Санкт-Петербургский государственный университет

Рац Даниил Владимирович

Выпускная квалификационная работа
Подход РФ к международной информационной безопасности

Уровень образования: Магистратура
Направление 41.04.05 «Международные отношения»
Основная образовательная программа
ВМ.5557.2021
«Дипломатия Российской Федерации и зарубежных государств»

Научный руководитель:
Профессор кафедры европейских исследований
Доктор Экономических Наук
Ткаченко Станислав Леонидович

Рецензент:
Профессор Северо-Западного Института Управления
РАНХиГС при Президенте Российской Федерации
Доктор юридических наук
Карцов Алексей Сергеевич

Санкт-Петербург
2023

Введение

Актуальность исследования.

XXI век стал веком Информационно-Коммуникативных Технологий. Научно-технический прогресс привел к повсеместному применению интернета. Актуальность темы обуславливается “интернетизацией” всех сфер жизни, в том числе и международной политики. По данным статистики Social 2020 люди в среднем проводят в интернете 6 часов в сутки.[1] Постоянно растущий объем данных в онлайн-пространстве делает их стратегическим ресурсом в борьбе за лидерство на мировой арене, а цифровой потенциал стал одним из определяющим фактором успешности государства. Всё больше угроз содержится в киберпространстве: террористические, военно-политические или даже преступные. Кибератаки приобретают все большее значение в международных отношениях. Корпорации, государственный учреждения, военнизированные структуры становятся зависимы от интернета, вследствие этого растет разрушительный потенциал кибератак. Это приводит к тому, что информационная безопасность становится одним из главных направлений деятельности государств. Скорость и стоимость утечек данных в результате кибератак постоянно растут.

В марте 2023 г. была опубликована новая Национальная стратегия кибербезопасности США, что говорит о множестве изменений в понимании проблемы и политике американского руководства.

Государства, частные структуры и даже сети хактивистов огромные возможности для атак в киберпространстве. С начала СВО в начале 2022 г. резко возросло количество кибератак, как на гос учреждения, так и на частные лица.[2] Так, например, хакерское движение “Anonymous” объявили

---

[1] Digital 2020: 3.8 billion people use social media.[Электронный ресурс]// We are social. URL: https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media/ (Дата обращения 10.12.2022)

[2] Число кибератак на госучреждения России в 2022 году выросло на четверть. // ТАСС. URL: https://tass.ru/ekonomika/16981635 (Дата обращения 12.03.2023)

России “кибервойну”.[3] А по словам генерала Пола Накасоне американские военные хакеры участвовали в “наступательных хакерских операциях для поддержки Украины”.[4] В 2006 г. в России количество преступлений в компьютерной сфере было около 20 тыс., в 2021 г. 517 тыс. На 2022 г. использованием ИКТ совершено каждое четвёртое преступление.[5] Технически возможно осуществить кибератаки на транспортную инфраструктуру, электросети, плотины, химические заводы, атомные электростанции и другие важнейшие объекты. Эти атаки могут иметь далеко идущие последствия, привести к большому количеству жертв среди гражданского населения и значительным физическим разрушениям.

Несмотря на очевидную угрозу, до сих пор поведение государств, компаний и людей не регулируется на международной арене.

Начиная с 1998 г. Российская дипломатия добивается принятия резолюции ООН об Информационной безопасности, предполагающий комплексный, всеобъемлющий подход, основанный на интернационализации, демилитаризации и “деидеологизации” интернета. Данный подход отвергался в связи с тем, что для западной стороны такой подход выглядел как система контроля интернета. Вся проблематика международной информационной безопасности тесно связана с Российско-американским противостоянием на международной арене в политической, экономической, технологической, идеологических сферах.

Поиск взаимовыгодных соглашений и идей, постоянное нарастание угроз в интернет пространстве привели к значительному продвижению в вопросах выработки универсальных правил поведения государств в интернете. Были

---

[3] The cybersecurity impact of Operation Russi by Anonymous. // ComputerWeekly.com. URL: https://www.computerweekly.com/feature/The-cyber-security-impact-of-Operation-Russia-by-Anonymous (Дата обращения 05.12.2022)

[4] US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command. // Skynews. URL: https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (Дата обращения 05.03.2023)

[5] Международная безопасность в среде информационно-коммуникационных технологий : Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / А. А. Стрельцов, А. Я. Капустин, Т. А. Полякова [и др.] ; Национальная Ассоциация международной информационной безопасности. – Москва : НАМИБ, 2023. – 132 с.

заключены соглашения в рамках ШОС, двусторонние соглашения, а также созданы несколько рабочих групп в рамках ООН. Однако, в связи с обострением военно-политической обстановки, резкой поляризации мира и усилением соперничества между великими державами оборвался прогресс в достижении взаимовыгодного соглашения.

Цель исследования: Исследовать особенности российского подхода, его эволюцию и проблемы обеспечения международной информационной безопасности.

Задачи исследования

- Определить уровень угроз информационной безопасности
- Выяснить различия в определениях основных понятий, касающихся международной информационной безопасности.
- Исследовать концепцию киберсдерживания в контексте информационной безопасности.
- Исследовать нормативно-правовую базу РФ в контексте достижения режима международной информационной безопасности
- Рассмотреть концепции и резолюции, выдвигаемые Россией и США в ООН, затрагивающие информационную безопасность
- Исследовать двусторонние и многосторонние соглашения по вопросам международной информационной безопасности
- Исследовать киберконфликт между РФ и США

Объект исследования : международная информационная безопасность

Предмет исследования : Российские концепции и инициативы по международной информационной безопасности

Научная гипотеза

В сложившейся военно-политической обстановке на мировой арене реальным фактором поддержания международной информационной безопасности является политика сдерживания в киберпространстве.

Методология исследования

В процессе исследование использовался дискурс-анализ, для определения различий в понимании проблемы между разными акторами. При этом автор придерживается конструктивистской теории и считает, что действия тех или иных акторов основаны на ценностях и социальной реальности, в которой находятся эти акторы.

Кроме того была использованная теория секьюритизации, т.к. проблема международной информационной безопасности затрагивает проблему суверенитета, в частности, информационного суверенитета, и угрозу его нарушения.

Для анализа развития проблематики во времени был использован историко-описательный метод познания.

В качестве источниковой базы для исследования было использовано множество документов, международных соглашений, концепций. К таковым относится “Концепция Конвенции ООН об обеспечении международной информационной безопасности” 2021 г. являющееся собой видение Российского руководства о гипотетическом режиме международной информационной безопасности в рамках ООН.

Из доктринальных документов Российской Федерации взята Доктрина Информационной безопасности 2016 г., которая определяет основные угрозы, термины, политику в отношении информационной безопасности, указ “Основы государственной политики Российской Федерации в области международной информационной безопасности” 2021 гг., в соответствии с которым Российская дипломатия добивается создания режима международной информационной безопасности. Стратегия национальной безопасности 2021 гг., которая определяет ценности и понимание российского руководства проблематики безопасности. Использовано множество резолюций ООН, таких как “Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности” и “Противодействие использованию информационно коммуникационных технологий в преступных целях”, Из международных соглашений можно

выделить “Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности.” , “Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности”

Дж. Б. Гудвин, А. Кульпин, К. Ф. Раушер, В. Ященко совместно с другими экспертами института “Восток-Запад” и Института проблем информационной безопасности МГУ разработали основы критической терминологии в контексте российско-американских отношений. Данный сборник терминов является важной попыткой экспертного сообщества по преодолению различий в понимании проблематики информационной безопасности. Попыткой, которая в данный момент не является востребованной ни в двустороннем, ни в многостороннем формате.

Дж. Микинс в своей работе “Жизнь в (цифровом) отрицании: Российский подход к киберсбердживанию” провёл анализ российских концепций и практик по кибер сдерживанию, политики обеспечения информационной безопасности в целом и практик наступательных кибероперацій, определив киберпространство как одно из самых эффективных инструментов проявления силы.

Исследована глава по кибербезопаности монографии Терехова А.Н. и Ткаченко С.Л. “Политическая экономии информационно-коммуникационных технологий: место России на глобальном рынке”. Авторы провели кейс-стади “вмешательства русских хакеров в выборы в США”, обнаружив высокую степень политизированности вопроса и манипулятивную сущность атрибуции России.

Использованы работы М. Баезнер и П. Робином по анализу информационного противостояния РФ и США. Исследователи пришли к выводу, что конфликт, вызванный кибератаками на США в 2016 г. привели к новой вехе развития кибербезопасности. Эксперты также признали разрушительное влияние информационной войны, и даже признали необходимость вовлечения

государства в противостоянии информационным угрозам. Однако авторы сохранили приверженность термину “кибербезопасности”, т.е. ограничивались лишь техническими аспектами безопасности.

Также для изучения взаимоотношений США и РФ в области информационной безопасности использована работа Зиновьевой Е.С. и Яникеевой И.О. для исследования истории взаимодействия двух держав. Авторы концентрируют внимание на взаимодействие по дипломатической линии и видят в укреплении взаимного доверия в цифровой среде основу будущего режима информационной безопасности.

В работе использованы статьи экспертов РСМД О. Шакирова и С. Себекина для анализа политики РФ в области сдерживания в киберпространстве, а также работы российской дипломатии в рамках ООН и других организаций, таких как СНГ, БРИКС, ШОС.

Бойко С.М. - Начальник Департамента проблем безопасности в информационной сфере аппарата Совета безопасности Российской Федерации, в своих статьях провел анализ политики РФ в области МИБ, а также анализ основных угроз информационной безопасности с точки зрения Российского правительства.

Работа Дженсена Е.Т. посвящены применимости международного права к киберпространству, в том числе анализу Таллинского Мануала 2.0., который представляет из себя взгляд множества экспертов на терминологию кибербезопасности, его связью с международным правом.

Обоснование структуры работы

В Главе 1 проводиться анализ теоретической составляющей международной-информационной безопасности : различия в подходах и определениях как внутри РФ, так и по сравнению с подходами за рубежом, а также изучены нормативно-правовые основы подхода РФ к проблематике

В Главе 2 рассмотрена деятельность РФ на международной арене по созданию режима международной информационной безопасности в рамках

ООН, в рамках многосторонних международных организаций и объединений и двусторонние отношения по проблематике между РФ и США.

Глава 1. Концепт международной информационной безопасности

1.1. Подходы к определению угроз и термина информационной безопасности

Бывший президент корпорации по управлению доменными именами и IP-адресами ICANN Р. Бекстром сформулировал три принципа интернета:

1. Всё, что имеет доступ в интернет может быть взломано
2. Всё имеет доступ к интернету
3. Таким образом, все становится уязвимым. Мир вступает в фазу бесконечной борьбы с киберугрозами, которые постоянно совершенствуются[6]

В 1995 г. RAND Corporation по заказу МО США провела исследование “информационного противоборства”. Результатом исследования стало появление термина Strategic information warfare - “использование государствами глобального информационного пространства и инфраструктуры для проведения стратегических военных операций и уменьшения воздействия на собственный информационный ресурс”[7]

Использование компьютерных сетей во вред другому государству породило конспект “кибервойны”, понимаемую как ”действия национального государства по проникновению в компьютеры или сети другого государства с целью

[6] Beckstrom, Rob. Speech at the London Conference on Cyberspace. // ICANN. November 2, 2011. URL: https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf (Дата обращения 07.03.2023)

[7] Molander R. C., Riddile A. S., & Wilson P. A. Strategic Information Warfare: A New Face of War. / R.C. Molander, A.S. Riddile, P.A. Wilson. // RAND Corporation. URL : http://www.jstor.org/stable/10.7249/mr661osd (Дата обращения 03.03.2023)

причинения вреда или нарушения работы”[8]. Однако это определение весьма ограничено, поскольку не включает негосударственных субъектов, например, хактивистов, группы и корпоративный шпионаж. Более того, открыто обсуждается вопрос о том, можно ли считать кибервойну "настоящей войной", поскольку в ней нет физических "линий фронта".[9]

И термин “кибервойна” и “информационная война” не могут быть использованы в международном праве, по причине отсутствия термина “война в Уставе ООН. Эти термины необходимы для описания конфликта между государствами. В связи с этим необходимо выделить понятия “кибератаки”, “компьютерной атаки” или “информационной атаки”. Министерство обороны США определяет данное явление так : “Компьютерные сетевые атаки — это действия, предпринимаемые с использованием компьютерных сетей для того, чтобы испортить или уничтожить информацию, находящуюся в компьютерах и компьютерных сетях или компьютеры и сами сети”[10]

По утверждению Саймонса связь между информационной войной и сменой режима очевидна, поскольку физические, информационные и когнитивные аспекты информационной войны переплетаются и влияют на восприятие и реакцию участников. Он разделяет 2 желаемых результата информационной войны:

1. Обоснование военных усилий по смещению того или иного правительства
2. Подрыв легитимности правительства, объекта информационной войны, тем самым ограничивая его способность защищаться и ограничивая его возможности.[11]

---

[8] Abdyraeva C. “Cyber Warfare.” The Use of Cyberspace in the Context of Hybrid Warfare.: Means, Challenges and Trends. / C. Abdyraeva // OIIP - Austrian Institute for International Affairs - 2020 - P. 36

[9] Abdyraeva C. “Cyber Warfare.” The Use of Cyberspace in the Context of Hybrid Warfare.: Means, Challenges and Trends. / C. Abdyraeva // OIIP - Austrian Institute for International Affairs - 2020 - P. 36

[10] Капустин А.Я. Угрозы международной информационной безопасности: формирование концептуальных подходов / А.Я. Капустин // Журнал российского права. - 2015. №8 (224). URL: https://cyberleninka.ru/article/n/ugrozy-mezhdunarodnoy-informatsionnoy-bezopasnosti-formirovanie-kontseptualnyh-podhodov (дата обращения: 17.05.2023).

[11] Simons G. The Evolution of Regime Change and Information Warfare in the 21st Century. / G.Simons // Journal of International Analytics. - 2020;11(4) - P. 72-90.

Негосударственные и спонсируемые государством субъекты осуществляют стратегические кибератаки на объекты критической инфраструктуры и взламывают корпоративные сети с целью кражи информации о конкретных лицах или установки вирусов и шпионских программ. Во-вторых, государства проводят операции информационной войны в киберсфере, которые намеренно используются для манипулирования данными, например, для намеренного влияния на общественное мнение с помощью инструментов и ботов для формирования интернет-контента и/или распространения дезинформации с целью подорвать доверие общества к национальным институтам. [12] Можно считать, что в условиях развития концепций киберпвойны киберпространство рассматривается как "пятое пространства", используемого для достижения политических целей.[13]

Одним из ключевых понятий проблемы МИБ является киберпространство. Изначально придуманный писателем фантастом У.Гибсоном термин происходит от слова "кибернетика" наука, изучающая общие принципы функционирования и передачи информации в машинах, живых организмах и человеческом обществе. Данный термин не имеет общепризнанного определения, однако большинство государственных источников, наряду с исследователем согласны с тем, что киберпространство шире, чем интернет[14]

Киберпространство можно рассматривать, с одной стороны, как суверенную территорию, а с другой - как глобальное общее достояние.Россия и Китай поддерживают многосторонний подход, при котором государства участвуют во взаимодействии и сотрудничают в принятии решений относительно политики и допустимой деятельности в киберпространстве. Эта модель, ориентированная на государство, способствует усилению регулирования информации. США и их союзники поддерживают модель с участием многих заинтересованных сторон, в которой управление Интернетом включает все

[12] Abdyraeva C. "Cyber Warfare." The Use of Cyberspace in the Context of Hybrid Warfare.: Means, Challenges and Trends. / C. Abdyraeva // OIIP - Austrian Institute for International Affairs - 2020 - P. 36

[13] Данельян А.А., Гуляева Е.Е. Международно-правовые аспекты кибербезопасности. / А.А. Данельян, Е.Е. Гуляева // Московский журнал международного права. - 2020. - С. 44-53

[14] Данельян А.А., Гуляева Е.Е. Международно-правовые аспекты кибербезопасности. / А.А. Данельян, Е.Е. Гуляева // Московский журнал международного права. - 2020. - С. 44-53

соответствующие заинтересованные стороны, такие как частный сектор, гражданское общество, научные круги и частные лица, в дополнение к правительствам.[15]

“Cyber” означает “связанные с электронными коммуникационными сетями, особенно с Интернетом” [16] Различие терминов заключается в том, что “Информационная безопасность” носит антропоцентрический характер, в то время как “Кибербезопасность” - технический. [17]

В 2010 г. Международный союз электросвязи определил кибербезопасность как “Набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя”[18]

Со стороны Международной организации по стандартизации термин кибербезопасность означает “сохранение конфиденциальности, целостности и доступности информации в киберпространстве”[19]

Используя методы текстуального анализа Д. Шальц, Р. Башруш, Дж. Уолл провели различные семантические и лексические анализы определений из 28 авторитетных источников. В результате исследования они определили кибербезопасность как “Подход и действия, связанные с процессами управления рисками безопасности, которым следуют организации и государства для защиты конфиденциальности, целостности и доступности данных и активов, используемых в киберпространстве. Концепция включает руководящие принципы, политики и подборки гарантий, технологий,

---

[15] Stadnik I. What Is an International Cybersecurity Regime and How We Can Achieve It? / I. Stadnik // Masaryk University Journal of Law and Technology. - 2017 - 11(1):129 -P. 129 - 154

[16] Oxford Advanced Learner’s Dictionary. URL: https://www.oxfordlearnersdictionaries.com/definition/english/cyber?q=cyber (Дата обращения 28.02.2023)

[17] Ваничкина А.С. Концептуальная парадигма дискурса информационной безопасности.// А.С. Ваничкина Материалы IV Международной научной конференции. Москва, 2021. — 2021 — С. 209 - 2013.

[18] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[19] ISO, 2012. ISO / IEC 27032:2012. // Information Technology Security techniques – Guidelines for cybersecurity. URL: https://www.iso27001security.com/html/27032.html (Дата обращения 14.05.2023)

инструментов и обучение для обеспечения наилучшей защиты для состояния киберпространства и ее пользователей.”[20]

Исследователи также приводят результаты исследования исследовательской и консалтинговой компании Gartner Inc. Они предлагают использовать термин кибербезопасность только в контексте практики обеспечения безопасности, связанной с сочетанием наступательных и оборонительных действий с использованием или опорой на информационные технологии и/или операционные технологические среды и системы. Авторы утверждают, что она представляет собой надмножество практик безопасности, таких как информационная безопасность, ИТ-безопасность и другие смежные практики. В то же время приводится другая точка зрения о том, что кибербезопасность является подмножеством информационной безопасности[21]

Одной из важнейших задач национальной безопасности развитых стран современного мира стало обеспечение критически важной инфраструктуры (КВИ) от кибервоздейсвтий. Международное сообщество так и не выработало общее определение данного понятия, однако таковые есть на национальном уровне. Так, в России используется определение КВИ “объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок;”[22]

При этом отдельно существует Федеральный закон “О безопасности критической информационной инфраструктуры Российской Федерации”,

[20] Schatz D. Bashroush R. Wall J. Towards a More Representative Definition of Cyber Security. / D. Schatz, R. Bashroush, J. Wall // Journal of Digital Forensics, Security and Law. - 2017 Vol. 12: No. 2, Article 8. - P. 53 - 74

[21] Schatz D. Bashroush R. Wall J. Towards a More Representative Definition of Cyber Security. / D. Schatz, R. Bashroush, J. Wall // Journal of Digital Forensics, Security and Law. - 2017 Vol. 12: No. 2, Article 8. - P. 53 - 74

[22] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. // Совет безопасности Российской Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document113/ (Дата обращения 5.05.2023)

который определяет критически важную информационную инфраструктуру как “информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности”[23]

Основной концепт этого закона заключается в том, что лица, владеющие критической инфраструктурой, должны гарантировать ее безопасность, при этом государство берет на себя обязательство оказывать им полное содействие.[24]

Кибератаки, осуществляемые государственными и негосударственными субъектами, такими как преступные группы, террористы и частные лица, являются широко распространенной проблемой, затрагивающей как отдельных людей, так и национальную безопасность во всем мире. Центр передового опыта по совместной киберзащите в Таллинне, Эстония, организовал многолетний процесс сбора мнений экспертов о том, как международное право применяется к кибердеятельности. Первое Таллиннское руководство было посвящено законам, связанным с кибератаками во время вооруженных конфликтов, а второе, известное как Таллинн 2.0, охватывает более широкий спектр кибер-операций, в том числе вне вооруженных конфликтов.

Эксперты утверждают , что принцип суверенитета применим к киберпространству, следовательно “Государство не должно проводить кибероперации, нарушающие суверенитет другого государства.”[25]

---

[23] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ // КонсультантПлюс. URL: http://www. consultant.ru/document/cons_doc_LAW_220885 (Дата обращения 5.05.2023)

[24] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[25] Jensen E.T. The Tallinn Manual 2.0: Highlights and insights./ E.T. Jensen // Georgetown Journal of International law. - 2017 - vol. 48 - P. 735 - 778.

По их мнению также важным принципом кибербезопасности является принцип “должной осмотрительности”, т.е. “государство должно проявлять должную осмотрительность, не допуская, чтобы его территория, территория или киберинфраструктура под его правительственным контролем использовалась для кибероперaций, которые затрагивают права других государств и приводят к серьезным негативным последствиям для них” Эксперты также говорят о применимости международного права к вопросам кибербезопасности, о том, что государство “несет международную ответственность за деяние, связанное с киберпространством, которое может быть присвоено государству и которое представляет собой нарушение международно-правового обязательства”[26]

По мнению авторов Таллинского мануала киберпространство не отличается от других сфер отношений и не требует особых подходов к его правовому регулированию. Однако существует точка зрения, гласящая, что не все принципе международного права могут быть применены к киберпространству. Такие концепты как акт агрессии, применение силы и вооруженное нападение не могут быть применены к кибератаке. Концепция информационной войны не может быть применена к понятию войны в ее международно-правовом смысле.[27]

А. Стрельцов подчеркивает значение статьи 41 и статьи 42 Устава ООН, которые различают две основные формы силы: силу, связанную с применением оружия, и силу, не связанную с применением оружия. Стрельцов подчеркивает, что злонамеренное использование информационно-коммуникационных технологий (ИКТ) в первую очередь регулируется положениями, изложенными в статье 2 (4) Устава ООН. Эта статья обязывает государства-члены воздерживаться от применения или угрозы применения силы в их международном взаимодействии, в том числе в киберпространстве. По мнению Стрельцова, несмотря на очевидный

[26] Jensen E.T. The Tallinn Manual 2.0: Highlights and insights./ E.T. Jensen // Georgetown Journal of International law. - 2017 - vol. 48 - P. 735 - 778.

