УДК 327
ББК 66.4
И74

«Информационная безопасность: влияние пандемии COVID-19» :
И74 сборник докладов международной научной конференции (Москва, 20 мая 2021 г.) / под редакцией Е. С. Зиновьевой ; Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Центр международной информационной безопасности и научно-технического сотрудничества. — Москва : МГИМО–Университет, 2021. — 340, [1] с.

ISBN 978-5-9228-2468-2

В сборнике представлены доклады участников международной научной конференции «Информационная безопасность: влияние пандемии COVID-19», проходившей в МГИМО МИД России 20 мая 2021 года. Пандемия COVID-19 способствовала форсированной цифровизации общества и вывела на передний план глобальной повестки дня угрозы информационной безопасности, которые нуждаются в согласованных ответах со стороны мирового сообщества. В докладах освещаются основные направления международного сотрудничества в сфере информационной безопасности с учетом интересов и внешнеполитических приоритетов Российской Федерации.

Для специалистов в области международных отношений и широкого круга читателей, интересующихся вопросами информационной безопасности.

УДК 327
ББК 66.4

ISBN 978-5-9228-2468-2

СОДЕРЖАНИЕ

СЕКЦИЯ 1
«ПРАВИЛА ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ»

Предисловие

20 мая 2021 года в МГИМО МИД России прошла международная научная конференция «Информационная безопасность в условиях пандемии COVID-19». Конференция была ориентирована на академическое сопровождение внешней политики и международного сотрудничества Российской Федерации в сфере информационной безопасности, а также ставила своей задачей расширение тематики научных исследований в данной области.

Пандемия COVID-19 способствовала форсированному переводу в цифровую сферу многих аспектов повседневной деятельности и вывела на передний план глобальной повестки дня угрозы информационной безопасности, которые нуждаются в согласованных ответах со стороны мирового сообщества.

Представленные в настоящем издании доклады посвящены основным направлениям международного сотрудничества в сфере информационной безопасности с учетом интересов и внешнеполитических приоритетов Российской Федерации и тематически структурированы в рамках следующих пяти подразделов, соответствующих названиям секций конференции:

— пленарная сессия: «Глобальные проблемы информационной безопасности и внешнеполитические инициативы России»;
— секция 1: «Выработка правил ответственного поведения государств в глобальном информационном пространстве»;
— секция 2: «Содействие преодолению цифрового разрыва и наращиванию потенциала по защите национального киберпространства»;
— секция 3: «Применимость норм международного права к информационному пространству»;
— секция 4: «Обеспечение кибербезопасности индустрии 4.0: роль бизнеса».

Важность, своевременность и актуальность темы конференции обусловлена принятием 12 апреля 2021 года Указом Президента Российской Федерации новой редакции документа стратегического планирования в сфере информационной безопасности — «Основ государственной политики Российской Федерации в области международной информационной безопасности». Ключевым направлениям реализации задач, поставленных в данном документе, посвятили свои выступления участники пленарной сессии конференции. В рамках тематических секций участники дискуссии осветили различные подходы к реализации практических шагов в сфере укрепления международного сотрудничества в сфере информационной безопасности на площадке ООН и региональных организаций, в том числе путем выработки мер доверия на международном уровне, представили различные концептуальные взгляды на природу угроз международной информационной безопасности, охарактеризовали роль бизнес-структур в укреплении информационной безопасности и возможные направления расширения их участия в международном сотрудничестве и внешней политике России на данном направлении, а также рассмотрели важнейшую проблему применимости международного права к информационной сфере и обсудили возможные направления его адаптации с учетом особенностей ИКТ-среды.

Е. С. Зиновьева, доктор политических наук,
профессор кафедры мировых политических процессов,
заместитель директора Центра
международной информационной безопасности
и научно-технологической политики МГИМО МИД России,
модератор пленарной сессии и секции 2 конференции
«Информационная безопасность: влияние пандемии COVID-19»

ПЛЕНАРНАЯ СЕССИЯ

«ГЛОБАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕЖДУНАРОДНЫЕ ИНИЦИАТИВЫ РОССИЙСКОЙ ФЕДЕРАЦИИ»

А. В. Торкунов,
академик РАН, ректор МГИМО МИД России

ПЕРЕДОВОЙ ОПЫТ НАУЧНОЙ И УЧЕБНО-МЕТОДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ МГИМО МИД РОССИИ В СФЕРЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: в докладе охарактеризованы основные направления научно-исследовательской и учебно-методической деятельности МГИМО МИД России в области международной информационной безопасности.

Ключевые слова: информационная безопасность, международная информационная безопасность, научно-педагогическая работа.

XXI век стал эпохой стремительного развития информационно-коммуникационных технологий. Процессы повсеместной цифровизации получили дополнительный импульс под влиянием пандемии коронавируса. Пандемия ускорила цифровой переход во всех сферах общественных отношений. Мы это ощутили и на своем уровне, когда весь образовательный процесс пришлось переносить в онлайн-среду. МГИМО с успехом справился с новыми вызовами, и качество образовательного процесса не только не пострадало, но и повысилось благодаря новым цифровым инструментам обучения.

Однако, помимо несомненных выгод и новых возможностей, повсеместная цифровизация порождает и угрозы международной информационной безопасности. С сожалением должен отметить, что глобальное цифровое пространство становится ареной для межгосударственной конкуренции и конфликтов, активно действуют в нем преступные и террористические группировки. Значимость проблемы международной информацион-

ной безопасности подтверждается статистическими данными. По данным ВЭФ, к концу 2021 года потери мировой экономики от кибератак могут достичь 6 трлн долл.[1] Международная информационная безопасность является стратегическим вызовом глобального масштаба, который может быть разрешен только коллективными усилиями всего международного сообщества. Развитие новых технологий, таких как «интернет вещей», машинное обучение и технологии искусственного интеллекта, блокчейн-технологии и ряд других, способствует появлению дополнительных рисков.

Россия является активным участником глобальной кибердипломатии. Наша страна ориентирует международное сообщество на выработку четких правил поведения в глобальном информационном пространстве, направленных на незыблемость государственного суверенитета, предупреждение конфликтов с использованием информационно-коммуникационных технологий, уважение Устава ООН и мирное развитие технологий в интересах всего мирового сообщества.

Мне особенно приятно отметить, что МГИМО МИД России первым из российских гуманитарных вузов активно включился в научную и педагогическую работу на данном направлении. В структуре МГИМО действует Центр международной информационной безопасности и научно-технологической политики, который занимается профильными исследованиями. Данный центр является единственным в России, занимающимся на системной основе изучением и преподаванием в сфере международно-политических аспектов информационной безопасности. Результатом научной работы стала публикация серии научных статей и монографий, которые получили признание в академическом сообществе. Сотрудники МГИМО также принимают

[1] World Economic Forum Global Risks Report 2021. 16th edition. URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (дата обращения: 11.05.2021).

участие в работе межведомственных делегаций на переговорах в области обеспечения информационной безопасности, реализуемых по инициативе МИД России, и, таким образом, вносят весомый вклад в академическую дипломатию на данном направлении.

Активно ведется образовательная работа. В МГИМО на различных уровнях образования (бакалавриат, магистратура, аспирантура и программы повышения квалификации) включены учебные дисциплины по проблемам международной информационной безопасности. Соответствующие компетенции востребованы сегодня не только на дипломатической службе, но и в различных федеральных органах исполнительной власти, силовых структурах, а также в рамках бизнес-структур, некоммерческих организаций. Важным вкладом в подготовку профессиональных кадров стала публикация в 2019 году учебника в трех томах под редакцией А. В. Крутских «Международная информационная безопасность: теория и практика», который был переиздан в 2021 году[2]. Учебник стал первым в мире комплексным изданием по данной теме и представляет собой фактически ее научную онтологию.

Кроме того, на площадке МГИМО на регулярной основе проходят конференции, форумы, семинары и круглые столы, в ходе которых обсуждаются всевозможные аспекты цифровой повестки с учетом перспективных направлений технологического развития и современных трансформаций международной системы. Подобный обмен мнениями способствует формированию комплексного представления о перспективных направлениях внутренней политики и взаимодействия на международном уровне в сфере информационной безопасности.

---

[2] Международная информационная безопасность. Теория и практика. В трех томах. Том 2. Учебник для вузов / Под общ. ред. А. В. Крутских. — 2-е изд., перераб. и доп. — М.: Аспект Пресс, 2021. — 384 с.

Подводя итог выступлению, хочу отметить, что под влиянием пандемии коронавируса проблемы информационной безопасности обострились. Можно сказать, что мы столкнулись с «киберпандемией», которая проявляется не только в виде посягательства на частную жизнь рядовых граждан. Глубокую озабоченность вызывают акты кибертерроризма, зафиксированный в период эпидемии рост количества «нападений» на объекты здравоохранения, финансовые, образовательные структуры, международные организации. Однако, в отличие от пандемии коронавируса, киберпандемию остановить вакциной невозможно. Тем не менее международное сообщество может и должно строить и укреплять глобальную систему иммунитета против «киберпандемии». И важнейший вклад в формирование международного режима информационной безопасности вносит кибердипломатия Российской Федерации. МГИМО же играет существенную роль в подготовке кадров на данном направлении и в научном сопровождении дипломатии. Мы будем и далее наращивать свой потенциал в данной области в соответствии с решением Президента, воплощенным в «Основах государственной политики в области международной информационной безопасности»[3].

Список использованных источников и литературы

1. Основы государственной политики Российской Федерации в области международной информационной безопасности // утв. Указом Президента Российской Федерации от 12 апреля 2021 года № 213. — URL: http://www.publication.pravo.gov.ru/Document/View/0001202104120050/ (дата обращения: 11.05.2021).

[3] Основы государственной политики Российской Федерации в области международной информационной безопасности // утв. Указом Президента Российской Федерации от 12 апреля 2021 года № 213. — URL: http://www.publication.pravo.gov.ru/Document/View/0001202104120050/ (дата обращения: 11.05.2021).

2. Международная информационная безопасность. Теория и практика. В трех томах. Том 2. Учебник для вузов / Под общ. ред. А. В. Крутских. — 2-е изд., перераб. и доп. — М.: Аспект Пресс, 2021.— 384 с.
3. World Economic Forum Global Risks Report 2021. 16th edition. URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (дата обращения: 11.05.2021).

С. М. Бойко,
канд. ист. наук, начальник Департамента
проблем безопасности в информационной сфере
аппарата Совета Безопасности Российской Федерации

ГОСУДАРСТВЕННАЯ ПОЛИТИКА РОССИИ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРЕЕМСТВЕННОСТЬ КУРСА, ПРИВЕРЖЕННОСТЬ ЦЕЛИ

Аннотация: в статье рассматриваются новые основные направления государственной политики Российской Федерации в области международной информационной безопасности, а также подходы к формированию глобальной системы обеспечения международной информационной безопасности.

Ключевые слова: государственная политика, международная информационная безопасность, система обеспечения международной информационной безопасности, угрозы международной информационной безопасности, межгосударственное сотрудничество, механизмы межгосударственного взаимодействия.

12 апреля 2021 года Указом Президента Российской Федерации № 213 были утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности[4].

Основы, как документ стратегического планирования, отражают официальные взгляды на сущность международной

[4] Основы государственной политики Российской Федерации в области международной информационной безопасности / утв. Указом Президента Российской Федерации от 12 апреля 2021 года № 213. — URL: http://www.publication.pravo.gov.ru/Document/View/0001202104120050/ (дата обращения: 11.05.2021).

информационной безопасности. В них дано обновленное определение этого базового понятия, которое содержит ключевые подходы, положенные в основу формирования позиции государства в указанной области.

Во-первых, это приоритет общепризнанных принципов и норм международного права в глобальном информационном пространстве с учетом специфики информационно-коммуникационных технологий (далее — ИКТ).

Во-вторых, равноправное партнерство государств мирового сообщества вне зависимости от уровня их информатизации и развития информационной инфраструктуры. А также вовлечение в решение задач обеспечения международной информационной безопасности наряду с государственными структурами всех заинтересованных сторон — научного и экспертного сообщества, неправительственных организаций, деловых кругов.

И, в-третьих, поддержание международного мира, безопасности и стабильности в информационной сфере.

Как отметил 26 марта 2021 года на заседании Совета Безопасности Российской Федерации Президент Российской Федерации В. В. Путин, новые Основы сохранили преемственность нашего стратегического курса на предотвращение конфликтов в информационном пространстве[5].

В документе подтверждена приверженность ранее заявленной цели государственной политики — содействие формированию с учетом национальных интересов России системы обеспечения международной информационной безопасности.

Необходимость формирования такой системы обусловлена потребностью в противодействии стремительно нарастающим угрозам в информационной сфере.

---

[5] Выступление Президента Российской Федерации В. В. Путина на заседании Совета Безопасности 26 марта 2021 года. — URL: http://www.kremlin.ru/events/president/news/65231/ (дата обращения: 11.05.2021).

Новые Основы дают расширенный по сравнению с аналогичным документом 2013 года перечень основных угроз международной информационной безопасности. При этом, ключевые из этих угроз, составляющую так называемую «триаду», остаются неизменными[6].

Прежде всего, это относится к угрозам использования ИКТ в военно-политических и иных сферах в целях осуществления в глобальном информационном пространстве действий, препятствующих поддержанию международного мира, безопасности и стабильности.

Большое внимание в документе уделяется угрозам использования данных технологий в террористических и экстремистских целях, а также для вмешательства во внутренние дела суверенных государств.

Наряду с сохранением традиционных угроз совершения преступлений в сфере компьютерной информации в новых Основах впервые актуализируются нарастающие угрозы использования ИКТ для совершения различных видов мошенничества. В период пандемии COVID-19 это стало особенно очевидным.

Также впервые в качестве одних из основных угроз международной информационной безопасности представлены угрозы использования ИКТ для проведения компьютерных атак на информационные ресурсы государств.

Особое внимание в Основах уделено угрозам использования отдельными государствами технологического доминирования в глобальном информационном пространстве. Раскрыты истинные цели такого доминирования. Это — монополизация рынка ИКТ, ограничение доступа других государств к передовым технологиям, усиление их технологической зависимости от

[6] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года / утв. Президентом Российской Федерации 24 июля 2013 года, № Пр-1753. — URL: https://www.garant.ru/products/ipo/prime/doc/70541072/ (дата обращения: 11.05.2021).

доминирующих в сфере информатизации государств, а также сохранение информационного неравенства между развитыми и развивающимися странами.

Трансграничный характер перечисленных угроз и масштабы их возможных последствий объективно свидетельствуют о невозможности противодействия им в одиночку. Данное обстоятельство диктует необходимость развития сотрудничества с нашими зарубежными партнерами на различных уровнях: глобальном, региональном, многостороннем и двустороннем.

Согласно Основам, ключевым содержанием такого сотрудничества должны стать вопросы формирования системы обеспечения международной информационной безопасности и противодействия упомянутым угрозам.

В этих целях в новом документе определены основные направления реализации государственной политики. Они конкретизируют содержание задач, решение которых позволит достичь заявленной цели.

Данные направления соответствуют стратегическим ориентирам политики России, обозначенным Президентом Российской Федерации на заседании Совета Безопасности 26 марта 2021 года.

Первый ориентир — это продвижение российских инициатив в рассматриваемой области, активизация участия в переговорном процессе, открытость для диалога и конструктивного взаимодействия со всеми партнерами.

Особое внимание должно быть уделено работе на площадке Организации Объединенных Наций и развитию сотрудничества с ближайшими партнерами России по ОДКБ, СНГ, ШОС и БРИКС.

Второй ориентир — налаживание механизмов практического сотрудничества, обмен опытом, совместное реагирование на компьютерные инциденты, подготовка кадров, проведение научных исследований.

Новые Основы нацеливают на создание различных механизмов межгосударственного взаимодействия. Это относится

к обмену информацией об угрозах использования ИКТ в террористических и экстремистских целях, а также информацией о компьютерных инцидентах. К расследованию преступлений в сфере компьютерной информации и случаев мошенничества с использованием ИКТ, к обмену методиками таких расследований и соответствующей судебной практикой.

Большое значение придается созданию механизма контроля за использованием ИКТ для предотвращения их использования в целях вмешательства во внутренние дела суверенных государств.

Впервые подчеркнута необходимость формирования механизма межгосударственного взаимодействия в интересах предотвращения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, а также обмена информацией о передовых практиках в указанной области.

Приоритетным должно стать оказание помощи ближайшим партнерам России, в том числе в построении систем информационной безопасности, в предоставлении им соответствующих технологий и технических средств, в совместном расследовании преступлений.

В Основах нашли свое отражение и другие новые векторы реализации государственной политики в рассматриваемой области, обозначенные главой государства как третий стратегический ориентир.

Это активное использование возможностей научных и экспертных кругов, делового сообщества, а также укрепление действующих и формирование новых международных дискуссионных площадок как в стране, так и за рубежом для продвижения подходов и инициатив России.

Следует признать, что эффективное решение поставленных задач возможно только при условии их серьезного научно-исследовательского, аналитического и методического обеспечения с участием российских ученых и экспертов.

Реализация основных направлений государственной политики Российской Федерации в области международной информационной безопасности потребует консолидации усилий всех заинтересованных сторон. Впереди — большая кропотливая работа.

Координация этой работы, как подчеркнул 26 марта 2021 года Президент России, будет возложена на аппарат Совета Безопасности и Министерство иностранных дел. Взаимодействие планируется организовать в форматах целевых межведомственных групп.

Таким образом, сохранив преемственность стратегического курса на предотвращение межгосударственных конфликтов в глобальном информационном пространстве и подтвердив приверженность нацеленности государства на содействие формированию системы обеспечения международной информационной безопасности, Основы 2021 года наглядно демонстрируют новые стратегические ориентиры России в столь значимой для национальной безопасности сфере.

Список использованных источников и литературы

1. Основы государственной политики Российской Федерации в области международной информационной безопасности // утв. Указом Президента Российской Федерации от 12 апреля 2021 года № 213. — URL: http://www.publication.pravo.gov.ru/Document/View/0001202104120050/ (дата обращения: 11.05.2021).
2. Выступление Президента Российской Федерации В. В. Путина на заседании Совета Безопасности 26 марта 2021 года. — URL: http://www.kremlin.ru/events/president/news/65231/ (дата обращения: 11.05.2021).
3. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года // утв. Президентом Российской Федерации 24 июля 2013 года, № Пр-1753. — URL: https://www.garant.ru/products/ipo/prime/doc/ 70541072/ (дата обращения: 11.05.2021).

Н. Н. Мурашов,
заместитель директора Национального координационного центра по компьютерным инцидентам (НКЦКИ)

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО УПОЛНОМОЧЕННЫХ ОРГАНОВ В ЦЕЛЯХ СНИЖЕНИЯ ВРЕДОНОСНОЙ ДЕЯТЕЛЬНОСТИ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Аннотация: в докладе рассмотрены основные направления деятельности НКЦКИ в сфере международного сотрудничества по обеспечению информационной безопасности.

Ключевые слова: международная информационная безопасность, международное сотрудничество, угрозы международной информационной безопасности.

Национальный координационный центр по компьютерным инцидентам (НКЦКИ) является одним из элементов Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, обеспечивающий решение практических задач по защите национального и глобального информационного пространства.

Как специалист, детально знающий, как функционирует глобальная сеть связи, я могу утверждать, что именно технологические ее особенности являются первопричиной многих проблем международной информационной безопасности, прежде всего, таких, как использование информационного пространства в криминальных и террористических целях.

Изначально разработанная для военных, интернет-технология получила коммерческое использование, что привело к изменению функционала и круга пользователей сети. Это привело к появлению новых протоколов и усилению механизмов без-

опасности, однако принцип функционирования сети остался прежним. Как и раньше, это саморегулирующаяся динамическая инфраструктура. Она развивается и поддерживается ИКТ—индустрией. Поэтому главная цель — коммерческая выгода.

А решение вопросов информационной безопасности является сложным и затратным делом, кроме того, существенно тормозит выпуск на рынок новых продуктов и услуг. Поэтому вопросы безопасности ИКТ, в том числе сети Интернет, решаются ровно в том объеме, который сохраняет привлекательность цифровой среды.

В результате, с технической точки зрения, мы имеем сеть, основанную на устаревших принципах и расположенную в многочисленных юрисдикциях инфраструктуру. Роль государств в глобальном управлении интернетом минимальна.

Все российские инициативы по укреплению международной информационной безопасности направлены на изменение текущего положения, причем в интересах всего мирового сообщества. Я хочу кратко рассказать о двух из них, поскольку принимал участие в их разработке.

Первая из них направлена на создание международно-правовых условий для пресечения использования сети в террористических целях.

Ни для кого не секрет, что террористы оперативно осваивают и используют современные средства передачи информации. С их помощью они осуществляют связь между собой и пособниками. Ситуация осложняется тем, что приложения для мобильных устройств со стойкой криптографией стали продуктом массового потребления и доступны для скачивания через интернет.

К ним относятся многочисленные мессенджеры, почтовые сервисы, средства закрытой голосовой и видеосвязи. Они распространяются посредством сети Интернет и без всякого контроля пересекают государственные границы. На мобильном устройстве такие приложения генерируют ключ шифрования для каждого сеанса связи.

Получить доступ к зашифрованной информации может только обладатель этого ключа. У провайдеров указанных услуг, как правило, есть техническая возможность получить ключ. Но они не хотят открыто оказывать содействие специальным службам и правоохранительным органам. Это можно понять: они боятся потерять доверие пользователей и, как следствие, бизнес. При этом отсутствие правового регулирования использования стойкой криптографии, не позволяет требовать выполнения национального законодательства по проведению специальных мероприятий в отношении террористов и преступников.

В результате годами выстроенная система законного перехвата информации перестает быть эффективной. Перед каждой страной стоит вопрос, как решить проблему доступа к зашифрованной информации в интересах общественной безопасности.

Возможны различные пути. Можно попытаться достичь соглашения о предоставлении ключей шифрования с каждым производителем приложений со стойкой криптографией. По такому пути пошли государства — участники разведывательного союза «Пять глаз» и обязали подконтрольные им компании предоставлять ключи шифрования или расшифрованные сообщения.

Но для подавляющего большинства стран это чрезвычайно долгий и малоперспективный путь взаимодействия с чужой правовой системой. Но, даже если его осилить, вы не получите гарантированного результата, поскольку на рынке практически постоянно появляются новые услуги, а их операторы часто меняют юрисдикцию.

Исходя из этого, Российская Федерация разработала концепцию контртеррористической инициативы, которая обеспечит всем правоохранительным органам и специальным службам законный доступ к зашифрованной информации. Цель может быть достигнута путем создания необходимых международных правовых условий для реализации процедур депонирования ключей шифрования и доступа к зашифрованной информации.

Значительных сложностей в технической реализации инициативы Россия не видит.

При разработке инициативы принимались во внимание следующие принципы:

— соблюдение прав человека;
— суверенное равенство всех стран;
— унифицированные требования.

Преимуществом предложенного Россией подхода является глобальность, универсальность, защита тайны переписки, информационная безопасность. Каждое государство сохранит контроль над своим информационным пространством и хранящейся на его территории ключевой информацией.

Сохранение суверенитета над своим национальным информационным пространством вопрос очень актуальный, но трудно разрешимый. Одной из проблем является низкая прозрачность сети. Как я уже говорил, есть различные технологические особенности, которые как будто специально сделаны для использования сети в противоправных целях. Различные инструменты анонимизации затрудняют выявление источников компьютерной атаки или другого вредоносного трафика. Отсутствуют инструменты контроля проверки подлинности источника информации и подтверждения ее целостности.

Помимо этого, активно действует «темный» и «глубокий» интернет, где процветают сайты с детской порнографией, хакерскими услугами, продажей наркотиков и оружия. Мы всем мировым сообществом боремся с этими видами преступлений, но ничего не предпринимаем для ликвидации очага их распространения. Технически это можно сделать, изменив некоторые принципы работы интернет. Задумайтесь, почему этого не происходит? Ответ очевиден, есть силы, которые намеренно поддерживают «глубокий» интернет и в этой «мутной воде» занимаются противоправными деяниями.

В этой связи я хочу привести высказывание бывшего директора ЦРУ Майкла Хэйдена:

«Глобальные телекоммуникации устроены таким образом, что мы (США) можем оказывать на них огромное влияние, так как фактически играем на своём поле. Мы должны пользоваться этим своим преимуществом. Более того, …должны защищать то, что защищает нас».

Самым ярым противником реформирования принципов функционирования сети Интернет являются США. Они боятся потерять контроль над глобальными потоками данных. Именно поэтому Вашингтон, отринув так твердо отстаиваемые правила свободного рынка, так отчаянно сопротивляются поставкам в другие страны китайских технологий для сетей связи 5G.

Напомню, что суверенное равенство является одним из базовых принципов Устава ООН. США неоднократно заявляли, что международное право, прежде всего Устав ООН, применимы к информационному пространству. Исходя из этого, Россия высказала идею, что для всех стран должны быть созданы равные условия для обеспечения своего суверенитета. Для этого прозрачность глобального информационного пространства должна быть повышена, чтобы государства могли гарантировать безопасность своих национальных сегментов сети Интернет.

Эту техническую задачу можно решать поэтапно и различными методами. Например, возможно создание единой технологически и политически нейтральной системы надежной идентификации всех устройств, подключенных к сети Интернет.

Повышение прозрачности информационного пространства позволит правоохранительным органам всех государств достоверно определять свою часть цепочки передачи информации и обмениваться ею с заинтересованными сторонами. Лакуны, где могут действовать преступники, практически исчезнут, и принцип неотвратимости наказания будет работать. Для контроля выполнения в информационном пространстве норм международного права будет создана необходимая техническая основа. Необоснованные обвинения в осуществлении компьютерных атак исчезнут сами собой, поскольку данные всегда можно

будет проверить. Истинный виновник будет обязан ответить за свои деяния.

Однако США и их ближайшие союзники не спешат обсуждать подобные инициативы. Все это показывает, что главные усилия наши оппоненты тратят на создание видимости активных действий по обеспечению международной информационной безопасности. На деле они отвлекают мировое сообщество от решения насущной и ключевой проблемы — реформирования принципов функционирования глобальной сети.

Мы отлично понимаем, что это не простая задача, поскольку сеть стала неотъемлемой частью государственного управления, экономики и жизни обычных граждан. Но приступать к осознанию необходимости ее решения необходимо.

А. В. Крутских,
д-р ист. наук, специальный представитель
Президента Российской Федерации по вопросам
международного сотрудничества
в области информационной безопасности,
директор Департамента международной информационной
безопасности МИД России

ДИПЛОМАТИЯ РОССИИ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: в докладе рассмотрены основные направления и успехи дипломатии России в области формирования международного режима информационной безопасности.

Ключевые слова: международная информационная безопасность, международное сотрудничество, внешняя политика России.

Несмотря на вызовы, с которыми столкнулось человечество под влиянием пандемии коронавирусной инфекции, переговорный процесс и международное сотрудничество, направленные на противодействие киберпандемии и поиск институциональной «кибервакцины» от актуальных угроз международной информационной безопасности, в 2020–2021 году ознаменовались рядом успехов российской дипломатии.

Россия продолжает держать курс на отстаивание национальных интересов и формирование глобальной системы информационной безопасности. Выработка правил ответственного поведения государств в информационном пространстве и недопущение возникновения в нем конфликтов являются нашими важнейшими приоритетами. В нынешних сложных условиях значительное количество государств разделяют российские инициативы и подходы в сфере международной информационной безопасности (МИБ).

