всех заинтересованных сторон;

e) актуализированы (обновляться по мере необходимости).

Государства-участники должны хранить документированную информацию о целях деятельности СММИБ.

При планировании способов достижения установленных целей деятельности СММИБ Государство-участник должно определить:

a) критерии (показатели) достижения целей;

b) выделяемые для достижения целей ресурсы;

c) лиц, ответственных за планирование;

d) сроки завершения планируемых мероприятий;

e) способы оценки результатов деятельности.

Раздел 7. Обеспечение и поддержка деятельности СММИБ

7.1. Ресурсы

Государство-участник должно определить и обеспечить наличие ресурсов, необходимых для создания, внедрения, поддержки и постоянного улучшения СММИБ.

7.2. Квалификация

Государство-участник должно:

a) определять необходимую квалификацию для лиц(а), выполняющих(его) работу под его контролем, которая влияет на обеспечение деятельности СММИБ;

b) принимать при необходимости меры по получению необходимой квалификации и проводить оценивание результативности принятых мер;

c) сохранять соответствующую документированную информацию в качестве свидетельств наличия необходимой квалификации.

П р и м е ч а н и е — Применяемые меры могут включать, например, проведение тренинга, наставничество или перераспределение обязанностей среди имеющихся работников, а также наем или привлечение к работам по контракту лиц, имеющих необходимую квалификацию.

7.3. Осведомленность

Лица, выполняющие работу под контролем Государства-участника, имеющую отношение к функциям СММИБ, должны быть осведомлены о:

a) политике деятельности СОМИБ Государства-участника;

b) их вкладе в обеспечение результативности СММИБ, включая пользу от улучшения деятельности СММИБ;

c) последствиях несоблюдения требований СММИБ.

7.4. Взаимодействие

Государство-участник должно определять необходимость своего взаимодействия внутри СММИБ и с внешними сторонами по вопросам, имеющим отношение к функциям СММИБ, включая следующие:

a) цели и предмет взаимодействия;

b) подходящий момент и сроки взаимодействия;

c) стороны взаимодействия;

d) уполномоченные лица для взаимодействия;

e) процедуры осуществления взаимодействия.

7.5. Документирование информации

7.5.1. Общие положения

Документированная информация СММИБ должна включать:

a) документированную информацию, требуемую в соответствии с настоящим стандартом;

b) документированную информацию, определяемую Государством-участником как необходимую для обеспечения результативности СММИБ.

П р и м е ч а н и е — Объем документированной информации, относящейся к СММИБ, в разных Государствах-участниках может быть различным, в зависимости от:

a) размеров национального сегмента ИКТ-среды, видов деятельности, осуществляемых с ее использованием;

b) сложности процессов ММИБ;

c) степени участия в СММИБ (п.1.2).

7.5.2. Создание и обновление документированной информации

При создании и обновлении документированной информации Государство-участник должно обеспечить надлежащие:

a) идентификацию и описание (например, название, дата, автор или номер для ссылок);

b) формат (например, язык, версия программного обеспечения, графика) и носитель информации (например, бумажный, электронный);

c) проверку и подтверждение ее пригодности и адекватности.

7.5.3. Управление документированной информацией

Требуется осуществлять управление документированной информацией СММИБ с целью обеспечения:

a) доступности и пригодности информации для использования в случае необходимости;

b) надлежащей защиты информации (например, от нарушения конфиденциальности, ненадлежащего использования или нарушения целостности).

Для управления документированной информацией Государства-участника необходимо обеспечить возможность осуществления следующих (если это применимо) действий:

c) распространение, обеспечение доступа, поиска и использования информации;

d) безопасное хранение и сохранность информации;

e) управление изменениями информации;

f) архивное хранение и уничтожение информации.

Государство-участник должно идентифицировать и управлять документированной информацией из внешних источников, необходимой для осуществления планирования и функционирования СММИБ.

Раздел 8. Функционирование СММИБ

8.1. Оперативное планирование и контроль деятельности СММИБ

Государство-участник должно планировать, реализовывать и контролировать процессы, необходимые для: соответствия требованиям СММИБ; осуществления действий и достижения целей СММИБ.

Государство-участник должно хранить документированную информацию в объеме, необходимом для обеспечения уверенности в том, что процессы СММИБ/СОМИБ были выполнены в соответствии с планами.

Государство-участник должно организовать управление запланированными изменениями СММИБ и обеспечить анализ последствий незапланированных изменений, принимая меры по смягчению любых неблагоприятных последствий.