[27] Данельян А.А., Гуляева Е.Е. Международно-правовые аспекты кибербезопасности. / А.А. Данельян, Е.Е. Гуляева // Московский журнал международного права. 2020; С. 44-53

потенциал использования ИКТ в военных целях, большинство экспертов сходятся во мнении, что ИКТ не подпадают под категорию оружия.[28]

Существует мнение о том, что концепция применения силы ООН не охватывает террористов и негосударственных субъектов. Учитывая, что кибератаки не подпадают под обычные категории, используемые международно признанными правилами ведения войны, принято считать, что государства должны воспринимать хакерские атаки как форму преступной деятельности.[29]

По мнению экспертов НАМИБ а рамках ИКТ возможно применение принципа добросовестного соблюдения норм, по примеру принципа добросовестного выполнения международных обязательств, принимаемых в соответствии с Уставом ООН. В случае создания международного соглашения по международной информационной безопасности каждое государство не должно допускать злонамеренные, противоречащие международному праву, наносящие преднамеренный вред критически важной инфраструктуре. Данный потенциальный проект должен включать режим безопасности объектов критически важной инфраструктуры. [30]

Важным вопрос кибербезопасности является проблема атрибуции, т.е. заявление об ответственности личности, организации, государства в совершенном действии. Использование традиционных средств воздействия - армию и флот не оставляли никаких сомнений в причастности государства, того же нельзя сказать о кибератаках. Наиболее сложный юридический вопрос в области атрибуции возникает со стороны негосударственных субъектов, которые могут работать в качестве доверенных лиц государства или каким-либо образом действовать от имени государства, не имея на это четких юридических полномочий.

---

[28] Данельян А.А., Гуляева Е.Е. Международно-правовые аспекты кибербезопасности. / А.А. Данельян, Е.Е. Гуляева // Московский журнал международного права. - 2020. - С. 44-53

[29] Stahl W.M. Кибербезопасность и международное право. / W.M. Stahl. // Международное право. URL: https://interlaws.ru/kiberbezopasnost-i-mezhdunarodnoe-pravo/ (Дата обращения 17.05.2023)

[30] Международная безопасность в среде информационно-коммуникационных технологий : Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / А. А. Стрельцов, А. Я. Капустин, Т. А. Полякова [и др.] ; Национальная Ассоциация международной информационной безопасности. – Москва : НАМИБ, 2023. – 132 с.

Не всегда существует железное прямое доказательство того, кто совершил преступление, и бывает трудно или даже невозможно определить виновного по имеющимся уликам и информации. Проблема также осложняется тем, что разглашение информации о возможностях технической разведки может подорвать будущие возможности этой разведки. [31]

Проблемным является и то, что на данный момент не существует общепринятых механизмов обмена объективной информацией для решения споров в ИКТ среде. Государства редко берут на себя ответственности за инцидент, что приводит к невозможности применения механизмов решения споров согласно уставу ООН.[32]

Конвенция о киберпреступности, принятая 23 ноября 2001 года в Будапеште, подписавшую которую большая часть стран Европы, Южной Америки, Кавказа, Австралия, Япония, Филиппины, США и Канада является одним из немногих примеров многостороннего соглашения по киберпреступности. Ее целями являются:

- Усиление кибербезопасности: Конвенция направлена на содействие разработке эффективных мер по предотвращению и борьбе с киберпреступностью. Она стремится создать основу для международного сотрудничества между государствами-членами с целью укрепления их потенциала в области кибербезопасности.
- Гармонизация законодательства: Конвенция поощряет государства-члены к принятию и применению национальных законов и нормативных актов, направленных на эффективное противодействие киберпреступности. Она направлена на гармонизацию законодательства и обеспечение последовательного правового подхода в различных юрисдикциях, что позволяет наладить сотрудничество в расследовании и преследовании киберпреступной деятельности.

---

[31] Newman L.H. Hacker Lexicon: What Is the Attribution Problem? / L.H. Newman. // Wired. URL: https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/ (Дата обращения 09.05.2023)

[32] Международная безопасность в среде информационно-коммуникационных технологий : Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / А. А. Стрельцов, А. Я. Капустин, Т. А. Полякова [и др.] ; Национальная Ассоциация международной информационной безопасности. – Москва : НАМИБ, 2023. – 132 с.

- Содействие международному сотрудничеству: Конвенция направлена на содействие международному сотрудничеству между государствами-членами в расследовании, преследовании и пресечении киберпреступлений. Она способствует обмену информацией и обеспечивает механизмы взаимной правовой помощи, экстрадиции и сотрудничества по уголовным делам, связанным с киберпреступностью.
- Защита прав человека: Конвенция подчеркивает важность защиты прав человека и основных свобод в контексте расследования киберпреступлений. Она призывает государства-члены обеспечить соблюдение принципов законности, необходимости, пропорциональности и неприкосновенности частной жизни при принятии любых мер по борьбе с киберпреступностью.
- Наращивание потенциала и обучение: Конвенция поощряет инициативы по наращиванию потенциала для укрепления знаний и навыков правоохранительных, судебных органов и других соответствующих заинтересованных сторон в борьбе с киберпреступностью. Она поощряет обмен передовым опытом, предоставление технической помощи и организацию учебных программ.[33]

Множество стран, включая Россию, не присоединились к конвенции и вряд ли присоединятся. Проблема заключается в Статье 32, эта статья позволяет государству-участнику получать доступ к информации, находящейся в другом государстве, через границу, не уведомляя власти государства, в котором находится источник информации. Что по своей сути является нарушением суверенитета государства, права человека на конфиденциальность.[34]

В сентябре 2011 года был опубликован "Проект конвенции о международной информационной безопасности". Этот проект содержал множество терминов,

[33]Council of Europe: Convention on Cybercrime. // European Treaty Series - №. 185 - Budapest. November 23, 2001. URL: https://rm.coe.int/1680081561 (Дата образения 15.05.2023)

[34] Данельян А.А., Гуляева Е.Е. Международно-правовые аспекты кибербезопасности. / А.А. Данельян, Е.Е. Гуляева // Московский журнал международного права. - 2020. - С. 44-53

список угроз, принципы безопасности, меры предотвращения конфликтов и предотвращения правонарушений в информационном пространстве. [35]

Концепция оперирует термином “информационная безопасность”, понимаемую как “ состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве”[36] и “международную информационную безопасность” как “состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве”[37]

Угрозами в данной концепции обозначены:

- Использование ИКТ для актов агрессии
- Деструктивное воздействие на критически важные структуры государства
- Неправомерное использование информационных ресурсов другого государства без согласования с государством
- Использование ИКТ для вмешательство в систему другой страны, психологическое воздействие на население
- Использование ИКТ в террористических и экстремистских целях
- Дезинформация, манипулирование. разрушение традиций и ценностей
- Создание условий цифровой зависимости
- Приобретения контроля над национальными информационными ресурсами другого государства.[38]

---

[35] Конвенция об обеспечении международной информационной безопасности (концепция). // Комитет государственной думы по международным делам. URL: https://interkomitet.ru/blog/2011/09/22/konventsiya-ob-obespechenii-mezhdunarodnoj-informatsionnoj-bezopasnosti-kontseptsiya/ (Дата обращеня 02.04.2023)

[36] Конвенция об обеспечении международной информационной безопасности (концепция). // Комитет государственной думы по международным делам. URL: https://interkomitet.ru/blog/2011/09/22/konventsiya-ob-obespechenii-mezhdunarodnoj-informatsionnoj-bezopasnosti-kontseptsiya/ (Дата обращеня 02.04.2023)

[37] Конвенция об обеспечении международной информационной безопасности (концепция). // Комитет государственной думы по международным делам. URL: https://interkomitet.ru/blog/2011/09/22/konventsiya-ob-obespechenii-mezhdunarodnoj-informatsionnoj-bezopasnosti-kontseptsiya/ (Дата обращеня 02.04.2023)

[38] Конвенция об обеспечении международной информационной безопасности (концепция). // Комитет государственной думы по международным делам. URL: https://interkomitet.ru/blog/2011/09/22/konventsiya-ob-obespechenii-mezhdunarodnoj-informatsionnoj-bezopasnosti-kontseptsiya/ (Дата обращеня 02.04.2023)

Данные угрозы нельзя назвать полностью техническими, они , скорее политические, касающиеся политической стороны вопроса.

Эксперты Conflict Studies Research Centre совместно с Институтом проблем информационной безопасности провели исследование концепта, в котором указали, что множество терминов являются проблемными. В комментарии содержится подробный анализ ключевых положений проекта конвенции, направленного на создание основы для международного сотрудничества в области информационной безопасности. Авторы отмечают, что проект конвенции подчеркивает необходимость сотрудничества государств в предотвращении кибератак, а также призывает к созданию глобальной системы мониторинга для обнаружения и реагирования на киберугрозы.

Однако в комментарии также подчеркивается ряд проблем, связанных с проектом конвенции. Авторы отмечают, что язык конвенции расплывчат и открыт для толкования, что может привести к разногласиям и путанице в ее применении. Они также отмечают, что в проекте конвенции значительное внимание уделяется государственному суверенитету, что может ограничить способность международных организаций играть роль в продвижении информационной безопасности.

Авторы утверждают, что хотя проект конвенции является позитивным шагом в направлении расширения международного сотрудничества в области информационной безопасности, есть несколько областей, в которых его можно улучшить. Они считают, что формулировки конвенции должны быть более точными и что в ней следует сделать больший акцент на роли международных организаций в продвижении информационной безопасности.[39]

В 2021 г. была опубликована новая концепция “Концепция Конвенции ООН об обеспечении международной информационной безопасности” Она

[39] Russia’s “Draft Convention on International Information Security”. A Commentary. // Conflict Studies Research Centre — 2012. URL: http://www.conflictstudies.co.uk/files/20120426_CSRC_IISI_Commentary.pdf (Дата обращения 13.04.2023)

оперирует теми же терминами, но включает в себя значительно расширенный список угроз:

- Использование ИКТ в военно-политических целях
- Использование ИКТ в террористических целях
- Использование ИКТ для вмешательство в дела суверенных государств
- Преступное использование ИКТ (создание вирусов, нарушение конфиденциальности)
- Использование информационных ресурсов, находящихся в юрисдикции другого государства
- Использование ИКТ в ущерб правам человека, в том числе нарушение его конфиденциальности
- Нарушение функционирования сети Интернет
- Создание условий технологической зависимости
- Включение в ИКТ недекларируемых возможностей
- Неосторожное использование технологий
- Монополизация рынка ИКТ
- Покровительство хакерам на своей территории, использование посредников для совершения противоправных деяний в ИКТ
- Дезинформация, приводящая к тяжким последствиям для граждан
- Отсутствие механизмов деанонимизации информационного пространств[40]

В 2011 г. эксперты института "Восток-Запад" совместно с экспертами из Института проблем информационной безопасности в рамках двустороннего проекта опубликовали "Основы критически важной терминологии", в 2014 г. было опубликовано второе издание словаря.

Российский взгляд на информационную безопасность подчеркивает, что информация - это целостная концепция, включающая различные компоненты, и кибер - лишь один из них. Россияне делят информацию на естественную и искусственную, причем кибер - это техническое представление информации.

[40] Концепция Конвенции ООН об обеспечении международной информационной безопасности [Электронный ресурс]. Режим доступа: http://www.scrf.gov.ru/security/information/document112/ (Дата обращения 18.03.2023)

Российская сторона считает, что обсуждение информации должно включать все аспекты, а не только кибер. Кроме того, российская концепция информационной безопасности не ограничивается техническими аспектами, такими как кибер, скорее, она охватывает множество измерений, включая человеческие, социальные, духовные, политические и технические аспекты. Российское руководство считает, что информационная безопасность включает в себя защиту населения от терроризма и цензуры.[41]

Американская сторона считает, что фокусироваться нужно на "кибер" аспекте информационной безопасности. Американцы не считают защиту информации чем-то, что должно включать цензуру или любые попытки контролировать информированность населения.[42]

По результату работы экспертов было определенно 40 терминов, касающихся МИБ, в том числе определение "информационная безопасность", понимаемую как "свойство информационного пространства противостоять угрозам, реагировать на них и восстанавливаться", а "кибербезопасность" - свойство киберпространства (киберсистемы) противостоять намеренным и/или не намеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз." В данном подходе различие заключается в использовании терминов киберпространства, понимаемого как "электронная (включая фотоэлектронные и пр.) среда, (посредством) которой информация создается, передается, принимается, хранится, обрабатывается и уничтожается." и информационное пространство - "любая среда, в которой информация создается, через которую передается, принимается, в которой хранится, обрабатывается и уничтожается."[43], т.е. различие между сугубо технической электронной средой и любой другой средой, содержащую информацию.

---

[41] The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2 / J. B. Goodwin III [et al.]. - EastWest Institute Policy Report Series. - 2014. - P. 76

[42] The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2 / J. B. Goodwin III [et al.]. - EastWest Institute Policy Report Series. - 2014. - P. 76

[43] The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2 / J. B. Goodwin III [et al.]. - EastWest Institute Policy Report Series. - 2014. - P. 76

Согласно позиции России, органы с компетенцией в этой области должны обсуждать и регулировать Интернет в целом. Основное внимание следует уделять новым формам использования сети, которые могут вмешиваться в дела других государств, влиять на внутриполитические процессы и манипулировать общественным мнением. Россия обеспокоена не только технологиями, но также контентом всемирной сети.[44]

Существует традиционная “триада” угроз в сфере ИКТ:

1. Использование ИКТ в военно-политических целях, подразумевающее ущемление суверенитета.
2. Использование ИКТ в преступных целях, нарушающее законодательство стран
3. Использование ИКТ в террористических целях, подразумевающее пропаганду, привлечение сторонников и внутреннюю коммуникацию.[45]

С техниической сторон вопроса В сфере ИКТ можно выделить три отдельные группы деяний, имеющих характер правонарушений и требующих преследования в рамках действующего законодательства:

1. DDoS-атаки представляют собой отправку огромного количества автоматически сгенерированных сообщений с целью намеренно затруднить работу определенного сервера
2. Хищение данных, хранимых в цифровой форме, и их дальнейшее использование в преступных целях;
3. нелегальное проникновение в управляющие системы различных организаций и управление от их имени в собственных, по сути своей преступных, целях[46]

Казарин, анализируя вред “кибер физическим системам”, понимаемых как “система, в которой осуществляется тесная (возможно, полная) конвергенция

---

[44]Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[45] Международная информационная безопасность: подходы России / А.В.Крутских, Е.А.Зиновьева, В.И.Булва, М.Б.Алборова, Ю.А.Юдина; под ред. А.В.Крутских, Е.С.Зиновьева. — Москва, 2021. — 48 с

[46] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

физических и информационно-вычислительных (компьютерных) процессов для создания качественно нового уровня (и охвата) управления и обеспечения функционирования естественных и/или искусственных объектов.”[47], в число которых входит интернет вещей, индустриальный интернет, “умные” энергетические сети, системы больших данных, системы облачных и туманных вычислений, системы дополнительной реальности, робототехнические системы, выделяет уровни опасности угроз. Низкий - при котором возможны нарушения устойчивости функционирования объектов, высокий - при котором нарушено функционирование критически важной инфраструктуры и критический - при котором возможны техногенные катастрофы, нарушение социальной стабильности и межгосударственные конфликты.[48]

Говоря об угрозах МИБ ряд исследователей выдвигает два типа воздействия - информационно-техническое, т.е. использование ИКТ в качестве оружия и информационно-гуманитарное, т.е. использование контента для вмешательства в дела суверенных государств.[49]

Стрельцов и Смирнов считают деятельность Х. Клинтон по “защите права на свободу слова и продвижению социальной сети «Твиттер» для высказывания своих политических настроений” вмешательством в дела суверенных государств, вменяя бывшему Государственному Секретарю США разжигания Арабской Весны, основываясь на публикациях Викиликс.[50]

По мнению Бруно Тосы Де Алькантары концепция информационной безопасности основывается на “советской коллективной памяти необходимости сильного и централизованного государственного контроля”, с

---

[47] Казарин О.В. Шаряпов Р.А. Ященко В.В. Многофакторная классификация угроз информационной безопасности киберфизических систем / О.В. Казарин, Р.А. Шаряпов, В.В. Ященко // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». -2018. № 1 (1). - С. 39–55.

[48] Казарин О.В. Шаряпов Р.А. Ященко В.В. Многофакторная классификация угроз информационной безопасности киберфизических систем / О.В. Казарин, Р.А. Шаряпов, В.В. Ященко // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». -2018. № 1 (1). - С. 39–55.

[49] Казарин О.В. Скиба В.Ю. Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности / О.В. Казарин, Ю.В. Скиба, Р.А. Шаряпов // История и архивы. 2016. №1 (3). URL: https://cyberleninka.ru/article/n/novye-raznovidnosti-ugroz-mezhdunarodnoy-informatsionnoy-bezopasnosti (дата обращения: 17.05.2023).

[50] Стрельцов А.А. Смирнов А.И. Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям / А.А. Стрельцов, А.И. Смирнов // Международная жизнь. URL: https://interaffairs.ru/jauthor/material/1940 (Дата обращения 19.05.2023)

такой точки зрения не важны международные права в отношении свободы выражения и неприкосновенности частной жизни. [51]

Похожего мнения придерживается и Джосс Микинс, заявляя, что Российский концепт информационной войны является “Это широкая концепция, опирающаяся на советские традиции рефлексивного управления, дезинформации, маскировки и провокации и охватывающая электронную войну, PSYOPS, стратегические коммуникации и информационные, кибер операции,”[52]

Важной проблемой информационной безопасности является применение сдерживание в информационной и/или киберсферы. Российские исследователи настаивают на том, что невозможность точной атрибуции, т.е. обвинения, приводит к тому, что третья сторона может провоцировать другие стороны на конфликт,попытки атрибуции без международного соглашения о технических стандартах приведут к необоснованным и ошибочным обвинениям и, как следствие, к эскалации конфликта и общему снижению уровня стратегической стабильности. Кроме того Российская сторона считает, что логика ядерного сдерживания не может и не должна применяться к киберпространству.[53] Природа кибероружия в том, что наступательное кибероружие гораздо шире распространено, чем оборонительное. «Ядерное оружие – это оружие сдерживания, а кибероружие применяется каждый день, и оно применяется наступательно»[54]

Способность государств сотрудничать в области кибербезопасности зависит от их способности различать инструменты и стратегии наступательной и оборонительной кибервойны. Даже если странам удастся договориться о четком определении кибероружия, провести различие между наступательными и оборонительными кибервозможностями будет крайне

[51] De Alcantara B.T. SCO and Cybersecurity: Eastern Security Vision for Cyberspace./ de Alcantara B.T. //International Relations and Diplomacy - 201. Vol. 6. № 10. - P. 549-555

[52]Meakins J. Living in (Digital) Denial: Russia’s Approach to Cyber Deterrence. / J. Meakins // European Leadership Network // JSTOR. URL: http://www.jstor.org/stable/resrep22130 (Дата обращения 09.04.2023)

[53] Meakins J. Living in (Digital) Denial: Russia’s Approach to Cyber Deterrence. / J. Meakins // European Leadership Network // JSTOR. URL: http://www.jstor.org/stable/resrep22130 (Дата обращения 09.04.2023)

[54] Толстухина А. Мы не должны играть в безумства на взрывоопасном информационном поле./ А. Толстухина // Международная жизнь. URL : https://interaffairs.ru/news/show/17460 (Дата обращения 27.03.2023)

сложно. С точки зрения множества экспертов создание международной организации, ответственной за контроль над кибер оружием по типу МАГАТЭ невозможно.[55]

“Российский образец” информационной безопасности во многом происходит из политики Президента В.В. Путина. Речь идет о политики “Разумного консерватизма”, который основывается на сохранении власти и стабильности, национализме, геополитическими устремлениями, тревогами и личном переживании краха СССР.[56]

“Традиционный ценности”, которые, по мнению Российского руководства, оказываются под угрозой своего существования являются одной из опор как внутренней, так и внешней политики РФ. “Стабильность превыше всего” является основной идеей государственности В.В. Путина.[57]

Россия признает необходимость установления определенных правил поведения государств в информационном пространстве с целью обеспечения стабильности и безопасности. Это включает заключение международных соглашений, подразумевающих “демилитаризацию” информационной сферы то есть от любых возможных агрессивных действий в информационной сфере.[58]

1.2.Нормативно-правовая база обеспечения информационной безопасности РФ

Первая доктрина информационной безопасности, определяющая термин в российском правовом поле была “Доктрина информационной безопасности Российской Федерации от 9 го сентября 2000 г.” В ней определялось, что “информационная безопасность является состояние защищенности ее

[55] Stadnik I. What Is an International Cybersecurity Regime and How We Can Achieve It? / I. Stadnik // Masaryk University Journal of Law and Technology. - 2017 - 11(1):129 -P. 129 - 154

[56] Колтон Тимоти. В чём смысл путинского консерватизма? [Электронный ресурс]// Международный дискуссионный клуб Валдай. Режим доступа: https://ru.valdaiclub.com/a/highlights/putinskiy-konservatizm/

[57] Kaylan M. Kremlin values: Putin’s Strategic Conservatism./ M. Kaylan. // World Affairs - 2014 vol. 177, № 1 - P. 9–17. URL: http://www.jstor.org/stable/43555061. (Дата обращения 12.03.2023)

[58] Зиновьева Е.С. Анализ внешнеполитических инициатив России в области международной информационной безопасности. / Е.С. Зиновьева // Вестник МГИМО университета - 2014. - С.47-52.

национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.”[59]

Сам термин “информационная безопасность” в Российской Федерации определяется в “Доктрине информационной безопасности Российской Федерации”, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. №646. Согласно доктрине “Информационная безопасность Российской Федерации (далее - информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;”[60]

Ключевые идеи Доктрины информационной безопасности РФ 2016 г.:

- Концепция информационной безопасности как комплексного подхода к защите информации от различных угроз и рисков, включая технические, социальные и политические аспекты.
- Понимание информации как важного национального ресурса, который необходимо защищать и использовать в интересах национальной безопасности.
- Значение информационных технологий и интернета для экономического, социального и культурного развития России, а также их потенциала для использования в качестве инструмента международного влияния.