Свидетельством тому явилось принятие 75-й сессией Генеральной Ассамблеи ООН российского проекта резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[7]. При поддержке подавляющего большинства государств в системе ООН будет вновь создан подлинно демократичный, инклюзивный и доступный для всех стран переговорный механизм по вопросам обеспечения МИБ — новая Рабочая группа открытого состава (РГОС) — сроком на пять лет.

В рамках деятельности новой РГОС появилась возможность учреждения специализированных подгрупп по различным аспектам ее мандата, что позволит привлекать к переговорам научное сообщество, неправительственные организации и частный бизнес, как равноправных акторов цифровой среды, и в целом активизировать процесс выработки в ней мер доверия и «правил игры».

Мандат Группы предусматривает в качестве приоритета продолжение дальнейшей выработки норм, правил и принципов ответственного поведения государств в информационном пространстве и путей их имплементации, при необходимости, внесения в них изменений или формулирования дополнительных правил поведения; рассмотрение инициатив государств, направленных на обеспечение безопасности в сфере использования ИКТ; и организацию под эгидой ООН регулярного институционального диалога с широким кругом государств-участников. Помимо этого, РГОС призвана продолжить выработку общего понимания существующих и потенциальных угроз в сфере информационной безопасности, в том числе безопасности данных, и возможных совместных мер по их предотвращению и противодействию им, а также общего понимания того, как международ-

[7] Резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» A/RES/75/240 от 31 декабря 2020 г. URL: https://undocs.org/ru/A/RES/75/240 (дата обращения: 12.08.2021)

ное право применяется к использованию ИКТ государствами, мер укрепления доверия и наращивания потенциала.

К сожалению, в условиях дефицита доверия между государствами и настойчивого желания некоторых из них использовать свои технологические преимущества для доминирования в цифровом пространстве, пока не приходится ожидать скорейшего решения вопроса о принятии международного кодекса поведения в ИКТ-среде, тем более в статусе юридического обязательства. Между тем, хотел бы напомнить, что еще в 2018 г. по инициативе России Генассамблея ООН утвердила первоначальный свод правил, норм и принципов ответственного поведения в информационном пространстве[8].

При этом необходимо, чтобы разработка любых универсальных договоренностей, а также согласование путей урегулирования имеющихся в ИКТ-сфере проблем оставались прерогативой государств, обладающих исключительным суверенитетом в данной области.

Значительные позитивные сдвиги мы наблюдаем и на треке противодействия киберпреступности. За последние два-три года эта тема стала неотъемлемой частью повестки дня многих переговорных площадок и в первую очередь ООН. Разгул киберкриминала, который наиболее ярко проявил себя в период пандемии COVID-19, затронул все без исключения страны и слои общества, представ уже глобальной проблемой, которая требует соответствующего ответа. Эта «индустрия» является высоко прибыльной, но при этом ее деяния не всегда наказуемы. Международное сотрудничество правоохранительных органов в этой сфере, мягко говоря, далеко от идеала и нуждается в серьезной международно-правовой настройке. Российские инициативы в ООН как раз реагируют на эти вызовы современности.

[8] Резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» A/73/27 от 5 декабря 2018 г. — URL: https://undocs.org/ru/A/RES/73/27 (дата обращения: 05.05.2021).

В этом году мы внесли очередной проект резолюции Генассамблеи ООН по этой теме[9]. Задачей было выработать и утвердить правила работы созданного по инициативе России и еще 46 государств Специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях, чтобы дать старт практической разработке конвенции. Мы эту задачу выполнили. Более того, если при принятии аналогичных резолюций 2018 и 2019 годов[10] ряд государств выступал категорически против обсуждения проблематики информпреступности в рамках ООН, в этом году наш документ был принят консенсусом. Два года назад мы жестко отстаивали только саму идею необходимости создания такого универсального инструмента. Сейчас же мировое сообщество спорило, как мы будем это делать, доказывая друг другу, что им эта конвенция нужна больше всех и она должна была начать работать уже вчера. Это объективная потребность и четко выраженная политическая воля государств.

Это раньше в ООН государства 10 лет обсуждали, надо ли поднимать ту или иную тему, потом 10 лет готовили первые проекты документов. У нас времени на раскачку не было. Российской дипломатии в текущей непростой политической конъюнктуре удалось чуть более чем за год создать и запустить полноценную переговорную площадку. Теперь же первую скрипку будут играть не дипломаты, а правоохранительные органы и юристы, лучшие в своем деле, которые в реальной жизни борются с киберкриминалом.

---

[9] Резолюция ГА ООН A/RES/ 75/282 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 12 мая 2021 г. — URL: https://undocs.org/ru/A/RES/75/282 (дата обращения: 05.05.2021).

[10] Резолюция ГА ООН A/RES/74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 27 декабря 2019 г. — URL: https://undocs.org/ru/A/RES/74/247 (дата обращения: 12.08.2021)

Им предстоит в сжатые сроки — за 2,5 года — разработать глобальную конвенцию в рамках Спецкомитета с участием всех заинтересованных сторон и представить её Генассамблее ООН на рассмотрение и утверждение в ходе ее 78-й сессии — в 2023 году. Для этих целей Спецкомитет проведет 7 субстантивных сессий: 4 — в Нью-Йорке, включая первую и две последние, 3 — в Вене. Первая встреча намечена на январь 2022 г. Будет очень динамичный процесс.

Россия, стоящая у истоков переговорного процесса по вопросам международной информационной безопасности и более двадцати лет формирующая основные концептуальные подходы и передовые идеи, словно камертон, уловила новые вибрации киберсферы. Мы стали инициатором создания нового алгоритма переговорного процесса по вопросам МИБ и широкая поддержка международным сообществом наших инициатив демонстрирует их своевременность и востребованность.

Список использованных источников и литературы

1. Резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» A/RES/75/240 от 31 декабря 2020 г. URL: https://undocs.org/ru/A/RES/75/240 (дата обращения: 12.08.2021)
2. Резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» A/73/27 от 5 декабря 2018 г. — URL: https://undocs.org/ru/A/RES/73/27 (дата обращения: 05.05.2021).
3. Резолюция ГА ООН A/RES/ 75/282 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 12 мая 2021 г. — URL: https://undocs.org/ru/A/RES/75/282 (дата обращения: 05.05.2021).
4. Резолюция ГА ООН A/RES/74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 27 декабря 2019 г. — URL: https://undocs.org/ru/A/RES/74/247 (дата обращения: 12.08.2021).

В. А. Шин,
канд. ист. наук, заместитель директора Департамента
международной информационной безопасности МИД России

ОСНОВНЫЕ ИТОГИ РАБОТЫ ДЕПАРТАМЕНТА МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МИД РОССИИ В 2020–2021 ГОДАХ

Аннотация: в выступлении описываются особенности структуры и деятельности Департамента международной информационной безопасности (ДМИБ) МИД России. Департамент состоит из четырех отделов, на которые возложены задачи, покрывающие все ключевые направления обеспечения международной информационной безопасности (МИБ): профильное сотрудничество в многостороннем, региональном и двустороннем форматах, противодействие использованию информационно-коммуникационных технологий (ИКТ) в преступных целях, взаимодействие по вопросам невоенных аспектов применения ИКТ.

Ключевые слова: Департамент международной информационной безопасности (ДМИБ) МИД России, международная информационная безопасность, информационно-коммуникационные технологии (ИКТ), многостороннее, региональное и двустороннее сотрудничество в сфере обеспечения МИБ, противодействие использованию ИКТ в преступных целях, невоенные аспекты использования ИКТ.

Нам еще только предстоит оценить всю глубину и масштаб тектонических, фундаментальных по своей сути изменений глобального геополитического и геоэкономического ландшафта, вызванных продолжающейся пандемией коронавирусной инфекции. Очевидно, что мир уже никогда не будет прежним. Пандемия выступила мощным катализатором и ускорителем многих разноплановых, комплексных процессов, одним из которых,

бесспорно, является тотальная цифровизация всех сфер человеческой жизнедеятельности. Оставляя за скобками размышления о том, во благо или во вред нам новая цифровая реальность, хотел бы подчеркнуть: обратной стороной происходящего является экспоненциальное нарастание рисков и угроз в информационной среде, требующих координации и реагирования, а в идеале — принятия широкого спектра упредительных мер. При этом с учетом трансграничного характера возникающих угроз особое значение приобретает международное сотрудничество в сфере обеспечения информационной безопасности.

В данном контексте чрезвычайно своевременным стало создание в декабре 2019 года в соответствии с Указом Президента Российской Федерации в структуре МИД России нового подразделения — Департамента международной информационной безопасности[11]. Появление департамента наглядно говорит о том внимании, которое руководство нашей страны уделяет вопросам обеспечения безопасности в сфере информационно-коммуникационных технологий, а также демонстрирует востребованность усилий российской дипломатии в тесной координации с другими компетентными российскими ведомствами по выработке эффективных ответов на возникающие в этой сфере вызовы и угрозы. Понятно, что при всей многоаспектности информационной безопасности в фокусе нашей деятельности — задачи продвижения российских приоритетов в сфере информбезопасности на международной арене.

Позвольте подробнее остановиться на структуре и задачах нового подразделения. Осмелюсь предположить, что ДМИБ является департаментом нового, гибридного типа, сочетающим

[11] Указ Президента Российской Федерации от 27 декабря 2019 г. № 626 «О внесении изменений в Указ Президента Российской Федерации от 11 июля 2004 г. № 865 «Вопросы Министерства иностранных дел Российской Федерации» и в Положение, утвержденное этим Указом» // Информационно-правовой портал «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/73258599/ (дата обращения: 19.05.2021).

в себе черты как территориальных, так и функциональных подразделений МИД России. Отличительной чертой ДМИБ является глобальный географический охват при одновременной четкой тематической сфокусированности.

Структурно Департамент состоит из четырех отделов, работа в которых сосредоточена на всех ключевых направлениях обеспечения МИБ.

Первый из них — отдел ООН и глобальных форумов по МИБ. Его деятельность в первую очередь сконцентрирована вокруг проблематики Первого комитета Генеральной Ассамблеи Организации Объединенных Наций — вопросов международного мира и безопасности. В рамках ООН действуют два профильных переговорных формата: Группа правительственных экспертов ООН (ГПЭ) и Рабочая группа ООН открытого состава (РГОС). На данном направлении неоспоримым успехом российской дипломатии стало принятие 12 марта 2021 г. итогового доклада созданной по нашей инициативе в 2018 г. РГОС ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[12]. Уже в ближайшее время состоятся важные мероприятия по линии упомянутых площадок. 24–28 мая в виртуальном формате пройдет четвертая, итоговая сессия ГПЭ, а 1–2 июня в Нью-Йорке пройдет первая, организационная сессия новой РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ, для участия в которой послезавтра в США направляется российская делегация во главе с вашим покорным слугой.

Второй отдел занимается вопросами борьбы с информационной преступностью и терроризмом, а также мерами доверия

[12] Сообщение для СМИ «Об итогах деятельности Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности» // МИД России, 15.03.2021. — URL: https://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/4632970 (дата обращения: 19.05.2021).

и сотрудничества в Европе. Усилия работающих в нем дипломатов также во многом направлены на переговорные процессы в рамках ООН. В частности, наша страна стала инициатором процесса разработки под эгидой всемирной Организации всеобъемлющей международной конвенции по противодействию использованию ИКТ в преступных целях в рамках специального межправительственного комитета экспертов открытого состава[13]. Его организационная сессия состоялась 10–12 мая в Нью-Йорке при непосредственном участии делегации ДМИБ. Нельзя сказать, что все прошло гладко, итоги оргсессии — смешанные, но это только лишний раз демонстрирует, что на направлении обеспечения МИБ питать каких-то иллюзий не приходится. В поведении наших оппонентов, прежде всего западных, напористо реализующих собственную повестку дня и, поверьте, не стесняющихся в выборе методов и средств для достижения своих целей, нет и намека на приличия и дипломатичность в традиционном понимании этих слов. В этой связи мы твердо и последовательно защищаем интересы Российской Федерации и намерены далее продолжить выработку международно-правового инструмента, столь необходимого мировому сообществу в связи с разгулом информационной преступности.

Третья структурная единица нашего департамента — отдел регионального и двустороннего сотрудничества в области МИБ. На данном направлении ведется интенсивная работа по выстраиванию архитектуры межправительственных соглашений по МИБ между Россией и нашими зарубежными партнерами. Только за первые месяцы текущего года уже подписано два таких докумен-

[13] Резолюция Генеральной Ассамблеи ООН № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях», принята 27.12.2019 // Организация Объединенных Наций. — URL: https://undocs.org/ru/A/RES/74/247 (дата обращения: 19.05.2021).

та — с Ираном[14] и Киргизией[15]. Готовы к подписанию аналогичные соглашения с рядом стран Центральной, Западной и Юго-Восточной Азии, а также Латинской Америки. Не меньшее внимание уделяется вопросам многостороннего взаимодействия в различных региональных форматах, в первую очередь СНГ, ОДКБ, ШОС, БРИКС, АСЕАН. За последнее время был принят целый ряд важных документов, в частности, совместные заявления глав государств-участников СНГ[16] и Совета глав государств-членов ШОС о сотрудничестве в области МИБ[17], утвержден концептуальный документ о запуске диалогового партнерства Россия — АСЕАН по безопасности в сфере использования ИКТ и самих ИКТ[18].

---

[14] Сообщение для СМИ «О переговорах Министра иностранных дел Российской Федерации С. В. Лаврова с Министром иностранных дел Исламской Республики Иран М. Д. Зарифом» // МИД России, 26.01.2021. — URL: https://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4544717 (дата обращения: 19.05.2021).

[15] Сообщение для СМИ «О подписании Соглашения между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудничестве в области обеспечения международной информационной безопасности» // МИД России, 26.02.2021. — URL: https://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost//asset_publisher/UsCUTiw2pO53/content/id/4600397 (дата обращения: 19.05.2021).

[16] Совместное заявление глав государств — участников Содружества Независимых Государств о сотрудничестве в области обеспечения международной информационной безопасности // Президент России, 18.12.2020. — URL: http://www.kremlin.ru/supplement/5601 (дата обращения: 19.05.2021).

[17] Заявление Совета глав государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности // Шанхайская организация сотрудничества, 10.11.2020. — URL: http://rus.sectsco.org/documents/(дата обращения: 19.05.2021).

[18] Сообщение для СМИ «Об участии заместителя Министра иностранных дел России И.В.Моргулова в Совещании старших должностных лиц Россия — АСЕАН» // МИД России, 26.01.2021. — URL: https://www.mid.ru/web/guest/asean/-/asset_publisher/0vP3hQoCPRg5/content/id/4542722 (дата обращения: 19.05.2021).

Четвертый отдел отвечает за невоенные аспекты использования ИКТ. К сфере его ведения относятся столь актуальные и животрепещущие темы, как, например, вопросы управления интернетом. Кстати, в 2025 г. юбилейный XX Форум ООН по управлению интернетом — пожалуй, главная площадка по обсуждению вопросов регулирования «глобальной сети» — пройдет в России. Помимо этого, сотрудники отдела занимаются продвижением российских интересов в рамках еще одной важной организации — Международного союза электросвязи (МСЭ). Эта организация, что весьма непривычно для нашей темы, была создана еще в XIX в. и до сих пор занимается вопросами развития коммуникационных технологий в глобальном контексте. В сентябре–октябре 2022 года на Полномочной конференции МСЭ в Бухаресте состоятся выборы его генерального секретаря, и одним из кандидатов на этот пост является россиянин Рашид Рустамович Исмаилов — ранее замминистра связи и коммуникаций Российской Федерации, а ныне — руководитель ПАО «Вымпелком».

Деятельность департамента весьма разнообразна и покрывает все важнейшие направления обеспечения МИБ. На каждом из них наши дипломаты действуют с полной самоотдачей, в условиях напряженного графика и огромного количества задач, а сама специфика темы заставляет регулярно адаптироваться к новым меняющимся условиям и не упускать из виду мельчайшие детали. Порой работа в буквальном смысле ведется в круглосуточном режиме, особенно сейчас, в условиях продолжающейся пандемии, когда большое количество мероприятий проходит в онлайн-формате.

Тот факт, что сама тематика современных технологий объективно ближе и понятнее молодежи, очевиден и на примере ДМИБ. «Костяк» нашего департамента составляют молодые сотрудники, зачастую — те, кто совсем недавно вышел из студенческих аудиторий. Сочетание их «запала» и энтузиазма с опытом и знаниями руководства, а также сформировавшаяся

у нас творческая атмосфера позволяют нам уверенно и смело подходить к решению самых сложных задач на благо нашей страны.

Проблематика МИБ представляется невероятно интересной и перспективной для будущих дипломатов. Очевидно, что информационные и цифровые технологии с нами «всерьез и надолго» — а пока они есть, будет сохраняться и вопрос обеспечения их безопасности.

Студентам, интересующимся МИБ, нужно активно «вливаться» в тему. Отличной площадкой для этого является ЦМИБ МГИМО МИД России[19], сотрудники которого вносят значительный интеллектуальный вклад в осмысление данной проблематики. Уверен, что тот, кто придет в ЦМИБ, а впоследствии, при желании стать дипломатом, и в ДМИБ, ни разу не пожалеет о сделанном выборе. Пример работающих у нас сотрудников показывает, что люди, едва придя в департамент, моментально увлекаются и глубоко погружаются в тему, поэтому мы всегда будем рады видеть у нас новые лица. Думаю, можно было бы подумать и о том, чтобы в качестве эксперимента попробовать спроецировать уже апробированные в МГИМО форматы и по аналогии с «Моделью ООН» провести «Модель РГОС». На наш взгляд, это позволило бы интересующимся ребятам глубже прочувствовать тематику МИБ и стало бы их первым шагом на тернистой, но увлекательной стезе, ведущей в наш департамент.

Список использованных источников и литературы

1. Заявление Совета глав государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности // Шанхайская организация сотрудни-

[19] Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России . URL: https://mgimo.ru/about/structure/ucheb-nauch/ciis/ (дата обращения: 19.05.2021).

чества, 10.11.2020. — URL: http://rus.sectsco.org/documents/ (дата обращения: 19.05.2021).

2. Резолюция Генеральной Ассамблеи ООН № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях», принята 27.12.2019 // Организация Объединенных Наций. — URL: https://undocs.org/ru/A/RES/74/247 (дата обращения: 19.05.2021).
3. Совместное заявление глав государств — участников Содружества Независимых Государств о сотрудничестве в области обеспечения международной информационной безопасности // Президент России, 18.12.2020. — URL: http://www.kremlin.ru/supplement/5601 (дата обращения: 19.05.2021).
4. Сообщение для СМИ «О переговорах Министра иностранных дел Российской Федерации С. В. Лаврова с Министром иностранных дел Исламской Республики Иран М. Д. Зарифом» // МИД России, 26.01.2021. — URL: https://www.mid.ru/ru/foreign_policy/news//asset_publisher/cKNonkJE02Bw/content/id/454477 (дата обращения: 19.05.2021).
5. Сообщение для СМИ «О подписании Соглашения между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудничестве в области обеспечения международной информационной безопасности» // МИД России, 26.02.2021. URL: https://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/4600397m (дата обращения: 19.05.2021).
6. Сообщение для СМИ «Об итогах деятельности Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности» // МИД России, 15.03.2021. — URL: https://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/4632970 (дата обращения: 19.05.2021).
7. Сообщение для СМИ «Об участии заместителя Министра иностранных дел России И. В. Моргулова в Совещании старших должностных лиц Россия — АСЕАН» // МИД России, 26.01.2021. — URL: https://www.mid.ru/web/guest/asean/-asset_publisher/0vP3hQoCPRg5/content/id/4542722 (дата обращения: 19.05.2021).

8. Указ Президента Российской Федерации от 27 декабря 2019 г. № 626 «О внесении изменений в Указ Президента Российской Федерации от 11 июля 2004 г. № 865 «Вопросы Министерства иностранных дел Российской Федерации» и в Положение, утвержденное этим Указом» // Информационно-правовой портал «Гарант». — URL: https://www.garant.ru/products/ipo/prime/doc/73258599/ (дата обращения: 19.05.2021).
9. Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России. — URL: https://mgimo.ru/about/structure/ucheb-nauch/ciis/ (дата обращения: 19.05.2021).

А. И. Смирнов,
д-р ист. наук, профессор, главный научный сотрудник
Центра международной информационной безопасности
и научно-технологической политики МГИМО МИД России,
генеральный директор Национальной ассоциации
международной информационной безопасности

АКТУАЛЬНЫЕ ЗАДАЧИ НАЦИОНАЛЬНОЙ АССОЦИАЦИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: в статье рассматривается роль Национальной ассоциации международной информационной безопасности (НАМИБ) в условиях глобальной цифровой трансформации и в контексте новых «Основ государственной политики Российской Федерации в области международной информационной безопасности» (2021 г.). В проблеме ломки миропорядка все большую роль играет инфогенный нарратив. Коллективный Запад активно использует информационно-коммуникационные технологии (ИКТ) для гибридного сдерживания России, в том числе ведения когнитивной войны с целью десуверенизации.

Ключевые слова: международные отношения, международная информационная безопасность, когнитивная война, информационно-коммуникационные технологии, цифровая трансформация.

Человечество вошло в зону тотальной ломки миропорядка. Подрывную роль в этой проблеме многие эксперты отводят инфогенному нарративу. Действительно, планета охвачена беспрецедентной цифровой трансформацией. Мощный импульс к обострению геополитического противоборства придала пандемия коронавируса. Человечество с каждым днем все больше осознаёт её гигантские масштабы, ведущие эксперты сравнива-

ют с Великой депрессией и называют величайшим глобальным вызовом со времен Второй мировой войны.

При этом пандемия COVID-19 стала триггером как многих преимуществ, так и угроз цифрового мира. С учетом особой остроты данной проблемы Генеральный секретарь ООН А. Гутерриш предложил 11 июня 2020 г. дорожную карту по быстрым технологическим изменениям для достижения Повестки дня на период до 2030 года целей устойчивого развития (ЦУР)[20]. Её драйвером стали интернет-технологии, которые вызвали и продолжают вызывать тектонические сдвиги в развитии цивилизации. По сути, человечество вступило в новый фазовый переход, сравнимый по значению, например, с созданием письменности. При этом на смену микроэлектронике в драйверы развития пришел новый технологический уклад: нано-, био-, инфо- и когнитивные технологии. На основе Industry 4.0 стремительно развивается цифровая экономика, киберфизические системы, искусственный интеллект, квантовые вычисления, блокчейн, связь поколения 5G и иные прорывные технологии.

В этих условиях ведущие страны разрабатывают и реализуют разнообразные доктрины и стратегии по внедрению данных технологий с целью геополитического доминирования. В данном контексте следует отметить, что особое негативное воздействие на Российскую Федерацию оказывается со стороны США и их сателлитов. Данный постулат подтверждается, в частности, недавним докладом «НАТО 2030»[21], который нацелен на про-

[20] Remarks to the Virtual High-level Meeting of Rapid Technological Change on the Achievement of the Sustainable Development Goals // United Nations Secretary General, 11.06.2020. — URL: https://www.un.org/sg/en/content/sg/speeches/2020-06-11/remarks-rapid-technological-change-achievement-of-the-sustainable-development-goals (дата обращения 19.05.2021).

[21] «НАТО — 2030: трансатлантическая повестка дня на будущее» // НАТО: официальный сайт, 04.07.2021. — URL: https://www.nato.int/cps/ru/natohq/opinions_184636.htm (дата обращения 19.05.2021).

должение гибридного воздействия на Россию и её союзников: политико-дипломатического, экономического, военного и информационного. Ключевую роль в информационно-психологическом манипулировании массовым сознанием россиян играют центры НАТО в Риге, Таллине, Хельсинки.

В силу этого неоценимое значение и стратегическую важность в создании безопасного глобального информационного пространства имеют новые «Основы государственной политики в области международной информационной безопасности». Данный документ направлен на продвижение российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в этой сфере, на содействие созданию международно-правовых механизмов предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве и на организацию межведомственного взаимодействия.

В новых Основах нашли свое отражение и другие новые векторы реализации госполитики в области МИБ, — активное использование возможностей научных и экспертных кругов, делового сообщества, а также укрепление действующих и формирование новых международных дискуссионных площадок как в России, так и за рубежом для продвижения российских подходов и инициатив[22].

Эти ориентиры закреплены в новых направлениях государственной политики и связаны с совершенствованием механизма участия представителей российского научного и экспертного сообщества в научно-исследовательском, аналитическом и научно-методическом обеспечении продвижения инициатив России по формированию системы обеспечения МИБ.

[22] Основы государственной политики Российской Федерации в области международной информационной безопасности / утв. Указом Президента Российской Федерации от 12 апреля 2021 года № 213. — URL: http://www.publication.pravo.gov.ru/Document/View/0001202104120050/ (дата обращения: 11.05.2021).

Нам очень приятно и вместе с тем ответственно отметить, что Президент В. В. Путин при рассмотрении проекта Основ на заседании Совета Безопасности России 26 марта 2021 г. подчеркнул роль нашей Ассоциации: «…в эффективной реализации государственной политики, обозначенной в новой редакции „Основ", надо активнее использовать возможности научных и экспертных кругов, делового сообщества, в том числе, конечно, Национальной Ассоциации международной информационной безопасности»[23].

МГИМО является одним из соучредителей нашей Ассоциации, позвольте в этой связи выразить уверенность, что ЦМИБ и другие заинтересованные подразделения продолжат сотрудничество с НАМИБ на данном треке. Назову одну из самых острых проблем по теме МИБ — использование глобальной медиасферы для силовых подходов к разрешению споров и вмешательства во внутренние дела суверенных государств. Недавние события в Беларуси, в Гонконге и т.д. — тому подтверждение.

Проблема злоупотребления США свободой слова в целях глобального информационного доминирования становится все более угрожающей. В СМИ достоверная информация, активно перемешивается с «фейками» и рассчитана на «примитивные умы» населения с конечной целью — представить противника как смертельного врага. При этом Запад ведет когнитивную или ментальную войну — подавление сознания и мировоззрения противника.

Развитие когнитивной и ментальной войны в ИКТ-среде повышает риск возникновения конфликтов, способных нарушить международный мир. Данный тезис подтверждается в т.ч. разработкой в 2019 г. Пентагоном стратегии «Троянский конь»

[23] Президент провёл в режиме видеоконференции заседание Совета Безопасности, в ходе которого рассматривался проект «Основ государственной политики Российской Федерации в области международной информационной безопасности» // Официальный сайт Президента России, 26.03.2021. — URL: http://www.kremlin.ru/events/president/news/65231 (дата обращения: 19.05.2021).

для инспирирования протестов «пятой колонны», включая «кибербунты» с использованием новейших интернет-платформ и гаджетов.

Таким образом, инфогенный фактор стал одним из главных компонентов «гибридных войн», включающих также оказание политического, экономического и военного давления. Причина распространения «гибридных войн» понятна — они не требуют объявления войны. При этом США и их сателлиты безуспешно пытаются обвинить Россию и её союзников в хакерских атаках, дезинформации и пропаганде. При таком подходе доказательной базой становится «коллективная атрибуция», то есть совместное определение или назначение источника атаки. Основным фактором в определении виновного является политический контекст, а аргументом — тезис «хайли лайкли» (highly likely) — «с высокой вероятностью». Эксперты России едины в том мнении, что обеспечение устойчивого функционирования и безопасного использования ИКТ-среды человеком, обществом и государством возможно лишь на основе международного сотрудничества в ООН, а также в ШОС, БРИКС, ОДКБ и в иных форматах.