Процессы управления деятельностью СОМИБ Государства-участника Соглашения, осуществляемые с использованием аутсорсинга, должны быть определены и контролироваться[95].

8.2. Оценка рисков нарушения МИБ и рисков возникновения инцидентов МИБ

Государство-участник должно проводить оценку рисков нарушения МИБ и рисков возникновения инцидентов МИБ через запланированные интервалы времени или в случае выявления новых или потенциальных угроз или произошедших существенных изменений, учитывая критерии рисков нарушения МИБ, установленные в соответствии с 6.1.2 a).

Государство-участник должно хранить документированную информацию о результатах проведенных оценок рисков нарушения МИБ и рисков возникновения инцидентов МИБ.

8.3. Обработка рисков нарушения МИБ

Государство-участник должно реализовывать план обработки рисков нарушения МИБ и рисков возникновения инцидентов МИБ, а также хранить документированную информацию об этих результатах.

Раздел 9. Оценивание исполнения функций СММИБ

9.1. Мониторинг, оценка защищенности, анализ и оценивание

Государство-участник должно оценивать деятельность СММИБ, а также ее результативность.

Государство-участник должно определить:

a) объекты мониторинга и оценки защищенности, включая процессы, меры и средства предотвращения проявления рисков нарушения МИБ;

b) методы проведения мониторинга, оценки защищенности, анализа и оценивания, обеспечивающие уверенность в достоверности результатов[96].

c) сроки проведения мониторинга и оценки защищенности;

d) ответственного за осуществление мониторинга и оценку защищенности;

---

95 Аутсорсинг — передача одним юридическим лицом (контрактором) другому юридическому лицу (субконтрактору) работ или услуг и принятие их к выполнению этим другим юридическим лицом (субконтрактором) на основании договора

96 Примечание — Допустимыми признаются методы, дающие сопоставимые и воспроизводимые результаты

e) период, за который осуществляется анализ результатов мониторинга и оценки защищенности;

f) ответственного за анализ и оценивание этих результатов, а также за хранение соответствующей документированной информации в качестве свидетельства результатов мониторинга и оценки защищенности.

9.2. Внутренний аудит СММИБ

Государства-участники должны через запланированные интервалы времени проводить аудиты СММИБ с целью определения того, насколько СММИБ:

a) соответствует: 1) собственным требованиям государства к СММИБ; 2) требованиям настоящего стандарта;

b) эффективно реализована и поддерживается.

Государство-участник должно:

a) планировать, разрабатывать, реализовывать и поддерживать программу(ы) участия в аудите СММИБ, включая определение периодичности и методов проведения аудита, ответственность, требования к планированию и предоставление отчетности аудита.

b) определять критерии и область проведения каждого аудита СММИБ;

c) выбирать аудиторов и сопровождать проведение аудитов СММИБ для обеспечения уверенности в объективности и беспристрастности процесса аудита;

d) обеспечивать предоставление результатов аудитов СММИБ соответствующим лицам, утвержденным Государствами-участниками;

e) хранить документированную информацию в качестве свидетельств реализации программ(ы) аудита и результатов аудита СММИБ.

9.3. Проверка со стороны уполномоченного органа Государств-участников

Уполномоченный орган Государств-участников должен проводить проверку СММИБ через запланированные интервалы времени в целях обеспечения уверенности в сохраняющейся ее приемлемости, адекватности и результативности. Проверка со стороны уполномоченного органа Государств-участников должна включать рассмотрение:

a) состояния выполнения решений по результатам предыдущих проверок со стороны уполномоченного органа Государств-участников;

b) изменений внешних и внутренних факторов, касающихся СММИБ;

c) отзывов о результатах деятельности по обеспечению информационной безопасности, включая тенденции в:

1) выявлении несоответствий и применении корректирующих действий;

2) результатах мониторинга и оценки защищенности;

3) результатах аудита;

4) достижении целей МИБ;

d) отзывов от заинтересованных сторон;

e) результатов оценки рисков нарушения МИБ и статуса выполнения плана обработки этих рисков;

f) возможностей для постоянного улучшения СММИБ.

Результаты проверки со стороны уполномоченного органа Государства-участника должны включать решения, относящиеся к возможностям постоянного улучшения и к необходимости внесения изменений в СММИБ. Государства-участники должны хранить документированную информацию в качестве свидетельства результатов проверок со стороны уполномоченного органа.