[59] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895). // Информационно-правовой портал Гарант.ру. URL: https://base.garant.ru/182535/ (Дата обращения (05.03.2023)

[60] Указ Президента Российской Федерации от 5 декабря 2016 г. №646 “Доктрина информационной безопасности Российской Федерации” // Электронный фонд правовых и нормативно-технических документов. URL:: https://docs.cntd.ru/document/420384668?marker=6560IO (Дата обращения 05.03.2023)

- Угрозы информационной безопасности, включая киберпреступность, кибершпионаж, кибертерроризм, информационную войну и манипуляции в информационном пространстве.
- Значение международного сотрудничества в области информационной безопасности, включая участие в международных организациях, развитие диалога и консультаций с другими странами, а также участие в разработке международных стандартов и норм.
- Необходимость защиты государственной информации, информационных систем и критической информационной инфраструктуры России[61]

Абдусаламов Р.А. положительно оценивает новую Доктрину, указывая на эволюцию её положений относительно изменений в технологическом пространстве и то, что эти положения направлены в сторону совершенствования национальной безопасности, однако не рассматривает тот факт, что в новой доктрине смещен акцент с защиты прав и свобод граждан России на получение информации на противодействие враждебным действиям.[62]

Доктрина отражает тренд Российского государства на увеличение полномочия государственных органов, а также свойственный ему патернализм. Интересы государства стоят чётко выше интересов личности.[63] . Количество угроз значительно увеличилось, их акцент смещен в сферу технологий коммуникаций и бытовых цифровых технологий. [64]

Гриценко В.В. отмечает важность понятия информационной сферы и тот факт, что в Доктрине 2000 г. она отсутствует, в то время как в новой доктрине

---

[61] Указ Президента Российской Федерации от 5 декабря 2016 г. №646 “Доктрина информационной безопасности Российской Федерации” // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/420384668?marker=6560IO (Дата обращения 05.03.2023)

[62] Абдусаламов Р.А. К вопросу о совершенствовании доктринальных положений в области обеспечения информационной безопасности./ Р.А. Абдусаламов, Л.В. Магдилова, Д.А. Рагимханова.// Юридический вестник ДГУ. — 2017. — Т 24. — № 4 — С. 165-169

[63] Шариков П.А. Степанова Н.В. Подходы США, ЕС и России к проблеме информационной политики./ П.А. Шариков, Н.В. Степанова // Современная Европа — 2019. — № 2. — С. 73 - 83.

[64] Костенко Н.И. Международная информационная безопасность в рамках международного права (методология, теория)./ Н.И. Костенко// Российский журнал правовых исследований. — 2018. — № 4. (17) — С. 9-16

она четко определена.[65] Информационная сфера определяется как “совокупность информации, объектов информатизации информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.”[66]

Терехов и Ткаченко считают, что в доктрине особенно важны положения об отсутствии международно правовых норм, которые регулировали бы отношения между государствами в информационном пространстве.[67]

Стоит выделить оценку угроз в доктрине “Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.”[68]

В доктрине не уточняется что такое информационно-психологическое воздействие. Согласно Макаренко С.И.“Информационно-психологическое воздействие информационное, психотронное или психофизическое воздействие на психику человека, оказывающее влияние на восприятие им реальной действительности, в том числе на его поведенческие функции, а также в некоторых случаях на функционирование органов и систем

---

[65] Грищенко В.В. Доктрина информационной безопасности Российской Федерации: Сущность, современное значение и организационно-правовые основы. Административное/ В.В. Грищенко.// Административное право и административный процесс. — 2017 — № 1— С. 78-88

[66] Указ Президента Российской Федерации от 5 декабря 2016 г. №646 “Доктрина информационной безопасности Российской Федерации” // Электронный фонд правовых и нормативно-технических документов. URL:: https://docs.cntd.ru/document/420384668?marker=6560IO (Дата обращения 05.03.2023)

[67] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[68] Указ Президента Российской Федерации от 5 декабря 2016 г. №646 “Доктрина информационной безопасности Российской Федерации” // Электронный фонд правовых и нормативно-технических документов. URL:: https://docs.cntd.ru/document/420384668?marker=6560IO (Дата обращения 05.03.2023)

человеческого организма”[69] Каждый человек является носителем собственного видения мира, своих идеалов и взглядов. Каждый человек может быть подвергнуть этому воздействию для изменения этих идеалов и взглядов как в негативную, так и положительную сторону.

Шакиров отметил, что в Доктрине 2000 г. отсутствует термин “сдерживание”, в то время как в новой отмечается, что стратегическое сдерживание в ИКТ названо первым среди остальных направлений в обеспечении информационной безопасности во внешней политике. [70]

В “Военной доктрине Российской Федерации” 2014 г. использование ИКТ в военно-политических целях отнесено к основным внешним опасностям. Особенно подчеркивается опасность внешнего информационного воздействия на население.[71]

Хоть в Доктрине информационной безопасности и упоминается необходимость международного сотрудничество, а также зарубежных угроз эту доктрину нельзя назвать определяющим для внешней политики Российской Федерации.

Таковым можно считать Указы Президента Российской Федерации об основах государственной политики в области международной информационной безопасности.

Первым указом был “Основы государственной политики Российской Федерации в области международной информационной безопасности до 2020 года” от 24.07.2013 г.

В данном документе международная информационная безопасность понимается как “такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также

---

[69] Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века / С. И. Макаренко. – Санкт-Петербург : Издательство «Наукоемкие технологии» -2017. – 546 с.

[70] Шакиров О.И. Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве / О.И. Шакиров // Международная аналитика. – 2020. – Том 11 (4). – С. 147–170

[71] Меньшиков П.В. Актуальные аспекты обеспечения информационного суверенитета России. / П.В. Меньшиков // Международные коммуникации — 2018. — 20 марта. №5. URL: https://intcom-mgimo.ru/2017/2017-05/information-sovereignty-of-russia (Дата обращения 15.05.2023)

деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.”[72]

При этом обозначены угрозы международной информационной безопасности - это использование информационного оружия в военно-политических целях, террористических, вмешательство во внутренние дела государства, совершение преступлений в информационной сфере.[73]

В новом Указе Президента Российской Федерации от 12 апреля 2021 г. № 213 “ Основы государственной политики Российской Федерации в области международной информационной безопасности” сущность международной информационной безопасности определена как: “такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности.”[74]

По сравнению с предыдущими основами политики полностью исчезло упоминание прав личности и общества. Вместо “критически важной инфраструктуры” мы видим более широкое понятие “поддержание международного мира, безопасности и стабильности.”

Количество и качество угроз также видоизменилось. К их списку также добавилось “использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий”[75]

---

[72] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утверждены Президентом Российской Федерации 24 июля 2013 г N ПР-1753)// Кодификация.РФ. URL: https://rulaws.ru/acts/Osnovy-gosudarstvennoy-politiki-Rossiyskoy-Federatsii-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasn/ (Дата обращения 07.03.2023)

[73] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утверждены Президентом Российской Федерации 24 июля 2013 г N ПР-1753)// Кодификация.РФ. URL: https://rulaws.ru/acts/Osnovy-gosudarstvennoy-politiki-Rossiyskoy-Federatsii-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasn/ (Дата обращения 07.03.2023)

[74] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 “ Основы государственной политики Российской Федерации в области международной информационной безопасности” // Электронный фонд правовых и нормативно-технических документов. Режим доступа: https://docs.cntd.ru/document/603255343

[75] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 “ Основы государственной политики Российской Федерации в области международной информационной безопасности” // Электронный фонд правовых и нормативно-технических документов. Режим доступа: https://docs.cntd.ru/document/603255343

Можно сказать, что Российское руководство пытается добиться “цифрового суверенитета”. Основываясь на понятиях суверенитета в разных областях, Кучерявый выделяет понятие “верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве. “[76]

Необходимость достижения цифрового суверенитета происходит из проблемы “цифрового разрыва”, т.е. неравенства в распределении ресурсов ИКТ между странами. Цифровой разрыв опасен тем, что “киберсила” государства напрямую влияет на его влияние. Речь идёт как о кибероружии, так и информационных, т.е. политических средствам влияния.[77]

Важность информационной безопасности для государства и общества подчеркивается в Концепции внешней политики Российской Федерации от 30о ноября 2016 г. В ней утверждается “ На передний план, наряду с военной мощью, выдвигаются такие важные факторы влияния государств на международную политику, как экономические, правовые, технологические, информационные.”[78]

Согласно концепции : “Россия принимает необходимые меры для обеспечения национальной и международной информационной безопасности, противодействия угрозам государственной, экономической и общественной безопасности, исходящим из информационного пространства, для борьбы с терроризмом и иными криминальными угрозами с применением информационно-коммуникационных технологий, противодействует их использованию в военно-политических целях, не соответствующих нормам международного права, включая действия, направленные на вмешательство во внутренние дела государств или

[76] Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира/ М.М. Кучерявый // Управленческое консультирование — 2014 г. — № 9 — С. 7-13

[77] Ющенко В.А. Международная информационная безопасность: общая характеристика и Российский подход к изучению. / В.А. Ющенко // Русская политология. - 2018. № 4 (9) - С. 55 - 61

[78] Указ Президента РФ от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // Официальные сетевые ресурсы Президента России. URL: http://www.kremlin.ru/acts/bank/41451 (Дата обращения 23.02.2023)

представляющие угрозу международному миру, безопасности и стабильности, добивается выработки под эгидой ООН универсальных правил ответственного поведения государств в области обеспечения международной информационной безопасности, в том числе посредством интернационализации на справедливой основе управления информационно-телекоммуникационной сетью "Интернет".”[79]

В новой Концепции внешней политики РФ 2023 г. важность информационной безопасности обозначена более четко и развернуто.

В первую очередь указано, что национальным интересом России является “Развитие безопасного информационного пространства, защита российского общества от деструктивного иностранного информационно-психологического воздействия”[80]

В концепции также говориться о том, что в случае если ИКТ используются иностранным государствами для нарушения суверенитета и территориальной целостности РФ, то она готова ответить как симметрично, так и асимметрично.

Данный отход от симметричных или мер мирного урегулирования говорит о смене устоявшегося подхода. Эта мера может быть вызвана тем, что США применяют принцип “дипломатические, информационные, военные (как кинетические, так и кибернетические), финансовые, разведывательные и правоохранительные меры в ответ на кибератаки” зафиксированный в Национальной Стратегии Кибербезопасности США[81]

Политика в отношении МИБ стала также более структурированной:

“В целях обеспечения международной информационной безопасности, противодействия угрозам в ее отношении, укрепления российского

---

[79] Указ Президента РФ от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // Официальные сетевые ресурсы Президента России. URL: http://www.kremlin.ru/acts/bank/41451 (Дата обращения 23.02.2023)

[80] Указ Президента Российской Федерации от 31 марта 2023 года № 229 "Об утверждении Концепции внешней политики Российской Федерации". [Электронный ресурс]// Официальные сетевые ресурсы Президента Российской Федерации. Режим доступа: http://kremlin.ru/events/president/news/70811 (Дата обращения 16.04.2023)

[81] National Cybersecurity Strategy. [Электронный ресурс]// The White House. — 2023. Режим доступа: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

суверенитета в глобальном информационном пространстве Российская Федерация намерена уделять приоритетное внимание:

1) укреплению и совершенствованию международно-правового режима предотвращения и разрешения межгосударственных конфликтов и регулирования деятельности в глобальном информационном пространстве;

2) формированию и совершенствованию международно-правовых основ противодействия использованию информационно-коммуникационных технологий в преступных целях;

3) обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети «Интернет» на основе равноправного участия государств в управлении данной сетью и недопущению установления иностранного контроля над ее национальными сегментами;

4) принятию политико-дипломатических и иных мер, направленных на противодействие политике недружественных государств по милитаризации глобального информационного пространства, по использованию информационно-коммуникационных технологий для вмешательства во внутренние дела государств и в военных целях, а также по ограничению доступа других государств к передовым информационно-коммуникационным технологиям и усилению их технологической зависимости.”[82]

Рост значимости информационной безопасности показателен на примере Стратегий национальной безопасности РФ.

В стратегии национальной безопасности РФ от 2015 г. информационная безопасность встречается, как одна из угроз, однако она выступает как одна из многих в ряду других.[83]

[82] Указ Президента Российской Федерации от 31 марта 2023 года № 229 "Об утверждении Концепции внешней политики Российской Федерации". [Электронный ресурс]// Официальные сетевые ресурсы Президента Российской Федерации. Режим доступа: http://kremlin.ru/events/president/news/70811 (Дата обращения 16.04.2023)

[83] Указ Президента РФ от 31.12.2015 N 683 "О Стратегии национальной безопасности Российской Федерации" // RG.RU. URL: https://rg.ru/documents/2015/12/31/nac-bezopasnost-site-dok.html (Дата обращения 01.03.2023)

В Стратегии национальной безопасности от 2021 г. информационная безопасность выделена в подраздел в рамках главы “Обеспечение национальной безопасности”.

В ней обозначена угроза вмешательства во внутренние дела государства с помощью информационно-коммуникационных технологий, дестабилизация общественно-политической ситуации, выведение из строя объектов инфраструктуры, а также стремление транснациональных корпораций занять монопольное положение в сети “Интернет”. Кроме того упомянуты “информационно-психологические диверсии”, которые угрожают “культурному суверенитету России” [84]

Понятие культурный суверенитет в российском правовом поле было закреплено в Основах государственной культурной политики. Таковым считается “Совокупность социально-культурных факторов, позволяющих народу и государству формировать свою идентичность, избегать социально-психологической и культурной зависимости от внешнего влияния, быть защищенными от деструктивного идеологического и информационного воздействия, сохранять историческую память, придерживаться традиционных российских духовно-нравственных ценностей.” [85]

Замечу, что в стратегии не указаны конкретные “транснациональные корпорации”. Однако таковыми можно считать такие корпорации как Google, Meta, Twitter. Себекин считает, что суть конфликта лежит в неприятии западно-либеральных ценностей, хранение данных и распространение информации. Исследователь также замечает, что в ответ на злонамеренное использование ИКТ возможны применение асимметричных мер, т.е. любых,

[84] Указ Президента Российской Федерации от 02.07.2021 г. № 400 “О Стратегии национальной безопасности Российской Федерации” // Официальные сетевые ресурсы Президента России. URL: http://www.kremlin.ru/acts/bank/47046 (Дата обращения 07.03.2023)

[85] Указ Президента РФ от 25.01.2023 N 35 "О внесении изменений в Основы государственной культурной политики, утвержденные Указом Президента Российской Федерации от 24 декабря 2014 г. N 808" // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_438209/ (Дата обращения 12.03.2023)

вплоть до военных.[86] Позже этот принцип распространяется и на “Концепцию внешней политики РФ 2023 г.”

Ни в одном документе стратегического планирования, в том числе, касающихся вопросов информационной безопасности ни разу не использовалась приставка “кибер-”. Можно сделать вывод о том, что с точки зрения российской государственности информационная безопасность это не техническое понятие, но политическое. Оно включает в себя, помимо проблем компьютерной безопасности и хакерства, такие разные по своему содержанию проблемы как сохранение “культурного суверенитета”, противодействие вмешательству во внутренние дела, монополизация интернет-пространства со стороны корпораций.

Глава 2. Деятельность РФ по обеспечению международной информационной безопасности

2.1. Деятельность Российской дипломатии в ООН

Именно Российская Федерация стала первым инициатором обсуждения международной информационной безопасности в ООН. В 1998 г. был предложен проект резолюции “ «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»” . 23 декабря 1999 г. консенсусом Генеральной Ассамблеей ООН была принята резолюция A/RES/54/49 “Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности”

[86] Себекин С.А. Как Россия будет защищаться от информационных угроз. / С.А. Себекин // РСМД. Режим доступа : https://russiancouncil.ru/blogs/s-sebekin/kak-rossiya-budet-zashchishchatsya-ot-informatsionnykh-ugroz/?sphrase_id=84549522 (Дата обращения 06.03.2023)

Резолюция призывала начать процесс выработку общих понятий информационной безопасности, а также начать обсуждение выработки международных принципов. [87]

В ответном письме генеральному секретарю Российская дипломатия, на ряду с определением ключевых терминов выдвинуло несколько принципов международной информационной безопасности:

Принцип I о равенстве государств в вопросах защиты своего информационного поля, уважение суверенитета государств

Принцип II об ограничении разработки и использовании сред воздействия и нанесении ущерба другим государствам, в том числе распространение информации, противоречащей законодательству других стран, а также психологическое воздействие

Принцип III о формирование международной-правовой основы в рамках ООН

Принцип IV Ответственность акторов зя деятельность в информационном пространстве

Принцип V Мирное урегулирование споров. [88]

Изначальные предложения Российской дипломатии были раскритикованы позицией США и Великобританией. Речь касалась угрозе военного применения ИКТ и запрещения таковых технологий, сопоставимости воздействия оружия массового уничтожения и информационного оружия. [89]

Резолюция была принята без голосования 20го ноября и 2000 г., 19го ноября 2001 г., 22 ноября 2002 г. и 8 декабря 2003 г. При этом в новой версии резолюции прописана идея исследования концепций международной

---

[87]Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности [Электронный ресурс]: резолюция Генер. Ассамблеи Орг. Объедин. Наций 54/49 от 23 декабря 1999. A/RES/54/49 // URL: https://ifap.ru/ofdocs/un/5449.pdf. (Дата обращения 04.03.2023)

[88] Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Доклад Генерального секретаря [Электронный ресурс] 10 июля 2010. A/55/140. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/535/04/PDF/N0053504.pdf?OpenElement (Дата обращения: 04.03.2023)

[89] Ромашкина Н.П. Проблема международной информационной безопасности в ООН. / Н.П. Ромашкина // Мировая экономика и международные отношения — 2020 — т. 64, № 12 — с. 25-32

информационной безопасности, для чего требуется в 2004 г. созвать правительственных экспертов. [90]

С начала нулевых центральной проблемой выработки режима международной информационной безопасности оказалось проблема понимания терминов. В 2004 г. была создана первая Группа правительственных экспертов ООН (ГПЭ). В группу вошли представители 15 стран: Беларуси, Малайзии, Мали, Мексики, Республики Корея, России, США, Франции, ЮАР. Председателем группы был избран российский дипломат А.В. Крутских - в 2004 г. заместитель директора Департамента по вопросам безопасности и разоружения МИД России, ныне директор Департамента международной информационной безопасности МИД России.

Однако сторонам не удалось достигнуть общего консенсуса - представитель США не поддержал итоговый текст документа. На лицо оказался конфликт дискурсов, эксперт из США предложил использовать термин кибербезопасность, т.е. сугубо технический термин.[91]

Сергей Бойко - Начальник департамента проблем безопасности в информационной сфере аппарата Совета безопасности Российской Федерации, назвал неудачу первой работы ГПЭ фальстартом, но подчеркнул важность начала диалога по такой сложной проблемы. [92]

По мнению Хели Тийрма-Клаар причиной неудачи первой группы являлось то, что период до 2007 года характеризовался низким уровнем осведомленности о киберугрозах среди руководителей высшего звена, дипломатов и военных. Только в 2007 году широкая общественность узнала, что киберпространство стало источником стратегического риска, способного дестабилизировать ситуацию в стране и вызвать масштабные политические и

---

[90] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. м [Электронный ресурс]: резолюция Генер. Ассамблеи Орг. Объедин. Наций 57/53 от 30 декабря 2002 г. A/RES/57/53 // URL: https://ifap.ru/ofdocs/un/5753.pdf (Дата обращения 04.03.2023)

[91] Ромашкина Н.П. Проблема международной информационной безопасности в ООН./ Н.П. Ромашкина// Мировая экономика и международные отношения — 2020 — т. 64, № 12 — с. 25-32

[92]Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее / С.М. Бойко // Международная жизнь. — 2016 — № 8. URL: https://interaffairs.ru/jauthor/material/1718 (Дата обращения 13.03.2023)

.

экономические потрясения. Эстония стала жертвой первой публично известной кибер-операции. Никогда ранее масштабные кибератаки не использовались для "наказания" страны за действия, противоречащие внешнеполитическим интересам другой страны. Это событие вывело кибербезопасность на первый план для высокопоставленных лиц, принимающих решения в области внешней политики и политики безопасности.[93]

Судя по разнообразию и объему различных атак, вполне вероятно, что они были совершены множеством различных лиц. Единственный человек, осужденный за участие в атаках, был признан ответственным за незначительную часть атак, а дальнейшее расследование застопорилось из-за отсутствия сотрудничества со стороны Российских властей. Многие из обнаруженных атак были подробно описаны на различных русскоязычных форумах и сайтах, которые были легко доступны для тех, кто был заинтересован в поиске способа участия в атаках. Большинство этих инструкций были чрезвычайно просты в исполнении, что делало предварительный опыт злоумышленников неважным. Российское правительство последовательно отрицает свою прямую причастность к кибератакам, поразившим Эстонию весной 2007 года. По мнению Рейна Отиса это утверждение соответствует действительности. Примечательно, однако, что нет никаких доказательств и того, что российское правительство предприняло меры по смягчению ситуации.[94]

8 декабря 2005 г. снова была принята Российская резолюции, однако на этот раз США не поддержали проект резолюции. В ней также призывалось созвать ГПЭ в 2009 г. с теми же целями, что и раньше.[95]

---

[93] Tiirmaa-Klaar H. The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body. / H.Tiirmaa-Klaar // Hague Centre for Strategic Studies — 2021. - P. 3-14. URL: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf (Дата обращения 01.04.2023)

[94] Ottis R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. / R. Ottis // Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Режим доступа: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (Дата обращения 02.04.2023)

[95] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. м [Электронный ресурс]: резолюция Генер. Ассамблеи Орг. Объедин. Наций 60/45 от 8 декабря 2005 г. A/RES/60/45 // URL:

С 2005 по 2008 гг. РФ регулярно предлагала новые резолюции и все они неизменно отвергались со стороны США. Но Российская дипломатия сумела присоединить к проекту резолюции коспонсоров - Армения, Беларусь, Казахстан, Китай, Кыргызстан, Мьянма, Никарагуа, Таджикистан, Узбекистан. [96]

Работа ГПЭ в 2009 оказалась более продуктивной. Это связывают с приходом на пост Президента США демократа Барака Обамы,[97] а также быстрым развитием ИКТ. Она завершилась консенсусом, который предполагал несколько пунктов:

1. реализация угроз в сфере ИКТ наносят урон экономике, национальной и международной безопасности.
2. Были признана особенности технологии ИКТ , а именно их широкая доступность, безнаказанность исполнителей угроз.
3. ИКТ могут быть использованы для подрывной деятельности со стороны как негосударственных (преступные элементы и террористы), так и государственных субъектов
4. Постоянно растущий масштаб и изощренность преступной деятельности
5. Террористы будут использовать ИКТ для нападения
6. Государства разрабатывают ИКТ для ведений войны и разведки.
7. Существуют физические лица и организации, которые осуществляют посреднические функции в осуществлении подрывной деятельности
8. Постоянно растущее количество уязвимых мест в критической инфраструктуре
9. Система поставок ИКТ, а также включение в продукцию вредоносных функций может сказаться на национальной безопасности

---

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/32/PDF/N0549032.pdf?OpenElement (Дата обращения 06.03.2023)

[96] Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее / С.М. Бойко // Международная жизнь. — 2016 — № 8. URL: https://interaffairs.ru/jauthor/material/1718 (Дата обращения 13.03.2023)

[97] Ромашкина Н.П. Проблема международной информационной безопасности в ООН. / Н.П. Ромашкина // Мировая экономика и международные отношения — 2020 — т. 64, № 12 — с. 25-32

10. Различия в оснащенности ИКТ, законодательной практике мешает созданию безопасной информационной среды.[98]

Можно назвать успехом Российской дипломатии тот факт, что в тексте документа используется термин как информационная безопасность, так и кибербезопасность. А также наличие рекомендаций, которые предлагали продолжение диалога, потребность в выработке общей терминологии, укрепление доверия и уменьшение рисков. [99]

В 2011 г. году Россия вместе с Китаем, Таджикистаном и Узбекистаном представила концепцию “Правила поведения в области обеспечения международной информационной безопасности”

Эта концепция предполагает:

1. “Уважение суверенитета, территориальной целостности и политической независимости всех государств, уважение прав и основных свобод человека, а также уважение многообразия истории, культуры и социального устройства всех стран
2. Отказ от использования ИКТ во враждебных целях
3. Сотрудничать в борьбе с киберпреступностью и кибертерроризмом
4. Независимый контроль на сферой ИКТ
5. Подтверждать права и обязанности каждого государства, в соответствии с надлежащими нормами и правилами, в отношении законной защиты своего информационного пространства и критической информационной инфраструктуры от ущерба в результате угроз, вмешательства, атак и актов агрессии
6. Уважать права и свободы в информационном пространстве в соответствии с национальным законодательством
7. Создание международного механизма управления Интернетом

---

[98]Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности [Электронный ресурс]: 30 июля 2010. A/65/201. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/59/PDF/N1046959.pdf?OpenElement (Дата обращения 08.03.2023)

[99] Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее / С.М. Бойко // Международная жизнь. — 2016 — № 8. URL: https://interaffairs.ru/jauthor/material/1718 (Дата обращения 13.03.2023)

8. Способствовать углублению осознания всеми элементами обществ

9. Содействовать развивающимся странам в наращивании их возможностей в сфере информационной безопасности и в ликвидации цифрового разрыва

10. Укреплять двустороннее, региональное и международное сотрудничество, способствовать работе ООН

11. Любой спор должен с помощью процедур мирного урегулирования.”[100]

С самого начала переговорного процесса в центре дискуссии оказался вопрос применения международного права в сфере ИКТ. Западные правительства всегда подчеркивали применимость существующего международного права. Ожидалось, что государства разработают правовые нормы, кодифицированные этими существующими сводами законов, и что это окажет огромное стабилизирующее воздействие на киберпространство.