С учетом раскола в ООН при выработке норм и правил ответственного поведения государств в ИКТ-среде президент НАМИБ В. Шерстюк подчеркнул, что международное право не работает, а когда перестаёт работать сила права, начинает работать право силы.

В этом контексте несколько слов о Национальной Ассоциации международной информационной безопасности. НАМИБ была учреждена в апреле 2018 г. в целях содействия развитию частно-государственного партнерства в области безопасности использования ИКТ. Согласно Уставу, Ассоциация в упреждающем режиме проводит проработку проблемных вопросов обеспечения МИБ в интересах формирования переговорных позиций государственных органов.

За три года работы Ассоциация приняла участие в десятках крупных международных форумах, из них в половине выступи-

ла организатором или соорганизатором. В условиях пандемии в 2020–2021 гг. среди крупных мероприятий следует отметить участие в VIII Пекинской конференции по интернет-безопасности, организация XIV Международного форума в Москве по проблемам международной и информационной безопасности, III медиафорума в Нижнем Новгороде и др. Члены президиума сделали свыше сотни докладов и опубликовали десятки статей, приняли участие во втором издании учебника «Международная информационная безопасность: теория и практика» в трех томах под редакцией спецпредставителя Президента России, члена Президиума НАМИБ, директора ЦМИБ А. В. Крутских.

Список использованных источников и литературы

1. Международная информационная безопасность: Теория и практика: В трех томах. Том 2. Учебник для вузов / Под общ. ред. А. В. Крутских. — 2-е изд., перераб. и доп. — М.: Издательство «Аспект Пресс», 2021. — 384 с.
2. «НАТО — 2030: трансатлантическая повестка дня на будущее» // НАТО: официальный сайт, 04.07.2021 — URL: https://www.nato.int/cps/ru/natohq/opinions_184636.htm (дата обращения 19.05.2021).
3. Президент провёл в режиме видеоконференции заседание Совета Безопасности, в ходе которого рассматривался проект «Основ государственной политики Российской Федерации в области международной информационной безопасности» // Официальный сайт Президента России, 26.03.2021. — URL: http://www.kremlin.ru/events/president/news/65231 (дата обращения: 19.05.2021).
4. Remarks to the Virtual High-level Meeting of Rapid Technological Change on the Achievement of the Sustainable Development Goals // United Nations Secretary General, 11.06.2020 — URL: https://www.un.org/sg/en/content/sg/speeches/2020-06-11/remarks-rapid-technological-change-achievement-of-the-sustainable-development-goals (дата обращения 19.05.2021).

Б. Н. Мирошников,
вице-президент ГК «Цитадель»

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: в докладе представлена характеристика основных направлений противодействия угрозам информационной безопасности — в том числе использованию ИКТ и интернета в преступных целях и в целях ведения информационных гибридных войн.

Ключевые слова: информационная безопасность, угрозы информационной безопасности, информационная преступность, информационные войны, гибридные войны.

Одно из главных соображений, которое хотел бы высказать: увы, мы опоздали и опаздываем по всем направлениям обеспечения информационной безопасности.

Из различных статистических данных МВД, Прокуратуры, СК, отчетов всевозможных служб безопасности и аналитиков мы регулярно узнаем о росте преступности в ИТ среде, о росте числа жертв этих преступлений, об огромном и постоянно увеличивающимся ущербе от этих преступлений. Что в этом списке? На первом месте мошенничество. Затем — кража или утечка персональных данных, хищения, вымогательство.

Отсюда вывод — несмотря на огромную работу правоохранительных органов, отчаянные усилия Роскомнадзора, другие меры — все-таки мы не дорабатываем. Коль скоро все эти негативные показатели растут и растут, да еще и с ускорением. Посмотрите цифры, они регулярно публикуются. Очевидно, что наши меры пока недостаточны, если нам не удается надежно защитить свое информационное пространство, интересы государства, бизнеса и простых граждан в нем. Причин тут много.

Поэтому правильно, что мы собираемся в таких залах и в таком составе, чтобы изучать проблему, ее масштабы, наших поражений, источники наших побед. Нельзя же сказать, что ничего не делалось. Напомню Вам о мерах, уже реализованных на данном направлении.

С 1997 года — УК получил новую Главу 28 — преступления в сфере компьютерной информации — так она тогда называлась. В 1998 году в составе МВД (август) и в составе ФСБ (октябрь) были созданы подразделения, в функции которых входила борьба с преступлениями в сфере высоких технологий.

То, что сделано за эти более чем двадцать лет — это очень много и очень ценно, так как во многом это был путь по целине. Что еще важно, так это то, что наши достижения в этой области широко известны и признаны. Для справки скажу: в 2006 году МВД России провело первую международную конференцию в Москве в здании Центра международной торговли, посвященную борьбе с киберпреступностью и кибертерроризмом. Приехали представители более чем 40 стран, включая Великобританию, Китай и США. Это и было признание. Мы продемонстрировали свои достижения и выдвинули инициативы. Их содержание до сих пор узнается во многих международных документах, ибо они были пронизаны здравым смыслом и пониманием ситуации. С тех пор Россия последовательно и упорно отстаивает интересы международной информационной безопасности. Наши новые инициативы постоянно выдвигаются на площадках разного уровня. Хотя не всегда их там ждут.

Обстановка в ИКТ среде усложняется и проблем становится все больше. Важно понимать, что технологически интернет — это единая трансграничная среда, работающая по единым протоколам по всей планете. Иначе она не была бы глобальной. Но этот факт одновременно означает, что любые острые проблемы, так называемые инциденты, носят также трансграничный характер. Их расследование, а также вопросы регулирования нужно решать всем участникам этих процессов

вместе. Причины инцидентов в сетях различны — от нападения враждебных государств и действий преступных группировок до ошибки персонала или сбоя работы оборудования. Соответственно и реагирование должно быть различным. Однако как установить причину? Очевидно, что это сложный процесс. А бывает, что не все хотят установить истину, кто-то хочет воспользоваться случаем, чтобы устроить истерику или спровоцировать нападение другим оружием… Зачастую проведение информационных атак прикрывается действиями хакеров или хулиганов.

Поэтому так необходимо создавать когорту квалифицированных специалистов, способных в составе международных бригад проводить международное расследование киберинцидентов. Пока нет ни бригад специалистов, ни процедур международного расследования. Их надо формировать, и никуда мы от этого не денемся! А пока активно обсуждается такая проблема, как атрибуция — принятый термин — определение источника угрозы или нападения. Однозначных решений пока нет. Это лишь один пример нерешенных проблем. Но их много. Пандемия усугубила ситуацию. Количество преступлений и киберинцидентов резко возросло, так как переход «на удаленку» повысил уязвимость многих сетей. С другой стороны, по понятным причинам сократились контакты между специалистами, правоохранительными органами. Многие переговорные обязанности легли на плечи дипломатов.

Условия для международных переговоров сегодня не самые благоприятные, санкции и изоляционизм не лучший фон для поиска истины. Необходимо преодолевать и предвзятость, и двойные стандарты, и навязывание чужой воли. Нужны новые знания, понимание технологических процессов, механизмов взаимодействия. И опять, как никогда ранее, возникают главные требования — доверие и прозрачность!

Разумеется, в любом новом деле всегда возможны и ошибки, и заблуждения. Это неизбежно и даже полезно, так как

приобретается бесценный опыт, «опыт, сын ошибок трудных». Да, он порой дается очень дорого.

Разумеется, в любом новом деле рождаются мифы и заблуждения, от которых нужно избавляться — чем быстрее, тем лучше. Ну вот, например. Почему-то решили, что ИКТ — это особая среда, особый мир. Это заблуждение повторяется с удивительным постоянством. На самом деле, уважаемые мои друзья, это никакая не особая среда. Это лишь инструментарий, который люди придумали для своего удобства. И не надо его очеловечивать, романтизировать и тому подобное. Если это и среда, то технологическая, где царствует закон Ома и другие великие формулы. Какие функции, например, выполняет, наш замечательный интернет? Первое — это хранение информации. Второе — это средство связи. И третье — это средство массовой информации. Все остальное — производное от этих функций.

Следовательно, появляется и второе заблуждение — что для ИКТ среды нужны особые законы. Но ведь у нас уже есть законодательство регулирующее информационную сферу, связь, а также и закон о СМИ. Чего же вам еще нужно? Пользуйтесь! Применяйте! А те авторы, которые придумывают новые законы или статьи с припиской «с использованием сети Интернет» или что-то в этом роде, оказывают, на мой взгляд, плохую услугу правоприменителям, засоряя и без того непростое законодательство. Скажите пожалуйста, для вас имеет значение, как вас оклеветали — с помощью листовок, с помощью надписи на заборе вашей фирмы или какой-нибудь гадостью в социальных сетях? Скорее всего, ваш ответ — да какая разница? А если Вы стали жертвой мошенников? Вам важно, что мошенничество осуществлялось с помощью интернета или наперстка? Вероятно, принципиальной разницы нет — осуществляются ли правонарушения с использованием ИКТ или без, важен сам факт правонарушений и последующей правоприменительной практики.

Все большее распространение получает такое понятие, как гибридная война, которая, однако, не является принципиально новым явлением в истории человечества. Раскрою вам секрет: все войны, которые вело человечество на протяжении истории были гибридными. Чтобы в этом убедиться, посмотрите на военные кампании Чингисхана и Наполеона, изучите, что писали о войне К. фон Клаузевиц или великий полководец А. В. Суворов, Сунь Цзы или Никколо Макиавелли, которого можно назвать певцом гибридной войны. Вспомните детали Первой и Второй мировых войн. И всем ясно, что «гибридная война» — это просто очередная фигура речи.

Информационные войны давно идут на планете, идут не прекращаясь, но меняя названия — психологическая атака, идеологическая борьба, вражеская пропаганда… И все, что делали «Радио Свобода», «Голос Америки» и их коллеги — это и была информационная война, которую мы, к сожалению, сто раз проиграли. Очевидно, это не наш вид спорта. Против нас десятилетиями напряженно работают огромные аппараты профессионалов, получающие огромные деньги, выступающие единым фронтом под управлением весьма талантливых дирижеров. Впрочем, вам про это расскажут, возможно немного не так. Как бы то ни было, это тоже ваш будущий фронт.

Главный цивилизационный конфликт сегодня — это растущая пропасть между способностью человека к восприятию и обработке информации и безумный рост количества информации, производимой человеком на планете. Человеческая природа за последние пару тысяч лет осталась неизменной. А вот количество информации увеличилось и постоянно растет в геометрической прогрессии. Важно не растеряться и создать алгоритмы разумного обращения с этим растущим массивом и равноправного взаимодействия между государствами.

Информация и информационная безопасность. На сегодняшний день — это самое интересное, важное и захватывающее.

Тот, кто будет заниматься этой темой, автоматически оказывается на передовой главнейших проблем цивилизации.

И напоследок. У всеобщей информатизации и цифровизации есть обратная сторона. Деформируются человеческие способности, падает грамотность, наблюдаются различные негативные культурологические последствия. В том числе страдает и язык! Великий и могучий русский язык. А это одна из наших главных скреп! Убежден, что национальная идея России, которую мы мучительно ищем многие годы, заключается всего в одном слове — Достоинство. Вот за это и предстоит побороться молодому поколению дипломатов. Согласитесь, мало достоинства в том, что в великий русский язык затягиваются всякие «тренды» и «треки», «фактчекинги» и «месседжи». Им что, языка Пушкина и Толстого, Чехова и Достоевского не хватает? Или они его просто не знают и не могут выразить свою мысль? Согласитесь, мало достоинства в неграмотном и подобострастном «в Украине», когда языковые холопы в одночасье отказываются от традиционной грамотной формулы «на Украине» по требованию полуграмотных представителей страны, где русский язык давно даже не государственный!

А без достоинства, уважения трудно отстаивать интересы государства, особенно в такой трудной дисциплине, как международная информационная безопасность.

СЕКЦИЯ 1

«ПРАВИЛА ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ»

Д. В. Глухов,
атташе Департамента международной
информационной безопасности МИД России

ВЫРАБОТКА ПРАВИЛ, НОРМ И ПРИНЦИПОВ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ ПОД ЭГИДОЙ ООН: РЕАЛИИ И ПЕРСПЕКТИВЫ

Аннотация: в статье описывается подход Российской Федерации к вопросу о выработке правил, норм и принципов ответственного поведения государств в информационном пространстве. Автор подчеркивает, что формулирование соответствующих рамок может осуществляться исключительно под эгидой Организации Объединенных Наций как единственной подлинно глобальной площадки. Соответствующая работа осуществляется в рамках двух профильных форматов — узкой по составу Группы правительственных экспертов (ГПЭ) ООН и широкой Рабочей группы ООН открытого состава (РГОС). Одним из главных приоритетов российской дипломатии на данном направлении является работа над приданием правилам, нормам и принципам, имеющим на сегодняшний день добровольный характер, статуса юридически обязывающих.

Ключевые слова: международная информационная безопасность, информационно-коммуникационные технологии, информационное пространство, правила, нормы и принципы ответственного поведения государств, Организация Объединенных Наций, Группа правительственных экспертов ООН, Рабочая группа ООН открытого состава.

Вопрос о важности определения рамок действий государств в информационном пространстве находится на мировой повестке дня на протяжении уже довольно долгого времени, но при этом с каждым годом становится все более насущным и актуальным,

а формулирование неких «границ дозволенного и недозволенного» является долгим и комплексным процессом. Во-первых, мир, в котором мы живем, по-прежнему неоднороден как с точки зрения уровня развития, так и с точки зрения интересов государств в цифровой среде. Во-вторых, сама тематика международной информационной безопасности (МИБ) является по-прежнему весьма новой для мира, и ситуация в ней может меняться в буквальном смысле каждый день параллельно с интенсивным развитием информационно-коммуникационных технологий (ИКТ). Некоторые нормы могут попросту терять актуальность, а новые реалии требуют выработки принципиально новых. Это отчетливо демонстрируют и события последнего года — пандемия коронавирусной инфекции заставляет как государства, так и других игроков смотреть на ситуацию под новым углом.

Одно мы можем сказать точно: выработка общих для всех «правил игры» в информационном пространстве, которые учитывали бы интересы всех государств, может осуществляться только под эгидой единственной поистине глобальной площадки — Организации Объединенных Наций. Именно в рамках ООН мы стремимся закрепить российский подход к вопросам формирования глобальной архитектуры МИБ, основанный на принципах предотвращения конфликтов в информационном пространстве, недопущения его милитаризации и использования ИКТ исключительно в мирных целях.

Уже более двух десятилетий назад наша страна заложила основы разработки универсальных правил, норм и принципов ответственного поведения государств в сфере ИКТ. Исторически именно Россия стала инициатором профильной дискуссии в формате ООН, когда в 1998 г. внесла в Первом комитете Генеральной Ассамблеи резолюцию «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[1], ставшую впоследствии ежегодной.

[1] Резолюция Генеральной Ассамблеи ООН № 53/70.

В 2004 г. была создана тематическая Группа правительственных экспертов (ГПЭ) ООН[2]. Инновационность данного формата в тот момент была неоспорима — впервые под эгидой всемирной Организации начал функционировать механизм обсуждения проблематики МИБ, пусть и в узком составе (участие в работе Группы в рамках каждого созыва принимали 10–20 экспертов в личном качестве). Из пяти созванных ГПЭ три (2010, 2013 и 2015 гг.) завершились принятием итоговых докладов. Особое значение с точки зрения темы, которую мы сейчас обсуждаем, имел документ 2015 г. Тогда участникам удалось добиться консенсуса и сформулировать 11 добровольных международных правил, норм и принципов ответственного поведения государств в информационном пространстве[3]. Впоследствии их перечень был развит в российской резолюции № 73/27[4], принятой Генассамблеей в декабре 2018 г. В частности, там были закреплены такие положения, как:

— важность межгосударственного сотрудничества в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ;
— необходимость выполнения государствами их международных обязательств в отношении международно-противоправных деяний, приписываемых им в соответствии с международным правом;

[2] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. — URL: https://cutt.ly/Ambdx2S (дата обращения: 19.05.2021).

[3] Доклад Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, 22.07.2015 // Организация Объединенных Наций. — URL: https://undocs.org/pdf?symbol=ru/a/70/174 (дата обращения: 19.05.2021).

[4] Резолюция Генеральной Ассамблеи ООН № 73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принята 05.12.2018 // Организация Объединенных Наций. — URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27 (дата обращения: 19.05.2021).

— недопустимость использования государствами посредников для совершения международно-противоправных деяний с использованием ИКТ и необходимость обеспечения неиспользования их территории для совершения таких деяний;
— а также ряд других положений, касающихся сотрудничества и обмена информацией, оказания взаимопомощи, необходимости уважения основных прав и свобод человека в эпоху цифровых технологий, защиты критической информационной инфраструктуры, обеспечения целостности каналов поставки, поддержания деятельности групп экстренной готовности к компьютерным инцидентам и важности сотрудничества государств с частным сектором в области осуществления правил ответственного поведения государств.

Нами выдвигались и другие инициативы, оформленные в качестве документов ООН. Так, в сентябре 2011 года в ходе 66-й сессии Генеральной Ассамблеи ООН было распространено официальное письмо на имя Генерального секретаря со стороны постоянных представителей Китая, России, Узбекистана и Таджикистана при ООН, в приложении к которому содержался принятый в июне 2011 г. на саммите Шанхайской организации сотрудничества в Астане (Казахстан) проект «Правил поведения в области обеспечения международной информационной безопасности»[5]. По прошествии чуть более трех лет эти правила были пересмотрены с учетом поступивших замечаний и предложений, и в январе 2015 г. был распространен их актуализированный перечень[6].

---

[5] Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12.09.2011 на имя Генерального секретаря Организации Объединенных Наций и приложение к нему // Организация Объединенных Наций. — URL: https://undocs.org/pdf?symbol=ru/A/66/359 (дата обращения: 19.05.2021).

[6] Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 09.01.2015 на имя Генерального секретаря Организации Объединенных Наций и приложение к нему // Организация

По мере все большего ускорения темпов технологического развития и перехода вопросов обеспечения МИБ в разряд ключевых для каждой без исключения страны становилось очевидно, что в мире формируется запрос на новые инклюзивные форматы, в рамках которых учитывалось бы мнение всех без исключения. Было понятно, что выработка правил, норм и принципов больше не может осуществляться в клубных форматах — востребованы универсальные площадки. В этих целях в 2018 г. по российской инициативе была запущена Рабочая группа ООН открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[7]. Ее качественно отличала степень охвата — в отличие от ГПЭ, в ней был представлен не небольшой круг экспертов, а все 193 государства-члена ООН, представители которых могли высказывать свое мнение на равноправной и справедливой основе. Одним из приоритетов мандата Группы в соответствии с резолюцией №73/27[8] была «дальнейшая выработка норм, правил и принципов ответственного поведения государств и путей их реализации; при необходимости, внесения в них изменений или формулирования дополнительных правил поведения».

В марте 2021 г. по итогам деятельности РГОС был принят итоговый доклад[9], в котором были четко подтверждены достигнутые ранее международным сообществом договоренности по правилам, нормам и принципам, закрепленные в российской резолюции 2018 г. Успешное завершение работы Группы озна-

Объединенных Наций. — URL: https://cutt.ly/ZmbdO4V (дата обращения: 19.05.2021).

[7] Open-ended Working Group // United Nations. — URL: https://www.un.org/disarmament/open-ended-working-group/ (дата обращения: 19.05.2021).

[8] Резолюция Генеральной Ассамблеи ООН № 73/27.

[9] Final Substantive Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, adopted on March 12, 2021 // United Nations. — URL: https://cutt.ly/4mbTebs (дата обращения: 19.05.2021).

меновало собой неоспоримый успех нашей дипломатии: всему миру удалось добиться консенсуса, и формат РГОС еще раз продемонстрировал свою востребованность и жизнеспособность.

Немаловажно отметить, что пандемия коронавирусной инфекции заставила страны в рамках РГОС акцентировать внимание на нормах, касающихся защиты критической информационной инфраструктуры, в первую очередь — объектов здравоохранения и научно-исследовательских центров, занимающихся поиском ответов на вызовы пандемии. Так, в итоговом документе содержится вывод государств о том, что COVID-19 указал на важность защиты медицинских учреждений и служб путем имплементации соответствующих норм.

Что касается перспектив выработки правил, норм и принципов ответственного поведения государств под эгидой ООН, то работа на данном направлении будет и далее продолжена в уже апробированном и зарекомендовавшем себя универсальном формате РГОС. 31 декабря 2020 г. Генеральная Ассамблея ООН приняла предложенную Россией резолюцию о создании новой Группы по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025[10]. Организационная сессия новой РГОС состоится в Нью-Йорке уже совсем скоро — 1–2 июня, и очное участие в ней примет российская делегация.

Данный механизм будет носить поистине инновационный характер: в дополнение к таким чертам, как универсальность и инклюзивность, заложенным в предыдущую РГОС, впервые в истории работа по проблематике МИБ на ооновском треке будет носить не просто дискуссионный, а именно переговорный характер. Этому, в частности, будет способствовать предусмотренная мандатом новой Группы возможность тематической

[10] Резолюция Генеральной Ассамблеи ООН № 75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принята 31.12.2021 // Организация Объединенных Наций. — URL: https://undocs.org/ru/A/RES/75/240 (дата обращения: 19.05.2021).

специализации обсуждений путем создания подгрупп. В рамках новой РГОС российская дипломатия направит усилия на содержательную работу по выработке новых правил, норм и принципов, а также, что еще более важно, по приданию им статуса обязательных в формате универсального юридически обязывающего инструмента.

К сожалению, наши подходы к вопросам обеспечения МИБ, в том числе применительно к правилам, нормам и принципам, разделяют не все. В нашей профильной деятельности мы сталкиваемся с деструктивной деятельностью ряда других государств, стремящихся «размыть» главенствующую роль ООН и передать ее полномочия региональным форматам. Этим государствам выгодно сохранить за собой «свободу рук» и возможность вольно трактовать нормы и принципы, по которым уже достигнуты договоренности мирового сообщества.

В этой связи, полагаем принципиально важным продолжить деятельность по приданию согласованным правилам статуса обязательных, в том числе в формате универсального юридически обязывающего инструмента. Намерены направить на это значительные усилия в предстоящий пятилетний период работы новой РГОС. Наши уверенные и последовательные шаги на данном направлении будут и далее способствовать удовлетворению потребности всего мирового сообщества в сфере МИБ — обеспечению безопасной и стабильной ИКТ-среды.

Список использованных источников и литературы

1. Доклад Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, 22.07.2015 // Организация Объединенных Наций. — URL: https://undocs.org/pdf?symbol=ru/a/70/174 (дата обращения: 19.05.2021).
2. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. — URL: https://cutt.ly/Ambdx2S (дата обращения: 19.05.2021).

3. Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 09.01.2015 на имя Генерального секретаря Организации Объединенных Наций и приложение к нему // Организация Объединенных Наций. — URL: https://undocs.org/pdf?symbol=ru/A/66/359 (дата обращения: 19.05.2021).
4. Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12.09.2011 на имя Генерального секретаря Организации Объединенных Наций и приложение к нему // Организация Объединенных Наций. — URL: https://cutt.ly/1mbTd5k (дата обращения: 19.05.2021).
5. Резолюция Генеральной Ассамблеи ООН № 53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принята 04.12.1998 // Организация Объединенных Наций. — URL: https://cutt.ly/UmbTucO (дата обращения: 19.05.2021).
6. Резолюция Генеральной Ассамблеи ООН № 73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принята 05.12.2018 // Организация Объединенных Наций. — URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27 (дата обращения: 19.05.2021).
7. Резолюция Генеральной Ассамблеи ООН № 75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принята 31.12.2021 // Организация Объединенных Наций — URL: https://undocs.org/ru/A/RES/75/240 (дата обращения: 19.05.2021).
8. Final Substantive Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, adopted on March 12, 2021 // United Nations. — URL: https://cutt.ly/0mbjCcK (дата обращения: 19.05.2021).
9. Open-ended Working Group // United Nations. — URL: https://cutt.ly/HmbTjaF (дата обращения: 19.05.2021).

А. В. Шевченко,
д-р полит. наук, профессор,
зав. кафедрой государственного управления
и национальной безопасности РАНХиГС

МЕЖДУНАРОДНО-ПОЛИТИЧЕСКИЙ ДИСКУРС: ПУБЛИЧНАЯ ЛЕГИТИМАЦИЯ ПРАВИЛ «ДУРНОЙ ПАРРЕСИИ»

Аннотация: в статье рассматриваются возможности междисциплинарного подхода к оценке современного международно-политического дискурса. В актуальное исследовательское поле выводится феномен парресии (с греческого — «говорить без страха и стыда», «свобода слова») как способ оглашения объективно скрытых или намеренно замалчиваемых фактов обнажить истинное положение дел. Исследуются эффекты «дурной парресии», характеризующие публичную международно-политическую деятельность в период ослабления демократических институтов.

Ключевые слова: демократия, дискурс, интенция, парресия, парресиаст, политические коммуникации, свобода слова, семантический сдвиг.

В условиях пандемии усилилась деструктивная динамика подвижных конструкций международно-политической системы. Прежде всего это заметно на состоянии коммуникативных связей между сторонами, образующими семантическую основу межгосударственных отношений. Долгоживущие конфликты интерпретаций фактов и событий «коллективным Западом» и противными сторонами подпитались энергией вакцинного противоборства, что придало ускорения семантическим сдвигам в международно-политическом дискурсе относительно ряда системообразующих смысловых констант: демократия, порядок, право, правило, сила.

Именно об этом и в этот момент пишет министр иностранных дел России С. В. Лавров в статье «О праве, правах и правилах»: «…в русском языке „право“ и „правило“ — однокоренные слова. Для нас настоящее, справедливое правило неотделимо от права. В западных языках иначе. В английском, например, право — „law“, а правило — „rule“. Чувствуете разницу? „Rule“ — это больше не про право (в смысле общепризнанных законов), а про то, какие решения принимает тот, кто правит, управляет. Также отметим, что однокоренное слово с „rule“ — „ruler“, одно из значений которого „линейка“. Получается, что своей концепцией „правил“ Запад хотел бы всех выстроить по своей линейке, в свою шеренгу»[11].

Говоря о том, что «получается», российский министр вскрывает настоящие намерения противной стороны, интенционально скрытые в слегка облагороженном дискурсе международных отношений с участием политики Дж. Байдена, в отличие от агрессивно-несдержанной риторики США времен правление Б. Обамы и Д. Трампа: «Внедряя свою концепцию «миропорядка, основанного на правилах», Запад преследует цель увести дискуссии по ключевым темам в удобные ему форматы, куда несогласных не приглашают».

Семантические сдвиги в международно-политическом дискурсе, обусловленные кардинальными геополитическими, политэкономическими и геоэкономическими изменениями конца XX — начала XXI вв., имеют психологическую и психофизиологическую основу (что имманентно свойственно этой трансформации) — см., например, исследование Д. Моизи[12].

«Новый курс» на возвращение США своей ролевой доминанты в мире, измененном политэкономическими технологиями остановки коронавирусной пандемии, сопровождается и соответствующей нормам дипломатического приличия коммуника-

[11] Лавров С. В. О праве, правах и правилах //Коммерсантъ — 28.06.2021. № 109/П.

[12] Моизи Д. Геополитика эмоций. Как культуры страха, унижения и надежды трансформируют мир. — М.: МШПИ, 2010.