Раздел 10. Улучшение деятельности СММИБ

10.1. Несоответствие и корректирующие действия

При появлении несоответствия уполномоченные органы Государств-участников должны:

a) реагировать на несоответствие и, если применимо: 1) предпринять необходимые действия, чтобы контролировать и устранить его; 2) устранять последствия несоответствия;

b) оценивать необходимость корректирующих действий по устранению причин несоответствия, чтобы избежать его повторения или появления в другом месте посредством:

1) анализа несоответствия;

2) определения причин появления несоответствия;

3) определения наличия подобных несоответствий или потенциальных(ой) возможностей (и) их возникновения;

c) выполнять необходимые корректирующие действия;

d) анализировать результативность предпринятых корректирующих действий;

e) вносить при необходимости изменения в СММИБ.

Корректирующие действия должны быть адекватны последствиям выявленных несоответствий.

Государства-участники должны хранить документированную информацию в качестве свидетельства о:

- характере несоответствий и любых последующих предпринимаемых действиях;
- результатах любых корректирующих действий.

10.2. Постоянное улучшение

Государства-участники должны постоянно улучшать приемлемость, адекватность и результативность деятельности СММИБ.

Заключение

В результате выполнения НИР показано, что базовым условием начала практического применения норм ответственного поведения государств в ИКТ-среде является равноправное сотрудничество, основанное на «суверенитете государств, международных нормах и принципах, проистекающих из суверенитета», по следующим вопросам:

- согласование процедур и механизмов закрепления в международном договоре цифровых идентификаторов (цифровых адресов) объектов ИКТ-среды, находящихся под суверенитетом государства;
- оснащение критически важных объектов национальной зоны ответственного поведения специальным программным обеспечением и техническим оборудованием, применение которого создаст условия для поддержания правового режима границы зоны ответственного поведения государств в ИКТ-среде, а также международного правового режима безопасности объектов критической информационной инфраструктуры;
- соблюдение обязательств, вытекающих из норм ответственного поведения государств в ИКТ-среде, и, в частности, обязательства по нормативно-техническому регулированию отношений в области: предупреждения и пресечения противоправной деятельности в ИКТ-среде с учетом положений морского, воздушного и космического права; деятельности «заведомо противоречащей международному праву» и «наносящей преднамеренный ущерб критически важной инфраструктуре»; совершения «международно-противоправных деяний с использованием ИКТ» и «вредоносного использования ИКТ, способного создать условия для нарушения международного мира и безопасности», «террористического и преступного использования ИКТ»; оказания помощи государствам, критически важная инфраструктура которых становится объектом злонамеренных действий и другой деятельности, не способствующей поддержанию международного мира и безопасности;
- гармонизация норм ответственного поведения государств в ИКТ-среде и норм национального права, регулирующих отношения в области осуществления информационной деятельности в различных сферах общественной жизни;
- оказание взаимопомощи, преследование лиц, виновных в террористическом и преступном использовании ИКТ в соответствии с положениями всеобъемлющей конвенции по противодействию информационной преступности российского проекта конвенции ООН по противодействию использованию ИКТ в преступных целях;

- обеспечение надёжной и прямой связи между государствами в целях предотвращения и урегулирования серьезных инцидентов в сфере использования ИКТ и ослабления напряженности в кризисных ситуациях.

Перспективными направлениями решения этих вопросов является принятие универсального соглашения по применению норм ответственного поведения государств в ИКТ-среде, а также международного стандарта технического регулирования в области системы менеджмента международной информационной безопасности.

Настоящая монография содержит результаты комплексного исследования проблем практического применения норм ответственного поведения государств в ИКТ-среде и предложения по решению этих проблем.

Монография будет полезна специалистам в области политологии, юриспруденции, обеспечения безопасности использования ИКТ, а также всем, кто интересуется проблематикой международной информационной безопасности.

МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ В СРЕДЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

КОЛЛЕКТИВНАЯ МОНОГРАФИЯ ПО ПРОБЛЕМЕ ПРИМЕНЕНИЯ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ

ПОД РЕДАКЦИЕЙ ПРОФ. А.А. СТРЕЛЬЦОВА, ПРОФ. А.Я. КАПУСТИНА, ПРОФ. Т.А. ПОЛЯКОВОЙ, ПРОФ. А.С. МАРКОВА, Б.Н. МИРОШНИКОВА

Подписано в печать 20.03.2023. Гарнитура Times.
Формат 60x84/8. Объем 15.35 усл. печ. л.
Тираж 100 экз.