Однако предложенная в 2011 г. концепция предусматривает создание специального инструмента ООН. В этом контексте западные правительства опасаются, что юридически обязывающий документ будет использован авторитарными странами для контроля интернета. [101]

С 2012 по 2013 гг. заседала третья по счёту ГПЭ. На этот раз председателем группы стал австралийский дипломат Д.Стоукс. Результатом работы группы стала привязка нормов МИБ к международному праву.[102]

Последняя версия отчета включала предложения по стандартам, правилам и этическим принципам ответственного поведения государств. В нем также содержатся рекомендации по мерам укрепления доверия и обмена информацией, а также предложения по расширению возможностей. Примечательно, что в докладе вводится понятие о том, что государства

---

[100] Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 года на имя Генерального секретаря [Электронный ресурс]: 14 сентября 2011. A/66/359. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement

[101] Tiirmaa-Klaar H. The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body. / H.Tiirmaa-Klaar // Hague Centre for Strategic Studies — 2021. - P. 3-14. URL: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf (Дата обращения 01.04.2023)

[102] Ромашкина Н.П. Проблема международной информационной безопасности в ООН. / Н.П. Ромашкина // Мировая экономика и международные отношения — 2020 — т. 64, № 12 — с. 25-32

обязаны выполнять свои международные обязательства в отношении приписываемых им международно-противоправных действий. Государства должны воздерживаться от использования посредников для участия в такой международно-противоправной деятельности. Более того, государства должны прилагать усилия для предотвращения незаконного использования негосударственными субъектами информационно-коммуникационных технологий (ИКТ) на своей территории. [103]

Сильнейшие мировые державы согласились, что на киберпространство должны распространяться нормы Устава ООН, международного права и принципа государственного суверенитета. Таким образом, этот документ заключает киберпространство и связанные с ним киберугрозы в рамки международных отношений. По сути, он подтверждает, что США и их партнеры отказываются рассматривать киберпространство как общий ресурс всего человечества, требующий пересмотра существующих норм в отношениях между суверенными государствами и принятия совершенно новых правовых решений.[104] При этом ни термин “киберпространство”, ни “информационное пространство” не были использованы, по причине неприятия терминов со стороны РФ и США.[105]

В следующем, 2014 г., состоялся четвертый созыв ГПЭ, который также привел к созданию в 2015 г. отчета о его работе. Главными достижениями группы являются принципы государственного суверенитета, разрешения споров мирными средствами и невмешательства во внутренние дела других государств распространяются и на киберпространство. Признание того, что государства должны соблюдать свои обязательства по международному праву по соблюдению и защите прав человека и основных свобод. Согласие с тем,

---

[103] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Электронный ресурс]: резолюция, принятая Генер. Ассамблеей Орг. Объедин. Наций 68/98* от 24 июня 2013 г. A/68/98*. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf?OpenElement (Дата обращения 9.04.2023)

[104] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[105] Stadnik I. What Is an International Cybersecurity Regime and How We Can Achieve It? / I. Stadnik // Masaryk University Journal of Law and Technology. - 2017 - 11(1):129 -P. 129 - 154

что ООН должна играть ведущую роль в выработке общего понимания применения международного права и норм, правил и принципов ответственного поведения государств.[106]

Идеи российской дипломатии были отражены в новом документе такими идеями как сотрудничество с целью предотвращения конфликтов в киберпространстве, обладании государствами юрисдикции над информационно-коммуникационной инфраструктурой, расположенной на их территориях, государственный суверенитет, суверенное равенство, разрешение споров мирными средствами и невмешательство во внутренние дела других государств, государства не должны использовать посредников для совершения международно-противоправных деяний с применением ИКТ и должны обеспечивать, чтобы их территория не служила для совершения таких деяний, обвинения в организации и совершении противоправных деяний в сфере ИКТ, выдвигаемые против государств, должны быть обоснованными и доказанными.[107]

Кроме того в 2015 г. РФ с партнёрами по ШОС представила новую концепцию правил поведения в области обеспечения международной информационной безопасности. Обновленный проект включает в себя изменения первоначального текста, такие как расширенные определения, уточнение понятий, а также обновления, отражающие технологический прогресс и новые вызовы в области информационной безопасности.

Некоторые из ключевых изменений в обновленном проекте включают: Добавление преамбулы, в которой подчеркивается важность кодекса поведения для укрепления международного мира и безопасности в киберпространстве.

---

[106] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Электронный ресурс]: резолюция, принятая Генер. Ассамблеей Орг. Объедин. Наций 70/174 от 22 июля 2015 г. A/70/174. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (Дата обращения 09.03.2023)

[107] Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее / С.М. Бойко // Международная жизнь. — 2016 — № 8. URL: https://interaffairs.ru/jauthor/material/1718 (Дата обращения 13.03.2023)

Включение новых принципов, касающихся защиты критической инфраструктуры, повышения осведомленности о кибербезопасности и важности соблюдения прав человека и основных свобод в киберпространстве. Расширение сферы действия кодекса поведения за счет включения негосударственных субъектов, таких как организации частного сектора и отдельные лица.[108]

Как и в 2011 г. западные правительства опасались, что концепция будет способствовать дальнейшему контролю за контентом, изменениям в управлении Интернетом и в основном будет использоваться для легитимации цензуры авторитарными режимами, они решительно выступили против появления юридически обязательного документа во время обсуждения в Первом комитете ООН.[109]

ГПЭ по МИБ пятого созыва начал свою работу в 2016 г. и закончил работу в 2017 г.. Впервые с 2004 г. стороны не пришли к консенсусу. Проект итогового доклада отказались подписать РФ, страны БРИКС и СНГ. В 2016 г. США обвинили РФ в вмешательство в выборы Президента США, Ключевой проблемой оказалось то, что НАТО признала о возможности реагирования на кибератаку всеми возможными средствами, в том числе военными. РФ, страны БРИКС и СНГ не поддержали проект , предлагаемый США. [110]

Кроме того РФ Китай, Куба и ряд других стран возражали против включения в доклад термина «международное гуманитарное право». “Мы не можем принять такое утверждение, так как оно узаконило бы сценарий войны и военных действий в контексте ИКТ.” - заявил представитель Кубы. [111]

---

[108] Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря. [Электронный ресурс] резолюция, принятая Генер. Ассамблеей Орг. Объедин. Наций 69/723 от 13 января 2015 г. A/69/723 . URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/04/PDF/N1501404.pdf?OpenElement (Дата обращения 10.03.2023)

[109] Tiirmaa-Klaar H. The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body. / H.Tiirmaa-Klaar // Hague Centre for Strategic Studies — 2021. - P. 3-14. URL: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf (Дата обращения 01.04.2023)

[110] Ромашкина Н.П. Проблема международной информационной безопасности в ООН. / Н.П. Ромашкина // Мировая экономика и международные отношения — 2020 — т. 64, № 12 — с. 25-32

[111] Schmitt M. The Sixth United Nations GGE and International Law in Cyberspace. / M. Schmitt // Just Security. URL: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ (Дата обращения 25.03.2023)

Именно с этого момента в рамках ООН начинают работать две параллельные структуры - Рабочая Группа Открытого Состава (РГОС) и Группа Правительственных Экспертов (ГПЭ), РФ входит в обе структуры.

РГОС была создана по инициативе РФ, которая настаивала на создание более инклюзивной структуры - к работе РГОС были приглашены все все государства, а также негосударственные акторы.

ГПЭ основывается на проекте США “Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности” от 22 декабря 2018 г., РГОС основывается на проекте РФ “Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности” от 5 декабря 2018 г.

ГПЭ включается в себя 25 членов, РГОС 193. ГПЭ допускает в своей работе только правительственных экспертов, РГОС приглашает в свою работу другие заинтересованные стороны, при главенствующей роли государств. И ГПЭ и РГОС обладает мандатом на выработку норм, правил и принципов поведения государств, мер укрепления доверия, мер в области наращивания потенциала, применимость международного права к киберпространству, но только РГОС обладает мандатом на выработку существующих и потенциальных угроз, формирование регулярного институционального диалога под эгидой ООН, актуальных международных концепций в сфере глобальной безопасности IT-систем. [112]

Оценка разделения переговорного процесса на 2 формата неоднозначна. РФ и США обвинили друг друга в расколе. Россия пыталась позиционировать себя как сторонник демократического участия и инклюзивности, выступая за создание РГОС. Российский представитель раскритиковал предложение США о создании новой Группы правительственных экспертов (ГПЭ) как "эксклюзивного клуба", который не учитывает мнения всех членов ООН. Во время обсуждения предложения Россия выборочно умолчала о своей роли в блокировании предыдущего консенсусного доклада. Российское

[112] Международная информационная безопасность: подходы России / А.В.Крутских, Е.А.Зиновьева, В.И.Булва, М.Б.Алборова, Ю.А.Юдина; под ред. А.В.Крутских, Е.С.Зиновьева. — Москва, 2021. — 48 с

предложение подверглось критике со стороны США и их союзников за неверное описание и выборочное цитирование формулировок из предыдущих докладов ГПЭ. [113]

Однако полного размежевания не произошло. РФ всё ещё участвует в работе ГПЭ, а США в работе РГОС. Кроме того существует неформальный принцип: председателем РГОС может стать только участник ГПЭ. [114]

В марте 2021 г. завершилась работа РГОС первого созыва. В итоговом докладе содержались указания на увеличение риска использования ИКТ в межгосударственных конфликтах, опасность использования ИКТ в атаках на критическую инфраструктуру, в которую входят медицинские учреждения, финансовые структуры, энергетика, водоснабжение, транспортные и санитарные службы. Кроме итогового доклада принят доклад председателя Юрга Глаубера, в котором содержались те идеи, по которым сторонам не удалось договориться. В них входят: формирование регулярного институционального диалога, принятие юридически обязывающего документа, выработке механизмов атрибуции кибератак, применимость международного гуманитарного права в ИКТ.[115]

Доклад подтверждает достигнутые ранее договоренности в рамках ГПЭ, однако не привнес ничего нового. Такой результат является следствием резкого увеличения количества участников, сторонам пришлось заново приходить к общему знаменателю, а действительно неразрешенные вопросы вынести на следующие заседания.[116]

Параллельно с заседанием РГОС закончилась работа и ГПЭ шестого созыва. В его итоговом докладе зафиксировано, что международное гуманитарное

---

[113] The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. URL: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased (Дата обращения 16.04.2023)

[114] Kaspar L. Cyber norms in nyc: takeaways from the OEWG meeting and UNIDIR cyber stability conference./ L. Kaspar, H. Sheetal.// Global Partners Digital. URL: https://www.gp-digital.org/cyber-norms-in-nyc-takeaways-from-the-oewg-meeting-and-unidir-cyber-stability-conference/ (Дата обращения 17.04.2023)

[115] Международная информационная безопасность: подходы России / А.В.Крутских, Е.А.Зиновьева, В.И.Булва, М.Б.Алборова, Ю.А.Юдина; под ред. А.В.Крутских, Е.С.Зиновьева. — Москва, 2021. — 48 с

[116] Шакиров О.И. Широкий киберконсенсус. / О.И Шакиров // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/shirokiy-kiberkonsensus/ (Дата обращения 27.03.2023)

право может быть применимо к ИКТ в случае вооруженного конфликта. ГПЭ с осторожностью относилась к тому, чтобы выйти за рамки достижений предыдущих ГПЭ в области международного права. Например, остается неурегулированным спор о том, является ли суверенитет основной нормой международного права или, как предложил генеральный прокурор Великобритании в 2018 году, всего лишь принципом, который сам по себе не имеет обязательной силы. В докладе несколько раз упоминается суверенитет, в том числе содержится требование уважения суверенитета других государств, но ни разу прямо не охарактеризовано его как обязательное правило. [117]

В декабре 2021 года Австралия и Канада отправили письмо от более чем 140 представителей мультистейкхолдерного сообщества, в котором предлагалось расширить возможности для участия негосударственных акторов, например, позволить организациям без консультативного статуса в ООН участвовать и обеспечить прозрачность возражений государств-членов по поводу аккредитации. Такой подход вызвал критикой российской стороны. Резкое увеличение количества негосударственных переговорщиков приведет к тому, что “государства просто не будут иметь достаточного времени для выступлений”[118]

В результате сложилась практика неформальных консультаций, участвовать в которых смогли и не аккредитованные участники. Со стороны РФ таковыми участниками были Центр международной информационной безопасности МГИМО, НИУ ВШЭ, Национальная ассоциация международной информационной безопасности, Школа международной информационной

[117] Schmitt M. The Sixth United Nations GGE and International Law in Cyberspace. / M. Schmitt // Just Security. URL: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ (Дата обращения 25.03.2023)

[118] Шакиров О. И. Киберпереговоры с участием всех заинтересованных сторон./ О.И Шакиров// РСМД. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/kiberperegovory-s-uchastiem-vsekh-zainteresovannykh-storon/?sphrase_id=96227596 (Дата обращения 09.03.2023)

безопасности Дипломатической академии, Центр информационной безопасности университета Иннополис, Dr.Web., РСМД[119]

Россия выступает за практику неформального участия негосударственных представителей в РГОС. При этом серьезные коррективы в работу РГОС внесла военно-политическая обстановка в мире, так в июле 2022 г. на очередной сессии РГОС некоторые западные IT-компании и неправительственные организации не были допущены к участию в сессии из-за блокировки Россией процесса их аккредитации, а также были ограничены некоторые структуры, связанные с Российской Федерацией, из-за вето со стороны Украины. Кроме того, главе российской делегации на РГОС Андрею Крутских было отказано в визе США.[120]

К апрелю 2022 был достигнут консенсус:

“Обязательство государств-членов взаимодействовать с заинтересованными сторонами на систематической, устойчивой и предметной основе.

Возможность участия в работе РГОС соответствующих неправительственных организаций, имеющих статус ЭКОСОС, а также возможность участия других заинтересованных неправительственных организаций на основе отсутствия возражений в качестве наблюдателей.

Председатель также подтвердил, что РГОС будет продолжать организовывать неофициальные консультативные встречи с заинтересованными сторонами в межсессионный период, что позволит более широкому кругу неаккредитованных организаций также внести свой вклад”[121]

В 2021 же году был опубликован новая Концепция Конвенции ООН об обеспечении международной информационной безопасности. Именно эту концепцию РФ продвигает в рамках работы РГОС. В ней указано 15

---

[119] Шакиров О. И. Киберпереговоры с участием всех заинтересованных сторон./ О.И Шакиров// РСМД. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/kiberperegovory-s-uchastiem-vsekh-zaintereso vannykh-storon/?sphrase_id=96227596 (Дата обращения 09.03.2023)

[120] В Нью-Йорке со скандалом открылась сессия РГОС по кибербезопасности. // Московский комсомолец. URL: https://www.mk.ru/politics/2022/07/26/v-nyuyorke-so-skandalom-otkrylas-sessiya-rgos-po-kiberbezopasnosti.html (Дата обращения 15.11.2022)

[121] OEWG Agrees on Modalities for Multistakeholder Participation After Silent Procedure. URL: https://letstalkcyber.org/news/oewg-agrees-on-modalities-for-multistakeholder-participation-after-silent-procedure (Дата обращения 17.04.2023)

основных угроз МИБ, 14 принципов обеспечения МИБ, 14 мер предотвращения конфликтов в информационном пространстве. Отдельно выделены меры противодействия использованию информационного пространства в террористических и преступных целях, а также меры укрепления доверия[122]

По мнению В. Вебера эта концепция является проблематичной. Автор утверждает, что российское предложение, которое подчеркивает государственный суверенитет и контроль над потоком информации, является расплывчатым и может быть использовано для оправдания цензуры и государственного контроля над интернетом. “В нем упоминаются права человека, в первую очередь право на неприкосновенность частной жизни. Все остальные права, такие как свобода слова и собраний, не имеют приоритета.”[123]

Россия также является инициатором другого переговорного формата. Резолюция, принятая Генеральной Ассамблеей 27 декабря 2019 года. “Противодействие использованию информационно коммуникационных технологий в преступных целях” призывала “Учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, в полной мере учитывая существующие международные документы и предпринимаемые на национальном, региональном и международном уровнях усилия по борьбе с использованием информационно-коммуникационных технологий в преступных целях, в частности работу и итоги работы Межправительственной группы экспертов

[122] Концепция Конвенции ООН об обеспечении международной информационной безопасности. [Электронный ресурс] // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document112/ (Дата обращения 16.03.2023)

[123] Weber V. The Dangers of a New Russian Proposal for a UN Convention on International Information Security/ V. Weber // Council on Foreign Relations. URL: https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-interna ional-information-security (Дата обращения 10.04.2023)

открытого состава для проведения всестороннего исследования проблемы киберпреступности”[124]

В рамках данного комитета РФ предложила свою концепцию “Конвенции Организации Объединенных Наций о противодействии использованию информационно коммуникационных технологий в преступных целях”

В первой главе российского предложения по Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях изложены цели, сфера применения и определения предлагаемой конвенции.

В начале главы сформулированы цели конвенции, которые включают укрепление международного сотрудничества по предотвращению и борьбе с преступным использованием ИКТ и содействие защите прав человека и основных свобод.

Далее определяется сфера применения конвенции, которая охватывает широкий спектр преступной деятельности, совершаемой с использованием ИКТ, включая мошенничество, кражи, торговлю запрещенными товарами и террористическую деятельность. Предлагаемая конвенция также призвана решить проблему транснациональной организованной преступности и использования ею ИКТ.

В главе также приводятся определения ключевых терминов, используемых во всем документе. Например, "информационно-коммуникационные технологии" определяются как "совокупность технических средств и методов, позволяющих обрабатывать, хранить и передавать цифровые данные и информацию". Другие термины, определенные в главе, включают "преступное использование ИКТ", "компьютерная система" и "жертва".

Механизмами выполнения конвенции являются:

---

[124] Противодействие использованию информационно коммуникационных технологий в преступных целях. [Электронный ресурс] резолюция, принятая Генер. Ассамблеей Орг. Объедин. Наций 74/247 от 20 января 2020 г. A/RES/74/247. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/31/PDF/N1944031.pdf?OpenElement (Дата обращения 10.03.2023)

Национальные меры: Каждое государство-участник должно принять необходимые меры для реализации положений Конвенции в своих национальных правовых системах, включая принятие необходимого законодательства.

Международное сотрудничество: Конвенция призывает к международному сотрудничеству между государствами-участниками в таких областях, как обмен информацией и передовым опытом, совместные расследования и судебные преследования, а также взаимная правовая помощь.

Предполагается создание Конференции государств-участников Конвенции, которая принимает все необходимые правила и процедуры

Конвенция учреждает Международную техническую комиссию для оказания помощи государствам-участникам в реализации ее положений, в том числе путем предоставления обучения, консультаций экспертов и финансовой поддержки.

Конвенция также предусматривает создание Секретариата для обеспечения административной и логистической поддержки Конференции сторон и оказания помощи государствам-участникам в реализации Конвенции.[125]

В целом, хоть и ГПЭ и РГОС и Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии ИКТ в преступных целях занимаются вопросами связанными с информационной безопасностью, Специальный комитет фокусируется на преступной деятельности, а ГПЭ и РГОС - на ответственном поведении государств в киберпространстве в контексте международной безопасности.

При этом деятельность российской дипломатия во всех трёх форматах сильно не различается, а действует по одним и тем же принципам. “Россия в тесной координации с единомышленниками продолжит работу по разработке эффективного всеобъемлющего документа с опорой на национальное законодательство и принципы Устава ООН в ходе очередной сессии (Вена,

[125] Конвенция Организации Объединенных Наций о противодействии использованию информационно коммуникационных технологий в преступных целях. Проект 29.06.2021.// Undocs.org. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (Дата обращения 25.03.2023)

11-21 апреля 2023 года), будет добиваться юридически обязывающего характера соглашения”[126]

Суммируя работу и прогресс ГПЭ, как главного переговорного процесса по проблематике МИБ эстонский “посол по вопросам кибер дипломатии” Хели Тирма-Клаар говорит, что “В самом общем виде можно сделать вывод, что ГПЭ достигали консенсуса, когда проходили в благоприятном геополитическом контексте, когда напряженность между ведущими державами была относительно низкой или существовала общая заинтересованность в достижении соглашения. Напряженность между ведущими державами была относительно низкой, или же существовала общая заинтересованность в достижении соглашения. Другие элементы, играющие роль в успешном исходе переговоров, состоят из квалификации председателей, ожиданий членов группы, региональная динамика, эффективные усилия по организации обратных каналов и растущая профессионализация членов ГПЭ.”[127]

В целом Российская дипломатия по итогам более чем 20 летней работы в рамках ООН по созданию режима МИБ задала тон обсуждения и внесла вклад в развитие правовых норм. [128]

2.2. Деятельность Российской дипломатии в рамках ШОС, СНГ, ОДКБ, БРИКС, АСЕАН

[126] О четвертой сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности. // Министерство иностранных дел Российской Федерации. URL: https://mid.ru/ru/foreign_policy/news/1849347/ (Дата обращения 26.03.2023)

[127] Tiirmaa-Klaar H. The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body. / H.Tiirmaa-Klaar // Hague Centre for Strategic Studies — 2021. - P. 3-14. URL: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf (Дата обращения 01.04.2023)

[128] Дубень А. К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению / А. К. Дубень // Международное право и международные организации. – 2022. – № 1. – С. 24-33.