тивной тональностью. Так, издание «Politico» раскрывает приемы маскирования содержания задуманного президентом США глобального форума сторонников демократии по-американски простой лингвистической уловкой: саммит планируется назвать не «Саммитом демократий», а «Саммитом за демократию». Тогда возможность присутствия на нем получат и те страны, «которые хотели бы добиться укрепления народовластия, однако испытывают с этим сложности»[13].

Изменился ли сам международный коммуникант, представленный обобщенным образом коллективного Запада? Однозначно, нет, ибо это значило бы отказ или хотя бы уступку противной стороне при предъявлении, отстаивании или защите своих национальных интересов, что является одной из функций международно-политической коммуникации. Могут измениться формы контроля или давления на партнеров (что, например, очевидно по отчетам и комментариям СМИ о саммите G7 в июне 2021 г. на Корнуолле), на международные организации (ВОЗ, Секретариат ООН по климату). То есть, выбирается иная, атональная, коммуникативная стратегия, но содержательные установки на доминирование с позиций силы не меняются.

Это подтверждает и протокольно-вежливое публичное признание госсекретаря Белого дома Э. Блинкена в злоупотреблениях США в сфере международных отношений: «Я знаю, что некоторые наши действия последних лет подрывали основанный на правилах мировой порядок и заставляли другие страны задаваться вопросом, привержены ли мы ему», успокоившего общественность обещанием благонамеренного взаимодействия с рядом многосторонних институтов.

Атональные технологии имеют ту же природу, что и описанный Г. Бейтсоном и П. Вацлавиком феномен «двойной связи» — форму парадоксальной коммуникации, в рамках которой содер-

[13] Газета «Коммерсантъ» № 219/П от 30.11.2020 — URL: https://www.kommersant.ru/doc/4593083 (Дата обращения 15.05.2021).

жание коммуникации противоречит ситуативному контексту. Она создается при наложении двух семио-семантических кодов в ходе коммуникативной ситуации или же при наложении двух интерпретационных стратегий в ходе единого коммуникативного акта. «В результате возникает система неполного взаимопонимания, противоречивых распоряжений, ущербности коммуникативного процесса»[14].

«Двойная связь» разрывается простым приемом, но требующим политической воли, — прямое и однозначное называние вещей своими именами. Так поступила российская сторона в ответ на очередной пассаж американского официоза о новых санкциях и причинах высылки российских дипломатов из США. По словам корреспондента «Коммерсантъ FM», министр иностранных дел Сергей Лавров в ответ не стал стесняться в выражениях: «Линия США в отношении России абсолютно тупиковая, может быть, даже тупая. Она не приносит никакого результата с точки зрения тех целей, которые объявлялись, когда вводились санкции. …Слова звучат неубедительно. Будем ждать конкретных дел»[15].

Столь же определенно высказал свою позицию относительно установления «мирового порядка, основанного на правилах», председатель комиссии Совета Федерации по информационной политике Алексей Пушков: «…это произвол США и ближайших союзников, поскольку он основан на правилах, которые устанавливают в Вашингтоне. И он не обеспечивает „международного мира“ — это ложь».

В условиях, когда система международных отношений восприняла коммерческо-политическую модель функционирования,

---

[14] Франко «Бифо» Берарди. Душа за работой. От отчуждения до автономии. /Пер. с итал. Кирилла Чекалова — М.: ООО «Издательство Грюндриссе», 2019. С. 77.

[15] Лавров отказал Западу в праве навязывать миру «универсальные нормы» — URL: https://e-news.su/mnenie-i-analitika/380849-lavrov-otkazal-zapadu-v-prave-navjazyvat-miru-universalnye-normy.html (Дата обращения 14.05.2021).

такое коммуникативное поведение, обеспеченное массмедийными технологиями, стало нормой[16]. При этом вектор дискурса, ранее направленный внутрь международно-политической системы отношений в силу особенностей ее структуры, развернулся в сторону широкой общественности, все более вовлекаемой в актуальные политические повестки. Цель такого разворота — убедить (навязать, заставить) международное сообщество в признании «политически правильных» решений, действий или оценок, при этом продвигать односторонние подходы, игнорируя признанные коллективные механизмы выработки решений.

Этот коммуникативный ход, ожидаемо неприемлемый той частью мирового сообщества, которая имеет иное представление о способах реализации своих суверенных прав в международных отношениях, поддается продуктивному исследованию, если придерживаться понятия о дискурсе как жизненном предконтексте, «в котором просматривается мир идей и идеологий, а также пласт явлений, их порождающих, и, в то же время, их включающий» (Макс Фрай).

Что же просматривается в современном международно-политическом дискурсе? Мы видим признаки деградации демократической идеи, сжимающейся в лоне «авторитарного либерализма» до состояния своего раннего коммуникативного выражения.

Свобода слова как демократическая ценность имеет множество эталонов измерения, включая философские, этические, политические, психологические. Вновь обращаясь к лекциям М. Фуко, прочитанным в Калифорнийском университете в Беркли почти 40 лет назад, открываем еще одну меру, заключенную в смыслах и значениях понятия парресии, сформированных в периоды становления демократии[17].

---

[16] Кругляк Е. Е. Дипломатический дискурс социальных медиа (лингвистический аспект) URL: http://www.discourseanalysis.org/ada20_2/st187.shtml (дата обращения: 20.04.2021).

[17] Фуко М. Речь и истина. Лекции о парресии (1982–1983) /пер. с фр. Д. Кралечкина; под науч. ред. М. Маяцкого. — М.: ИД «Дело» РАНХиГС, 2020.

Термин «*парресия*» переводится с греческого как «говорение всего», «говорить без страха и стыда», «смелость / мужество высказывания истины», «свобода слова». Это специфическая форма публичной деятельности, цель которой — посредством оглашения объективно скрытых или намеренно замалчиваемых фактов обнажить истинное положение дел, при этом целенаправленно и осознанно вызвать недовольство собеседников, нарушить общественный консенсус и так же осознанно быть готовым страдать за личную дерзость.

На разных этапах политического развития общества смысловые рамки феномена парресии определялись степенью зависимости мужества и ответственности парресиаста за изрекаемую истину. В психологическом плане для оратора и общества важно определение способности субъекта не только мыслить истину, но и реально быть готовым высказывать ее другим.

М. Фуко толкует парресию как осознанное, решительное «*взятие слова*». Парресиастом может считаться тот, кто действительно отвечает тем требованиям, которые предъявляет к нему самое истина, ибо он претендует быть ее носителем. Парресиаст не должен подстраиваться под требования допустимых публичных приличий, закрепляемых современной ему политической культурой с целью «обязать субъекта высказывать истину (или брать на себя эту задачу по собственной воле)». «Парресия появляется как разрыв с традиционными формами риторики и письма. Или же как нечто пренебрегающее ими: парресия — это действие, …она позволяет речи непосредственно на души… посредством своего рода сопряжением речи и движения мысли или их взаимной прозрачности»[18].

В аксиологии античной парресии, обеспечивающей развитие основ демократии, М. Фуко выделяет три периода, которые без

[18] Фуко М. Речь и истина. Лекции о парресии (1982–1983) /пер. с фр. Д. Кралечкина; под науч. ред. М. Маяцкого. — М.: ИД «Дело» РАНХиГС, 2020. С. 54.

труда находят аналогии в современном обществе. Эпикуреизм: парресия служит образцом взаимной откровенности внутри общин людей, стремящихся к мудрости. Стоицизм: парресиаст выступает наставником статусного собеседника, достигающий дружеских отношений с ним. Тут Фуко опирается на характеристики трибуна, взятые из «Законов» Платона, где философ адвокатирует парресиасту как советнику Государя, смысл деятельности которого — исправлять личные недостатки вассала. Но — с его же изволения, то есть, изрекать истину в режиме предоставления возможности проговаривать то, что считается общественно неприемлемым, ответственность при этом лежит на Государе.

Но и этот платоновский типаж уступает публичную трибуну изложения истины современнику такого политического режима, при котором реализуется всеобщее право говорить все, что угодно, и это есть показатель «правильного функционирования демократии». Античный философ определяет это явление как «дурную паррессию», зачастую поощряемую самой демократией.

Фуко относит этот, третий, тип парресии к кинизму (от древнегреческого κύων (собака) и/или Κῠνόσαργες (Киносарг, холм в Афинах[19]). Вместе с приемами возрождения «добродетельной демократии» кинизм ввел в политическую моду «дурную парресию» — презентацию философского содержания ранней демократии, раздвигающей рамки публичного властвования в сторону простолюдия.

Парресиасты этой когорты в этическом плане разительно отличаются от представителей первых двух направлений, что

[19] Кинизм как философское течение сформировался на сломе политического мира греческих полисов после распада империи Александра Македонского и обострении борьбы за доминирование правителей тех государств, которые ранее входили в империю. Полисы, где каждый гражданин мог быть участником политической жизни, утратили это свойство. Власть и влияние стали доступны знатным или богатым. Добродетель обесценилась, общественная жизнь пришла в анемичное состояние. Радикальный способ восстановления «демократии для всех» предложили киники.

дает им основание для формирования специфических направлений политической культуры, усиливающих разрушительные тенденции в конструкции демократии.

У Платона, пишет Фуко, «дурная парресия служит характеристикой дурного демократического строя, в котором кто угодно может обратиться к гражданам и сказать им что угодно, даже … вещи, как нельзя более опасные для полиса»[20].

Эта мера гражданской зрелости / незрелости актуальна во всяком историческом случае и во все политические времена, в чем убеждает и опыт древних, описанный в трактатах Платона «Государство» и «Законы», и знание реалий современного международно-политического дискурса. Не этим ли отличился К. Пауэлл в 2003 г. в высоком собрании ООН?

Ареной международно-политической парресии нынешнего столетия стали трибуны Совета Безопасности ООН, международных саммитов, брифингов и пресс-конференций и иных форм бытования официального дипломатического дискурса (вспомним приснопамятные выступления в ООН У. Чавеса (2006 г.), М. Каддафи (2009 г.) и др.). Сегодня, по мнению журналиста-международника Аркадия Дубнова, провоцирующие высказывания парламентариев и непротокольное коммуникативное поведение — неизбежная часть демократической жизни. Эпатажные перформансы (игра на публику украинских парламентариев в ПАСЕ), скрытый цинизм и неприкрытая грубость, личные нападки (речь британского представителя М. Райкрофта на заседании СБ ООН, спровоцировавшего резкую ответную реакцию представителя РФ В. Сафронкова), жонглирование определениями — «киллер», «гангстер», «преступник» — по отношению к главам государств, противостоящим политике мирового гегемона, — все эти приемы «дурной парресии» активно присутствуют в публичном между-

[20] Фуко М. Речь и истина. Лекции о парресии (1982–1983) /пер. с фр. Д. Кралечкина; под науч. ред. М. Маяцкого. — М.: ИД «Дело» РАНХиГС. С. 98.

народно-политическом дискурсе, поощряемые, как во времена кинизма, самой демократией. Из содержания нормы, предписывающей участникам межгосударственных отношений выполнение определенных институциональных действий, влекущих за собой правовые последствия, изымается ее сердцевина — обязывающая и ограничительная функция.

Массмедиа с азартом живописуют и цитируют акты «дурной паресии» с участием влиятельных фигур международного масштаба и взрываются негодованием, когда публичные издёвки, хамство, цинизм пресекаются или получают адекватный ответ. И сами массовые коммуникации, производящие те пласты международно-политического дискурса, в которых формируются и внедряются идеи и идеологии, не гнушаются приемов «дурной парресии» (наиболее показательная провокативная политика журнала Charlie Hebdo).

Исследование технологий международно-политического дискурса, маркируемого понятием «дурной парресии», имеет ряд особенностей, обусловленных свойствами политической хронотопологии и международно-правового дискурса. И есть ряд исследований, указывающих на продуктивную возможность междисциплинарного исследования феномена парресии. Это, например, когнитивно-дискурсивный подход к изучению языка права Е. А. Бородиной, указывающий на такую характеристику правового дискурса как статусность и ролевая нормативная предопределенность его участников в предписанных правом актах институциональной коммуникации[21]. Автор делает акцент на том, что функции и особенности юридического дискурса всецело определяются сущностью права как регулятивного явления. Международное право обладает таким же регулятором.

[21] Бородина Е. А. Функции юридического дискурса в рамках когнитивно-дискурсивного подхода на примере международно-правовых актов — URL: https://cyberleninka.ru/article/n/funktsii-yuridicheskogo-diskursa-v-ramkah-kognitivno-diskursivnogo-podhoda-na-primere-mezhdunarodno-pravovyh-aktov/viewer (дата обращения: 20.04.2021).

Поскольку публичные дебаты по поводу отстаивания национальных интересов на международно-политических площадках априори имеют конфликтогенную основу, то по внутренней структуре они сравнимы с конкурирующей состязательностью сторон обвинения и защиты в судебном процессе. Такого рода коммуникации обладают особенностями, на которые указывает Н. Г. Храмцова:

— интенциональность (принцип равнодействия мотива и цели деятельности);
— коммуникативная установка на конфликт (принцип включения агрессивно-защитного механизма);
— соотношение формы и содержания (принцип эмоционально-психологического давления, при котором содержание теряет свой смысл за восприятием агрессивной формы);
— стереотипность восприятия и оценки поведения (принцип отождествления факта и пересказа (или его интерпретации);
— олицетворение коллективного ожидания и представления о необходимости, благе, справедливости (принцип харизматического господства созданного, истолкованного или применённого нормативного акта)[22].

Совокупность принципов правового дискурса в полной мере применима к анализу международно-политического дискурса. При этом возникает возможность выявлять потенциалы стратегических коммуникаций, обеспечивающих современные геополитические игры. Например, можно достаточно полно представить изменение структуры политической системы под влиянием Атлантической хартии, которую организаторы Саммита за демократию намерены заложить в основу строительства мирового порядка по западным «правилам», приверженности обязательствам в рамках НАТО как единственно легитимного,

[22] Храмцова Н. Г. Дискурс-правовой анализ: от теории к практике применения. Монография. — Курган: Изд-во Курганского гос. ун-та, 2012. С. 105, 119.

по заявлению бывшего генсека НАТО Расмуссена, центра принятия решений. На самом деле такая стратегия, основанная на глобальном политическом высокомерии, «оставляет Запад на „неправильной стороне истории“».

Введение эффектов «дурной парресии» в исследовательское пространство международно-политического дискурса позволяет рационально и адекватно оценивать аксиологические параметры современного мира, своевременно корректировать политики национальных и международных стратегических коммуникаций.

Список использованных источников и литературы

1. Берарди, Франко «Бифо». Душа за работой. От отчуждения до автономии. / Пер. с итал. К. Чекалова — М.: ООО «Издательство Грюндриссе», 2019.
2. Бородина Е. А. Функции юридического дискурса в рамках когнитивно-дискурсивного подхода на примере международно-правовых актов — URL: https://cyberleninka.ru/article/n/funktsii-yuridicheskogo-diskursa-v-ramkah-kognitivno-diskursivnogo-podhoda-na-primere-mezhdunarodno-pravovyh-aktov/viewer (Дата обращения — 20.04.2021).
3. Газета «Коммерсантъ» №219/П от 30.11.2020 — URL: https://www.kommersant.ru/doc/4593083 (Дата обращения 15.05.2021).
4. Кругляк Е. Е. Дипломатический дискурс социальных медиа (лингвистический аспект) — URL: http://www.discourseanalysis.org/ada20_2/st187.shtml (Дата обращения 20.04.2021).
5. Лавров отказал Западу в праве навязывать миру «универсальные нормы» — URL: https://e-news.su/mnenie-i-analitika/380849-lavrov-otkazal-zapadu-v-prave-navjazyvat-miru-universalnye-normy.html (дата обращения 14.05.2021).
6. Лавров С. В. О праве, правах и правилах // Коммерсантъ — 28.06.2021. №109/П.
7. Моизи Д. Геополитика эмоций. Как культуры страха, унижения и надежды трансформируют мир. — М.: МШПИ, 2010.
8. Фуко, М. Речь и истина. Лекции о парресии (1982–1983) /пер. с фр. Д. Кралечкина; под науч. ред. М. Маяцкого. — М.: ИД «Дело» РАНХиГС, 2020.
9. Храмцова Н. Г. Дискурс-правовой анализ: от теории к практике применения**.** Монография. — Курган: Изд-во Курганского гос. ун-та, 2012.

А. Г. Цветкова,
старший эксперт Национальной ассоциации
международной информационной безопасности,
стажер Дипломатической академии МИД России

ПРОБЛЕМА МЕР ДОВЕРИЯ В ОБЛАСТИ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ: РЕАЛЬНОСТЬ И ПЕРСПЕКТИВЫ

Аннотация: данная статья призвана осветить некоторые из наиболее интересных актуальных подходов к проблеме мер доверия в ИКТ-среде, главным образом, России и США, препятствия к их реализации и возможные перспективы в данном направлении.

Ключевые слова: меры укрепления доверия, киберпространство международная информационная безопасность, векторы движения России в сфере МИБ, условия низкого доверия, риски кибератак, конфронтация.

В марте 2021 г. был завершен мандат Рабочей Группы открытого состава Организации Объединенных Наций (далее по тексту — РГОС, РГОС ООН), и мы получили возможность изучения итоговых документов Рабочей группы[23]. Было отмечено, что государства подтвердили сохраняющуюся актуальность мер укрепления доверия (далее по тексту — МД), рекомендованных в консенсусных докладах Группы Правительственных экспертов ООН (далее по тексту — ГПЭ).

Практические МД были рекомендованы в каждом из консенсусных докладов ГПЭ. В дополнение к этим рекомендациям, учи-

[23] На основе Итогового содержательного доклада, а также Резюме Председателя РГОС ООН — URL: https://www.un.org/disarmament/open-ended-working-group/ (дата обращения: 11.08.2021).

тывающим специфику ИКТ, в консенсусной резолюции 43/78 (H) Генеральная Ассамблея утвердила разработанное Комиссией ООН по разоружению руководство в области МД, содержащее ценные принципы, цели и характеристики МД, которые могут быть приняты к сведению при разработке новых мер, учитывающих специфику ИКТ[24].

Исходя из данных ссылок, содержащихся в Итоговом докладе РГОС, приходится констатировать, что, как и в процессе разработки Предварительного проекта Итогового доклада РГОС, рассматриваемого государствами-участниками весной 2020 г., акцент делается на нормы из доклада ГПЭ 2015 г. — вместо ссылок на принятую резолюцию Генеральной Ассамблеи ООН 73/27[25] с первым сводом из 13 правил ответственного поведения государств.

Государства обсудили желательность и жизнеспособность создания глобального репозитория МД под эгидой ООН с целью обмена политикой, передовой практикой, опытом и оценками реализации МД[26]. Согласно позиции Российской Федерации[27], в этом нет реального решения проблемы обеспечения международной информационной безопасности (далее по тексту — МИБ).

Кроме того, в документе, в том числе в разделе, посвященном мерам доверия, не соблюдена идея непредвзятого описания состоявшихся в РГОС дискуссий. Отдельные подразделы проекта

---

[24] п. 44 Итогового содержательного доклада РГОС ООН — URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 11.08.2021).

[25] Резолюция Генеральной Ассамблеи ООН 73/27.

[26] п. 31 Резюме Председателя РГОС ООН. — URL: https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf (дата обращения: 11.08.2021).

[27] Комментарий РФ по «нулевому» проекту доклада Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. — URL: https://front.un-arm.org/wp-content/uploads/2021/02/Russian-commentary-on-the-OEWG-zero-draft-report-RUS.pdf (дата обращения: 11.08.2021).

доклада сформулированы в формате аналитического — на деле необъективного — пересказа обсуждений в рамках Группы. Положения, отражающие позицию лишь отдельных стран, подаются как согласованные от лица всех государств («государства отметили, что…»). В то же время ранее согласованные постулаты зачастую камуфлируются в формулировке «некоторые государства отметили, что…»[28].

Это ведет к эрозии ранее достигнутого консенсуса по таким стержневым вопросам, как необходимость соблюдения государствами принципов Устава ООН, неиспользования ИКТ в военных целях, невмешательства во внутренние дела других стран и т.д.[29] Такова позиция России в отношении итогов работы РГОС ООН. Каковы же актуальные подходы самой России к проблеме мер доверия?

В сентябре 2020 г. в своем Заявлении[30] Президент В. В. Путин предложил США одобрить комплексную программу практических мер по перезагрузке наших отношений в сфере использования ИКТ. Данная Программа фактически представляет собой актуальный перечень мер укрепления доверия.

Далее, уже через месяц, в октябре 2020 г. Президент В. В. Путин в своем выступлении на заседании дискуссионного клуба «Валдай» назвал киберпространство «площадкой для апробирования» мер укрепления доверия между конкурирующими государствами[31].

---

[28] Комментарий РФ по «нулевому» проекту доклада Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. — URL: https://cutt.ly/UmbkYCy (дата обращения: 11.08.2021).

[29] Там же.

[30] Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. — URL: http://www.kremlin.ru/events/president/news/64086 (дата обращения: 18.05.2021).

[31] Материалы заседания дискуссионного клуба «Валдай». URL: http://kremlin.ru/events/president/transcripts/64261 (дата обращения: 18.05.2021).

Президент России напомнил об обращении к Соединённым Штатам с предложением начать комплексное обсуждение вопросов МИБ и выразил надежду на то, что после выборов президента США следующая администрация «откликнется на приглашение начать разговор по этой теме»[32].

И США действительно откликнулись, правда спустя более чем полгода. Сейчас активно обсуждаются переговоры двух Президентов летом 2021 г. и сотрудничество в киберсфере будет среди тем возможного саммита Владимира Путина и Джо Байдена[33].

Тогда же, в ответ на сентябрьское Заявление В. В. Путина, Министерство юстиции США выдвинуло заочное и бездоказательное обвинение шести россиянам в международном хакерстве, помощник генерального прокурора США по национальной безопасности Джон Демерс назвал инициативу России лживой риторикой, циничной и дешевой пропагандой, а госсекретарь США Майкл Помпео назвал Россию одним из величайших разрушителей глобального интернета[34].

12 апреля 2021 г. в России были утверждены новые Основы государственной политики Российской Федерации в области международной информационной безопасности[35].

В преддверии обсуждения проекта Основ Президентом В. В. Путиным были отмечены принципиальные векторы движения России в сфере МИБ, в том числе и то, что Россия по-прежнему открыта для диалога и взаимодействия; серьёзное внима-

---

[32] Там же.

[33] МИД назвал одну из тем возможного саммита Путина и Байдена. — URL: https://ria.ru/20210428/sammit-1730347254.html (дата обращения: 18.05.2021).

[34] U.S. Charges Russian Intelligence Officers in Major Cyberattacks. — URL: https://www.state.gov/united-states-charges-russian-military-intelligence-officers-for-cyber-crimes/ (дата обращения: 18.05.2021).

[35] Основы государственной политики Российской Федерации в области международной информационной безопасности. — URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 18.05.2021).

ние следует уделить налаживанию механизмов практического сотрудничества в сфере МИБ; нам необходимы обмен опытом и совместное реагирование на компьютерные инциденты; важно оказывать помощь нашим партнерам в построении систем информационной безопасности, предоставлять им технологии и совместно расследовать киберинциденты[36].

Все перечисленные аспекты отражены в Основах и могут быть смело отнесены к мерам укрепления доверия, на развитие которых Россия нацелена сегодня. Выработка мер укрепления доверия является одним из основных направлений реализации государственной политики РФ в области МИБ[37].

Меры укрепления доверия являются не только краеугольным вопросом национальных стратегий в части МИБ, но также выбираются в качестве темы для неофициальных переговоров на треках 1.5 и 2. Так, при участии бывших официальных лиц и действующих экспертов из России, Китая и США, имеющих компетенции и полномочия на отражение позиций своих стран, а также при посредничестве организации-медиатора *(название и принадлежность организации не публикуются по соображениям конфиденциальности)*, в конце 2020 г. был проведен неофициальный диалог, темой которого стали «Инновация и универсализация эффективных мер доверия (далее по тексту — кибер-МД) для предотвращения эскалации конфликтов в киберпространстве».

По итогам переговоров участниками констатировался тот факт, что на сегодняшний день кибер-МД не достигли своих целей по содействию прозрачности, коммуникации и сдержанности, особенно между государствами, имеющими состязательные или конкурентные отношения. Причины этого варьируются от отсутствия

[36] Заседание Совета Безопасности. — URL: http://kremlin.ru/events/security-council/65231 (дата обращения: 18.05.2021).

[37] Основы государственной политики Российской Федерации в области международной информационной безопасности. — URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 18.05.2021).

согласованных стандартов верификации и политической воли до трудности повышения прозрачности в изначально скрытом киберпространстве. Кроме того, существует необходимость выработать общее понимание того, что сработало, а что нет в предыдущих соглашениях и их механизмах, включая двусторонние соглашения.

Большое значение приобретает развитие концепции «МД в условиях низкого уровня доверия». Переговоры сторон в условиях низкого доверия должны базироваться на общем осознании возросших рисков — это поможет стимулировать подлинный интерес к поиску общих позиций и политическую волю к достижению конструктивного соглашения.

Участники диалога признали, что восприятие рисков по-прежнему относительно невелико и расходится: например, Россия видит в качестве основных рисков кибератаки против объектов критической информационной инфраструктуры (далее по тексту — КИИ), а США — операции кибервлияния и шпионаж. При этом, подобные разногласия не должны препятствовать параллельному обсуждению различных рисков и что России и США следует, к примеру, рассмотреть операции влияния в контексте пандемии и, возможно, разработать новый механизм МД для устранения этого нового риска.

Ключевые выводы переговоров разделяются как российской, так и американской, и китайской сторонами. Вероятно, это редкий, если не исключительный на сегодня, случай достижения общего понимания по чувствительной проблеме МД. К сожалению, в современной политической ситуации позиция США продолжает оставаться конфронтационной по отношению к России.

В марте 2021 г. газета «The Wall street journal» опубликовала статью[38], согласно которой «РФ нарушает требование не подры-

[38] Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other COVID-19 Vaccines, U.S. Officials Say. — URL: https://www.wsj.com/articles/russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200 (дата обращения: 18.05.2021).

вать ответные меры на пандемию в других странах, используя операции влияния. Подобные публикации не могут быть расценены иначе, кроме как откровенная русофобская риторика, влекущая за собой развитие мер недоверия, в то время как Россия стремится к диалогу по развитию мер доверия».

Буквально через 10 дней после данной публикации, в ходе слушаний в подкомитете Палаты представителей США по разведке и специальным операциям, эксперт по кибербезопасности Агентства военной разведки Джеймс Салливан заявляет, что Россия и Китай, главные противники США, участвуют в тайной войне, используя дезинформацию, атакуя общественность и правительство США, чтобы подорвать социальную сплоченность, экономику, моральные устои и систему госуправления Америки. Москва «ведет борьбу за информационное поле как в мирное, так и военное время, используя электронные и иные средства»[39].

Согласно Докладу Национальной разведки США об «иностранных угрозах» в выборы 2020, Россией был использован ключевой стратегический инструмент — использование «прокси»-структур разведки для продвижения «нарративов влияния» — вводящих в заблуждение или необоснованных обвинениях против президента Байдена — через СМИ, официальных лиц, и известных личностей, включая близких к Дональду Трампу[40].

Такова базовая позиция США. Однако стоит отметить и некоторые позитивные сигналы.