Существует вероятность того, что роль ООН по вопросу выработки режима информационной безопасности будет снижаться из-за невозможности основных сторон (США, РФ, КНР) договорится в связи с политическими осложнениями.[129] В концепции внешней политики РФ 2023 г. из национальных интересов страны были убраны положения о верховенстве ООН.[130] В этой связи важным направлением деятельности Российской дипломатии по созданию режима международной информационной безопасности является сотрудничество в региональных и межгосударственных объединений.

15 июня 2006 г. принято Заявление глав государств-членов ШОС по МИБ. В этом заявлении выражена озабоченность использованию ИКТ в преступных, террористических и военно-политических целях.

“Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности” было заключено в 2009.

Во второй статье Соглашения определены следующие угрозы:

1. “ разработка и использование информационного оружия и подготовка к ведению информационной войны;
2. информационный терроризм;
3. информационная преступность;
4. использование доминирующего положения в киберпространстве в ущерб интересам и безопасности других государств;
5. распространение информации, наносящей вред политическим системам;
6. природные и/или человеческие угрозы безопасному и стабильному функционированию глобальной и национальной информационной инфраструктуры.” [131]

---

[129] Сидорова Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН. / Т.Ю. Сидорова // Сибирский юридический вестник. - 2020 - № 3 (90). - С 103-108.

[130] Указ Президента Российской Федерации от 31 марта 2023 года № 229 "Об утверждении Концепции внешней политики Российской Федерации". // Официальные сетевые ресурсы Президента Российской Федерации. Режим доступа: http://kremlin.ru/events/president/news/70811 (Дата обращения 16.04.2023)

[131] Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. // Электронный фонд

ШОС перенесла свои идеи уважения суверенитета, невмешательства во внутренние дела государств, равенства и взаимного уважения в выполнении международных норм и борьбы против трех зол (т.е. сепаратизма, экстремизма и терроризма) в киберпространство.критикуется модель управления Интернетом, центром которой являются Соединенные Штаты. Определения войны и информационного терроризма в приложениях к документу очень близки к китайско-российским представлениям, неся в то же время влияние многостороннего подхода и взаимного доверия. Кроме того, существует предложение о международном участии в дебатах по кибербезопасности/информационной инфраструктуре. [132]

В 2013 году была создана Совместная рабочая группа по пресечению использования сети Интернет в террористических, сепаратистских и экстремистских целях, в работе которой принимают участие эксперты компетентных органов государств-членов ШОС и представителей Исполнительного комитета Региональной Антитеррористической структуры ШОС. В рамках этой инициативы проводятся меры по предупреждению и пресечению использования или угрозы использования компьютерных сетей в террористических целях, осуществляется обмен информацией о значимых выявленных фактах распространения информации в социальных сетях. Заседания группы проводятся регулярно, в том числе в 2023 г.[133]

Кроме того в рамках ШОС регулярно проводятся учения по противодействию интернет-терроризму. В декабре 2019 г. были проведены учения “Сямэнь - 2019” страны объединения при координации Региональной антитеррористической структуры практически отработали вопросы применения положений нормативно-правовой базы ШОС, регламентирующих совместную деятельность в области противодействия кибертерроризму, сбора и фиксации электронных доказательств, проведения

правовых и нормативно - технических документов. URL: https://docs.cntd.ru/document/902289626 (Дата обращения 07.04.2023)

[132] De Alcantara B.T. SCO and Cybersecurity: Eastern Security Vision for Cyberspace./ de Alcantara B.T. //International Relations and Diplomacy - 2021. Vol. 6. № 10. - P. 549-555

[133] Rakhimov, S. A. International Cooperation within the SCO in the Field of Information Security./ S.A. Rahimov // International Journal of Social Science Research and Review - 2023 - Vol 6. Issue 3 - p. 475-479.

судебных экспертиз и технических исследований, анализа и оценки полученных цифровых данных. В рамках сотрудничества в ШОС был установлен эффективный обмен оперативными данными о распространении террористического и экстремистского контента в Интернете. Был разработан механизм для блокировки такого контента, что привело к удалению или ограничению доступа к более чем 23 тысячам интернет-ресурсов, содержащих материалы террористического и экстремистского характера.[134]
В Самаркандской декларации ШОС от 16 сентября 2022 г. закреплены несколько положений, касающихся международной информационной безопасности, в том числе объявлено о создании Центра Информационной безопасности ШОС в Республике Казахстан. Руководители государств призвали к сотрудничеству в области международной информационной безопасности и подтвердили, что ООН играет центральную роль в борьбе с угрозами в информационном пространстве. Они также поддержали создание безопасного, справедливого и открытого информационного пространства, с уважением к государственному суверенитету и невмешательству.
Государства-члены высказали свою категорическую противодействие милитаризации сферы ИКТ, и поддержали разработку универсальных правил, принципов и норм ответственного поведения государств.
Декларация подчеркнула, что все страны имеют равные права на регулирование интернета, а также суверенное право на управление им в своем национальном сегменте. Кроме того, она призвала к разработке всеобъемлющей международной конвенции по борьбе с использованием ИКТ в преступных целях под эгидой ООН. Государства также призвали к расширению сотрудничества правоохранительных органов для защиты прав человека и борьбы с преступным использованием ИКТ, а также к практическому сотрудничеству в области права и правосудия и криминалистики.[135]

---

[134] Rakhimov, S. A. International Cooperation within the SCO in the Field of Information Security./ S.A. Rahimov // International Journal of Social Science Research and Review - 2023 - Vol 6. Issue 3 - p. 475-479.
[135] Самаркандская декларация Совета глав государств-членов Шанхайской организации сотрудничества : 16 сент. 2022 // Официальные сетевые ресурсы Президента России. URL: http://www.kremlin.ru/supplement/5841

Себекин подчеркивает, что идея недопустимости милитаризации киберпространства, по его мнению это является следствием политической ситуации, которая привела к увеличению количества кибератак.[136]

Дивьян Джиндалу считает, что “В течение последних 20 лет Россия активно развивала партнерские отношения для сотрудничества в киберсфере на двусторонних, многосторонних и региональных платформах с Западом. Однако СВО привела к тому, что сотрудничество с Западом прекратилось. Запад с подозрением относится к дипломатическим усилиям России, рассматривая их как способ отвлечь внимание от необходимости значимого сотрудничества в области создания норм в киберпространстве и борьбы с киберпреступностью.

В связи с этим Россия может искать поддержки у других стран, причем наиболее вероятным кандидатом на более тесное партнерство является Китай. И Россия, и Китай выступают за "киберсуверенитет" и право государств регулировать интернет в своих национальных интересах. Они также обладают необходимыми возможностями кибернаблюдения и могут действовать во фрагментированном киберпространстве, изолированном от глобального интернета”[137]

В рамках БРИКС информационная безопасность начинает занимать важное место с 2011 г. По итогам саммита БРИКС в г. Санья была принята декларация, в которой провозглашалось “Мы выражаем приверженность сотрудничеству в укреплении международной информационной безопасности.”[138]

В 2013 г. Этеквинская декларация БРИКС зафиксировала “Мы признаем исключительно важную позитивную роль, которую играет интернет в мире в плане содействия экономическому, социальному и культурному развитию. Мы считаем важным вносить вклад и участвовать в мирном, безопасном и открытом

---

[136] Себекин С.А. Роль Шанхайской организации сотрудничества и БРИКС в обеспечении международной информационной безопасности в условиях продолжающегося конфликта на Украине / С.А. Себекин // Российско-китайские исследования. — 2022. — Т. 6, № 4. — С. 276–287.

[137] Jindal D. Can India & Russia Resuscitate Cyber Relationship?/ D. Jindal // Modern diplomacy. URL: https://moderndiplomacy.eu/2022/06/08/can-india-russia-resuscitate-cyber-relationship/

[138] Декларация, принятая по итогам саммита БРИКС (г.Санья, о.Хайнань, Китай, 14 апреля 2011 года)// Официальные сетевые ресурсы Президента России. URL: http://www.kremlin.ru/supplement/907 (Дата обращения 05.04.2023)

киберпространстве, и мы подчеркиваем, что безопасность при использовании информационных и коммуникационных технологий (ИКТ) с применением универсально признанных норм, стандартов и практик имеет первостепенную важность."[139] Там же было предложено создать Рабочую группу экспертов по вопросам безопасности в сфере использования ИКТ[140]

Форталезская декларация 2014 еще сильнее показало значимость вопроса МИБ для стран-участниц. Конкретизируется использование опасения об использовании ИКТ террористами, осуждается электронная слежка, а также "Мы будем изучать возможности для сотрудничества в области борьбы с киберпреступлениями и подтверждаем нашу приверженность выработке универсального и имеющего обязательную юридическую силу международно-правового документа в данной области. Мы считаем, что центральная роль в данном вопросе принадлежит Организации Объединенных Наций. Мы согласны с тем, что необходимо сохранять ИКТ, и в частности Интернет, как инструмент мира и развития и не допускать их использования в качестве оружия. Кроме того, мы обязуемся сотрудничать друг с другом в выявлении возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования ИКТ."[141]

Рабочая группа была создана в июне 2015 года в Москве во время председательства России в БРИКС (в соответствии с регламентом группы, председателем является эксперт из государства, которое председательствует в текущем году в БРИКС). В Уфимской декларации, принятой 9 июля 2015 года на VII саммите БРИКС, Рабочей группе были поручены задачи по инициированию сотрудничества в следующих областях:

"Обмен информацией и передовой практикой в вопросах безопасности в сфере использования ИКТ;

---

[139] Этеквинская декларация и Этеквинский план действий // Официальные сетевые ресурсы Президента России. URL:http://www.kremlin.ru/supplement/1430 (Дата обращения 10.04.2023)

[140] Этеквинская декларация и Этеквинский план действий // Официальные сетевые ресурсы Президента России. URL:http://www.kremlin.ru/supplement/1430 (Дата обращения 10.04.2023)

[141] Форталезская Декларация (принята по итогам шестого саммита БРИКС) г.Форталеза, Бразилия, 15 июля 2014 года // Официальный сайт Президента РФ. URL: http://static.kremlin.ru/media/events/files/41d4f1dd6741763252a8.pdf (Дата обращения 04.04.2023)

Эффективная координация мер противодействия киберпреступности;
Выделение уполномоченных по связям в государствах-участниках;
Сотрудничество между странами БРИКС с использованием существующих групп реагирования на компьютерные инциденты в области компьютерной безопасности (CSIRT);
Совместные проекты в области НИОКР;
Укрепление потенциала, Разработка международных норм, принципов и стандартов."[142]

Кроме того впервые странами - участницами БРИКС провозглашалась необходимость создание "Разработки под эгидой ООН универсального юридически обязывающего инструмента по вопросам борьбы с использованием ИКТ в преступных целях"[143]

Именно Россия стала инициатором обсуждения проблем информационной безопасности в рамках БРИКС, РФ планировало подписать всеобъемлющее соглашение ещё в 2015[144], в 2017 Президент РФ В.В. Путин заявил "Предлагаем сообща сформировать соответствующую международно-правовую базу сотрудничества, а в перспективе - разработать и принять универсальные правила ответственного поведения государств в этой области. Важным шагом могло бы стать заключение межправительственного соглашения БРИКС по международной информационной безопасности".[145], однако этого не произошло

В 2016 г. рабочей группой была разработана "Дорожная карта практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ". Она включает в себя следующие меры:

---

[142] Уфимская декларация (Уфа, Российская Федерация, 9 июля 2015 года) // Официальный сайт Президента РФ. URL: http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf (Дата обращения 04.04.2023)

[143] Уфимская декларация (Уфа, Российская Федерация, 9 июля 2015 года) // Официальный сайт Президента РФ. URL: http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf (Дата обращения 04.04.2023)

[144] Муратшина К.Г. К вопросу о сотрудничестве в области информационной безопасности в рамках БРИКС/ К.Г. Мурташина. // Гуманитарное знание и искусственный интеллект: стратегии и инновации : 4-й молодежный конвент УрФУ : материалы международной конференции 26 марта 2020 года. — Екатеринбург : Изд во Урал. ун та, 2020. — С. 614-621.

[145] Путин предложил странам БРИКС заключить соглашение по информационной безопасности.// ТАСС. URL: https://tass.ru/politika/4523253 (Дата обращения 04.04.2023)

“- активизацию обмена подходами к политическим вопросам безопасности в сфере использования ИКТ (оценка событий на международной арене; развитие диалога о нормах, принципах и правилах, обеспечивающих открытую, безопасную, стабильную, доступную и мирную ИКТ-среду в рамках ООН; выработка общей позиции государств - участников БРИКС по ключевым вопросам проблематики; координация позиций на различных международных площадках);

- создание сети сотрудничества между национальными центрами (группами) реагирования на компьютерные инциденты (экстренной готовности к компьютерным инцидентам);

- углубление практического сотрудничества между уполномоченными ведомствами, отвечающими за безопасность в сфере использования ИКТ;

- проведение совместных исследований и разработок;

- создание механизма научного и исследовательского обмена между государствами БРИКС.”[146]

С этого момента прогресс по продвижению идеи о соглашении между странами БРИКС по вопросам МИБ замедлился. По итогам Пекинской Декларации 2022 г. заявлено “Мы подчеркиваем важность формирования нормативно правовых рамок для сотрудничества стран БРИКС по вопросам обеспечения безопасности в сфере использования ИКТ. Мы также признаем необходимость развития практического сотрудничества в рамках БРИКС посредством осуществления «дорожной карты» практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ и в рамках деятельности Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ.”[147]

Поддержку РФ в необходимости заключения договора по МИБ в рамках БРИКС по МИБ оказывает только Индия, другие страны участницы не заинтересованы

[146] Бойко С.М. Проблематика международной информационной безопасности на площадках ШОС и БРИКС / С.М. Бойко // Международная жизнь. URL: https://interaffairs.ru/news/show/21480 (Дата обращения 26.03.2023)
[147] Пекинская декларация XIV саммита БРИКС 23 июня 2022 года. // Официальный сайт Президента РФ. URL: http://special.kremlin.ru/supplement/5819 (Дата обращения 04.04.2023)

в заключении данного рода соглашении, они поддерживают деятельность в рамках ООН, но осторожно относятся к подобным юридически обязывающим соглашениям в рамках БРИКС, концепцию которого пытается продвинуть РФ.[148]

Проблемой также является то, что Бразилия подписала Будапештскую конвенцию по кибербезопасности, которая противоречит интересам РФ, Индии и Китая. В то же время возможное будущее расширение БРИКС за счет Аргентины и Саудовской Аравии может дать идеи заключения общего договора по кибербезопасности новую жизнь.[149]

Хоть и члены и БРИКС и ШОС поддерживают работу РГОС, а также идею привлечения различных стейкхолдеров к обсуждению проблем МИБ, в рамках этих двух объединений не идёт речи о привлечении частного сектора к обсуждению проблем кибербезопасности. [150]

Обсуждение проблем МИБ в рамках СНГ началось в 1996 г. Была принята “Концепция формирования информационного пространства Содружества Независимых Государств” , которая объявляла информационную безопасность одним из интересов Содружества.[151]
В 1999 г. подписана “Концепция информационной безопасности государств – участников Содружества Независимых Государств в военной сфере”. Этот документ определял цели, задачи, принципы обеспечения информационной безопасности, а также определил ряд угроз, к которым отнесли деятельность ряда государств, занимающихся разведывательной деятельностью, ориентация

---

[148] Муратшина К.Г. К вопросу о сотрудничестве в области информационной безопасности в рамках БРИКС/ К.Г. Мурташина. // Гуманитарное знание и искусственный интеллект: стратегии и инновации : 4-й молодежный конвент УрФУ : материалы международной конференции 26 марта 2020 года. — Екатеринбург : Изд во Урал. ун та, 2020. — С. 614-621.
[149] Jindal D. Cyber in BRICS: Agendas & Undercurrents for BRICS Summit 2022 / D. Jindal // Center for air power studies. URL : https://capsindia.org/cyber-in-brics-agendas-undercurrents-for-brics-summit-2022/ (Дата обращения 12.04.2023)
[150] Себекин С. А. Роль частного сектора в процессе построения МИБ на полях ООН, ШОС и БРИКС / С.А. Себекин // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/rol-chastnogo-sektora-v-protsesse-postroeniya-mib-na-polyakh-oon-shos-i-briks/ (Дата обращения 19.04.2023)
[151] Концепция формирования информационного пространства Содружества Независимых Государств // Исполнительный комитет Содружества Независимых Государств. URL: https://cis.minsk.by/page/7548 (Дата обращения 27.03.2023)

на импортное оборудование и программное обеспечение, отсутствие нормативно-правовой базы, возрастание масштаба компьютерной преступности, а также отсутствие единой политики в информационной сфере.[152]

2004 г. - создана Комиссия по информационной безопасности. Задачи новой структуры включают в себя следующее: разработка рекомендаций относительно взаимодействия государств-участников, организация обмена опытом, подготовка предложений по приоритетным направлениям деятельности, в том числе гармонизации национального законодательства, прогнозирование возможных угроз и определение рекомендаций по нейтрализации уже существующих угроз и т.д. [153]

2008 г. - принята Концепция сотрудничества государств участников в сфере обеспечения информационной безопасности. Это концепция определила основные термины, угрозы и методы выработки режима МИБ. К угрозам в данной концепции в числе прочих традиционных угроз отнесли "проведение третьими странами в информационном пространстве мероприятий, направленных на дестабилизацию социально политической обстановки, обострение международной конкуренции за обладание стратегически важной информацией и стремление ряда стран к доминированию в мировом информационном пространстве, зависимость от третьих стран-производителей программных и аппаратных средств при создании и развитии информационной структуры."[154], т.е. те угрозы, которые традиционно беспокоили руководство РФ в вопросах МИБ.

2013 г. - заключение соглашения "О сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности".

---

[152] Концепция информационной безопасности государств – участников Содружества Независимых Государств в военной сфере // Виртуальный компьютерный музей. URL: https://www.computer-museum.ru/document/sng2.htm (Дата обращения 28.03.2023)

[153] Лебедева Е.В. Информационная безопасность государств СНГ: этапы реализации. / Е.В. Лебедева // Национальная безопасность / nota bene. - 2016. - № 4. - С. 500-508.

[154] Лебедева Е.В. Информационная безопасность государств СНГ: этапы реализации. / Е.В. Лебедева // Национальная безопасность / nota bene. - 2016. - № 4. - С. 500-508.

Соглашение предусматривало то, что государства его подписавшие проводят политику сближения нормативных правовых актов и нормативно-методических документов в сфере обеспечения информационной безопасности. разработку межгосударственных стандартов в области информационной безопасности, совместимых с международными стандартами, совершенствование технологии защиты информационных систем и ресурсов от потенциальных и реальных угроз, передают информацию друг другу.[155]

В 2019 г. была создана новая “Стратегия обеспечения информационной безопасности государств - участников Содружества Независимых Государств”, сохраняющая преемственность с Концепцией 2008 г. и Соглашения 2013 г.

Данная стратегия включает в себя национальные интересы стран-участниц в области информационной безопасности, в том числе прописано необходимость формирования системы обеспечения международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном.[156]

В области угроз выделено использование ИКТ в:

1. “Военно-политических целях
2. Дискредитация суверенитета, нарушение территориальной целостности государств
3. В террористических целях, в том числе для оказания деструктивного воздействия на объекты критической информационной инфраструктуры
4. Для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка
5. Для совершения преступлений, в том числе связанных с неправомерным использованием информационных ресурсов”[157]

Данные угрозы в целом отражают видение РФ опасностей информационного пространства, сосредоточенную в основном на суверенитете и

---

[155] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности // Электронный фонд правовых и нормативных документов. URL: https://docs.cntd.ru/document/420278452 (Дата обращения 29.03.2023)

[156] Решение о Стратегии обеспечения информационной безопасности государств - участников Содружества Независимых Государств (Москва, 25 октября 2019) // Intermedia. URL: https://www.intermedia.ru/uploads/72b6a0.pdf (Дата обращения 29.03.2023)

[157] URL: https://www.intermedia.ru/uploads/72b6a0.pdf

информационном воздействии на общество, т.е. на политическую, а не технологическую сферу. [158]

Консолидация усилий по обеспечению информационной безопасности союза началась в 2008 г. с созданием “Программы совместных действий по формированию системы информационной безопасности государств-членов Организации Договора о коллективной безопасности”.

Программа предусматривала “разработку единого понятийного аппарата, Сравнительный анализ и совершенствование нормативной правовой базы государств-членов ОДКБ в сфере обеспечения информационной безопасности, анализ угроз информационной безопасности, создание модели системы информационной безопасности, разработку проекта Соглашения о сотрудничестве”[159]

В 2010 г. в устав ОДКБ было внесено положение о важности информационной безопасности. 8 статья устава ОДКБ гласит “Государства – члены взаимодействуют в сферах охраны государственных границ, обмена информацией, информационной безопасности, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, а также от опасностей, возникающих при ведении или вследствие военных действий.”[160]

В Стратегии коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года от 2016 г. подчеркнута важность информационной безопасности. Среди прочих угроз и вызовов коллективной безопасности ОДКБ выделены:

- “достижение в ряде случаев политических и экономических целей с использованием силы, в том числе экономического и информационного давления; практика вмешательства во внутренние дела государств;

[158] Международная информационная безопасность: подходы России / А.В.Крутских, Е.А.Зиновьева, В.И.Булва, М.Б.Алборова, Ю.А.Юдина; под ред. А.В.Крутских, Е.С.Зиновьева. — Москва, 2021. — 48 с

[159] Решение Совета коллективной безопасности Организации Договора о коллективной безопасности О Программе совместных действий по формированию системы информационной безопасности государств-членов Организации Договора о коллективной безопасности (Принято в г. Москве 05.09.2008) // Conventions. URL: https://www.conventions.ru/int/4329/ (Дата обращения 19.04.2023)

[160] Устав Организации Договора о коллективной безопасности от 7 октября 2002 года. // Организация Договора о коллективной безопасности. URL: https://odkb-csto.org/documents/documents/ustav_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_/#loaded (Дата обращения 19.04.2023)

- осуществление деструктивного идеологического и психологического воздействия на население государств – членов ОДКБ через электронные информационные сети и медиаресурсы;
- использование информационных и коммуникационных технологий в целях оказания деструктивного воздействия на общественно-политическую и социально-экономическую обстановку, а также манипулирования общественным сознанием в государствах – членах ОДКБ.”[161]

Помимо этого стратегическими целями и задачами ОДКБ в области информационной безопасности являются:

- “– формирование системы информационной безопасности государств – членов ОДКБ;
- развитие межгосударственного сотрудничества и укрепление межведомственной координации в сфере обеспечения информационной безопасности;
- совершенствование механизмов по противодействию угрозам в информационной сфере;
- проведение совместных мероприятий по противодействию и нейтрализации противоправной деятельности в информационно-телекоммуникационном пространстве государств – членов ОДКБ;
- взаимодействие в вопросах обеспечения международной информационной безопасности;
- выработка согласованных правил взаимодействия в информационной сфере, продвижение их на международный уровень;

[161] Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года 18.10.2016. // Организация Договора о коллективной безопасности. URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/#loaded (Дата обращения 19.04.2023)

- создание условий и реализация совместных практических мероприятий, направленных на формирование основ скоординированной информационной политики в интересах государств – членов ОДКБ.”[162]

В следующем, 2017 г., было заключено “Соглашение о сотрудничестве государств-членов организации договора о коллективной безопасности в области обеспечения информационной безопасности.”

Основываясь на Стратегии 2016 г., Соглашение представляет более подробную информацию и практические решения для обеспечения повестки дня ОДКБ в области информационной безопасности.

Статья 4 соглашения определяет направления сотрудничества:

- “Взаимодействие в разработке и продвижении правовых основ сотрудничества, содействие совершенствованию международной правовой базы;
- Формирование практических механизмов совместного реагирования на угрозы информационной безопасности;
- Развитие мер укрепления доверия в сфере обеспечения информационной безопасности;
- Совершенствование технологической основы обеспечения информационной безопасности;
- Создание условий для взаимодействия компетентных органов Сторон в целях реализации настоящего Соглашения.”[163]

одним из наиболее успешных свидетельств совместной деятельности ОДКБ в области информационной безопасности можно считать так называемые операции ПРОКСИ (Противодействие криминалу в сфере информации). Основной целью операций является выявление и пресечение функционирования в национальных сегментах Интернета таких

[162] Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года 18.10.2016. // Организация Договора о коллективной безопасности. URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/#loaded (Дата обращения 19.04.2023)

[163] Соглашение о сотрудничестве государств-членов организации договора о коллективной безопасности в области обеспечения информационной безопасности // Контурнорматив. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=334580 (Дата обращения 19.04.2023)

информационных ресурсов, содержание которых наносит или может нанести ущерб национальной и коллективной безопасности государств-членов. ПРОКСИ была начата в 2009 году. С 2014 г. операция получает постоянный статус. К 2020 г. в результате проведения ПРОКСИ выявлено 676 207 сайтов, так или иначе угрожающим коллективной безопасности ОДКБ, Из них была приостановлена деятельность информационных ресурсов 129 251 сайта, и было возбуждено 106 120 уголовных дел.[164]

В рамках ОДКБ создан Консультационный координационный центр по реагированию на компьютерные инциденты. Для координации совместных действий при Комитете секретарей советов безопасности ОДКБ сформирована Рабочая группа по вопросам информационной политики и информационной безопасности[165]

Одной из важных направлений политики РФ как в СНГ, так и ОДКБ по обеспечению информационной безопасности является гармонизация законодательства стран-членов данных организаций. В 2014 г. Межпарламентская Ассамблея СНГ приняла модельный закон “О критически важных объектах информационно-коммуникационной инфраструктуры». В 2014 г. также были внесены изменения в модельный закон “Об информатизации, информации и защите информации” 2005 г., новый модельный закон называется “Об информации, информатизации и обеспечении информационной безопасности” . [166]

Также в рамках ОДКБ создан модельный закон “Об информационной безопасности” 2021 г. Модельные законы “Об обеспечении защиты критически

[164] Храмцова А.А. ОДКБ и современные вызовы безопасности. / А.А. Храмцова. // сборник материалов VII Международной научно-практической конференции. Биробиджан, 30 апреля 2022 г. - С. 159-167.

[165] Киреева О. С. Проблема обеспечения информационной безопасности на евразийском пространстве (на примере ОДКБ) / О. С. Киреева // Евразийство: теоретический потенциал и практические приложения. – 2020. – № 10. – С. 158-162..

[166] Бондуровский В.В. Модельное законодательство СНГ и ОДКБ в сфере противодействия международному терроризму: состояние и направления совершенствования / В.В. Бондуровский // Евразийская интеграция: экономика, право, политика. 2016. №1 (19). URL: https://cyberleninka.ru/article/n/modelnoe-zakonodatelstvo-sng-i-odkb-v-sfere-protivodeystviya-mezhdunarodnomu-terrorizmu-sostoyanie-i-napravleniya (дата обращения: 11.05.2023).

важных объектов информационной инфраструктуры" и "О защите информации и кибербезопасности" находятся в разработке[167]

Арчаков считает последнюю "Стратегию обеспечения информационной безопасности государств — участников СНГ" и "Соглашение о сотрудничестве государств — членов ОДКБ в области обеспечения информационной безопасности" важным шагом, нивелирующим проблемы предыдущих концепций и соглашений : диссонанс понятийного аппарата, недостаточность правовой базы, недостаточная субъектность системы обеспечения информационной безопасности, диссонанс в определении угроз и целеполагания.[168]

АСЕАН

В 2005 г. был проведен первый саммит Россия-Асеан, начавшее партнёрство между региональной организацией и РФ. В 2015 г. создан Рабочий план по безопасности и использованию информационно-коммуникационных технологий, предусматривающий создание исследовательской группы по мерам укрепления доверия, предусматривающий механизмы обмена информации, [169]

В 2016 г. на саммите Россия-АСЕАН принят "Комплексный план действий по развитию сотрудничества между Россией и странами АСЕАН" , который провозглашал сотрудничество по противодействию угрозам безопасности, в том числе информационной.[170]

На третьем саммите Россия-АСЕАН в 2018 г. принято "Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности

---

[167] Модельный закон ОДКБ «О защите информации и кибербезопасности» - в повестке дня Экспертно – консультативного совета при Совете ПА ОДКБ. // Парламентская Ассамблея Организации Договора о коллективной безопасности. URL: https://paodkb.org/events/modelnyy-zakon-odkb-o-zaschite-informatsii-i (Дата обращения 19.04.2023)

[168] Арчаков В.Ю. О теоретико-методологических подходах к обеспечению международной информационной безопасности. / Ю.В. Арчаков // Журнал международного права и международных отношений. - 2019. № 3-4 (90-91). - С. 3—11..

[169] Горян Э.В. Сотрудничество России и АСЕАН в сфере кибербезопасности: промежуточные результаты и перспективы дальнейшего развития/ Э.В. Горян // Вопросы безопасности. 2018. №6. URL: https://cyberleninka.ru/article/n/sotrudnichestvo-rossii-i-asean-v-sfere-kiberbezopasnosti-promezhutochnye-rezultaty-i-perspektivy-dalneyshego-razvitiya (дата обращения: 12.05.2023).

[170] Комплексный план действий по развитию сотрудничества Российской Федерации и Ассоциации государств Юго-Восточной Азии (2016-2020). // Центр АСЕАН при МГИМО МИД России. URL: https://asean.mgimo.ru/images/partn/2016-2020-action-plan.pdf (Дата обращения 20.04.2023)

использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий”

Этот документ представляет общие принципы и выражает готовность государств противостоять международным конфликтам, которые могут возникнуть из-за незаконного использования ИКТ. Он также подчеркивает намерение России и стран АСЕАН развивать практическое сотрудничество в этой области, включая борьбу с использованием ИКТ в террористических и преступных целях. В документе признается важность разработки и принятия норм, правил и принципов ответственного поведения государств в информационном пространстве, а также акцентируется роль ООН в содействии диалогу по вопросам информационной безопасности. Также государства признают то, что они находятся на разных уровнях развития ИКТ и стремятся к преодолению цифрового разрыва. В качестве перспективной инициативы отмечается предложение России о создании постоянного Диалога Россия - АСЕАН по вопросам информационной безопасности.[171]

В 2021 г. Россия избрана сопредседателем механизма межсессионных встреч Регионального форума АСЕАН по безопасности (АРФ) по обеспечению безопасности ИКТ. [172]

Также заработал механизм Диалога Россия-АСЕАН по вопросам, связанным с обеспечением безопасности ИКТ. В 2021 г. Стороны договаривались о взаимодействии в рамках глобальных инициатив - РГОС, Спецкомитета по использованию ИКТ в преступных целях, Международного союза электросвязи, а также РФ предложила проект Рабочего плана межведомственного сотрудничества по обеспечению ИКТ.[173]

---

[171] Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 14 ноября 2018 года. // Президент России Официальный сайт. URL: http://special.kremlin.ru/supplement/5361 (Дата обращения 20.04.2023)

[172] Россия стала сопредседателем механизма форума АСЕАН по информационной безопасности. // ТАСС. URL: https://tass.ru/politika/12078021 (Дата обращения 20.04.2023)

[173] Об итогах первой встречи Диалога Россия - АСЕАН по вопросам, связанным с обеспечением безопасности ИКТ. // НАМИБ. URL: https://namib.online/2021/09/ob-itogah-pervoj-vstrechi-dialoga-rossija-asean-po-voprosam-svjazannym-s-obespecheniem-bezopasnosti-ikt/ (Дата обращения 20.04.2023)

На второй встрече диалога 2022 г. также подтвердилась необходимость необходимость сотрудничества на глобальном уровне. [174]

В связи с решением о преобразовании Совещания по взаимодействию и мерам доверия в Азии в международную организацию в 2022[175] г. необходимо отметить деятельность России по решению проблем МИБ в данном формате.

Россия предложила включить раздел «Безопасность в сфере использования ИКТ и самих ИКТ» в меры укрепления доверия стран-членов СВМДА . РФ назначена координатором по работам в данном направлении. [176]

2.3. Двусторонние отношения РФ и США в области информационной безопасности

Взаимодействие Соединенных Штатов с Россией неизбежно, обе страны относятся к числу немногих государств, имеющих как глобальные интересы, так и способность продвигать эти интересы. Оба государства взаимодействуют как в глобальных, так и двусторонние отношениях.

Одним из важных вопросов взаимоотношения РФ и США по вопросам информационной безопасности стоит проблема ICANN - Корпорация по по управлению доменными именами и IP-адресами" А. Крутских заявляет : "Несмотря на то, что ICANN формально является независимой некоммерческой организацией, фактически контроль над распределением имен и адресов Интернета осуществляет правительство США. Негосударственный статус ICANN выступает в роли «ширмы», призванной прикрыть американскую

[174] Об итогах второй встречи Диалога Россия-АСЕАН по вопросам, связанным с обеспечением безопасности ИКТ. // Посольская жизнь. URL: https://embassylife.ru/post/12437 (Дата обращения 20.04.2023)

[175] СВМДА преобразуется в международную организацию // ТАСС. URL: https://tass.ru/mezhdunarodnaya-panorama/16040685 (Дата обращения 02.04.2023)

[176] Лобанова О.С. О продвижении Российских подходов по международной информационной безопасности на профильных региональных площадках./ О.С. Лобанова // Сборник докладов участников XVI международного форума. Партнерство государства, бизнеса и гражданского общества при обеспечении международной безопасности. (19 - 22 сентября 2022 г. Москва) / Национальная ассоциация международной информационной безопасности - С. 154 - 156

гегемонию США."[177] Россия выступает за "интернационализацию" управления интернетом - передачу функций по управлению Интернетом в Международном Союзу Электросвязи.

Попытки начать двусторонние переговоры по кибер проблеме начались в 1998 г. по Российской инициативе, однако они не возымели успеха из-за незаинтересованности со стороны США.[178]

В 2013 г. в рамках "Группы восьми" РФ и США договорились о сотрудничестве в киберсфере. "Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия". В рамках договорённости была организована связь между группами реагирования на чрезвычайные ситуации в компьютерной среде. Так как одно из самых потенциально опасных угроз в кибер сфере являются атаки на ядерные объекты, обе страны договорились об обмене уведомления через Центры снижения ядерных рисков, а также прямую защищенную линию голосовой связи между Белым домом и Кремлём. Кроме того оговорено создание двусторонней рабочей группы по вопросам угроз в сфере использования ИКТ, эта группа создавалась для анализа угроз, обмена информацией, координации совместных действий. [179]

Уже 23 июня в РФ прибыл Эдвард Сноуден - бывший сотрудник АНБ США, раскрывший многие детали о системе незаконного наблюдения за гражданами любого государства, осуществляемой АНБ в интересах правительства США. РФ отказалось выдать Сноудена США, что вызвало дипломатический скандал.

---

[177] Крутских А.В. Международная информационная безопасность:в поисках консолидированных подходов // Вестник РУДН. Серия: Международные отношения, 2022 Vol. 22 No. 2 342—351

[178] Зиновьева Е. С., Яникеева И. О. Эволюция взаимодействия России и США в области международной информационной безопасности в исторической ретроспективе / Е.С. Зиновьева, И.О. Яникеева // Вестник Санкт-Петербургского университета. Международные отношения. - 2022. Т. Вып. 2. - С. 158–173.

[179] Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия. 17 июня 2003 г. // официальные сетевые ресурсы Президента России. URL: http://kremlin.ru/supplement/1479 (Дата обращения 27.04.2023)

Этот скандал нанес урон достигнутым договоренностям по кибербезопасности. [180]

Помимо этого достигнутые договоренности были сведены на нет украинским кризисом 2014 г., политикой Президента США Б. Обамы по сдерживанию России. [181]

Вплоть до 2017 г. РФ отрицало существование своих “кибервойск”, пока Министр Оборон С. Шойгу прямо не заявил о существовании этого рода войск.[182] Однако есть сведения о том, что “Войска информационных операций” были созданным в 2014 г. ТАСС, ссылаясь на свой источник заявило об этом 12 мая 2014 г. “ Предложение о создании такой структуры, предназначенной для кибернетического и информационного противоборства с вероятным противником, находилось в проработке не один год. Прошлогодние разоблачения экс-сотрудником ЦРУ Эдвардом Сноуденом глобальной электронной слежки со стороны АНБ США только ускорили процесс принятия решения”[183] Точную дату создания этой структуры назвать невозможно, но можно с уверенностью сказать, что необходимость в создании такого рода войск было продиктовано событиями 2014 г.

Американцы стали пионерами в этой области. О начале формирования кибервойск, специального подразделения Стратегического командования США, заявил генерал-лейтенант Кит Александр, глава Агентства национальной безопасности США, 5 мая 2009 года. Основной целью этого подразделения, по словам генерала, было обеспечение безопасности страны от атак через компьютерные сети и защита электронных систем. [184]

---

[180] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[181] Зиновьева Е. С., Яникеева И. О. Эволюция взаимодействия России и США в области международной информационной безопасности в исторической ретроспективе / Е.С. Зиновьева, И.О. Яникеева // Вестник Санкт-Петербургского университета. Международные отношения. - 2022. Т. Вып. 2. - С. 158–173.

[182] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[183] Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций. // ТАСС. URL: https://tass.ru/politika/1179830 (Дата обращения 19.04.2023)

[184] Буранов Н. Принципиальной новые войска / Н. Буранов. // ЭКСПЕРТ. URL: https://expert.ru/2017/03/1/kibervojna/ (Дата обращения 04.05.2023)

4-5 сентября 2014 г. в Уэльсе на саммите НАТО было заявлено, что в случае кибер нападения на члена НАТО может быть задействована 5 статья Атлантического договора. Каждый отдельный случай кибернападения должен быть оцениваться отдельно.[185]

Распространенность кибератак, спонсируемых государством, подтверждается тем, что они постоянно совпадают со случаями международных разногласий или конфликтов. Аннексия Крыма в 2014 году служит ярким примером, поскольку она вызвала возобновление напряженности в отношениях между Россией и США, что впоследствии привело к обвинениям России в проведении масштабных кибератак против Соединенных Штатов.[186]

С 2014 г. в двусторонних американо-российских отношениях наступает стадия “киберконфликта” , правительственные структуры США систематически взламываются, ценная информация крадётся. Президент Б. Обама официально обвиняет РФ в принадлежности к этим атакам, Президент РФ не подтверждает причастность России к взломе DNC, но добавляет, что США поддерживали и платили средствам массовой информации СМИ и неправительственным организации, чтобы вмешиваться в российскую политику. 35 российских дипломатов были высланы с территории США за кибератаки со стороны РФ во время выборов в США. [187] Летом 2016 года администрация рассматривала возможность проведения наступательных кибероперациий, но отказалась от них, отчасти из-за опасений спровоцировать дальнейшую агрессию России.[188]

Однако уже при Президенте Трампе подтвердилось, что американские кибервойска проводили атаки на российскую “фабрику троллей”[189]

---

[185] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[186] Abdyraeva C. “Cyber Warfare.” The Use of Cyberspace in the Context of Hybrid Warfare.: Means, Challenges and Trends. / C. Abdyraeva // OIIP - Austrian Institute for International Affairs - 2020 - P. 36

[187] Baezner M. Hotspot Analysis: Cyber-conflict between the United States of America and Russia / M. Baezner, P. Robin // Risk and Resilience Team Center for Security Studies, ETH Zürich. - 2017. Version 1 - P.26

[188] Lonergan E.D. Schneider J. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation. / E.D. Lonergan, J. Schneider // Journal of Cybersecurity - 2023. Volume 9, Issue 1 - P. 1 - 10.

[189] Thiessen M. A. Trump confirms, in an interview, a U.S. cyberattack on Russia. / M.A. Thiessen // The Washington Post. URL: https://www.washingtonpost.com/opinions/2020/07/10/trump-confirms-an-interview-us-cyberattack-russia/ (Дата обращения 15.04.2023)

Атрибуция России в хакерских атаках 2016 г. является дискуссионным вопросом. Терехов и Ткаченко называют “постправдой” атрибуцию РФ и последующую кампанию против “русских хакеров”, указывая на то, что для урегулирования конфликта не использовались созданные для этого механизмы диалога между экспертами по кибербезопасности. Ссылаясь на расследование организации “Профессионалы - ветераны разведки за здравомыслие” авторы подтверждают свой тезис, что утечка данных Демократического национального комитета была результатом не хакерской атаки, а внутренней утечкой. Делается это для отвода внимания публики от реальных проблем. Исследователи также отмечают, что американские политики и ученые представляют российские элементы “мягкой силы” , такие как канал RT, фонд “Русский Мир”, “Спутник” и др., как агрессивные средства информационной войны. [190]

Такую точку зрения западные ученые называют частью информационной войны РФ против Запада, наряду с представлением о том, что НАТО ведёт против России гибридную войну. По их мнению российское правительство РФ использует нарратив о том, что информационные кампании НАТО преследуют две основные цели. Во-первых, они стремятся очернить репутацию России среди русскоязычных стран. Во-вторых, они направлены на разжигание внутренних протестов и политических беспорядков, в первую очередь направленных на простых россиян. В результате в различных российских новостных статьях эти кампании описываются как форма информационно-психологического воздействия, направленного на российских граждан. Главным спонсором якобы выступают США, которые поддерживают российскую "несистемную оппозицию" и сотрудничают с русофобскими СМИ в таких странах, как Польша, Грузия, Эстония, Латвия и Литва.[191]

В 2016 г. в рамках НАТО был одобрен документ “Обязательство по кибер обороне”,

---

[190] Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

[191] Abdyraeva C. “Cyber Warfare.” The Use of Cyberspace in the Context of Hybrid Warfare.: Means, Challenges and Trends. / C. Abdyraeva // OIIP - Austrian Institute for International Affairs - 2020 - P. 36

Во время правления Президента Д. Трампа Россия предлагала несколько инициатив по взаимодействию в киберпространстве в 2017 и 2018, однако от обоих предложений президент отказался. По мнению Зиновьевой связано это с внутриполитической обстановкой в США, а именно из-за обвинений в сторону Д. Трампа о связях с русскими хакерами.[192] Так и в 2020 г. Президент РФ В. Путин предложит восстановить договорённости, достигнутые в 2014 г., но и это предложение оказалось отвергнутым администрацией Трампа.[193] Помимо ранее достигнутых договоренностей В. Путин также предложил заключить двустороннее соглашение о предотвращении инцидентов в информационном пространстве, а также “обменяться гарантиями невмешательства во внутренние дела друг друга, включая избирательные процессы, в том числе с использованием ИКТ и высокотехнологичных методов.”[194]

США официально связывают хакерскую группу APT 29 со службой внешней разведки РФ. Эта группа была ответственна за компанию против Национального комитета демократической партии США[195], а также за взлом системы американской компании SolarWinds. В результате взлома были скомпрометированы данные, сети и системы тысяч людей, когда SolarWinds по неосторожности поставила вредоносное ПО. Россия отвергла обвинения “Вредоносная деятельность в информационном пространстве противоречит принципам российской внешней политики, национальным интересам и

[192] Зиновьева Е.С. Международная информационная безопасность в двусторонних отношениях России и США. / Е.С. Зиновьева // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-v-dvustoronnikh-otnosheniyakh-rossii-i-ssha/ (Дата обращения 12.04.2023)

[193] Sullivan L. US-Russia Cybersecurity Cooperation: Future Paths and Historical Perspective / L. Sullivan // Geohistory. URL: https://geohistory.today/us-russia-cybersecurity-cooperation/#Bilateral_Efforts (Дата обращения 17.04.2023)

[194] Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. 25 сентября 2020 // Официальные сетевые ресурсы Президента России. URL: http://kremlin.ru/events/president/news/64086 (Дата обращеня 28.04.2023)

[195] Baezner M. Hotspot Analysis: Cyber-conflict between the United States of America and Russia / M. Baezner, P. Robin // Risk and Resilience Team Center for Security Studies, ETH Zürich. - 2017. Version 1 - P.26

пониманию межгосударственных отношений”[196] Президент Д. Байден наложил на РФ санкции в том числе, за якобы причастность к хакерским атакам.[197] Киберконфликт с США повлиял и на внутреннюю политику РФ. В 2018 г. бы принят “Закон о суверенном Рунете/интернете”, по словам сенаторов, подготавливающих закон “Подготовлен с учетом агрессивного характера принятой в сентябре 2018 года Стратегии национальной кибербезопасности США … Россия впрямую и бездоказательно обвиняется в совершении хакерских атак”[198]

Различие американского и российского подхода также виден и в использовании политики сдерживания угроз. Российский подход скорее направлен на “сдерживание посредством недопущения”, Т.е. укреплении защитной способности российского киберпространства. Россия практически не прибегает к политики публичной атрибуции, т.е. обвинения в совершении кибератак. В то время как США активно использует атрибуцию. В Национальной Киберстратегии США Министерства Обороны США 2018 г. предполагается сохранять мир как с помощью продвижения норм ответственного поведения государств, так и путем сдерживания, объектами сдерживания признаны Китай и Россия. Главный инструмент сдерживания США в киберпространстве - Киберкомандование, реализующее концепцию “передовой обороны”, т.е. пресечению источника киберугроз, а также “непрерывного соперничества, т.е. каждодневные действия против противников. [199] РФ переняло у США идею наказания за кибератаки. А.В Крутских в ответ на информацию о попыках

---

[196] Oladimeji S. Kerner S.M. SolarWinds hack explained: Everything you need to know / S. Oladimeji, S.M. Kerner // Whats.com. URL: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (Дата обращения 11.04.2023)

[197] Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government // The White House. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (Дата обращения 13.04.2023)

[198] Шакиров О.И. Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве / О.И. Шакиров // Международная аналитика. – 2020. – Том 11 (4). – С. 147–170

[199] Шакиров О.И. Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве / О.И. Шакиров // Международная аналитика. – 2020. – Том 11 (4). – С. 147–170

США внедрится в энергосистему РФ заявил “кто к нам с кибермечом придет, тот от кибермеча и погибнет”.[200]

“Киберстратегия” США претерпела значительные изменения по ходу времени . В 2011 г. Белый дом не делал акцент на военных средствах, хоть в стратегии 2011 г. была концепция сдерживания, упор делался на недопущении, т.е. повышении киберзащиты. [201]

Стратегия 2015 г. отличается от стратегии 2011 г. тем, что в нем прямо названы наиболее важные противники, включая как такие страны, как Россия, Китай, Иран и Северная Корея, так и негосударственные структуры. Кроме того, в нем определены пять ключевых целей, таких как подготовка и поддержание хорошо оснащенных войск для проведения кибер-операций, защита данных, информационных сетей Министерства обороны, готовность к защите США, создание и поддержание реальных возможностей для контроля вовлеченности и враждебности в киберпространстве, а также формирование глобальных союзов для предотвращения угрожающих ситуаций и обеспечения безопасности.[202]

стратегия 2018 года занимает гораздо более активную позицию, обязуясь "настойчиво защищать наши интересы". Это связано с тем, что документ рассматривает основной риск для США не как использование кибер-операций, а скорее как "бездействие". Кроме того, стратегия 2018 года призывает Министерство обороны "побеждать" и "упреждать" - два слова, которые заметно отсутствовали в предыдущей стратегии. В 2018 году предлагаются более широкие и активные миссии по защите передовых позиций, ежедневной конкуренции и подготовке к войне.[203]

Национальная Стратегия Кибербезопасности США 2023 г. выделяет несколько ключевых пунктов осуществления кибербезопасности:

---

[200] Крутских: Москву удивляет, что Трамп назвал статью о кибератаках против РФ госизменой // ТАСС.URL: https://tass.ru/politika/6566204 (Дата обращения 26.04.2023)

[201] Lonergan E.D. Schneider J. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation. / E.D. Lonergan, J. Schneider // Journal of Cybersecurity - 2023. Volume 9, Issue 1 - P. 1 - 10.