25 ноября 2020 г. был опубликован комплексный программный документ альянса НАТО под названием «НАТО 2030: вместе

[39] «Three Warfares»: U.S. pummeled by covert disinformation war waged by Russia, China. — URL: https://www.washingtontimes.com/news/2021/mar/16/us-pummeled-covert-disinformation-war-waged-china-/ (дата обращения: 18.05.2021).

[40] Разведка США: РФ вела кампанию по очернению Байдена в его бытность кандидатом. — URL: https://www.dw.com/ru/razvedka-ssha-rf-vela-kampaniju-poocherneniju-bajdena-v-ego-bytnost-kandidatom/a-56894060 (дата обращения: 18.05.2021).

в новую эру»[41]. Этот документ включает в себя в том числе блок размышлений на тему обмена информацией, рассматриваемого в качестве одной из ключевых мер доверия в контексте борьбы с киберугрозами.

В докладе подчеркивается, что доверие является ключевым компонентом эффективного обмена информацией; доверие не требует, чтобы участники любили друг друга или делились всем, а лишь означает, что участники разумно убеждены в том, что все другие стороны будут соблюдать согласованные правила. Политика и структура должны включать оперативные процессы, направленные на укрепление доверия и уверенности, особенно в тех случаях, когда между заинтересованными сторонами отсутствует личная интеграция[42].

В качестве основных препятствий на пути реализации данных постулатов отмечены такие проблемы, как неспособность и нежелание делиться разведывательной информацией об угрозах; необходимость установления границ ответственности и подотчетности между государством и частным сектором, поскольку большая часть объектов нападения в мире находится в собственности и под контролем частного сектора. Отдельно говорится о важности понимать друг друга — управление кибербезопасностью требует «стабильности ожиданий» в отношениях между всеми субъектами ИКТ.

Неделю назад в своем выступлении Джо Байден заявил[43], что официальная Москва не причастна к хакерскому взлому американской трубопроводной компании Colonial Pipeline, которая занимается доставкой нефтепродуктов по стране. По

---

[41] NATO 2030: Making a strong alliance even stronger. — URL: https://www.nato.int/nato2030/ (дата обращения: 18.05.2021).

[42] Sauerwein et al., 2017; Sillaber et al., 2016; Va: B Zquez et al., 2012; Wagner et al., 2019.

[43] Байден объявил Россию непричастной к хакерской атаке на трубопровод. — URL: https://ytro.ru/news/politics/2021/05/13/1481743.shtml (дата обращения: 18.05.2021).

его словам, Вашингтон напрямую контактирует с Москвой в вопросе принятия необходимых мер против тех, кто вымогает выкуп за запуск трубопровода, а также чтобы предотвратить в дальнейшем подобные преступные действия. Байден также сообщил, что хочет обсудить тему международных стандартов по кибербезопасности с президентом России Владимиром Путиным для совместной борьбы с видом мошенничества, когда власти устанавливают, что именно с территории их страны происходит атака.

Таким образом, несмотря на имеющуюся конфронтацию России и США в вопросах МИБ, включая меры доверия, прослеживается положительная динамика, а готовность к регулярным, пусть сегодня в основном и неофициальным дискуссиям, которую проявляют отечественные, американские, китайские представители наряду с экспертами других заинтересованных государств — сама по себе является общей мерой доверия.

Список использованных источников и литературы

1. Байден объявил Россию непричастной к хакерской атаке на трубопровод. — URL: https://ytro.ru/news/politics/ 2021/05/13/1481743.shtml (дата обращения: 18.05.2021).
2. Валентин Богданов, Доклад Национальной разведки (NIC) об «иностранных угрозах» в выборы 2020: что важно (а что не очень) — ЧАСТЬ II. — URL: https://telegramstore.com/catalog/channels/valentinbogdanov/3494 (дата обращения: 18.05.2021).
3. Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. — URL: http://www.kremlin.ru/events/president/news/64086 (дата обращения: 18.05.2021).
4. Итоговый содержательный доклад РГОС ООН. — URL: https://www.un.org/disarmament/open-ended-working-group/ (дата обращения: 18.05.2021).
5. Комментарий РФ по «нулевому» проекту доклада Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. —

URL: https://front.un-arm.org/wp-content/uploads/2021/02/Russian-commentary-on-the-OEWG-zero-draft-report-RUS.pdf (дата обращения: 18.05.2021).

6. Материалы заседания дискуссионного клуба «Валдай». — URL: http://kremlin.ru/events/president/transcripts/64261 (дата обращения: 18.05.2021).
7. МИД назвал одну из тем возможного саммита Путина и Байдена. — URL: https://ria.ru/20210428/sammit-1730347254.html (дата обращения: 18.05.2021).
8. Разведка США: РФ вела кампанию по очернению Байдена в его бытность кандидатом. — URL: https://www.dw.com/ru/razvedka-ssha-rf-vela-kampaniju-poocherneniju-bajdena-v-ego-bytnost-kandidatom/a-56894060 (дата обращения: 18.05.2021).
9. Резолюция Генеральной Ассамблеи ООН 73/27. — URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27 (дата обращения: 18.05.2021).
10. Резюме Председателя РГОС ООН. — URL: https://www.un.org/disarmament/open-ended-working-group/ (дата обращения: 18.05.2021).
11. «Three Warfares»: U.S. pummeled by covert disinformation war waged by Russia, China. — URL: https://www.washingtontimes.com/news/2021/mar/16/us-pummeled-covert-disinformation-war-waged-china-/ (дата обращения: 18.05.2021).
12. NATO 2030: Making a strong alliance even stronger. URL: https://www.nato.int/nato2030/ (дата обращения: 18.05.2021).
13. Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other COVID-19 Vaccines, U.S. Officials Say. URL: https://www.wsj.com/articles/russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200 (дата обращения: 18.05.2021).
14. U.S. Charges Russian Intelligence Officers in Major Cyberattacks. — URL: https://www.state.gov/united-states-charges-russian-military-intelligence-officers-for-cyber-crimes/ (дата обращения: 18.05.2021).

К. С. Бойко,
эксперт Национальной ассоциации
международной информационной безопасности

МЕРЫ УКРЕПЛЕНИЯ ДОВЕРИЯ: ЭВОЛЮЦИЯ ПОДХОДОВ НА ПЛОЩАДКЕ ООН

Аннотация: В статье рассматривается эволюция мер укрепления доверия на площадке ООН, нашедших отражение в докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2010, 2013 и 2015 годов, а также в докладе Рабочей группы открытого состава 2021 года.

Ключевые слова: меры укрепления доверия, информационно-коммуникационные технологии, Организация Объединенных Наций, Группа правительственных экспертов, Рабочая группа открытого состава.

Организация Объединенных Наций играет лидирующую роль в развитии и реализации глобальных мер укрепления доверия. Эта проблематика прочно вошла в практику деятельности профильных групп ООН.

Впервые о необходимости выработки мер укрепления доверия было сказано в докладе Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (далее — Группа правительственных экспертов, Группа) 2010 года. Уже тогда эксперты из 15 стран мира заявили о важности разработки мер, способных создать доверие, повысить транспарентность и стабильность, обеспечить обмен информацией и передовыми методами[44].

[44] Доклад Группы правительственных экспертов ООН A/65/201 от 30 июля 2010 года. — URL:// https://documents-dds-ny.un.org/doc/UNDOC/

Группа рекомендовала государствам — членам ООН разработать меры укрепления доверия в целях снижения риска возникновения неправильного восприятия в результате дезорганизации или нарушений, связанных с применением информационно-коммуникационных технологий (ИКТ).

В числе первоочередных мер были предложены:

— обмен мнениями по вопросу об использовании ИКТ в конфликтах;
— обмен информацией о национальных законах и национальных стратегиях обеспечения безопасности ИКТ, принципах и передовых методах;
— выработка общей терминологии и определений.

Доклад следующей Группы правительственных экспертов 2013 года уже не ограничивался общими рекомендациями, а включал самостоятельный раздел с первоначальным перечнем мер укрепления доверия[45].

В докладе вполне конкретно и развернуто были сформулированы цели выработки таких мер. Часть из них повторяла подходы, изложенные в докладе 2010 года. Это, прежде всего, нацеленность на повышение степени доверия, транспарентности и бóльшей предсказуемости.

Однако эксперты Группы в докладе 2013 года сформулировали новые цели, связанные с развитием сотрудничества, с уменьшением риска возникновения конфликтов благодаря снижению вероятности возникновения недопонимания, с решением проблем, вызывающих озабоченность государств в связи с использованием ИКТ. Кроме того, была обозначена главная цель этих мер — укрепление международной безопасности.

GEN/N05/453/65/PDF/N0545365.pdf?OpenElement (дата обращения: 13.05.2021).

[45] Доклад Группы правительственных экспертов ООН A/68/98 от 24 июня 2013 года. — URL:// https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf?OpenElement (дата обращения: 13.05.2021).

В качестве рекомендаций Группа предложила рассмотреть вопрос о разработке первоначальных практических мер укрепления доверия.

К ним, как и в докладе 2010 года, был отнесен добровольный обмен мнениями и информацией о национальных стратегиях, передовом опыте, процессах принятия решений, профильных национальных организациях и мерах по развитию международного сотрудничества в данной области.

Но были рекомендованы и новые меры, которые носили прикладной характер и касались:

— во-первых, создания на различных уровнях консультативных рамок для предотвращения деструктивных инцидентов с использованием ИКТ;
— во-вторых, межгосударственного обмена информацией о компьютерных инцидентах;
— в-третьих, организации взаимодействия между национальными группами экстренной готовности к компьютерным инцидентам и расширения сотрудничества по противодействию им.

По мнению экспертов, эти меры должны были позволить приобрести столь необходимый практический опыт и стать важным ориентиром для будущей работы.

Спустя два года, в 2015 году, новая Группа правительственных экспертов продолжила изучение проблематики мер укрепления доверия и также включила ее в свой итоговый доклад в виде отдельного раздела[46].

Целевые ориентиры выработки таких мер сохранили преемственность. В качестве основной цели, как и ранее, определялось повышению степени транспарентности, предсказуемости и стабильности.

[46] Доклад Группы правительственных экспертов ООН A/70/174 от 22 июля 2015 года. — URL:// https://documents-dds-ny.un.org/ doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата обращения: 13.05.2021).

Однако в докладе 2015 года цель выработки мер укрепления доверия выведена на качественно новый уровень, поскольку она уже была связана с содействием поддержанию международного мира и безопасности, с расширением межгосударственного сотрудничества для снижения угрозы конфликтов в информационной сфере.

Такое целеполагание предопределило рекомендации Группы государствам мирового сообщества в отношении следующих добровольных мер укрепления доверия:

— во-первых, определение контактных центров для рассмотрения серьезных инцидентов в сфере ИКТ;
— во-вторых, создание и поддержка механизмов проведения на различных уровнях консультаций для снижения риска ошибочного восприятия, эскалации и конфликта, которые могут быть вызваны инцидентами в сфере ИКТ;
— и, в-третьих, представление информации о национальных и транснациональных угрозах, факторах уязвимости и установленных скрытых функциях в продуктах ИКТ, передовых методах обеспечения информационной безопасности, а также о национальных подходах к категорированию критически важной информационной инфраструктуры.

Очевидно, что эти меры стали логическим продолжением линии Группы правительственных экспертов на расширение перечня практико-ориентированных мер.

Эти меры уже были нацелены на укрепление трансграничного сотрудничества в устранении транснациональных факторов уязвимости критической информационной инфраструктуры.

В данной области правительственные эксперты рекомендовали сосредоточиться на создании баз данных профильных национальных законодательств и стратегиях и их публичном представлении.

Прикладной характер имели рекомендации Группы, связанные с созданием механизмов проведения консультаций по вопросам защиты критически важной информационной ин-

фраструктуры, а также механизмов рассмотрения запросов, связанных с использованием ИКТ.

Важное значение придавалось выработке единых подходов к классификации инцидентов в сфере использования ИКТ с точки зрения их масштабов и серьезности для обмена информацией о них.

Новое качество в докладе 2015 года приобрели рекомендации о дополнительных мерах укрепления доверия по расширению сотрудничества.

Государства ориентировались на принятие добровольных соглашений:

— во-первых, по укреплению механизмов взаимодействия между соответствующими ведомствами по противодействию инцидентам в сфере безопасности ИКТ;
— во-вторых, по созданию координационных центров для обмена информацией о случаях злонамеренного использования ИКТ и оказания помощи в проведении расследований;
— в-третьих, по созданию национальных групп реагирования на компьютерные инциденты и поддержанию сотрудничества между ними;
— и в-четвертых, по выполнению просьб других государств в рамках расследования преступлений, связанных с использованием ИКТ для террористических целей или с другой злонамеренной деятельностью.

Эти меры выводили сотрудничество всех заинтересованных сторон на межгосударственный уровень.

Меры укрепления доверия стали предметом обсуждения и новой Группы правительственных экспертов, которая завершит свою работу 28 мая 2021 года, поэтому говорить о ее итогах пока преждевременно.

Данная проблематика находилась и в поле зрения нового дискуссионного механизма на площадке ООН — созданной по инициативе России Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций

в контексте международной безопасности (далее — Рабочая группа открытого состава, РГОС), итоговый доклад которой был принят консенсусом 10 марта 2021 года[47].

В этом докладе, как и в докладах Группы правительственных экспертов, отмечается, что меры укрепления доверия — это меры обеспечения транспарентности, сотрудничества и стабильности.

Сам диалог в рамках нового дискуссионного формата ООН был признан мерой укрепления доверия, поскольку способствовал открытому и транспарентному обмену мнениями по вопросам восприятия угроз и уязвимостей, ответственному поведению государств и других субъектов, обмену передовым опытом, стимулирующему коллективную разработку и имплементацию нормативных рамок в данной сфере.

Рабочая группа открытого состава рассмотрела цели мер укрепления доверия под углом обеспечения международного мира и безопасности в глобальном информационном пространстве.

Поэтому, как отмечено в итоговом докладе, эти меры должны способствовать:

— во-первых, предотвращению конфликтов, недопущению неверного восприятия и неправильного понимания, а также снижению напряженности;
— во-вторых, укреплению общей безопасности, устойчивости и мирного использования ИКТ;
— в-третьих, имплементации норм ответственного поведения государств, содействующих укреплению доверия и обеспечивающих большую ясность, предсказуемость и стабильность в сфере использования ИКТ государствами;
— в-четвертых, выработке общего понимания среди государств, содействуя тем самым обеспечению более мирной международной обстановки.

[47] Доклад Рабочей группы открытого состава A/AC.290/2021/CRP.2 от 10 марта 2021 года. – URL:// https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 13.05.2021).

Достижение этих целей, по мнению РГОС, поможет снизить недоверие, возникающее из-за недопонимания между государствами, а также создать основу для дополнительных, расширенных договоренностей и соглашений в будущем.

Рабочая группа открытого состава также пришла к выводу, что существование профильных государственных и региональных механизмов и структур, а также национальных центров реагирования на компьютерные инциденты крайне важно для достижения целей мер укрепления доверия.

Еще одним действенным инструментом, как считают эксперты РГОС, должны стать государственные контактные пункты, признанные экспертами самостоятельной мерой укрепления доверия, которые сами способствуют выполнению многих других мер.

Также были рекомендованы новые механизмы добровольного обмена государствами соответствующей информацией и опытом, в том числе Портал о политике в области кибербезопасности Института ООН по исследованию проблем разоружения.

Доклад закрепил общие подходы государств, представленных в Рабочей группе открытого состава, но часть предложений в рассматриваемой области, внесенных отдельными государствами, не получили консенсусной поддержки и были представлены в резюме председателя РГОС, ставшем, по сути, приложением к докладу группы.

Безусловно, спектр таких рекомендаций достаточно широк, он по-прежнему носит дискуссионный характер и требует тщательной проработки.

Поэтому не случайно обсуждение этой проблематики будет продолжено в 2021–2025 годах в формате новой Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ, также созданной по инициативе Российской Федерации.

Таким образом, на протяжении последнего десятилетия дискуссия о мерах укрепления доверия на площадке Органи-

зации Объединенных Наций прошла эволюционный путь от формулирования проблемы как таковой до выработки вполне конкретных, практико-ориентированных рекомендаций, нацеленных на создание прочной основы взаимодействия заинтересованных государств в борьбе с нарастающими вызовами и угрозами в информационной сфере.

Список использованных источников и литературы

1. Доклад Группы правительственных экспертов ООН A/65/201 от 30 июля 2010 года. — URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/453/65/PDF/N0545365.pdf? OpenElement (дата обращения: 13.05.2021).
2. Доклад Группы правительственных экспертов ООН A/68/98 от 24 июня 2013 года. — URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf? OpenElement (дата обращения: 13.05.2021).
3. Доклад Группы правительственных экспертов ООН A/70/174 от 22 июля 2015 года. — URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf? OpenElement (дата обращения: 13.05.2021).
4. Доклад Рабочей группы открытого состава A/AC.290/2021/CRP.2 от 10 марта 2021 года. — URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021- CRP.2.pdf (дата обращения: 13.05.2021).

О. В. Лебедева,
д-р ист. наук, профессор кафедры дипломатии
МГИМО МИД России

ЦИФРОВАЯ ДИПЛОМАТИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВО ВРЕМЯ ПАНДЕМИИ: ПЛЮСЫ И МИНУСЫ

Аннотация: в статье рассматриваются положительные и отрицательные аспекты трансформации дипломатии на фоне пандемии и влияние этого процесса на международную информационную безопасность. Сделан вывод о необходимости взвешенной оценки эффективности внедрения технологий в дипломатическую практику и, с учётом этого, разумной «перекалибровки» профессиональных процессов в данной сфере.

Ключевые слова: цифровая дипломатия, пандемия, информационная безопасность.

Пандемия наложила новые ограничения на дипломатическую профессию. Дипломаты не могли встречаться лично, совершать зарубежные поездки или организовывать встречи на высоком уровне. Миссии за рубежом не могли реализовать свое основное преимущество — вести информационно-аналитическую работу через личные контакты и организовывать очные мероприятия. Ведомствам иностранных дел по всему миру пришлось привыкнуть проводить большую часть своей работы онлайн, большей частью через незащищенные сети. Стали обычным явлением удаленные двусторонние встречи на политическом уровне, а также широкое распространение получили многосторонние конференции посредством зума.

Использование различных прилагательных и префиксов для описания дипломатии во время пандемии с акцентом на информационную безопасность, как правило, создает путаницу

в дискуссиях и политике в этой области. Эту путаницу можно было бы уменьшить, получив более четкие инструкции о том, что означают определенные термины, такие как «кибер», «цифровая» и «техническая» дипломатия. Например, относится ли «цифровая дипломатия» к переговорам по вопросам цифровой политики или это использование социальных сетей для публичной дипломатии?

Цифровая зависимость делает страны крайне уязвимыми к любому нарушению потоков данных. Поддержание потоков данных по всему миру жизненно важно для социальной стабильности, экономического благополучия и роста стран. Как пример, мы помним к каким серьезным экономическим потрясением привели нарушение работы электронной коммерции, электронного банкинга и услуг различных платформ, таких как Airbnb и Uber[48].

Глобальная геополитика в значительной степени зависит от доступа к основным интернет-кабелям, по которым осуществляется интернет-трафик между странами и континентами. В настоящее время более 90% всего глобального интернет-трафика проходит по подводным кабелям, которые в основном следуют старым географическим маршрутам, используемым телеграфными кабелями в девятнадцатом веке.

Мы можем наблюдать, что вокруг быстрорастущей технологической индустрии появились новые центры цифровой политики. В США цифровой экономический динамизм базируется в районе залива Сан-Франциско, где расположено большинство ведущих технологических компаний. Как показывает исследование Diplo, рост технодипломатии в районе залива, где более 50 стран развивают свое представительство либо через традиционные консульства в Сан-Франциско, либо через новые типы представительств, такие как Swissnex hub (Центр содействия бизнесу). Одновременно те же компании размещают большинство

[48] Зайцев Ю. К. Россия как международный донор: трудности в оценке помощи развитию // РСМД. — 07.08.2020. — URL: https://russiancouncil.ru/analytics-and-comments/analytics/rossiya-kak-mezhdunarodnyy-donor-trudnosti-v-otsenke-pomoshchi-razvitiyu/ (дата обращения: 11.08.2021).

своих подразделений управления в Вашингтоне или Бостоне, подчеркивая растущую взаимозависимость между правительствами и технологическими гигантами.

Такие же процессы мы можем наблюдать и в Китае, где большая часть цифровой активности происходит в районе Шэньчжэня, в то время как Пекин выступает в качестве центра регулирования и политики по цифровым вопросам.

Дипломатам сегодня приходится иметь дело с совершенно новым набором вопросов цифровой политики при продвижении интересов своих стран. Большинство из этих вопросов рассматриваются в контексте интернета и цифрового управления. Любой, кто ориентируется в этой области, должен знать о потенциальной терминологической путанице. Они используют цифровые инструменты в своей повседневной работе, начиная с переговоров и представительства, заканчивая коммуникацией и анализом политики. Хотя наиболее целенаправленным и эффективным является использование социальных сетей для продвижения публичной дипломатии (например, дипломатия Twitter, дипломатия Facebook), цифровые инструменты оказывают гораздо более существенное влияние на другие функции дипломатии.

Во время пандемии COVID-19 дипломатия перешла на онлайн-платформы для проведения конференций, такие как Zoom. Однако онлайн-встречи не так новы, как можно было бы подумать[49]. Многие европейские дипломатические ведомства уже давно используют этот инструмент для экономии расходов на командировки, поездки и очные встречи, у некоторых, особенно скандинавских стран, уже давно зрела мысль организовывать посольства не на постоянной основе, а по принципу ad hoc.

Однако онлайн-встречи имеют много плюсов и минусов с точки зрения информационной безопасности. Как показал

[49] Громогласова Е. С. Гуманитарная дипломатия в современных международных отношениях: опыт системного исследования / Е. С. Громогласова. — М.: ИМЭМО РАН. — 2018. — С. 25.

пандемический кризис, они обеспечивают непрерывность работы, но являются достаточно уязвимы для хакерского взлома. Они также увеличивают охват, позволяя участвовать без физического присутствия, что часто обусловлено командировочными и другими расходами. Одним из основных недостатков онлайн-встреч является отсутствие физического контакта, что важно для укрепления доверия и эмпатии, которые необходимы для решения, в частности, спорных и политических вопросов.

Twitter и Facebook в настоящее время являются самыми популярными электронными инструментами, используемыми дипломатическими службами во всем мире[50]. Twitter используется в качестве инструмента публичной дипломатии во многих странах. Еще предстоит выяснить, повлияют ли и как нынешние споры вокруг Twitter на дипломатию. Другие инструменты социальных сетей, используемые в публичной дипломатии, включают в себя Facebook, YouTube, FlickR, LinkedIn и Pinterest.

Можно выделить некоторые важные плюсы дипломатии во время пандемии:

— изменения в политической, социальной и экономической среде, в которой осуществляется дипломатия (например, характер и распределение власти, новые типы конфликтов и изменение характера суверенитета и взаимозависимости в международных отношениях);
— появление новых политических вопросов во внешней политике, таких как кибербезопасность, конфиденциальность, управление данными, электронная коммерция и киберпреступность;
— использование цифровых инструментов в практике дипломатии, таких как социальные сети, онлайн-конференции и анализ больших данных.

[50] Куриэль И. Кризис коронавируса и подъем цифровой дипломатии // МИД Израиля. — 01.07.2020. — URL: https://mfa.gov.il/MFARUS/PressRoom/BehindHeadlines/Pages/The-Covid-19-Crisis-and-the-Rise-of-Digital-Diplomacy.aspx (дата обращения: 11.08.2021).

В последнее время накапливаются жалобы на трудности и недостатки, которые создает дистанционная дипломатия. Некоторые отмечают, что трудно вести реальные переговоры и участвовать в реальных уступках и уступках без человеческого контакта, побочных разговоров и даже способности понимать язык тела. Способность строить и поддерживать значимые отношения подрывается. Точно так же повседневные вопросы могут решаться дистанционно на более низких уровнях, но более крупные решения неуловимы без личного участия лидеров. Например, на многостороннем саммите окончательные детали многих соглашений часто достигаются с помощью личной дипломатии лидеров, что требует неформальных частных обсуждений в кулуарах саммита. Эти возможности трудно воспроизвести в интернете[51].

В целом, существует повышенная склонность к неправильному восприятию и непониманию, а также большая угроза того, что искажение фактов пройдет незамеченным. Без дополнительных разговоров и уточнений, языка тела или ощущения межгрупповой динамики другой стороны дипломаты изо всех сил пытаются достичь более глубокого понимания. Технические барьеры, включая связь, язык и часовые пояса, делают онлайн-платформы ненадежными для переговоров, чувствительных ко времени, и влияют на способность достичь соглашения по существу. И такого понятия, как «неофициально», больше не существует. Дипломаты постоянно осознают, что все, сказанное на онлайн-платформе, может быть легко записано, что препятствует отклонениям от официальной позиции и, таким образом, подрывает тонкость дипломатической работы.

Наконец, онлайн-платформы сталкиваются с вопросами информационной безопасности. Они могут быть взломаны шпионскими агентствами, частными разведывательными организация-

[51] Шумилин А.И. Фактор пандемии во внешней политике Евросоюза // Научно-аналитический вестник Института Европы РАН. — 2020. — № 2. — URL: https://cyberleninka.ru/article/n/faktor-pandemii-vo-vneshney-politike-evrosoyuza (дата обращения: 11.08.2021).

ми или даже преступниками, и все это может помешать откровенному обмену. Существует также преднамеренное срывание встреч, иногда называемое «Зум-бомбежкой»[52]. Премьер-министр Великобритании Борис Джонсон опубликовал в Твиттере фотографию заседания кабинета министров, на которой был четко виден идентификатор масштабирования — напоминание о растущей опасности участия самозванцев или хакеров, скрывающихся в тени. В сочетании с использованием технологии глубокого фальшивого видео возможности для озорства и, что еще хуже, срыва мероприятий, достаточно значительны.

Несмотря на критику, некоторые дипломаты положительно отзывались об онлайн-дипломатии, хотя она была смешана с опасениями, что она может быть использована в качестве предлога для глубокого сокращения бюджета и принудительного сокращения числа сотрудников иностранных ведомств. Особенно настороженно к зуму относится старшее поколение дипломатов, опасаясь, что цифровые технологии полностью заменят практику личной дипломатии.

Одним из возможных общих результатов пандемии станет увеличение удаленной и онлайн-работы во всех областях, подкрепленное необходимостью перекалибровки профессиональных процессов из-за сокращения бюджетов. Однако ведомства иностранных дел должны инициировать и возглавлять эти изменения, а не быть вынужденными адаптироваться из-за сокращения бюджета, введенного их казначействами.

Взвешивая все «за» и «против» такой рационализации, миссии должны убедиться в том, что основные экспертные знания сохраняются внутри организации и что их посольства организованы таким образом, чтобы сосредоточиться на деятельности, которая не может осуществляться удаленно, такой как привлечение

[52] Чернышева Е. Сервис Zoom может стать менее популярным из-за проблем с безопасностью // РБК. — 14.04.2020. — URL: https://plus-one.rbc.ru/society/servis-zoom-ne-bezopasen (дата обращения: 11.08.2021).

общественности, налаживание конфиденциальных отношений и обеспечение своих столиц надежной местной перспективой, вытекающей из присутствия на местах. Наконец, укрепление безопасности и надежности онлайновых каналов дипломатической связи — ответственность, разделяемая правительствами и операторами платформ, — будет иметь решающее значение для предотвращения утечек, затруднений и недопонимания, которые могут поставить под угрозу успешную дипломатию.

И прежде всего нужно решить, является ли такой вид дипломатии достаточно эффективным. Дипломатия традиционно предполагает некоторую степень конфиденциальности. Поэтому любые цифровые технологии отнюдь не заменят полевую работу дипломата. Они также не смогут заменить и работу таких крупных центров многосторонней дипломатии как Женева, Нью-Йорк и Вена. Они по-прежнему остаются идеальным местом для реализации инициатив и проектов, реализуемых на разных уровнях разными организациями. Или, например, личные встречи конфликтующих сторон всегда были проявлением жеста доброй воли и символической ценности решения вопроса. Возможно ли все это в рамках переговоров в удаленном формате? Это остается большим вопросом.

Список использованных источников и литературы

1. Громогласова Е. С. Гуманитарная дипломатия в современных международных отношениях: опыт системного исследования / Е. С. Громогласова. — М.: ИМЭМО РАН. — 2018. — 124 с.
2. Зайцев Ю. К. Россия как международный донор: трудности в оценке помощи развитию // РСМД. — 07.08.20f0. — URL: https://russiancouncil.ru/analytics-and-comments/analytics/rossiya-kak-mezhdunarodnyy-donor-trudnosti-v-otsenke-pomoshchi-razvitiyu/ (дата обращения: 11.08.2021).
3. Куриэль И. Кризис коронавируса и подъем цифровой дипломатии // МИД Израиля. — 01.07.2020. — URL: https://mfa.gov.il/MFARUS/PressRoom/BehindHeadlines/Pages/The-Covid-19-Crisis-and-the-Rise-of-Digital-Diplomacy.aspx (дата обращения: 11.08.2021).

4. Чернышева Е. Сервис Zoom может стать менее популярным из-за проблем с безопасностью // РБК. — 14.04.2020. — URL: https://plus-one.rbc.ru/society/servis-zoom-ne-bezopasen (дата обращения: 11.08.2021).
5. Шумилин А. И. Фактор пандемии во внешней политике Евросоюза // Научно-аналитический вестник Института Европы РАН. — 2020. — №2. — URL: https://cyberleninka.ru/article/n/faktor-pandemii-vo-vneshney-politike-evrosoyuza (дата обращения: 11.08.2021).

А. К. Бобров,
канд. ист. наук,
старший преподаватель кафедры дипломатии
МГИМО МИД России

ЦИФРОВАЯ ДИПЛОМАТИЯ В ДЕЯТЕЛЬНОСТИ МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ В ЭПОХУ COVID-19: СРАВНИТЕЛЬНЫЙ АНАЛИЗ НАЦИОНАЛЬНЫХ ПРАКТИК

Аннотация: в статье проведен сравнительный анализ национальных практик использования цифровой дипломатии в деятельности различных Министерств иностранных дел. Национальный опыт внешнеполитических ведомств будет изучен с точки зрения изменений таких направлений деятельности как информационно-разъяснительная работа, протокол и консульская служба.

Ключевые слова: цифровая дипломатия, пандемия COVID-19, МИД России.

Пандемия коронавируса, официально начавшаяся в конце 2019 г. и с разной степенью интенсивности продолжающаяся вплоть до сегодняшнего дня, оказала значительное влияние не только на развитие естественных наук (биология, медицина, химия) и сопряженных с ними профессии (например, врачебное дело), но и на такие далёкие от них области человеческой деятельности как международные отношения и дипломатия. Так, например, ставшие привычными в последние месяцы социальное дистанцирование, самоизоляции, закрытие границ и другие виды санитарно-эпидемиологических ограничений привели к лавинообразному сокращению очных форматов взаимодействия (саммитов, встреч на высоком уровне, дипломатических приёмов, регулярных контактов со своими визави и многое другое), что, в свою очередь, заставило дипломатов обращаться к иным инструментам

коммуникации и привело к значительному увеличению внимания к современным методам и практикам цифровой дипломатии. В силу того факта, что с этим новым вызовом столкнулись дипломаты практических всех стран мира, основной целью этой статьи станет попытка проанализировать национальный опыт работы различных Министерств иностранных дел в период COVID-19, видимая часть которого касалась видоизменения, прежде всего, таких форм работы как информационно-разъяснительной работа, протокол и консульская деятельность.

Если говорить о последней, то с началом пандемии самой сложной проблемой стала необходимость возвращения на Родину тысячи туристов, в буквальном смысле слова «застрявших» в самых удалённых уголках планеты, причём если раньше Государственный департамент, МИД России или Кэ д'Орсе сталкивались с необходимостью точечных эвакуацией из одной или нескольких стран одного региона (как, например, это было в 2011 году во время «Арабской весны»), то в 2020 этот процесс стал поистине всемирным. Для осуществления в жизнь столь грандиозное меры в одной только наше стране был создан Оперативный штаб, в который вошли МИД, Минкомсвязи (обеспечивавший цифровое сопровождение этого процесса), Минтранспорта, Министерство здравоохранения, Роспетребнадзор, ФСБ и мн. др.[53] Как результат, Российская Федерация вывезла 312 тыс. человек[54], в то время как показатели многих других стран оказались несколько скромнее (так например, за 2020 г. США эвакуировали около 100 тыс. граждан[55], ФРГ — 50 тыс.,

[53] Интервью министра иностранных дел Российской Федерации С. В. Лаврова телеканалу «РТ», 29 июня 2020 г. — URL: https://russian.rt.com/russia/article/759438-lavrov-krasovskii-intervyu-koronavirus-epidemiya (дата обращения: 20.07.2021).

[54] Список осуществлённых рейсов. Сайт МИД России. — URL: https://www.mid.ru/vyvoznye-rejsy (дата доступа 20.07.2021).

[55] COVID-19 Recovery. The US Department of State. — URL: https://www.state.gov/covid-19-recovery/ (дата доступа 20.07.2021).

а Франция — около 10 тыс.)[56], причём в отличие от практики других стран наши рейсы были организованы на безвозмездной основе. Что же касается цифровой составляющей этого процесса, большим подспорьем для обработки дипломатами огромных массивов информации стало создание технических возможностей по отправке заявок через портал «Госуслуги»[57]. Если же обращаться наиболее интересным иностранным практикам, то нельзя не отметить разработку т.н. «чат-ботов»[58], которыми пользовались внешнеполитические службы США и ряда стран Европы. Написание грамотного алгоритма позволило бы «разгрузить» работу и сотрудников ЦА и РЗУ системы МИД России, самоотверженно трудившихся в наиболее сложные периоды пандемии, благодаря чему ставший популярным в наших СМИ хэштег «своих не бросаем» воспринимался многими не как пропагандистская акция, а настоящим девизом, олицетворявшим титанический труд сотен сотрудников отечественных Министерств и ведомств.

Что же касается протокола, то в силу известных ограничений многие традиционные события пришлось либо просто отменить, либо перевести в онлайн-формат. Так, например, впервые за всю историю существования ООН было принято решение отказаться от традиционной сентябрьский недели высокого уровня, открывающей очередную сессию Генеральной Ассамблеи ООН. Как результат, в 2020 году она прошла в формате записанных

---

[56] Overview of Repatriation Flights. The EU European Commission. 7 December 2020. — URL: https://ec.europa.eu/info/files/overview-repatriation-flights_en (дата обращения: 20.07.2021).

[57] Интервью министра иностранных дел Российской Федерации С. В. Лаврова телеканалу «РТ», 29 июня 2020 г. — URL: https://russian.rt.com/russia/article/759438-lavrov-krasovskii-intervyu-koronavirus-epidemiya (дата обращения: 20.07.2021).

[58] International Travel: Emergencies. The US Department of State. — URL: https://travel.state.gov/content/travel/en/international-travel/emergencies/what-state-dept-can-cant-do-crisis.html (дата обращения: 20.07.2021).

выступлений глав государств и правительств[59]. Похожим были организованы мероприятия в рамках Группы 20, БРИКС, ОДКБ и других институтах многосторонней дипломатии, саммит которых были, например, проведены путем организации конференций в Zoom. Технические возможности этой программы оказались весьма универсальными, позволив многим Министерствам не прекращать свои еженедельные Брифинги и другие виды встреч с представителями общественности.

Наконец, организация телемоста оказалось настоящим спасением и в самые острые периоды урегулирования региональных кризисов, когда, например, именно в таком формате 9 ноября 2020 г. было подписано трёхстороннее заявление глав государств России, Азербайджана и Армении[60], остановившее кровопролитие в Нагорном Карабахе, ставшее наиболее серьёзной и продолжительной эскалацией данного конфликта с 1994 года, или когда спецпосланник Генерального секретаря ООН по Ливии Стефани Уильямс организовала в рамках «Форума ливийского политического диалога» более сотни инклюзивных переговорых онлайн-сессий с самыми разными представителями ливийского общества, создав почву для достижения договоренностей между сторонами конфликта в феврале этого года в Женеве[61].

В этой связи, очень часто в научной литературе и средствах массовой информации можно встретить дискуссию о том, на-

---

[59] World Leasers Won't Gather at the UN for Annual Debate. The New York Times. 2020. — June 8th. — URL: https://www.nytimes.com/2020/06/08/world/un-general-assembly.html (дата обращения: 20.07.2021).

[60] Заявление Президента Азербайджанской Республики, Премьер-министра Республики Армения и Президента Российской Федерации. Официальный сайт Президента РФ В. В. Путина. — URL: http://kremlin.ru/events/president/news/64384 (дата обращения: 20.07.2021).

[61] Diplomacy Disrupted: the Zoom Where it Happens//The Economist, 2021 May 1st, P. 51st — URL: https://www.economist.com/international/2021/05/01/diplomacy-has-changed-more-than-most-professions-during-the-pandemic (дата обращения: 22.05.2021).

сколько цифровая дипломатия, в целом, способна заменить традиционную. На мой взгляд, наиболее точно необходимость поиска «золотой середины» между традиционными и новыми форматами взаимодействия обозначил в одном из своих выступлений министр иностранных дел Российской Федерации С. В. Лавров: «*личное общение невозможно заменить, особенно, когда речь идет о переговорах с иностранным партнером не „для галочки". Бывают визиты (назову их „визитами вежливости"), когда один зачитал, как все у нас неплохо, второй зачитал, как все у нас хорошо, договорились встречаться еще. Я немного утрирую, но бывают легкие визиты, на которых нет задачи провести переговоры и обязательно решить какую-то проблему в данный момент. Когда такие проблемы стоят на повестке дня конкретных переговоров, это уже сложно решать онлайн. Нужно видеть глаза, и не просто глаза на „плазме", а вживую. Есть вещи, которые трудно доверить даже самой защищенной видеоконференцсвязи. Это по-человечески должно быть понятно. Думаю, что после того, как все это успокоится (надеюсь, это произойдет быстро), какие-то элементы этой работы мы будем продолжать использовать, особенно когда речь идет о партнерах, которым логистически долго и непросто добираться — например, из Южной Америки. Это целая история: когда они планируют свои загранкомандировки, они должны состыковать три–четыре–пять стран, чтобы каждый раз не тратить по пятнадцать–шестнадцать часов на перелет в один конец*»[62].

В результате пандемии COVID-19 более разнообразной и творческой стала информационно-разъяснительная работа дипломатов, в рамках которой к ставшим традиционными публикациям на официальных сайтах и аккаунтах в социальных сетях (на платформах Twitter, Facebook, Instagram, ВКонтакте)

[62] Интервью Министра иностранных дел Российской Федерации С. В. Лаврова телеканалу «РТ», 29 июня 2020 г. — URL: https://russian.rt.com/russia/article/759438-lavrov-krasovskii-intervyu-koronavirus-epidemiya (дата обращения: 20.07.2021).

добавились такие новые форматы как организация флешмобов (в частности, для целевой аудитории платформы Тик-Ток), съемка телеобращений и создание других видов видео-контента, проведение виртуальных приёмов («ноу-хау» Посольства Швейцарии в Вашингтоне), организация VR экскурсий по живописным зданиям Посольств и многое другое[63]. Конечная цель таких, на первый взгляд, не совсем дипломатических видов активности заключается в том, чтобы увеличить аудиторию подписчиков, которые, дав согласие на потребление контента на регулярной основе, становятся реципиентами более серьёзной информации о внешнеполитических подходах той или иной страны. Тем не менее, несмотря на открытие в период пандемии «окна возможностей» по увеличению потенциальной аудитории подписчиков, одним из серьёзных ограничителей для распространения российской точки зрения на текущие события глобального, регионального и национального масштабов остаётся «спящий» характер многих аккаунтов системы МИД России, нынешняя аудитория каждого из которых не превышает ста человек, подписавшихся на крайне нерегулярные обновления контента. Для того, чтобы решить эту давно назревшую проблему предлагается закрепить за молодыми дипломатами, прибывающими в РЗУ, обязанность вести регулярную информационно-разъяснительную работу в социальных сетях своей дипломатической миссии.

Таким образом, можно с уверенностью утверждать, что потребность в осуществлении цифровой дипломатии в будущем будет только возрастать. Это будет означать не только необходимость обретения дипломатами дополнительных знаний и компетенций, но и физическое увеличение объёмов задействования информационно-коммуникационной инфраструктуры,

[63] McCluskey M. Their Doors May Be Closed, but Embassies Are Still Showing People the World // The Smithsonian Magazine, 2021, January 21st. — URL: https://www.smithsonianmag.com/travel/their-doors-may-be-closed-embassies-are-still-showing-people-world-180976821/ (дата обращения: 22.05.2021).

которую, в свою очередь, будет необходимо защищать от различных хакерских атак. Как отметил в своём недавнем интервью заместитель Министра иностранных дел О. В. Сыромолотов, «… *по данным Национального координационного центра по компьютерным инцидентам, большинство кибератак на Россию в 2020 году осуществлялось из адресного пространства США, Германии и Нидерландов. Нападениям подвергались объекты, связанные с разработками вакцин, государственного управления, финансового сектора, военно-промышленного комплекса, науки, образования, здравоохранения и транспорта*…»[64].

Безусловно, на данной момент объектом различных атак становятся другие объекты критической инфраструктуры, но это совершенно не означает, что дипломатия будет находится в стороне от этих процессов, подтверждением чему является не только скандал 10-летней давности, связанный с публикацией порталом Wikileaks депеш американских дипломатов, но и недавний кризис в США, возникший после хакерской атаки на Colonial Pipeline. В этой связи, как никогда актуальными становятся предложения РФ по принятию на глобальном уровне правил ответственного поведения в сети, продвигаемые нашей страной на различных площадках взаимодействия. Если наш неоднократный призыв будет наконец-то услышан, есть надежда, что по отношению и к этому комплексу новых вызовов и угроз всё мировое сообщество сумеет выработать адекватный коллективный иммунитет.

Список использованных источников и литературы

1. Интервью министра иностранных дел Российской Федерации С. В. Лаврова телеканалу «РТ», 29 июня 2020 г. — URL: https://russian.rt.com/russia/article/759438-lavrov-krasovskii-intervyu-koronavirus-epidemiya (дата обращения: 20.07.2021).

[64] Интервью заместителя министра иностранных дел РФ О. В. Сыромолотова агентству «РИА-Новости», 12 мая 2021 г. — URL: https://ria.ru/20210512/syromolotov-1731860706.html (дата обращения: 22.05.2021).

2. Список осуществлённых рейсов. Сайт МИД России. — URL: https://www.mid.ru/vyvoznye-rejsy (дата обращения: 20.07.2021).
3. COVID-19 Recovery. The US Department of State — URL: https://www.state.gov/covid-19-recovery/ (дата обращения: 20.07.2021).
4. Overview of Repatriation Flights. The EU European Commission. 7 December 2020. — URL: https://ec.europa.eu/info/files/overview-repatriation-flights_en (дата обращения: 20.07.2021).
5. International Travel: Emergencies. The US Department of State. — URL: https://travel.state.gov/content/travel/en/international-travel/emergencies/what-state-dept-can-cant-do-crisis.html (дата обращения: 20.07.2021).
6. World Leasers Won't Gather at the UN for Annual Debate. The New York Times. 2020. — June 8th. — URL: https://www.nytimes.com/2020/06/08/world/un-general-assembly.html (дата обращения: 20.07.2021).
7. Заявление Президента Азербайджанской Республики, Премьер-министра Республики Армения и Президента Российской Федерации. Официальный сайт Президента РФ В. В. Путина. — URL: http://kremlin.ru/events/president/news/64384 (дата обращения: 20.07.2021).
8. Diplomacy Disrupted: the Zoom Where it Happens//The Economist, 2021 May 1st, P. 51st — URL: https://www.economist.com/international/2021/05/01/diplomacy-has-changed-more-than-most-professions-during-the-pandemic (дата обращения: 22.05.2021).
9. McCluskey M. Their Doors May Be Closed, but Embassies Are Still Showing People the World// The Smithsonian Magazine, 2021, January 21st. — URL: https://www.smithsonianmag.com/travel/their-doors-may-be-closed-embassies-are-still-showing-people-world-180976821/ (дата обращения: 22.05.2021).
10. Интервью Заместителя Министра иностранных дел РФ О. В. Сыромолотова агентству «РИА-Новости», 12 мая 2021 г. URL: https://ria.ru/20210512/syromolotov-1731860706.html (дата обращения: 22.05.2021).

В. И. Булва,
помощник директора, эксперт
Центра международной информационной
безопасности и научно-технологической политики
МГИМО МИД России

ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ИНТЕРНЕТ-КОНТЕНТА: МЕЖДУНАРОДНОЕ ИЗМЕРЕНИЕ

Аннотация: в статье поднимается проблема отсутствия единого понятийного аппарата информационной сферы на международном уровне. Автор даёт рекомендации по разработке и принятию глобальных правил ответственного поведения государств в информационном пространстве, в том числе в отношении регулирования интернет-контента.

Ключевые слова: информационное пространство, противоправный контент, политика «двойных стандартов», правила ответственного поведения государств в информационном пространстве, Рабочая группа открытого состава, принципы международного права.

Блокировка аккаунтов и ограничение доступа на определенные сайты является обыденной практикой в любой стране. Вместе с тем, подобные шаги нередко становятся предметом споров между государствами, а также между бизнесом и государством. Это свидетельствует о том, что на уровне международного сообщества не сложилось общего подхода по противодействию распространению противоправного контента. Какие ключевые препятствия на пути взаимодействия существуют на современном этапе? Возможно ли их преодолеть?

Основная проблема кроется в том, что на международном уровне отсутствует единый понятийный аппарат. Приоритетное

использование в российской практике термина «информационная безопасность» вместо «кибербезопасности» объясняется тем, что в первом случае учитывается безопасность не только сетей и систем, но и информации, которая по ним передается и в них хранится[65]. Таким образом, российская трактовка более всеобъемлющая и она, в частности, позволяет включить в сферу международного регулирования борьбу с противоправным контентом.

Другой основополагающий термин в рамках данной тематики — «противоправный контент», понимание которого также варьируется от государства к государству. Невозможно вести эффективную борьбу с угрозой, которой не дано четкого определения, причем которое должно быть не просто поддержано всеми государствами, но и закреплено в рамках юридически обязывающего документа.

В Российской Федерации под противоправным контентом понимается информация, противоречащая российскому законодательству и содержащая пропаганду экстремизма, терроризма, наркомании, порнографии, жестокости и насилия. С 1 февраля 2021 г. на территории России действует закон, который возлагает на социальные сети обязанность модерировать онлайн-контент. Речь идет о таких публикациях, как порнографические изображения несовершеннолетних, информация, склоняющая детей «к совершению опасных для жизни незаконных действий», данные о способах изготовления и использования наркотиков, способы совершения самоубийства и призывы к нему, реклама дистанционной продажи алкоголя и интернет-казино, оскорбления человеческого достоинства и общественной нравственности, информация, выражающую «явное неуважение» к обществу, государству, официальным государственным символам, Конституции РФ или органам госвласти, призывы к массовым

[65] Зиновьева Е. С. Цифровая дипломатия, международная безопасность и возможности для России // Индекс безопасности. № 1 (104). — Том 19. — С. 217. — URL: http://www.pircenter.org/media/content/files/10/13559069820.pdf (дата обращения: 25.03.2021).

беспорядкам, экстремизму и участию в несогласованных публичных мероприятиях, а также информация, которая порочит людей по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства, работы и политическим убеждениям[66].

Запад отнюдь не уступает России в противодействии распространению противоправного контента. При этом, в США и европейских странах в центре внимания оказывается политически неугодный контент. Иными словами, происходит смещение акцента с защиты индивида и общества в ИКТ-пространстве на укрепление политического влияния путем фильтрации передаваемой массовой аудитории информации.

Складывается парадоксальная ситуация — государства-поборники демократических ценностей и прав человека приоритизируют интересы определенного политического истеблишмента над интересами рядового гражданина. При этом, политическая элита действует в тесной связке с крупными социальными платформами. Весьма показательным в этой связи будет блокировка аккаунтов отдельных политических деятелей после американских президентских выборов на фоне, когда в стране спокойно продолжает циркулировать призывы оказать отпор «внутренним террористам»[67].

Отсутствие единой трактовки понятия противоправного контента сохраняет за некоторыми странами свободу рук, а именно — возможность использовать онлайн-контент в качестве политического инструмента на международной арене. В итоге цифровая среда становится сферой реализации политики двойных стандартов. С одной стороны, не существует правовых

[66] Закон «Об информации, информационных технологиях и о защите информации». — Ст. 10.6. — URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 25.03.2021).

[67] Бутина М. Чем отличаются «внутренние террористы» в США и РФ? — URL: https://aif.ru/politics/opinion/chem_otlichayutsya_vnutrennie_terroristy_v_ssha_i_rf (дата обращения: 25.03.2021).

барьеров для принятия произвольных решений по блокировке неугодных (прежде всего, по политическим мотивам) платформ и сайтов. С другой стороны, эти же страны используют информационные каналы для распространения контента, способствующего укреплению их влияния (тем самым осуществляя ту самую деятельность, за которую обвиняют других).

Наглядная демонстрация политики «двойных стандартов» в области цензурирования — это блокировка аккаунтов, которую осуществляет Twitter. Блокируя аккаунты политических деятелей и международных дискуссионных клубов, данная социальная сеть игнорирует требования Роскомнадзора по удалению контента, который по российскому законодательству является противоправным. Речь идет о призывах к самоубийствам, детской порнографии и пропаганде наркотиков. Одним из показательных примеров стало невыполнение предписания российского регулятора удалить призывы о совершении 3 марта 2021 г. массового суицида, адресованного к несовершеннолетним[68]. В итоге, правоохранительные органы в этот день предотвратили несколько попыток совершения самоубийств несовершеннолетними.

Что касается использования информационного пространства, для некоторых стран оно служит идеальной площадкой продвижения собственных ценностных установок и ориентиров. Так, Европейский союз использует социальные сети для укрепления собственной нормативной силы посредством закрепления в других государствах европейского понимания демократии, прав человека, верховенства права.

Схожим образом цифровая среда используется Соединенными Штатами, которые проповедуют в интернете императивы надлежащего управления (good governance). Параллельно с распространением собственных идеалов, США проводят активную

[68] Роскомнадзор принял меры по защите российских граждан от влияния противоправного контента. — URL: https://rkn.gov.ru/news/rsoc/news73464.htm (дата обращения: 25.03.2021).

политику по дискредитации имиджа так называемых «врагов американского государства», среди которых фигурирует и Россия. В частности, они прибегают к практике публичного атрибутирования, санкционного давления и распространению фейков. Все это служит целям легитимации подобного поведения Запада путем придания России образа агрессора.

Итак, с учетом вышеизложенного, можем сделать вывод, что в настоящий момент крайне необходимо разработать и принять глобальные правила ответственного поведения государств в информационном пространстве, в том числе в отношении регулирования интернет-контента. Принимая во внимание растущую активность не только публичного, но и частного сектора в области распространения информации, а также её фильтрации, к обсуждению свода подобных норм следует привлечь представителей бизнеса и НПО.

Идеальной площадкой для таких дискуссий является Рабочая группа открытого состава, которая была создана по инициативе Российской Федерации в 2018 году[69], а 12 марта 2021 г. получила мандат ещё на 5 лет[70]. Уникальность Группы заключается в том, что она позволяет другим сторонам (бизнесу, НПО) принимать участие не просто в обмене мнением, а в согласовании норм, правил и принципов ответственного поведения. При этом, несмотря на прямое вовлечение этих сторон в диалог, ответственность за принятие и имплементацию решений несут государства. Именно поэтому, им отводится координирующая роль в данном процессе.

Что касается содержательной части кодекса поведения, то, в первую очередь, важно сформировать понятийный аппарат. Затем, следует прописать, что регулирование интернет-контента

[69] Резолюция ГА ООН A/73/PV.45 от 5 декабря 2018 г. —URL: https://undocs.org/ru/A/RES/73/27 (дата обращения: 05.05.2021).

[70] Final Substantive Report A/AC.290/2021/CRP.2 // UN General Assembly — URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 05.05.2021).

должно осуществляться в строгом соответствие с основополагающими принципами международного права, такими как невмешательство во внутренние дела, уважение суверенного равенства государств, соблюдение прав человека и основных свобод, обеспечение равноправия государств.

Помимо этого, необходимо закрепить положения, которые бы описывали механизм противодействия распространению нежелательного интернет-контента. Это необходимо для сведения к минимуму произвольных действий со стороны отдельных государств и компаний. Это касается в том числе сотрудничества по борьбе в информационном пространстве с неконвенциональными акторами — террористическими и экстремистскими группировками. На уровне мирового сообщества нет разногласий по поводу того, что кибертерроризм и киберэкстремизм представляют угрозу безопасности государства. Вместе с тем, не существует межгосударственного консенсуса по поводу того, как необходимо противодействовать данной угрозе, что сохраняет за отдельными странами широкое поле для маневра.

Для эффективного действия правил ответственного поведения, огромное значение имеет развитие механизма подотчетности, который бы позволял определить сферу и форму ответственности каждого стейкхолдера в информационном пространстве. В этой связи, следует придать данным нормам юридически обязательный характер, а на практике — учредить специальную комиссию по контролю за их выполнением.

Наконец, стоит обратить внимание на то, что глобальный уровень регулирования интернет-контента позволит создать юридический каркас. Взаимодействие в практической плоскости (развитие и укрепление системы мер доверия, обмен национальным опытом, сотрудничество правоохранительных органов, подготовка кадров и т.д.) легче проводить на двустороннем и региональном уровне с участием тех сторон, которые готовы сегодня готовы к этому. Особенно важно обеспечить внеблоковый характер взаимодействия. Подобное сочетание

глобального, регионального и двустороннего форматов позволяет избежать замыкания государств в своих группах без учета интересов других государств.

Список использованных источников и литературы

1. Зиновьева Е. С. Цифровая дипломатия, международная безопасность и возможности для России // Индекс безопасности. № 1 (104). — Том 19. — с. 217 — URL: http://www.pircenter.org/media/content/files/10/13559069820.pdf (дата обращения: 25.03.2021).
2. Закон «Об информации, информационных технологиях и о защите информации» — ст. 10.6 — URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 25.03.2021).
3. Бутина М. Чем отличаются «внутренние террористы» в США и РФ? — URL: https://aif.ru/politics/opinion/chem_otlichayutsya_vnutrennie_terroristy_v_ssha_i_rf (дата обращения: 25.03.2021).
4. Роскомнадзор принял меры по защите российских граждан от влияния противоправного контента — URL: https://rkn.gov.ru/news/rsoc/news73464.htm (дата обращения: 25.03.2021).
5. Резолюция ГА ООН A/73/PV.45 от 5 декабря 2018 г. — URL: https://undocs.org/ru/A/RES/73/27 (дата обращения: 05.05.2021).
6. Final Substantive Report A/AC.290/2021/CRP.2 // UN General Assembly — URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 05.05.2021).