[202] Lonergan E.D. Schneider J. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation. / E.D. Lonergan, J. Schneider // Journal of Cybersecurity - 2023. Volume 9, Issue 1 - P. 1 - 10.

[203] Kollars N. Schneider J. Defending forward: The 2018 Cyber Strategy is here. / N. Kollars, J. Schneider // War on the rocks. URL: https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/ (Дата обращения 19.04.2023)

- “Защита критически важной инфраструктуры
- Борьба с угрозами (всеми возможными средствами)
- Формирование рыночных сил для обеспечения безопасности и устойчивости
- Инвестиции в устойчивое будущее
- Создание международного партнерства для достижения общих целей”[204]

Шакиров, анализируя новую стратегию так охарактеризовал её эволюцию и преемственность. «Новая киберстратегия во многом строится на фундаменте прошлой версии этого документа. Преемственность видна прежде всего в части борьбы с угрозами. Именно при Дональде Трампе произошел поворот в сторону активных действий против государственных и негосударственных противников США в киберпространстве, Минобороны занялось так называемой передовой обороной, а ФБР — охотой на преступные группировки»[205] . При этом основным отличием от предыдущей стратегии является акцент на создание сильной системы киберзащиты внутри США. [206]

На фоне Российско-Американского саммита 2021 г. в Женеве начался процесс киберразрядки. В рамках саммита было уделено большое внимание кибербезопасости. Дж. Байден призвал РФ активнее бороться с киберпреступностью, договорится о запрете кибератак на критически важную инфраструктуру. [207] Именно по итогам этого саммита была создана Рабочая группа по проблемам обеспечения безопасности в сфере информационно-коммуникационных технологий. В ходе контактов в преддверии создания группы американская сторона требовала от РФ признать причастность к хакерским структурам. [208]

---

[204] Belles J. Key Points from the US National Cybersecurity Strategy 2023. / J. Belles. // Thales URL: https://cpl.thalesgroup.com/blog/encryption/us-cybersecurity-strategy-key-points-2023 (Дата обращеня 27.04.2023)
[205] Черненко Е. На виртуальном фронте всё стабильно / Е. Черненко. // Коммерсант. URL: https://www.kommersant.ru/doc/5861336 (Дата обращения 01.05.2023)
[206] Черненко Е. На виртуальном фронте всё стабильно / Е. Черненко. // Коммерсант. URL: https://www.kommersant.ru/doc/5861336 (Дата обращения 01.05.2023)
[207]Шакиров О.И. Киберсаммит Путина и Байдена. / О.И. Шакиров // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kibersammit-putina-i-baydena/ (Дата обращения 13.05.2023)
[208] Егоров И. Совбез РФ: Соединенные Штаты в очередной раз доказали, что им верить нельзя. / И. Егоров // Российская Газета. URL:

В рамках работы группы было установлено взаимодействие по обмену оперативной информацией о киберпреступлениях между Генеральной прокуратурой России и министерством юстиции США. Кроме того, были обменяны списки объектов критически важной информационной инфраструктуры обеих стран.[209]

В связи с эскалацией вооруженного конфликта на Украине США вышли из переговорного процесса, что привело к новому киберконфликту.[210]

МИД РФ выпустило заявление, в котором обвинило США в проведении массированной кибероперации против РФ. “Изощренные киберсредства используются для похищения личных данных российских граждан. В интернете распространяется фейковая информация с целью дезориентировать и деморализовать российское общество, дискредитировать действия Вооруженных Сил Российской Федерации и органов государственного управления, стимулировать противоправную активность в населении, затруднить работу различных отраслей экономики, посеять страх и нестабильность.”[211]

После слов главы американского киберкомандования Пола Накасоне о проведении наступательных операций в поддержку Украины в МИДе ещё раз призвали США не провоцировать Россию на ответные меры в киберпространстве, однако обе стороны перестали всячески реагировать на деятельность хакеров, атакующий “противника” внутри своих границ. МИД РФ назвал хакерскую группу Killnet “сообществом российских программистов” [212]

---

https://rg.ru/2022/04/07/sovbez-rf-soedinennye-shtaty-v-ocherednoj-raz-dokazali-chto-im-verit-nelzia.html (Дата обращения 01.05.2023)

[209] Егоров И. Совбез РФ: Соединенные Штаты в очередной раз доказали, что им верить нельзя. / И. Егоров // Российская Газета. URL: https://rg.ru/2022/04/07/sovbez-rf-soedinennye-shtaty-v-ocherednoj-raz-dokazali-chto-im-verit-nelzia.html (Дата обращения 01.05.2023)

[210] Шакиров. О. И. Взаимное предостережение: чем закончилась короткая киберразрядка между Россией и США. / О.И. Шакиров /// РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/vzaimnoe-predosterezhenie-chem-zakonchilas-korotkaya-kiberrazryadka-mezhdu-rossiey-i-ssha/?sphrase_id=96227596 (Дата обращения 08.03.2023)

[211] Заявление МИД России в связи с продолжающейся киберагрессией со стороны «коллективного Запада». // Министерство иностранных дел Российской Федерации. URL: https://www.mid.ru/ru/foreign_policy/news/1806906/ (Дата обращения 28.04.2023)

[212] Шакиров. О. И. Взаимное предостережение: чем закончилась короткая киберразрядка между Россией и США. / О.И. Шакиров /// РСМД. URL:

Яникеева И.О. , проведя анализ двусторонних отношений США и РФ, заметила, что никаких кибератак на объекты критически важной инфраструктуры после событий 2022 г. не произошло. Это объясняется “равновесием страха” обеих стран, что говорит о том, что реальным фактором, обеспечивающим безопасность, по крайней мере, в киберсфере является сдерживание.[213]

Существует и альтернативная точка зрения. В стратегии кибербезопасности Дж. Байдена отсутствует слово “сдерживание”. Это может указывать на несостоятельность данной политики.[214]

Анализируя угрозы, разделяемые и США и Россией Стадник выделяет использование ИКТ в террористических целях, киберпреступности, угрозу безопасности и функционированию интернета, кибератаки на критически важную инфраструктуру как основу потенциальных соглашений и норм по кибербезопасности.[215]

В тоже время нельзя не говорить как о “антироссийской” в США, так и “антиамериканской” риторике в РФ, Обе страны наращивают как кибервооружение, так и информационный потенциал именно для противостоянию друг другу, например. Дж. Байден пообещал , что заставит РФ заплатить за свою деятельность в киберпространстве.[216]

Если говорить о восприятии проблематики кибербезопаности в США, по мнению Смекаловой, в отличии от Российского подхода, он сильно зависит от внешнеполитической и внутриполитической ситуации и не отличается последовательностью. [217]

---

https://russiancouncil.ru/analytics-and-comments/analytics/vzaimnoe-predosterezhenie-chem-zakonchilas-korotkaya-kiberrazryadka-mezhdu-rossiey-i-ssha/?sphrase_id=96227596 (Дата обращения 08.03.2023)

[213] Яникеева И.О Российско-американские отношения в сфере обеспечения международной информационной безопасности . И. О. Яникеева // Мировая политика. 2022. №4. URL: https://cyberleninka.ru/article/n/rossiysko-amerikanskie-otnosheniya-v-sfere-obespecheniya-mezhdunarodnoy-informatsionnoy-bezopasnosti (дата обращения: 23.05.2023)

[214] Lin H. Where the New National Cybersecurity Strategy Differs From Past Practice/ H. Lin. URL: https://www.lawfareblog.com/where-new-national-cybersecurity-strategy-differs-past-practice (Дата обращения 08.05.2023)

[215] Stadnik I. What Is an International Cybersecurity Regime and How We Can Achieve It? / I. Stadnik // Masaryk University Journal of Law and Technology. - 2017 - 11(1):129 -P. 129 - 154

[216] Карасев П.А. Эволюция национальных подходов к ведению кибервойны / П.А. Карасев // Международная аналитика. – 2022. – Том 13 (2). – С. 79–94.

[217] Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры. / М.В. Смекалова // Вестн. Моск. ун-та. Сер. 25: Международные отношения и мировая политика. - 2019. № 1. - С. 47-69.

Заключение

В рамках исследования был проведен анализ подхода Российской Федерации к международной информационной безопасности, его эволюции и существующих проблем. Целью работы было выявление особенностей и недостатков этого подхода, а также оценка уровня угроз информационной безопасности в современном мире.

В ходе исследования были достигнуты следующие задачи. Во-первых, был определен уровень угроз информационной безопасности, связанных с международными процессами и деятельностью акторов в киберпространстве. Это позволило получить представление о сложности и многообразии вызовов, с которыми сталкиваются государства

Во-вторых, были выявлены различия в определениях основных понятий, касающихся международной информационной безопасности. Это позволило понять, что существует разногласие между различными государствами и акторами относительно того, что включает в себя информационная безопасность и какие меры необходимо принимать для ее обеспечения.

В-третьих, была исследована концепция киберсдерживания в контексте информационной безопасности. Рассмотрение этой концепции позволило оценить стратегические подходы и инструменты, которые Россия применяет для защиты своих интересов в киберпространстве и предотвращения возможных угроз.

В-четвертых, была проанализирована нормативно-правовая база Российской Федерации в контексте достижения режима международной информационной безопасности.

Кроме того, были рассмотрены концепции и резолюции, выдвигаемые Россией в ООН. Также были исследованы многосторонние соглашения по вопросам международной информационной безопасности. Рассмотрение этих соглашений

позволило выявить прогресс и сложности в процессе международного сотрудничества в области информационной безопасности

Можно говорить о том, что подход РФ к обеспечению информационной безопасности опирается как на мирные, так и силовые средства в рамках киберсдерживания. Процесс создания режима международной информационной безопасности осложнен не только расхождением в понимании проблематики среди экспертов и правителей различных стран, но и политической обстановке, а именно киберконфликту между США и РФ,

Исходя из идеи укрепления суверенитета Российское руководство продвигает свое видение информационной безопасности как концепции невмешательства в дела других стран при помощи союзников и коллег по ОДКБ, СНГ, ШОС и в меньшей степени БРИКС, АСЕАН. Опираясь на РГОС РФ старается вовлечь как можно больше акторов в процесс выработки правил поведения в информационной безопасности, при этом ограничивая участие негосударственных акторов.

Также в ходе исследования был проанализирован киберконфликт между Российской Федерацией и Соединенными Штатами. И РФ и США хоть и находятся в состоянии киберконфликта, но не предпринимают слишком разрушительных кибер операций против друг друга, что вызвано политикой киберсдерживания обеих стран. Со стороны политического аспекта информационной безопасности обе страны ограничивают доступ друг друга к своей внутренней политики и социума путем цензуры.

Исходя из проведенного исследования, можно заключить, что Российская Федерация имеет свой особый подход к международной информационной безопасности, основанный на идеях суверенитета, равенства и ответственного поведения государств в киберпространстве и информационном пространстве.

Список источников и литературы

Источники

1. Beckstrom, Rob. Speech at the London Conference on Cyberspace. // ICANN. November 2, 2011. URL: https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf (Дата обращения 07.03.2023)
2. Council of Europe: Convention on Cybercrime. // European Treaty Series - №. 185 - Budapest. November 23, 2001. URL: https://rm.coe.int/1680081561 (Дата образения 15.05.2023)
3. Digital 2020: 3.8 billion people use social media.[Электронный ресурс]// We are social. URL: https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media/ (Дата обращения 10.12.2022)
4. ISO, 2012. ISO / IEC 27032:2012. // Information Technology Security techniques – Guidelines for cybersecurity. URL: https://www.iso27001security.com/html/27032.html (Дата обращения 14.05.2023)
5. Oxford Advanced Learner’s Dictionary. [Электронный ресурс]// URL: https://www.oxfordlearnersdictionaries.com/definition/english/cyber?q=cyber (Дата обращения 28.02.2023)
6. The cybersecurity impact of Operation Russi by Anonymous. // ComputerWeekly.com. URL: https://www.computerweekly.com/feature/The-cyber-security-impact-of-Operation-Russia-by-Anonymous (Дата обращения 05.12.2022)
7. US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command. // Skynews. URL: https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (Дата обращения 05.03.2023)

8. В Нью-Йорке со скандалом открылась сессия РГОС по кибербезопасности. // Московский комсомолец. URL: https://www.mk.ru/politics/2022/07/26/v-nyuyorke-so-skandalom-otkrylas-sessiya-rgos-po-kiberbezopasnosti.html (Дата обращения 15.11.2022)
9. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Электронный ресурс]: резолюция, принятая Генер. Ассамблеей Орг. Объедин. Наций 68/98* от 24 июня 2013 г. A/68/98*. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf?OpenElement (Дата обращения 9.03.2023)
10. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Электронный ресурс]: резолюция, принятая Генер. Ассамблеей Орг. Объедин. Наций 70/174 от 22 июля 2015 г. A/70/174. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (Дата обращения 09.03.2023)
11. Декларация, принятая по итогам саммита БРИКС (г.Санья, о.Хайнань, Китай, 14 апреля 2011 года)// Официальные сетевые ресурсы Президента России. URL: http://www.kremlin.ru/supplement/907 (Дата обращения 05.04.2023)
12. Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности [Электронный ресурс]: 30 июля 2010. A/65/201. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/59/PDF/N1046959.pdf?OpenElement (Дата обращения 08.03.2023)
13. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895). //

Информационно-правовой портал Гарант.ру. URL: https://base.garant.ru/182535/ (Дата обращения (05.03.2023)

14. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Доклад Генерального секретаря [Электронный ресурс] 10 июля 2010. A/55/140. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/535/04/PDF/N0053504.pdf?OpenElement (Дата обращения: 04.03.2023)
15. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. м [Электронный ресурс]: резолюция Генер. Ассамблеи Орг. Объедин. Наций 57/53 от 30 декабря 2002 г. A/RES/57/53 // URL: https://ifap.ru/ofdocs/un/5753.pdf (Дата обращения 04.03.2023)
16. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. м [Электронный ресурс]: резолюция Генер. Ассамблеи Орг. Объедин. Наций 60/45 от 8 декабря 2005 г. A/RES/60/45 // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/32/PDF/N0549032.pdf?OpenElement (Дата обращения 06.03.2023)
17. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности [Электронный ресурс]: резолюция Генер. Ассамблеи Орг. Объедин. Наций 54/49 от 23 декабря 1999. A/RES/54/49 // URL: https://ifap.ru/ofdocs/un/5449.pdf. (Дата обращения 04.03.2023)
18. Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. 25 сентября 2020 // Официальные сетевые ресурсы Президента России. URL: http://kremlin.ru/events/president/news/64086 (Дата обращеня 28.04.2023)
19. Заявление МИД России в связи с продолжающейся киберагрессией со стороны «коллективного Запада». // Министерство иностранных дел Российской Федерации. URL:

https://www.mid.ru/ru/foreign_policy/news/1806906/ (Дата обращения 28.04.2023)

20. Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 14 ноября 2018 года. // Президент России Официальный сайт. URL: http://special.kremlin.ru/supplement/5361 (Дата обращения 20.04.2023)
21. Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций. // ТАСС. URL: https://tass.ru/politika/1179830 (Дата обращения 19.04.2023)
22. Комплексный план действий по развитию сотрудничества Российской Федерации и Ассоциации государств Юго-Восточной Азии (2016-2020). // Центр АСЕАН при МГИМО МИД России. URL: https://asean.mgimo.ru/images/partn/2016-2020-action-plan.pdf (Дата обращения 20.04.2023)
23. Конвенция Организации Объединенных Наций о противодействии использованию информационно коммуникационных технологий в преступных целях. Проект 29.06.2021.// Undocs.org. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (Дата обращения 25.03.2023)
24. Конвенция об обеспечении международной информационной безопасности (концепция). // Комитет государственной думы по международным делам. URL: https://interkomitet.ru/blog/2011/09/22/konventsiya-ob-obespechenii-mezhdunarodnoj-informatsionnoj-bezopasnosti-kontseptsiya/ (Дата обращения 02.04.2023)
25. Концепция Конвенции ООН об обеспечении международной информационной безопасности. [Электронный ресурс] // Совет Безопасности Российской Федерации. URL:

http://www.scrf.gov.ru/security/information/document112/ (Дата обращения 16.03.2023)

26. Концепция информационной безопасности государств – участников Содружества Независимых Государств в военной сфере // Виртуальный компьютерный музей. URL: https://www.computer-museum.ru/document/sng2.htm (Дата обращения 28.03.2023)
27. Концепция формирования информационного пространства Содружества Независимых Государств // Исполнительный комитет Содружества Независимых Государств. URL: https://cis.minsk.by/page/7548 (Дата обращения 27.03.2023)
28. Крутских: Москву удивляет, что Трамп назвал статью о кибератаках против РФ госизменой // ТАСС.URL: https://tass.ru/politika/6566204 (Дата обращения 26.04.2023)
29. Крутских А.В. Международная информационная безопасность:в поисках консолидированных подходов // Вестник РУДН. Серия: Международные отношения, 2022 Vol. 22 No. 2 342—351
30. Модельный закон ОДКБ «О защите информации и кибербезопасности» - в повестке дня Экспертно – консультативного совета при Совете ПА ОДКБ. // Парламентская Ассамблея Организации Договора о коллективной безопасности. URL: https://paodkb.org/events/modelnyy-zakon-odkb-o-zaschite-informatsii-i (Дата обращения 19.04.2023)
31. Об итогах второй встречи Диалога Россия-АСЕАН по вопросам, связанным с обеспечением безопасности ИКТ. // Посольская жизнь. URL: https://embassylife.ru/post/12437 (Дата обращения 20.04.2023)
32. Об итогах первой встречи Диалога Россия - АСЕАН по вопросам, связанным с обеспечением безопасности ИКТ. // НАМИБ. URL: https://namib.online/2021/09/ob-itogah-pervoj-vstrechi-dialoga-rossija-asea

n-po-voprosam-svjazannym-s-obespecheniem-bezopasnosti-ikt/ (Дата обращения 20.04.2023)

33. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. // Совет безопасности Российской Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document113/ (Дата обращения 5.05.2023)
34. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утверждены Президентом Российской Федерации 24 июля 2013 г N ПР-1753)// Кодификация.РФ. URL: https://rulaws.ru/acts/Osnovy-gosudarstvennoy-politiki-Rossiyskoy-Federatsii-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasn/ (Дата обращения 07.03.2023)
35. О четвертой сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности. // Министерство иностранных дел Российской Федерации. URL: https://mid.ru/ru/foreign_policy/news/1849347/ (Дата обращения 26.03.2023)
36. Пекинская декларация XIV саммита БРИКС 23 июня 2022 года. // Официальный сайт Президента РФ. URL: http://special.kremlin.ru/supplement/5819 (Дата обращения 04.04.2023)
37. Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря. [Электронный ресурс] резолюция, принятая Генер. Ассамблеей Орг. Объедин. Наций 69/723 от 13 января 2015 г. A/69/723 . URL:

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/04/PDF/N1501404.pdf?OpenElement (Дата обращения 10.03.2023)

38. Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 года на имя Генерального секретаря [Электронный ресурс]: 14 сентября 2011. A/66/359. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement (Дата обращения 08.03.2023)
39. Противодействие использованию информационно коммуникационных технологий в преступных целях. [Электронный ресурс] резолюция, принятая Генер. Ассамблеей Орг. Объедин. Наций 74/247 от 20 января 2020 г. A/RES/74/247. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/31/PDF/N1944031.pdf?OpenElement (Дата обращения 10.03.2023)
40. Путин предложил странам БРИКС заключить соглашение по информационной безопасности.// ТАСС. URL: https://tass.ru/politika/4523253 (Дата обращения 04.04.2023)
41. Решение Совета коллективной безопасности Организации Договора о коллективной безопасности О Программе совместных действий по формированию системы информационной безопасности государств-членов Организации Договора о коллективной безопасности (Принято в г. Москве 05.09.2008) // Conventions. URL: https://www.conventions.ru/int/4329/ (Дата обращения 19.04.2023)
42. Решение о Стратегии обеспечения информационной безопасности государств - участников Содружества Независимых Государств (Москва, 25 октября 2019) // Intermedia. URL: https://www.intermedia.ru/uploads/72b6a0.pdf (Дата обращения 29.03.2023)

43. Россия стала сопредседателем механизма форума АСЕАН по информационной безопасности. // ТАСС. URL: https://tass.ru/politika/12078021 (Дата обращения 20.04.2023)
44. СВМДА преобразуется в международную организацию // ТАСС. URL: https://tass.ru/mezhdunarodnaya-panorama/16040685. (Дата обращения 02.04.2023)
45. Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия. 17 июня 2003 г. // официальные сетевые ресурсы Президента России. URL: http://kremlin.ru/supplement/1479 (Дата обращения 27.04.2023)
46. Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. // Электронный фонд правовых и нормативно - технических документов. URL: https://docs.cntd.ru/document/902289626 (Дата обращения 07.04.2023)
47. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности // Электронный фонд правовых и нормативных документов. URL: https://docs.cntd.ru/document/420278452 (Дата обращения 29.03.2023)
48. Соглашение о сотрудничестве государств-членов организации договора о коллективной безопасности в области обеспечения информационной безопасности // Контурнорматив. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=334580 (Дата обращения 19.04.2023)
49. Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года 18.10.2016. // Организация Договора о коллективной безопасности. URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopas

nosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/#loaded (Дата обращения 19.04.2023)

50. Указ Президента РФ от 25.01.2023 N 35 "О внесении изменений в Основы государственной культурной политики, утвержденные Указом Президента Российской Федерации от 24 декабря 2014 г. N 808" // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_438209/ (Дата обращения 12.03.2023)
51. Указ Президента РФ от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // Официальные сетевые ресурсы Президента России. URL: http://www.kremlin.ru/acts/bank/41451 (Дата обращения 23.02.2023)
52. Указ Президента РФ от 31.12.2015 N 683 "О Стратегии национальной безопасности Российской Федерации" // RG.RU. URL: https://rg.ru/documents/2015/12/31/nac-bezopasnost-site-dok.html (Дата обращения 01.03.2023)
53. Указ Президента Российской Федерации от 02.07.2021 г. № 400 “О Стратегии национальной безопасности Российской Федерации” // Официальные сетевые ресурсы Президента России. URL: http://www.kremlin.ru/acts/bank/47046 (Дата обращения 07.03.2023)
54. Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 “ Основы государственной политики Российской Федерации в области международной информационной безопасности” // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/603255343 (Дата обращения 06.03.2023)
55. Указ Президента Российской Федерации от 31 марта 2023 года № 229 "Об утверждении Концепции внешней политики Российской Федерации". // Официальные сетевые ресурсы Президента Российской Федерации. Режим доступа: http://kremlin.ru/events/president/news/70811 (Дата обращения 16.04.2023)

56. Указ Президента Российской Федерации от 5 декабря 2016 г. №646 “Доктрина информационной безопасности Российской Федерации” // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/420384668?marker=6560IO (Дата обращения 05.03.2023)
57. Устав Организации Договора о коллективной безопасности от 7 октября 2002 года. // Организация Договора о коллективной безопасности. URL: https://odkb-csto.org/documents/documents/ustav_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_/#loaded (Дата обращения 19.04.2023)
58. Уфимская декларация (Уфа, Российская Федерация, 9 июля 2015 года) // Официальный сайт Президента РФ. URL: http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf (Дата обращения 04.04.2023)
59. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_220885 (Дата обращения 5.05.2023)
60. Форталезская Декларация (принята по итогам шестого саммита БРИКС) г.Форталеза, Бразилия, 15 июля 2014 года // Официальный сайт Президента РФ. URL: http://static.kremlin.ru/media/events/files/41d4f1dd6741763252a8.pdf (Дата обращения 04.04.2023)
61. Число кибератак на госучреждения России в 2022 году выросло на четверть. // ТАСС. URL: https://tass.ru/ekonomika/16981635 (Дата обращения 12.03.2023)
62. Этеквинская декларация и Этеквинский план действий // Официальные сетевые ресурсы Президента России. URL:http://www.kremlin.ru/supplement/1430 (Дата обращения 10.04.2023)

Литература

1. Abdyraeva C. “Cyber Warfare.” The Use of Cyberspace in the Context of Hybrid Warfare.: Means, Challenges and Trends. / C. Abdyraeva // OIIP - Austrian Institute for International Affairs - 2020 - P. 36

2. Baezner M. Hotspot Analysis: Cyber-conflict between the United States of America and Russia / M. Baezner, P. Robin // Risk and Resilience Team Center for Security Studies, ETH Zürich. - 2017. Version 1 - P.26

3. Belles J. Key Points from the US National Cybersecurity Strategy 2023. / J. Belles. // Thales URL: https://cpl.thalesgroup.com/blog/encryption/us-cybersecurity-strategy-key-points-2023 (Дата обращеня 27.04.2023)

4. De Alcantara B.T. SCO and Cybersecurity: Eastern Security Vision for Cyberspace./ de Alcantara B.T. //International Relations and Diplomacy - 201. Vol. 6. № 10. - P. 549-555

5. Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government // The White House. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (Дата обращения 13.04.2023)

6. Jensen E.T. The Tallinn Manual 2.0: Highlights and insights./ E.T. Jensen // Georgetown Journal of International law. - 2017 - vol. 48 - P. 735 - 778.

7. Jindal D. Cyber in BRICS: Agendas & Undercurrents for BRICS Summit 2022 / D. Jindal // Center for air power studies. URL : https://capsindia.org/cyber-in-brics-agendas-undercurrents-for-brics-summit-2022/ (Дата обращения 12.04.2023)

8. Kaspar L. Cyber norms in nyc: takeaways from the OEWG meeting and UNIDIR cyber stability conference./ L. Kaspar, H. Sheetal.// Global Partners Digital. URL: https://www.gp-digital.org/cyber-norms-in-nyc-takeaways-from-the-oewg-meeting-and-unidir-cyber-stability-conference/ (Дата обращения 17.04.2023)

9. Kaylan M. Kremlin values: Putin’s Strategic Conservatism./ M. Kaylan. // World Affairs - 2014 vol. 177, № 1 - P. 9–17. URL: http://www.jstor.org/stable/43555061. (Дата обращения 12.03.2023)
10. Kollars N. Schneider J. Defending forward: The 2018 Cyber Strategy is here. / N. Kollars, J. Schneider // War on the rocks. URL: https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/ (Дата обращения 19.04.2023)
11. Lin H. Where the New National Cybersecurity Strategy Differs From Past Practice/ H. Lin. URL: https://www.lawfareblog.com/where-new-national-cybersecurity-strategy-differs-past-practice (Дата обращения 08.05.2023)
12. Lonergan E.D. Schneider J. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation. / E.D. Lonergan, J. Schneider // Journal of Cybersecurity - 2023. Volume 9, Issue 1 - P. 1 - 10.
13. Meakins J. Living in (Digital) Denial: Russia’s Approach to Cyber Deterrence. / J. Meakins // European Leadership Network // JSTOR. URL: http://www.jstor.org/stable/resrep22130 (Дата обращения 09.04.2023)
14. Molander R. C., Riddile A. S., & Wilson P. A. Strategic Information Warfare: A New Face of War. / R.C. Molander, A.S. Riddile, P.A. Wilson. // RAND Corporation. URL : http://www.jstor.org/stable/10.7249/mr661osd (Дата обращения 03.03.2023)
15. Newman L.H. Hacker Lexicon: What Is the Attribution Problem? / L.H. Newman. // Wired. URL: https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/ (Дата обращения 09.05.2023)
16. OEWG Agrees on Modalities for Multistakeholder Participation After Silent Procedure. URL: https://letstalkcyber.org/news/oewg-agrees-on-modalities-for-multistakeholder-participation-after-silent-procedure (Дата обращения 17.04.2023)

17. Oladimeji S. Kerner S.M. SolarWinds hack explained: Everything you need to know / S. Oladimeji, S.M. Kerner // Whats.com. URL: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (Дата обращения 11.04.2023)
18. Ottis R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. / R. Ottis // Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Режим доступа: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (Дата обращения 02.04.2023)
19. Russia's "Draft Convention on International Information Security". A Commentary. // Conflict Studies Research Centre — 2012. URL: http://www.conflictstudies.co.uk/files/20120426_CSRC_IISI_Commentary.pdf (Дата обращения 13.04.2023)
20. Schatz D. Bashroush R. Wall J. Towards a More Representative Definition of Cyber Security. / D. Schatz, R. Bashroush, J. Wall // Journal of Digital Forensics, Security and Law. - 2017 Vol. 12: No. 2, Article 8. - P. 53 - 74
21. Schmitt M. The Sixth United Nations GGE and International Law in Cyberspace. / M. Schmitt // Just Security. URL: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ (Дата обращения 25.03.2023)
22. Simons G. The Evolution of Regime Change and Information Warfare in the 21st Century. / G.Simons // Journal of International Analytics. - 2020;11(4) - P. 72-90.
23. Stadnik I. What Is an International Cybersecurity Regime and How We Can Achieve It? / I. Stadnik // Masaryk University Journal of Law and Technology. - 2017 - 11(1):129 -P. 129 - 154
24. Stahl W.M. Кибербезопасность и международное право. / W.M. Stahl. // Международное право. URL: https://interlaws.ru/kiberbezopasnost-i-mezhdunarodnoe-pravo/ (Дата обращения 17.05.2023)

25. Sullivan L. US-Russia Cybersecurity Cooperation: Future Paths and Historical Perspective / L. Sullivan // Geohistory. URL: https://geohistory.today/us-russia-cybersecurity-cooperation/#Bilateral_Efforts (Дата обращения 17.04.2023)
26. The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2 / J. B. Goodwin III [et al.]. - EastWest Institute Policy Report Series. - 2014. - P. 76
27. The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. URL: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased (Дата обращения 16.04.2023)
28. Thiessen M. A. Trump confirms, in an interview, a U.S. cyberattack on Russia. / M.A. Thiessen // The Washington Post. URL: https://www.washingtonpost.com/opinions/2020/07/10/trump-confirms-an-interview-us-cyberattack-russia/ (Дата обращения 15.04.2023)
29. Tiirmaa-Klaar H. The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body. / H.Tiirmaa-Klaar // Hague Centre for Strategic Studies — 2021. - P. 3-14. URL: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf (Дата обращения 01.04.2023)
30. Weber V. The Dangers of a New Russian Proposal for a UN Convention on International Information Security/ V. Weber // Council on Foreign Relations. URL: https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security (Дата обращения 10.04.2023)
31. Абдусаламов Р.А. К вопросу о совершенствовании доктринальных положений в области обеспечения информационной безопасности./ Р.А. Абдусаламов, Л.В. Магдилова, Д.А. Рагимханова.// Юридический вестник ДГУ. — 2017. — Т 24. — № 4 — С. 165-169

32. Арчаков В.Ю. О теоретико-методологических подходах к обеспечению международной информационной безопасности. / Ю.В. Арчаков // Журнал международного права и международных отношений. - 2019. № 3-4 (90-91). - С. 3—11.
33. Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее / С.М. Бойко // Международная жизнь. — 2016 — № 8. URL: https://interaffairs.ru/jauthor/material/1718 (Дата обращения 13.03.2023)
34. Бойко С.М. Проблематика международной информационной безопасности на площадках ШОС и БРИКС / С.М. Бойко // Международная жизнь. URL: https://interaffairs.ru/news/show/21480 (Дата обращения 26.03.2023)
35. Бондуровский В.В. Модельное законодательство СНГ и ОДКБ в сфере противодействия международному терроризму: состояние и направления совершенствования / В.В. Бондуровский // Евразийская интеграция: экономика, право, политика. 2016. №1 (19). URL: https://cyberleninka.ru/article/n/modelnoe-zakonodatelstvo-sng-i-odkb-v-sfere-protivodeystviya-mezhdunarodnomu-terrorizmu-sostoyanie-i-napravleniya (дата обращения: 11.05.2023).
36. Буранов Н. Принципиальной новые войска / Н. Буранов. // ЭКСПЕРТ. URL: https://expert.ru/2017/03/1/kibervojna/ (Дата обращения 04.05.2023)
37. Ваничкина А.С. Концептуальная парадигма дискурса информационной безопасности.// А.С. Ваничкина Материалы IV Международной научной конференции. Москва, 2021. — 2021 — С. 209 - 2013.
38. Горян Э.В. Сотрудничество России и АСЕАН в сфере кибербезопасности: промежуточные результаты и перспективы дальнейшего развития/ Э.В. Горян // Вопросы безопасности. 2018. №6. URL: https://cyberleninka.ru/article/n/sotrudnichestvo-rossii-i-asean-v-sfere-kiberbezopa

snosti-promezhutochnye-rezultaty-i-perspektivy-dalneyshego-razvitiya (дата обращения: 12.05.2023).

39. Грищенко В.В. Доктрина информационной безопасности Российской Федерации: Сущность, современное значение и организационно-правовые основы. Административное/ В.В. Грищенко.// Административное право и административный процесс. — 2017 — № 1— С. 78-88

40. Данельян А.А., Гуляева Е.Е. Международно-правовые аспекты кибербезопасности. / А.А. Данельян, Е.Е. Гуляева // Московский журнал международного права. - 2020. - С. 44-53

41. Дубень А. К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению / А. К. Дубень // Международное право и международные организации. – 2022. – № 1. – С. 24-33.

42. Егоров И. Совбез РФ: Соединенные Штаты в очередной раз доказали, что им верить нельзя. / И. Егоров // Российская Газета. URL: https://rg.ru/2022/04/07/sovbez-rf-soedinennye-shtaty-v-ocherednoj-raz-dokazali-chto-im-verit-nelzia.html (Дата обращения 01.05.2023)

43. Зиновьева Е. С., Яникеева И. О. Эволюция взаимодействия России и США в области международной информационной безопасности в исторической ретроспективе / Е.С. Зиновьева, И.О. Яникеева // Вестник Санкт-Петербургского университета. Международные отношения. - 2022. Т. Вып. 2. - С. 158–173.

44. Зиновьева Е.С. Анализ внешнеполитических инициатив России в области международной информационной безопасности. / Е.С. Зиновьева // Вестник МГИМО университета - 2014. - С.47-52.

45. Зиновьева Е.С. Международная информационная безопасность в двусторонних отношениях России и США. / Е.С. Зиновьева // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-v-dvustoronnikh-otnosheniyakh-rossii-i-ssha/ (Дата обращения 12.04.2023)

46. Казарин О.В. Скиба В.Ю. Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности / О.В. Казарин, Ю.В. Скиба, Р.А. Шаряпов // История и архивы. 2016. №1 (3). URL: https://cyberleninka.ru/article/n/novye-raznovidnosti-ugroz-mezhdunarodnoy-informatsionnoy-bezopasnosti (дата обращения: 17.05.2023).
47. Казарин О.В. Шаряпов Р.А. Ященко В.В. Многофакторная классификация угроз информационной безопасности киберфизических систем / О.В. Казарин, Р.А. Шаряпов, В.В. Ященко // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». -2018. № 1 (1). - С. 39–55.
48. Капустин А.Я. Угрозы международной информационной безопасности: формирование концептуальных подходов / А.Я. Капустин // Журнал российского права. - 2015. №8 (224). URL: https://cyberleninka.ru/article/n/ugrozy-mezhdunarodnoy-informatsionnoy-bezopasnosti-formirovanie-kontseptualnyh-podhodov (дата обращения: 17.05.2023).
49. Карасев П.А. Эволюция национальных подходов к ведению кибервойны / П.А. Карасев // Международная аналитика. – 2022. – Том 13 (2). – С. 79–94.
50. Киреева О. С. Проблема обеспечения информационной безопасности на евразийском пространстве (на примере ОДКБ) / О. С. Киреева // Евразийство: теоретический потенциал и практические приложения. – 2020. – № 10. – С. 158-162.
51. Костенко Н.И. Международная информационная безопасность в рамках международного права (методология, теория)./ Н.И. Костенко// Российский журнал правовых исследований. — 2018. — № 4. (17) — С. 9-16
52. Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира/ М.М. Кучерявый // Управленческое консультирование — 2014 г. — № 9 — С. 7-13

53. Лебедева Е.В. Информационная безопасность государств СНГ: этапы реализации. / Е.В. Лебедева // Национальная безопасность / nota bene. - 2016. - № 4. - С. 500-508.
54. Лобанова О.С. О продвижении Российских подходов по международной информационной безопасности на профильных региональных площадках./ О.С. Лобанова // Сборник докладов участников XVI международного форума. Партнерство государства, бизнеса и гражданского общества при обеспечении международной безопасности. (19 - 22 сентября 2022 г. Москва) / Национальная ассоциация международной информационной безопасности - С. 154 - 156
55. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века / С. И. Макаренко. – Санкт-Петербург : Издательство «Наукоемкие технологии» - 2017. – 546 с.
56. Международная безопасность в среде информационно-коммуникационных технологий : Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / А. А. Стрельцов, А. Я. Капустин, Т. А. Полякова [и др.] ; Национальная Ассоциация международной информационной безопасности. – Москва : НАМИБ, 2023. – 132 с.
57. Международная информационная безопасность: подходы России / А.В.Крутских, Е.А.Зиновьева, В.И.Булва, М.Б.Алборова, Ю.А.Юдина; под ред. А.В.Крутских, Е.С.Зиновьева. — Москва, 2021. — 48 с.
58. Меньшиков П.В. Актуальные аспекты обеспечения информационного суверенитета России. / П.В. Меньшиков // Международные коммуникации — 2018. — 20 марта. №5. URL: https://intcom-mgimo.ru/2017/2017-05/information-sovereignty-of-russia (Дата обращения 15.05.2023)
59. Муратшина К.Г. К вопросу о сотрудничестве в области информационной безопасности в рамках БРИКС/ К.Г. Мурташина. // Гуманитарное знание и искусственный интеллект: стратегии и инновации :

4-й молодежный конвент УрФУ : материалы международной конференции 26 марта 2020 года. — Екатеринбург : Изд во Урал. ун та, 2020. — С. 614-621.
60. Ромашкина Н.П. Проблема международной информационной безопасности в ООН. / Н.П. Ромашкина // Мировая экономика и международные отношения — 2020 — т. 64, № 12 — с. 25-32
61. Себекин С.А. Как Россия будет защищаться от информационных угроз. / С.А. Себекин // РСМД. Режим доступа : https://russiancouncil.ru/blogs/s-sebekin/kak-rossiya-budet-zashchishchatsya-ot-informatsionnykh-ugroz/?sphrase_id=84549522 (Дата обращения 06.03.2023)
62. Себекин С. А. Роль частного сектора в процессе построения МИБ на полях ООН, ШОС и БРИКС / С.А. Себекин // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/rol-chastnogo-sektora-v-protsesse-postroeniya-mib-na-polyakh-oon-shos-i-briks/ (Дата обращения 19.04.2023)
63. Сидорова Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН. / Т.Ю. Сидорова // Сибирский юридический вестник. - 2020 - № 3 (90). - С 103-108.
64. Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры. / М.В. Смекалова // Вестн. Моск. ун-та. Сер. 25: Международные отношения и мировая политика. - 2019. № 1. - С. 47-69.
65. Стрельцов А.А. Смирнов А.И. Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям / А.А. Стрельцов, А.И. Смирнов // Международная жизнь. URL: https://interaffairs.ru/jauthor/material/1940 (Дата обращения 19.05.2023)
66. Терехов А. Н., Ткаченко С. Л. Политическая экономия информационно-коммуникационных технологий: место России на глобальном рынке / А. Н . Терехов, С. Л. Ткаченко // Нац. исслед. ун-т

«Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2019. — С. 191 - 249

67. Толстухина А. Мы не должны играть в безумства на взрывоопасном информационном поле./ А. Толстухина // Международная жизнь. URL : https://interaffairs.ru/news/show/17460 (Дата обращения 27.03.2023)

68. Храмцова А.А. ОДКБ и современные вызовы безопасности. / А.А. Храмцова. // сборник материалов VII Международной научно-практической конференции. Биробиджан, 30 апреля 2022 г. - С. 159-167.

69. Черненко Е. На виртуальном фронте всё стабильно / Е. Черненко. // Коммерсант. URL: https://www.kommersant.ru/doc/5861336 (Дата обращения 01.05.2023)

70. Шакиров. О. И. Взаимное предостережение: чем закончилась короткая киберразрядка между Россией и США. / О.И. Шакиров /// РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/vzaimnoe-predosterezhenie-chem-zakonchilas-korotkaya-kiberrazryadka-mezhdu-rossiey-i-ssha/?sphrase_id=96227596 (Дата обращения 08.03.2023)

71. Шакиров О. И. Киберпереговоры с участием всех заинтересованных сторон./ О.И Шакиров// РСМД. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/kiberperegovory-s-uchastiem-vsekh-zainteresovannykh-storon/?sphrase_id=96227596 (Дата обращения 09.03.2023)

72. Шакиров О.И. Киберсаммит Путина и Байдена. / О.И. Шакиров // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kibersammit-putina-i-baydena/ (Дата обращения 13.05.2023)

73. Шакиров О.И. Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве / О.И. Шакиров // Международная аналитика. – 2020. – Том 11 (4). – С. 147–170

74. Шакиров О.И. Широкий киберконсенсус. / О.И Шакиров // РСМД. URL:

https://russiancouncil.ru/analytics-and-comments/analytics/shirokiy-kiberkonsensus/ (Дата обращения 27.03.2023)

75. Шариков П.А. Степанова Н.В. Подходы США, ЕС и России к проблеме информационной политики./ П.А. Шариков, Н.В. Степанова // Современная Европа — 2019. — № 2. — С. 73 - 83.

76. Ющенко В.А. Международная информационная безопасность: общая характеристика и Российский подход к изучению. / В.А. Ющенко // Русская политология. - 2018. № 4 (9) - С. 55 - 61

77. Яникеева И.О Российско-американские отношения в сфере обеспечения международной информационной безопасности / И.О. Яникеева // Мировая политика. 2022. №4. URL: https://cyberleninka.ru/article/n/rossiysko-amerikanskie-otnosheniya-v-sfere-obespecheniya-mezhdunarodnoy-informatsionnoy-bezopasnosti (дата обращения: 23.05.2023)