В. А. Педанов,
аспирант МГИМО МИД России

РЕГИОНАЛЬНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ НОРМ, ПРАВИЛ И ПРИНЦИПОВ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ (КЕЙС АСЕАН)

Аннотация: Объектом исследования являются отношения, возникающие в рамках сотрудничества стран АСЕАН в сфере обеспечения международной информационной безопасности (далее — МИБ) на региональном уровне и их взаимоотношения с Россией. Авторы проводят обзор ландшафта международного сотрудничества в сфере МИБ и детально разбирают кейс АСЕАН. Интерес представляет проведённый анализ взаимоотношений стран в целом, с учётом исторических, экономических и геополитических факторов и, в частности, по вопросам обеспечения безопасности. Особое внимание уделяется особенностям политико-правовых механизмов сотрудничества по вопросам МИБ. Авторы приходят к выводу о взаимосвязи развития сотрудничества в сфере МИБ с развитием взаимной экономической интеграции и торговых связей. По заключению авторов представляется, что для развития регионального и международного сотрудничества в сфере МИБ необходимо наращивать экономические связи и культивировать взаимное доверие между странами, в том числе, предлагается ряд практических шагов в этом направлении.

Ключевые слова: международная информационная безопасность, кибербезопасность, АСЕАН, Россия, информационно-коммуникационные технологии.

Новым историческим этапом стало для международного сообщество развитие сотрудничества в сфере МИБ. Появление новых

угроз в информационном пространстве способствует развитию международного сотрудничества в сфере обеспечения МИБ, которое является закономерным следствием роста числа угроз в сфере информационно-коммуникационных технологий (далее — ИКТ) и желанием международного сообщества противостоять им. С развитием электронных вычислительных технологий появились риски их злонамеренного использования. В эпоху развития интернета эти риски кратно возросли. Новым глобальным вызовом международному сообществу стало внедрение ИКТ в критическую инфраструктуру и растущая роль киберфизических процессов. Занимая значительное место в структуре компонентов национальной безопасности, информационная безопасность становится предметом внимания и международного сообщества.

Эффективность групповых систем обеспечения безопасности привлекает внимание государств к решению проблем МИБ в рамках коалиционных инструментов[71]. В виду растущего экономического и политического значения в мире, а также ввиду личных профессиональных интересов авторов, представляется интересным анализ международного сотрудничества в сфере МИБ в рамках региона АСЕАН и его соотношения с российской позицией в международных сообществах. Целью настоящего исследования является анализ опыта сотрудничества стран АСЕАН в сфере МИБ и определение позитивных практик, возможных к рецепцированию всем международным сообществом.

Для России особенно значимо развитие взаимодействия со странам АСЕАН по вопросам МИБ. Следует отметить, что отношения России и стран АСЕАН выходят на новый качественный уровень с ноября 2018 года, когда в ежегодном Восточноазиатском саммите впервые принял участие не глава правительства,

[71] Бордюжа Н. Н. Эффективность системы коллективной безопасности на евразийском пространстве: реалии и перспективы // Национальные интересы: приоритеты и безопасность. 2006. №6. — URL: https://cyberleninka.ru/article/n/effektivnost-sistemy-kollektivnoy-bezopasnosti-na-evraziyskom-prostranstve-realii-i-perspektivy (дата обращения: 10.02.2021).

а президент России. В ходе визита Президента России был также проведён третий саммит Россия — АСЕАН, результатом которого стало совместное заявление сторон о стратегическом партнёрстве[72]. Интерес представляет то, какое значение было уделено именно вопросам совместной работы над обеспечением международной информационной безопасности. Помимо координации действий в привычных для сторон отраслей сотрудничество (экономическое, военно-промышленные вопросы), стороны достигли ряда договорённостей в сфере ИКТ, а именно:

1) укреплять сотрудничество на глобальных и региональных площадках в реагировании на традиционные и новые вызовы в сфере безопасности (международный терроризм, транснациональная преступность, угрозы в сфере использования информационно-коммуникационных технологий, незаконное производство и контрабанда наркотиков) (п. 15);
2) способствовать реализации Заявления Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ (п. 16).

Помимо общих договорённостей о стратегическом партнёрстве, отдельно было озвучено Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования ИКТ и самих информационно-коммуникационных технологий. Стороны договорились о ряде конкретных направления совместной деятельности в сфере ИКТ, а именно:

1) активизация совместных усилий по сокращению цифрового разрыва (п. 10);
2) наращивание национальных потенциалов и запуск образовательных программ и тренингов по различным вопросам безопасности в сфере использования ИКТ и самих ИКТ (п. 11);

[72] Совместное заявление III саммита Российская Федерация — АСЕАН о стратегическом партнёрстве, 14 ноября 2018 года. // Президент России: официальный сайт. — URL: http://kremlin.ru/supplement/5360. (дата обращения: 10.02.2021).

3) укрепление практического сотрудничества по безопасности в сфере использования ИКТ и самих ИКТ на таких направлениях, как борьба с использованием ИКТ в террористических целях и для иной преступной деятельности;
4) содействие укреплению и оптимизации существующих региональных механизмов по безопасности в сфере использования ИКТ и самих ИКТ (п. 13);
5) рассмотрение Ассоциацией государств Юго-Восточной Азии инициативы Российской Федерации об учреждении Диалога Россия — АСЕАН по вопросам, относящимся к безопасности ИКТ (п. 14)[73].

Государства АСЕАН и Россия достижением этих договорённостей подтвердили свою заинтересованность в поддержании стабильности и безопасности в сфере МИБ. Однако реализация практических мер в сфере обеспечения МИБ, несмотря на достигнутые договорённости, не всегда соответствует поставленным целям. Так, в ходе выступления директора Департамента МИБ МИД России А. В. Крутских на специальной сессии Министерской конференции АСЕАН по кибербезопасности V Сингапурской международной кибернедели 7 октября 2020 года, остро поставил актуальный для развития международного сотрудничества в сфере МИБ вопрос: «почему при наличии значительного числа авторитетных и работающих переговорных форматов мы все никак не можем договориться о создании так называемой вакцины от киберпандемии? Затягивается процесс внести хотя бы базовый порядок в набирающий в силу киберхаос?»[74]. В ходе выступления

[73] Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. // Президент России: официальный сайт. — Режим доступа: http://kremlin.ru/supplement/5361. (дата обращения: 10.02.2021).

[74] Министерство иностранных дел Российской Федерации. — Выступление специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной

А. В. Крутских призывает также «не обольщаться» в связи с достигнутым прогрессом в рамках международного переговорного процесса по вопросу об обеспечении МИБ. В качестве основной проблемы указывается, что сам переговорный процесс заменяется общеконцептуальной дискуссией, которая не приводит к существенному прогрессу.

При этом для государств АСЕАН обеспечение международной информационной безопасности представляет высокую значимость прежде всего в связи с активным развитием цифровой экономике в регионе, что стимулирует наращивание регионального сотрудничества между странами в сфере МИБ. Так исследованием ATKearney ВВП региона может быть увеличено на 35% (1 трлн долларов США) благодаря развитию цифровой экономике в период с 2018 по 2023 год[75]. Ввиду активного развития цифровой экономики и её активного проникновения во все сферы жизни общества в странах АСЕАН, эти государства становятся одной из главных мишеней для информационных атак.

Причиной этому служит недостаточно развитая система политических институтов в большей части стран, которые не способны, ввиду экономических, технологических и иных факторов, обеспечить должный уровень обеспечения безопасности информационных ресурсов. Сказывается нехватка специалистов в сфере обеспечения кибербезопасности и отсутствие сильных технологических школ с преемственностью знаний в значитель-

безопасности, директора Департамента международной информационной безопасности А. В. Крутских на специальной сессии Министерской конференции АСЕАН по кибербезопасности с диалоговыми партнерами V Сингапурской международной кибернедели в формате видеоконференции, 7 октября 2020 года. — URL: https://www.mid.ru/ ru/maps/sg/-/asset_publisher/5SAHbSOAdwNc/content/id/4372514 (дата обращения: 10.02.2021).

[75] ATKearney. Cybersecurity in ASEAN — AN Urgent Call to Action. — 2018. — URL: https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-inasean/files/assets/common/downloads/publication.pdf (дата обращения: 10.02.2021).

ной части региона. Исследование Ponomen Institute проведённого при поддержке IBM в 2017 году показывает, что в среднем для проведения кибератаки на критическую инфраструктуру в странах мира требуется порядка 180 дней, а для атак на инфраструктуру компаний в АСЕАН — около 65 дней[76].

Лидерство в части развития экосистемы обеспечения информационной безопасности, как в вопросах институционального управления, так и в вопросах подготовки кадров, занимает Сингапур[77]. Исторически тесные связи с Израилем — одним из ведущих государств в сфере развития технологий безопасности ИКТ, а также высокий уровень экономического развития и организации политических институтов, дают высокие возможности для развития суверенной программы информационной безопасности. Так, Сингапур был первым государством в АСЕАН, кто поднял тему кибербезопасности на законодательном уровне, опубликовав в 1993 году Акт о компьютерных злоупотреблениях и кибербезопасности (Computer Misuse and Cybersecurity Act 1993)[78]. Помимо этого, Сингапур совместно с Японией и Великобританией создал и поддерживает некоммерческую международную организацию The CyberGreen Institute, одной из ключевых задач которого является улучшение глобального киберздоровья (improving global cyber health)[79].

[76] Ponemom Institute. Cost of Data Breach Study: Global Overview. — Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC. — 2017. — URL: http://universe.byu.edu/wpcontent/uploads/2017/10/Ponemon-2017-Study.pdf (дата обращения: 10.02.2021).

[77] Горян Э. В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103–117.

[78] CSingapore status online. — Computer Misuse and Cybersecurity Act. — URL: https://sso.agc.gov.sg/Act/CMA1993 (дата обращения: 10.02.2021).

[79] См.: CyberGreen Institute. — URL: https://www.cybergreen.net (дата обращения: 10.02.2021).

Стоит отметить, что страны АСЕАН в целом предпринимают последовательные попытки укрепления цифровой экономики, в том числе с развитием международного сотрудничества в сфере МИБ. Целью такого сотрудничества является в том числе и дополнительная стимуляция развития цифровой экономики. Так, страны АСЕАН по инициативе Сингапура приняли и следуют Программе повышения киберпотенциала АСЕАН[80]. В рамках программы предполагаются:

— разработка Руководства по Стратегии борьбы с киберпреступностью, которое призвано помочь странам АСЕАН разработать или усовершенствовать свои национальные стратегии борьбы с киберпреступностью, что в свою очередь должно привести к более эффективному противодействию киберпреступности;
— проведение специализированных семинаров и тренингов, основанных на тенденциях в сфере киберпреступности для устранения пробелов в знаниях сотрудников уполномоченных органов, выявленных на предыдущем этапе;
— создание модулей онлайн-обучения для сотрудников национальных CERT стран АСЕАН по сбору и сохранению цифровых улик.

Таким образом, мы можем видеть, как документы политического характера находят своё практическое применение в рамках реализации договорённостей и развития международного сотрудничества в сфере МИБ[81].

Помимо сотрудничества на региональном уровне, страны АСЕАН выступают активным участником международного

[80] Interpol — ASEAN Cyber Capacity Development Project — URL: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project (дата обращения: 10.02.2021).

[81] Interpol — ASEAN Cyber Capacity Development Project. — Interpol's web page — URL: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project (дата обращения: 10.02.2021).

сотрудничества. Страны АСЕАН, ведут активную работу по совершенствованию своих взаимоотношений в сфере МИБ с ключевыми акторами в сфере международной информационной безопасности.

Сотрудничество в сфере обеспечения информационной безопасности с одним из наиболее значимых для АСЕАН партнёром — Китаем, было начато ещё в 2005 году, с принятием Пекинской декларации о сотрудничестве АСЕАН и Китая в области ИКТ в интересах общего развития[82]. В рамках этой декларации признавалось, что сетевая и информационная безопасность является важным компонентом информационного общества и при этом регион сталкивается с серьезной проблемой обеспечения такой безопасности. Стороны соглашаются на том, что они должны укреплять связь и сотрудничество в области сетевой и информационной безопасности, а также стремиться к созданию Координационных организаций АСЕАН — Китай для реагирования на чрезвычайные ситуации в области сетевой и информационной безопасности. Интерес вызывает, что в этом документе не поднимаются вопросы кибербезопасности, а подчёркивается важность работы над обеспечением именно информационной безопасности.

Рассматривая более поздние документы по вопросам сотрудничество в части обеспечения безопасности в сфере ИКТ, необходимо обратить внимание на План действий по имплементации Совместной Декларации АСЕАН — Китай — Стратегическое Партнёрство для Мира и Процветания 2016–2020[83], утверждённого по итогам Саммита АСЕАН — Китай 2016 года. В этом

[82] Beijing Declaration on ASEAN-China ICT Cooperative Partnership for Common Development Beijing. — ASEAN web page — URL: https://asean.org/beijing-declaration-on-asean-china-ict-cooperative-partnership-for-common-development-beijing/ (дата обращения: 10.02.2021).

[83] Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity. — ASEAN web page — URL: https://www.asean.org/storage/images/2015/November/27th-summit/ASEAN-China%20POA%20%202016-2020.pdf (дата обращения: 10.02.2021).

документе действия по имплементации договорённостей рассматриваются в контексте широкого ряда соглашений на уровне АСЕАН — Китай, включая такие сферы как торговля, финансов, управления природными ресурсами, транспорт, сотрудничество в сфере науки и космоса, туризм и ИКТ и так далее. Применительно к сфере ИКТ Китай и АСЕАН договорились:

— продолжать укреплять политический диалог через Совещание министров ИКТ АСЕАН и Китая;
— продолжать осуществление Меморандума о взаимопонимании между АСЕАН и Китаем о сотрудничестве в области информационно-коммуникационных технологий и Плана действий по осуществлению Пекинской декларации о сотрудничестве АСЕАН и Китая в области ИКТ в интересах общего развития.
— реализовать Механизм сотрудничества групп реагирования на компьютерные чрезвычайные инциденты (CERT) между АСЕАН и Китаем, оптимизировать меры реагирования и процедуры в области сетевой безопасности, содействовать обмену информацией и данными, а также осуществлять наращивание потенциала и проектное сотрудничество.
— продолжать совместную работу по улучшению взаимодействия информационно-коммуникационной инфраструктуры АСЕАН и Китая.
— укреплять сотрудничество в области развития сельских телекоммуникаций, расширения сетевых приложений и развития приложений электронной торговли.
— поддерживать реализации Генерального плана АСЕАН в области ИКТ на 2020 год[84].

На основе перечисленных в Плане задач можно сделать вывод, что сотрудничество в сфере МИБ между Китаем и АСЕАН уже

[84] Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity. — ASEAN web page — URL: https://www.asean.org/storage/images/2015/November/27th-summit/ASEAN-China%20POA%20%202016-2020.pdf (дата обращения: 10.02.2021).

имеет продолжительную историю и находит своё практическое применение в рамках реализации совместных CERT команд и обмена данными об инцидентах информационной безопасности.

Помимо сотрудничества с Китаем, АСЕАН также развивает сотрудничество с США в сфере МИБ. Так в рамках VI саммита АСЕАН — США 2018 году, лидеры АСЕАН и США приняли совместное Заявление о сотрудничестве в сфере кибербезопасности[85]. Стороны подтвердили, что, по их мнению, международное право, и, в частности, Устав ООН, применимо и имеет важное значение для поддержания мира, стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной среды ИКТ, и признают необходимость дальнейшего изучения того, как международное право применяется к использованию ИКТ государствами. Стороны также договорились наращивать кибернетический потенциал в борьбе с киберпреступностью, защитой критической информационной инфраструктурой, также, отдельно были выделены тезисы о необходимости совместного противодействия использования ИКТ в террористических целях. Высокую значимость также имеет пункт, в котором стороны договариваются совместно принимать меры по экономическому развитию цифровой инфраструктуры, с задействованием рыночных механизмов. Реализация договорённостей политического характера на посредством инструментов рыночной экономики, должна способствовать их эффективной имплементации и повышению взаимозависимости договаривающихся сторон друг от друга.

Всё более значимым становится сотрудничество АСЕАН и с другим региональным лидером — Японией. Сотрудничество между АСЕАН и Японией наименее конфликтно и высоко институализировано, что обусловливает потенциал дальнейшего политико-экономического развития, в том числе с внешними

[85] ASEAN —United States leaders' statement on cybersecurity cooperation. — ASEAN web page — URL: https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf (дата обращения: 10.02.2021).

игроками[86]. Сотрудничество Японии и АСЕАН в сфере МИБ с 2009 года находит своё выражение в проведении ежегодных конференций по вопросам политики в области кибербезопасности. Так, 20 октября 2020 г. была проведена XIII Конференция Японии / стран АСЕАН по вопросам политики в области кибербезопасности[87]. В ходе прошедшей встречи стороны подтвердили намерения о проведении таких совместных мероприятий, как киберучения, взаимное повышение осведомленности, наращивание киберпотенциала и взаимное уведомление об инцидентах информационной безопасности. Сотрудничество для реализации таких мероприятий ведётся на различных уровнях, включая взаимодействие на правительственном уровне, взаимодействие в академических кругах, а также на уровне частных корпораций и промышленности.

Анализируя развитие международного сотрудничества АСЕАН с другими региональными лидерами, складывается впечатление о недостаточности мер, предпринимаемых Россией в вопросах практической реализации договорённостей в сфере МИБ. Отсутствием совместных центров реагирования на инциденты информационной безопасности, низкий уровень взаимного проникновения на рынки частных компаний, работающих в сфере обеспечения информационной безопасности, а также, отсутствие непрерывного институацианализированного диалога между Россией и АСЕАН именно по вопросам МИБ, на текущий момент, негативно сказывается на практической реализации договорённостей политического характера.

---

[86] Мурашкин Н. Япония — АСЕАН: неизбежное партнерство для нового азиатского порядка? // РСДМ Электронный ресурс. — URL: https://russiancouncil.ru/analytics-and-comments/analytics/yaponiya-asean-neizbezhnoe-partnerstvo-dlya-novogo-aziatskog/ (дата обращения: 10.02.2021).

[87] Министерство по внутренним вопросам и связям, Япония. — Итоги XIII конференции АСЕАН по политике в области кибербезопасности. — Пресс-релиз 6 ноября 2020 г. — URL: https://www.soumu.go.jp/main_sosiki/joho_tsusin/rus/pressrelease/2020/11/06_01.html (дата обращения: 10.02.2021).

Безусловно, сотрудничество в сфере МИБ между Россией и странами АСЕАН поступательно развивается. Подтверждением этому служат перечисленные в начале работы договорённости и участие России в специальных сессиях Министерской конференции АСЕАН по кибербезопасности. Вопросы сотрудничества в сфере безопасности ИКТ поднимаются и в рамках других форматов. К примеру, 30 марта 2021 года состоялась XIX Заседание Совместного Комитета Сотрудничества Россия — АСЕАН, по вопросам развития Стратегического партнерства Россия — АСЕАН. В ходе встречи обсуждался широкий перечень вопросов, в том числе развитие сотрудничества по политическим вопросам и вопросам безопасности, в области борьбы со стихийными бедствиями, технологий и инноваций, безопасности ИКТ, борьбы с инфекционными заболеваниями, туризма и во многих других областях[88]. Однако, в сравнении с тем уровнем сотрудничества в сфере безопасности ИКТ, который существует по осям АСЕАН — Китай или АСЕАН — Япония, Россия несколько уступает. Во многом это связано с относительно низкой степенью развитости торгово-экономических взаимоотношений между странами АСЕАН и Россией.

Представляется, что для дальнейшего развития сотрудничества по вопросам безопасности ИКТ, Россия должна проводить скоординированную политику поддержки диалога Россия-АСЕАН по вопросам международной информационной безопасности, с привлечением представителей частного бизнеса и академической среды. Среди практических шагов, для развития и реализации договорённостей в сфере МИБ видится необходимым создание механизмов сотрудничества групп реагирования на компьютерные чрезвычайные инциденты (CERT) между АСЕАН и России, взаимное информирование об инци-

[88] On The 19th ASEAN — Russia Joint Cooperation Committee Meeting Press-Release. — March 30th, 2021, ASEAN Secretariat News — URL: https://asean.org/19th-asean-russia-joint-cooperation-committee-meeting-press-release/ (дата обращения: 10.02.2021).

дентах информационной безопасности, а также взаимное повышение осведомлённости об инцидентах.

Стоит отметить вызывающее одобрение стремление стран АСЕАН к обеспечению международной информационной безопасности, которое находит практическое выражение в активном развитии международного сотрудничества по этому вопросу. Среди стран, с которыми АСЕАН активно наращивает сотрудничество в этой сфере можно выделить Китай, Россию, Японию, страны коллективного Запада и Ближнего Востока. Развитием двухсторонних отношений, а также отношений на региональном уровне имеет высокое значение для формирования атмосферы взаимного доверия между государствами в сфере ИКТ, что в свою очередь способствует позитивному развитию международного сотрудничества в сфере МИБ.

Роль АСЕАН в этом процессе становится всё заметнее, и для России особенно важно обеспечить надёжное и эффективное сотрудничество с государствами АСЕАН по вопросам МИБ.

В качестве актуальных направлений для развития сотрудничества в сфере МИБ между Россией и АСЕАН стоит выделить наращивание торгово-экономических связей в сфере ИКТ, обмена информацией по актуальным инцидентам информационной безопасности, которое может выражаться в обмене данными между ГосСОПКА[89] и CERT-командами стран АСЕАН. Актуальным примером является существующий на сегодняшний день The CyberGreen Institute, к работе которого Россия могла бы присоединиться или же создать аналогичную организацию вместе с государствами АСЕАН. Как практический инструмент для наращивания работы в этом направлении можно рассматривать создание в рамках департаменте Международной информационной безопасности МИД России отдел (направление) по

[89] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак — www.gov-cert.ru/ (дата обращения 20.02.2021).

работе со странами АСЕАН. При этом, на наш взгляд, именно увеличение экономической взаимосвязи и обмен актуальными данными между государственными организациями, нацеленными на обеспечение информационной безопасности, поможет реализовывать международное и региональное сотрудничество на практическом уровне.

Список использованных источников и литературы

1. Бордюжа Н. Н. Эффективность системы коллективной безопасности на евразийском пространстве: реалии и перспективы. — Национальные интересы: приоритеты и безопасность. 2006. №6. // URL: https://cyberleninka.ru/article/n/effektivnost-sistemy-kollektivnoy-bezopasnosti-na-evraziyskom-prostranstve-realii-i-perspektivy/ (дата обращения: 10.02.2021).
2. Горян Э. В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103–117.
3. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак — URL:www.gov-cert.ru/ (дата обращения: 10.02.2021).
4. Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий // Президент России: официальный сайт. — URL: http://kremlin.ru/supplement/5361/ (дата обращения: 10.02.2021).
5. Министерство иностранных дел Российской Федерации. — Выступление специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности А. В. Крутских на специальной сессии Министерской конференции АСЕАН по кибербезопасности с диалоговыми партнерами V Сингапурской международной кибернедели в формате видеоконференции, 7 октября 2020 года. — URL: https://www.mid.ru/ru/maps/sg/-/asset_publisher/5SAHbSOAdwNc/content/id/4372514/ (дата обращения: 10.02.2021).

6. Министерство по внутренним вопросам и связям, Япония. — Итоги 13-й конференции АСЕАН по политике в области кибербезопасности. — Пресс-релиз 6 ноября 2020 г. — URL: https://www.soumu.go.jp/main_sosiki/joho_tsusin/rus/pressrelease/2020/11/06_01.html (дата обращения: 10.02.2021).
7. ASEAN — United States leaders' statement on cybersecurity cooperation. — ASEAN — URL: https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf/ (дата обращения: 10.02.2021).
8. ATKearney. Cybersecurity in ASEAN — AN Urgent Call to Action. — 2018 — URL: https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-inasean/files/assets/common/downloads/publication.pdf/ (дата обращения: 10.02.2021).
9. Beijing Declaration on ASEAN-China ICT Cooperative Partnership for Common Development Beijing . — ASEAN — URL: https://asean.org/beijing-declaration-on-asean-china-ict-cooperative-partnership-for-common-development-beijing/ (дата обращения: 10.02.2021).
10. CyberGreen Institute. — URL: https://www.cybergreen.net/ (дата обращения: 10.02.2021).
11. Interpol — ASEAN Cyber Capacity Development Project — URL: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project/ (дата обращения: 10.02.2021).
12. On The 19th ASEAN-Russia Joint Cooperation Committee Meeting Press-Release. — March 30th, 2021, ASEAN Secretariat News — URL: https://asean.org/19th-asean-russia-joint-cooperation-committee-meeting-press-release/ (дата обращения: 10.02.2021).
13. Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity. — ASEAN — URL: https://www.asean.org/storage/images/2015/November/27th-summit/ASEAN-China%20POA%20%202016-2020.pdf/ (дата обращения: 10.02.2021).
14. Ponemom Institute. Cost of Data Breach Study: Global Overview. — Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC. 2017. — URL: http://universe.byu.edu/wpcontent/uploads/2017/10/Ponemon-2017-Study.pdf/ (дата обращения: 10.02.2021).

Бай Яцзе,
аспирантка МГИМО МИД России

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ НОРМ, ПРАВИЛ И ПРИНЦИПОВ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ — ПОДХОДЫ КИТАЯ

Аннотация: В статье рассматриваются подходы Китая по международному сотрудничеству в области практического применения норм, правил и принципов ответственного поведения государств в ИКТ-среде.

Ключевые слова: международное сотрудничество, киберпространство, принципы ответственного поведения, Сообщество единой судьбы киберпространства

В 2020 году пандемия ускорила интеграцию жизни человечества и развитие киберпространства. Развитие ИКТ показало большие преимущества и положительные перспективы. Однако данный процесс порождает множество сложностей и неопределенностей. По этой причине управление киберпространством требует сотрудничества международного сообщества. Китай сейчас находится в критическом периоде трансформации, который может внести свой вклад в международное сотрудничество в глобальном киберпространстве.

В 2013 году председатель КНР Си Цзиньпин предложил международному сообществу новую концепцию — «Сообщество единой судьбы человечества». Эта концепция значит, что нам надо отстаивать свои интересы с учетом потребностей других стран, и мы содействуем общему развитию всех стран в стремлении к собственному развитию.

Через 2 года, 16 декабря 2015 года в Китае была представлена такая же концепция — «Создание сообщества единой судьбы

киберпространства». Это важная китайская идея в киберпространстве.

В этой концепции есть «четыре принципа» и «пять предложений»:

Первый принцип — уважать киберсуверенитет.

Как мы все знаем, принцип суверенного равенства, установленный Уставом Организации Объединенных Наций, является основной нормой современных международных отношений. Этот принцип охватывает все области межгосударственных обменов, поэтому он должен также применяться к киберпространству. В ноябре 2020 года Китайская академия социальных наук выпустила «Киберсуверенитет: теория и практика» (версия 2.0), в которой рассказываются, что нужно укреплять стратегическое взаимное доверие, уважать права стран, самостоятельно выбирать свой путь развития и выбирать модели управления интернетом. У каждой страны есть право на равноправное участие в управлении международным киберпространством.

26 марта 2021 г. президент В. В. Путин в выступлении на Заседании Совета Безопасности подчеркнул важность киберсуверенитета[90]. В этом вопросе позиции Китая и России совпадают.

Второй принцип — сохранять мир и безопасность.

Хотя ИКТ принесли многообещающие новые возможности для информационной прозрачности, информационного сотрудничества и глобального участия, они также создали беспрецедентные уязвимости, угрозы и риски безопасности киберпространства.

Например, кибертерроризм нарушает порядок безопасности киберпространства; вирусы распространяются быстро, разрушительны, их трудно предотвратить, а потери трудно оценить;

[90] Президент провёл в режиме видеоконференции заседание Совета Безопасности, в ходе которого рассматривался проект «Основ государственной политики Российской Федерации в области международной информационной безопасности» // Официальный сайт Президента России, 26.03.2021. — URL: http://www.kremlin.ru/events/president/news/65231 (дата обращения: 19.05.2021).

киберпреступность подрывает международную безопасность и угрожает управлению киберпространством. В то же время кибергегемонисты используют ИКТ, чтобы вмешиваться во внутренние дела других стран.

В сентябре 2020 года Китай предложил «Глобальную инициативу по безопасности данных»[91]. Эта инициатива уравновешивает взаимосвязь между техническим прогрессом, экономическим развитием и защитой национальной безопасности и социальных общественных интересов.

Третий принцип — содействовать открытому сотрудничеству.

Китай активно продвигает преодоление цифрового разрыва, глобальную оцифровку и развитие интернета, чтобы больше стран могли совместно извлекать выгоду.

В этом аспекте Китай и Россия поддерживают долгосрочное сотрудничество на протяжении многих лет.

В июне 2019 года, главы Китая и России подписали «Совместное заявление Российской Федерации и Китайской Народной Республики о развитии отношений всеобъемлющего партнерства и стратегического взаимодействия, вступающих в новую эпоху»[92], в этом заявлении в пункте 6 рассказывается о сотрудничестве России и Китая и о международной информационной безопасности.

В марте текущего года, министр иностранных дел КНР Ван И (Wang Yi) заявил, что Китай и Россия должны совместно бороться против «цветных революций» и распространения дезинформации, а также поддерживать свой суверенитет и политическую безопасность.

---

[91] Global Initiative on Data Security // MFA China, September 8, 2020. — URL: https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml (дата обращения: 24.09.2020).

[92] Совместное заявление Российской Федерации и Китайской Народной Республики о развитии отношений всеобъемлющего партнерства и стратегического взаимодействия, вступающих в новую эпоху // Официальный сайт Президента России, 5 июня 2019. — URL: http://kremlin.ru/supplement/5413 (дата обращения: 24.09.2021).

Четвертый принцип — построить хороший порядок.

Быстрое развитие ИКТ способствовало углублению глобальной коммуникации, ускорению обменов и интеграции человеческой цивилизации. В то же время, возникло много проблем с беспорядком распространения.

На макроуровне и развитые, и развивающиеся страны сталкиваются с проблемой «цифрового разрыва». Развивающиеся страны хотят изменить неравный порядок и сломать монополию на методы распространения информации.

На микроуровне распространение информации сталкивается со многими типичными трудностями. Например, широкое использование рекомендаций алгоритмов привело к возникновению проблемы «информационные коконы» и «эффекта эхо-камеры», скрытая разнообразная информация; «фейк ньюс» влияют на социальную стабильность всех стран; «фейк» и «дипфейк» еще больше усилили недоверие людей к обществу. Особенно во время пандемии, «информационная пандемия» размножалась и распространялась. Именно поэтому очень важно и актуально построить хороший порядок в киберпространстве.

Кроме этих четырёх принципов, в концепции «создание сообщества единой судьбы киберпространства» ещё есть пять важных предложений.

1. Укреплять строительство глобальной киберинфраструктуры и содействовать взаимосвязанности.
2. Создавать онлайн-платформы для культурных обменов и способствовать для продвижения биржи.
3. Содействовать развитию цифровой экономики и инноваций и содействовать общему процветанию.
4. Гарантировать кибербезопасность и содействовать упорядоченному развитию.
5. Построить систему управления интернетом и продвигать справедливость и равенство.

Эти пять предложения полностью объясняют усилия Китая по созданию сообщества единой судьбы киберпространства с та-

ких пяти аспектов, как строительства инфраструктуры, культуры, экономики, безопасности и системы управления интернетом.

Время	Сотрудничество / документ
11.2020	«Инициатива действий совместного создания сообщества единой судьбы киберпространства»
11.2020	«Киберсуверенитет: теория и практика (версия 2.0)»
09.2020	«Глобальная инициатива по безопасности данных»
11.2019	EU — China symposium on data security and personal information protection
11.2019	Форум по управлению использованием интернета
10.2019	Концептуальный документ «Совместное создание сообщества единой судьбы киберпространства»
06.2019	«Совместное заявление о развитии отношений всеобъемлющего партнёрства и стратегического взаимодействия, вступающих в новую эпоху»
03.2017	«Международная стратегия сотрудничества в киберпространстве»
06.2016	Совместное заявление о содействии развитию сферы информации и киберпространства
05.2015	«Соглашение о сотрудничестве в области обеспечения международной информационной безопасности»
04.2015	Четвертая Глобальная конференция по киберпространству
06.2009	«Соглашения между правительствами государств — членов ШОС о сотрудничестве в области международной информационной безопасности»

Таблица составлена для того, чтобы показать главные событий в области международные сотрудничества в ИКТ-среде, в которых участвовал Китай, и главные выпущенные документы, разъясняющих принципы ответственного поведения государства в отношениях между государствами в киберпространстве.

В 2017 году, Китай впервые официально опубликовал «Международную стратегию сотрудничества в киберпространстве»[93]. В этой стратегии разъясняются принципы, цели и планы участия Китая в международном сотрудничестве в области киберпространства.

Во второй строке таблицы указано, что в ноябре 2020 года во время распространения пандемии по всему миру в Китае была опубликована «Инициатива действий совместного создания сообщества единой судьбы киберпространства». Главные цели этой инициативы — это воспользоваться возможностями цифрового и интеллектуального развития, активно реагировать на риски и вызовы в киберпространстве. В инициативе включаются 20 действий в международном сотрудничестве в области практического применения.

Вышеизложенные принципы и предложения чётко демонстрируют нормы, правила и принципы, которые Китай отстаивает в Международном сотрудничестве. И показывают уверенность и решимость Китая содействовать созданию сообщества единой судьбы киберпространства.

Список использованных источников и литературы

1. Заседание Совета Безопасности. — URL: http://www.kremlin.ru/events/president/news/65231 (дата обращения: 18.05.2021).
2. Министр иностранных дел КНР: Китай и Россия должны объединить усилия, чтобы бороться с «цветными революциями» (South China Morning

[93] International Strategy of Cooperation on Cyberspace // MFA China, 2017. — URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (дата обращения: 24.09.2020).

Post, Китай). — URL: https://inosmi.ru/politic/20210309/249287241.html (дата обращения: 18.05.2021).

3. Президент провёл в режиме видеоконференции заседание Совета Безопасности, в ходе которого рассматривался проект «Основ государственной политики Российской Федерации в области международной информационной безопасности» // Официальный сайт Президента России, 26.03.2021. — URL: http://www.kremlin.ru/events/president/news/65231 (дата обращения: 19.05.2021).
4. Совместное заявление Российской Федерации и Китайской Народной Республики о развитии отношений всеобъемлющего партнерства и стратегического взаимодействия, вступающих в новую эпоху // Официальный сайт Президента России, 5 июня 2019 — URL: http://kremlin.ru/supplement/5413 (дата обращения: 24.09.2021).
5. 2th World Inernet Conference · Wuzhen Summit (China). — URL: http://www.cac.gov.cn/2015-12/16/c_1117480642.htm (дата обращения: 18.05.2021).
6. Global Initiative on Data Security // MFA China, September 8, 2020. — URL: https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml (дата обращения: 24.09.2020).
7. International Strategy of Cooperation on Cyberspace // MFA China, 2017. — URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (дата обращения: 24.09.2020).

СЕКЦИЯ 2

«СОДЕЙСТВИЕ ПРЕОДОЛЕНИЮ ЦИФРОВОГО РАЗРЫВА И НАРАЩИВАНИЮ ПОТЕНЦИАЛА ПО ЗАЩИТЕ НАЦИОНАЛЬНОГО КИБЕРПРОСТРАНСТВА»

Е. С. Зиновьева,
д-р полит. наук, профессор кафедры
мировых политических процессов, заместитель директора
Центра международной информационной безопасности
и научно-технологической политики
МГИМО МИД России

МЕЖДУНАРОДНО-ПОЛИТИЧЕСКОЕ ИЗМЕРЕНИЕ ЦИФРОВОГО РАЗРЫВА

Аннотация: в докладе рассмотрены основные проявления цифрового разрыва в современной мировой политике, в том числе обусловленные масштабной цифровизацией в условиях пандемии COVID-19. Кроме того, охарактеризованы усилия международного сообщества, направленные на преодоление цифрового неравенства и описаны внешнеполитические инициативы России на данном направлении.

Ключевые слова: цифровой разрыв, международная информационная безопасность, информационно-коммуникационные технологии (ИКТ).

Пандемия коронавирусной инфекции COVID-19 способствовала масштабной и повсеместной цифровизации и в очередной раз продемонстрировала важность доступа к информационно-коммуникационным технологиям (ИКТ) и актуализировала изучение международно-политической составляющей проблемы цифрового разрыва (под термином «цифровой разрыв» в настоящем докладе понимается неравномерность в доступе к ИКТ в масштабах отдельной страны, международно-политического региона или международной системы в целом).

Как отмечают эксперты Всемирного экономического форума, сегодня проблема неравномерного доступа к ИКТ является одним из важнейших вызовов международной безопасности

и стабильности[1]. Если ранее утверждение, согласно которому «вы умрете не от цифрового разрыва, Вы умрете от голода» широко цитировалось, а сама проблема воспринималась как политизированная и искусственно навязанная международному сообществу крупными западными ИТ-гигантами с целью расширить свои рынки сбыта, то сегодня ни у кого не вызывает сомнений ее высокая значимость и тесная увязка с вопросами обеспечения международной стабильности и безопасности.

Под влиянием эпидемии COVID-19 широкое распространение получила цифровая коммерция, он-лайн образование и удаленная работа. Эти сдвиги являются частью общемировых тенденций перехода к четвертой промышленной революции, наметившихся еще до эпидемии, и, вероятно, сохранятся и после победы человечества над вирусом. Однако повсеместная цифровизация не только позволила более эффективно организовать самоизоляцию и контроль над распространением вируса, но и способствовала появлению новых форм неравенства и усугубила уже существующие.

Согласно данным ВЭФ, на момент начала пандемии у 60% взрослого населения планеты не было необходимых цифровых навыков для удаленной работы и учебы, у многих студентов не было доступа к интернету — в Китае их число достигло 25%, в Мексике — 45% и 65% в Индонезии[2]. Согласно данным ЮНЕСКО, в 2020 году около 826 миллионов учащихся — половина из общего числа учащихся, — не посещающих школу из-за пандемии COVID-19, не имела доступа к домашнему компьютеру, а 43% (706 миллионов) — доступа к интернету в домашних условиях, в то время как цифровое дистанционное обучение используется для обеспечения непрерывности образования в по-

[1] World Economic Forum Global Risks Report 2021. 16th edition. URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (дата обращения: 11.05.2021).

[2] Там же.

давляющем большинстве стран[3]. Это неравенство представляет собой реальную угрозу непрерывности обучения в период беспрецедентных сбоев в системе образования и в долгосрочной перспективе способно подорвать уровень экономического развития стран и человеческого потенциала.

Цифровой разрыв создавал напряженность еще до пандемии — согласно данным МСЭ, в 2018 году только половина населения планеты имела доступ к интернету и международная организация призывала к большей цифровой инклюзивности[4]. Нужно сказать, что процент населения, имеющего доступ к интернету, существенно разнится по странам. Так, в странах с высоким уровнем доходов доступность интернета достигает 87%, однако в слаборазвитых странах она ниже 17%[5]. Внутри стран доступ к цифровым технологиям определяется социально-экономическим положением людей, и проблемы существуют в том числе и в странах с высоким уровнем дохода. На международном и межгосударственном уровне проблема приобретает политическое и геополитическое измерение.

Углубление цифрового разрыва и неравномерности доступа к новым ИКТ создает новые линии напряженности как внутри обществ в отдельных странах, так и на уровне международной системы и препятствует экономическому восстановлению стран и регионов. Однако обеспечение «цифровой инклюзивности» (то есть повсеместного доступа к ИКТ) наталкивается на цифровую зависимость, скорость внедрения новых передовых цифровых технологий и информационная манипуляция, пробелы в регулятивной

---

[3] Глубокий «цифровой разрыв» в дистанционном обучении / ЮНЕСКО. 20.04.2020. URL: https://ru.unesco.org/news/glubokiy-cifrovoy-razryv-v-distancionnom-obuchenii (дата обращения: 11.05.2021).

[4] Measuring information society report. ITU, 2018. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf (дата обращения: 11.05.2021).

[5] Internet World Stats. Internet Usage and Population Statistics. URL: www.internetworldstats.com (дата обращения: 11.05.2021).

базе в сфере ИКТ, в том числе на международном уровне, а также различия в уровне образования между странами и регионами.

Политические и экономические риски, связанные с углублением цифрового разрыва возрастают по мере того, как увеличивается зависимость экономики и всех остальных сфер жизни общества от ИКТ и в геометрической прогрессии растет объем данных. В итоговом докладе РГОС ООН по международной информационной безопасности, созданной по инициативе Российской Федерации, признается, что преимущества от цифровых технологий распределены по миру неравномерно и сокращение цифрового разрыва является одним из приоритетов международного сообщества. В контексте международной информационной безопасности отмечается, что недостаточный цифровой потенциал ряда стран не позволяет им выявлять, предотвращать и отражать акты враждебного использования ИКТ, что делает их еще более уязвимыми[6].

Таким образом, цифровой разрыв представляет собой комплексную проблему и пронизывает все уровни социально-экономического неравенства в современном мире, а также приобретает международно-политическое измерение. Нельзя не отметить, что повсеместная цифровизация, обусловленная во многом необходимостью обеспечить социальное дистанцирование в условиях современной пандемии коронавирусной инфекции, обострила экономическое и политическое измерение проблемы цифрового разрыва, который нуждается в согласованных ответах со стороны международного сообщества.

Более того, на современном этапе политизированность темы развития ИКТ привела к тому, что цифровой разрыв и цифровое неравенство становится составной частью проблематики международной информационной безопасности. Новый ци-

[6] UN Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report. A/AC.290/2021/CRP.2. 10.03.2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 11.05.2021).

фровой неоколониализм стран Запада усугубляет зависимость развивающихся стран и ставит их в уязвимое положение

Нужно отметить, что российская дипломатия всегда продвигает проблемы цифрового разрыва в качестве приоритетного направления деятельности международного сообщества. ООН неоднократно призывала государства к тому, чтобы сокращать цифровой разрыв и противодействовать цифровому неоколониализму стран Запада[7].

Список использованных источников и литературы

1. Лавров С. В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью // Внешнеэкономические связи. 2020. URL: https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4350978 (дата обращения: 11.05.2021).
2. Глубокий «цифровой разрыв» в дистанционном обучении / ЮНЕСКО. 20.04.2020. URL: https://ru.unesco.org/news/glubokiy-cifrovoy-razryv-v-distancionnom-obuchenii (дата обращения: 11.05.2021).
3. Internet World Stats. Internet Usage and Population Statistics. URL: www.internetworldstats.com (дата обращения: 11.05.2021).
4. Measuring information society report. ITU, 2018. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf (дата обращения: 11.05.2021).
5. World Economic Forum Global Risks Report 2021. 16th edition. URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (дата обращения: 11.05.2021).
6. UN Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report. A/AC.290/2021/CRP.2. 10.03.2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 11.05.2021).

[7] Лавров С. В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью // Внешнеэкономические связи. 2020. URL: https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4350978 (дата обращения: 11.05.2021).

Е. И. Нархова,
канд. полит. наук, третий секретарь Департамента
международной информационной безопасности МИД России

РОССИЯ НА АСЕАНОЦЕНТРИЧНЫХ ПЛОЩАДКАХ: РАСШИРЕНИЕ ПРАКТИЧЕСКОГО СОТРУДНИЧЕСТВА ПО МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: АСЕАН — один из ключевых партнеров России в Азиатско-Тихоокеанском регионе, который традиционно выступает со схожих с Россией позиций по международной информационной безопасности. Приверженность одним и тем же подходам логически подвела российскую внешнюю политику к необходимости активизации существующих и создания новых механизмов практического сотрудничества с «десяткой» на этом направлении, что нашло широкую поддержку среди партнеров.

Ключевые слова: международная информационная безопасность, АСЕАН, АРФ, АТР.

Одним из региональных внешнеполитических приоритетов России в области международной информационной безопасности (МИБ) является участие в работе асеаноцентричных механизмов. Казалось бы, географически Юго-Восточная Азия значительно удалена от российских границ, да и разница наших научно-технических возможностей с рядом небольших государств региона очень велика.

Однако практика показывает, что АСЕАН представляет собой перспективную площадку, ведь ее государства-члены демонстрируют неподдельный интерес к сотрудничеству в области МИБ. Почему это так? Во-первых, Юго-Восточная Азия переживает прямо сейчас бурный социально-экономический рост, сопровождающийся активным внедрением технологий четвер-

той промышленной революции. Во-вторых, на этом фоне они сталкиваются с непосредственными угрозами информационной безопасности, что заставляет их искать ресурсы для наращивания своего потенциала по противодействию им. В-третьих, АСЕАН в своей политике в меньшей степени подвержена идеологическому влиянию, в отличие, например, от европейских площадок, что позволяет Ассоциации и ее членам при сотрудничестве с Россией руководствоваться не мнением третьих стран, а непосредственно своими практическими нуждами.

С учетом этих факторов Москва в последние годы активизирует усилия на асеаноцентричных площадках по МИБ. Почему для нас это важно? В России вовремя зафиксировали тренд на смещение в Азиатско-Тихоокеанский регион центра мировой политической жизни, происходящее вслед за превращением АТР в «центр тяжести» мировой экономики. Для нас также важен поиск единомышленников, которые, как и мы, ориентированы на практическую работу и не на словах, а на деле заинтересованы в создании мирной информационной среды. Основными характеристиками такой среды в нашем общем представлении являются равные права всех ее участников, взаимодействие на основе одних и тех же норм и принципов и неприемлемость использования информпространства в военных целях.

Наконец, динамичность АСЕАН, представленность здесь стран с разным уровнем социально-экономического развития и вовлеченности в мировые экономические и политические процессы позволяют апробировать на региональном уровне те сюжеты МИБ, которые впоследствии, после их проработки и одобрения здесь, будут вынесены и на глобальный уровень, где АСЕАН также традиционно действует объективно, единогласно поддерживая наши инициативы по МИБ в ООН.

Мы приветствуем и привлечение десятки к руководству ооновскими процессами. В частности, в рамках деятельности первой Рабочей группы открытого состава ООН по достижениям в сфере информатизации и телекоммуникаций в контек-

сте международной безопасности представитель Сингапура председательствовал на межсессионной неформальной встрече государств-участников с деловыми и научными кругами. Не исключаем и возможность коллективного руководства АСЕАН новой профильной Рабочей группой при формальном председательстве одной из стран десятки.

Заинтересованность асеановцев в наращивании своего информационного потенциала для защиты от ИКТ-угроз определяет и направления нашего сотрудничества, которое в 2018 г. вышло на уровень стратегического партнерства. В том же году лидеры России и АСЕАН приняли совместное заявление о сотрудничестве в области обеспечения безопасности использования ИКТ и самих ИКТ, в котором зафиксирована идея учреждения Диалога Россия — АСЕАН по вопросам, связанным с обеспечением безопасности ИКТ. В январе 2021 г. был утвержден соответствующий концептуальный документ, что позволяет нам в ближайшие месяцы запустить Диалог.

Мы также активизировали работу с десяткой и ее диалоговыми партнерами в рамках Регионального форума АСЕАН по безопасности (АРФ), где еще в 2017 г. нашими усилиями создан специализированный механизм межсессионных встреч по безопасности в сфере использования ИКТ и самих ИКТ (МВ-ИКТ). В прошлом году мы при широкой поддержке стран-участниц инициировали здесь два новых масштабных направления деятельности. Первое из них — по терминологии по тематике МИБ. В 2021 г. мы совместно с Камбоджей запустили соответствующую дискуссию в рамках МВ-ИКТ и провели среди стран — участниц АРФ опрос, сформировав и распространив по итогам информативный сводный документ, который позволил нам обменяться опытом в области выработки и применения ИКТ-терминов, а также сформулировать, с какими общими вызовами мы сталкиваемся в связи с отсутствием единой международно утвержденной терминологии по МИБ.

Второе наше направление работы в МВ-ИКТ — это вопросы противодействия информационной преступности, которым мы

посвятили совместный с Китаем и Вьетнамом онлайн-семинар (23 и 26 апреля 2021 г.). К нему подключились представители 16 стран-участниц АРФ, а также Интерпола и Управления ООН по наркотикам и преступности. Всего на нашем мероприятии виртуально присутствовало порядка 100 экспертов от государственных структур, научного и бизнес-сообщества государств АРФ.

Мы рассчитываем развить успех этих инициатив и продолжить их реализацию в следующем году.

Кроме того, мы принимаем активное участие в крупнейших профильных региональных мероприятиях, в частности, на постоянной основе в Сингапурской международной кибернеделе. На 5-й Кибернеделе, которая в октябре прошлого года собрала более 6000 экспертов из 60 стран, российскую делегацию возглавил заместитель Министра иностранных дел О. В. Сыромолотов. Если Малайзия, как и планировала, запустит в этом году международную конференцию и выставку по кибероборонe и безопасности (CYDES), мы также рассчитываем «направить» туда представительную делегацию.

Наконец, мы рассматриваем возможность подключения к работе Центра наилучших практик АСЕАН по кибербезопасности, созданного в Сингапуре в прошлом году для обучения экспертов госструктур стран Ассоциации.

Перехожу к выводам. АСЕАН, как представляется, — это хороший пример структуры, сотрудничество с которой по МИБ интересно России и при этом вызывает самый живой отклик в Ассоциации. Такой запрос на взаимодействие с обеих сторон открывает широкие перспективы для совместной работы. Динамичное развитие государств-членов АСЕАН, их желание обеспечить безопасность информационной среды в регионе и деидеологизированный подход дают нам возможность выстраивать прямой, открытый и конструктивный диалог. Пандемия благодаря накопленному ранее опыту не затормозила существенно наше сотрудничество, и мы намерены и в дальнейшем наращивать его темпы.

А. В. Зинченко,
д-р ист. наук, профессор,
ведущий эксперт Центра международной информационной
безопасности и научно-технологической политики
МГИМО МИД России

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ COVID-ДИПЛОМАТИИ

Аннотация: в статье рассматривается относительно новое направление цифровой дипломатии, которое в американских и западноевропейских СМИ трактуется и приписывается России и Китаю: «ковид-дипломатия» и «вакцинная дипломатия». Дан краткий анализ политических и финансово-экономических факторов, характеризующих зарубежные информационные материалы международно-политическую деятельности по противодействию короновирусной инфекции в контексте обвинений России в использовании вакцины «Спутник V» в геополитических целях «гибридной войны».

Ключевые слова: «COVID-дипломатия», «вакцинная дипломатия», «гонка вацин», пандемия COVID-19, вакцина «Спутник V».

Менее чем за год пандемия COVID-19 вызвала беспрецедентное беспокойство по поводу здоровья населения по всему миру, а также обострила социально-экономические и политические отношения во многих странах. Так как большинство новостей о короновирусной пандемии распространяемые в СМИ и социальных сетях по своей сути являются тревожными, то дезинформация и сфабрикованные сообщения о COVID-19 только усугубляют депрессивные симптомы в общественном мнении населения. В марте 2021 года Всемирная организация здравоохранения (ВОЗ) впервые сообщила об ухудшении ментального здоровья по всему миру, спровоцированном пандемией. Более того, директор ВОЗ Тедрос Аданом Гебреисус, опираясь

на первичные исследовательские данные (стресс, тревога и депрессия затронули около 30% человечества), заявил об угрозе коллективной травмы от пандемии коронавируса как о более масштабной, чем травма от Второй мировой войны. Среди отягчающих обстоятельств глава ВОЗ выделил бесконечные потоки противоречивой информации о пандемии на различных цифровых коммуникационных платформах в условиях соблюдения требований самоизоляции[8].

Чтобы препятствовать стереотипизации и дискриминации, проявившихся в США и отдельных странах ЕС, Всемирная организация здравоохранения в мае 2021 г. решила обозначать мутации коронавируса SARS-CoV-2, выявленные в той или иной стране, буквами греческого алфавита. После консультаций со специально созванной группой ученых, первые четыре буквы (Альфа, Бета, Гамма и Дельта) достались штаммам, выявленным в Великобритании, Южной Африке, Бразилии и Индии. Аналитики ВОЗ подчеркивают, что новые обозначения легко произносимы и не стигматизируют какие-либо страны, при этом данная маркировка мутаций коронавируса не означает отказа от их научных наименований, которые будут применяться в медицинских исследованиях.

Однако на этом кризисном для мирового сообщества фоне виртуальные ресурсы сети интернет все больше пестрят весьма привлекательными для хайпа рубриками: «вакцинная дипломатия», «ковид-дипломатия» и др. По мнению экспертов по международной силовой политике, эти информационные вбросы стращают тем, что Россия и Китай, распространяя безвозмездно вакцины от коронавируса, токсично влияют на репутации США и стран ЕС.

Одним из первых активных сторонников «ковид-дипломатии» являлся президент США Дональд Трамп, который часто

[8] Муртазаев А. Потерянные во времени: как мы переживаем коллективную травму от COVID-19 // Forbes, 02.08.2021. — URL: https://www.forbes.ru/forbeslife/436397-poteryannye-vo-vremeni-kak-my-perezhivaem-kollektivnuyu-travmu-ot-covid-19 (дата обращения: 16.08.2021).

называл SARS-CoV-2 «китайским вирусом», намекая на лабораторную версию происхождения нового коронавируса. Однако данная версия даже в США первоначально считалась маргинальной и в основном была популярна у сторонников теорий заговора. Например, компания Facebook в феврале 2021 г. начала удалять посты в соцсети о лабораторном происхождении коронавируса наравне с публикациями о вреде вакцинации, а также о неэффективности или ядовитости вакцин. Но после того, как вновь избранный президент США Джо Байден 19 мая 2021 г. попросил разведку «удвоить» усилия по поиску источника COVID-19, а также рассмотреть «вопросы по Китаю», Facebook решила пересмотреть свою политику[9]. По данным The New York Times, перед этим американские спецслужбы проинформировала Белый дом, что не без помощи агентства Intel «получили доступ» к информации с китайских облачных серверов и задействует «экстраординарные» компьютерные мощности, для проверки версии об утечке вируса COVID-19 из лаборатории в Ухане[10].

В ответ, 26 мая 2021 г. представитель МИД КНР Чжао Лицзянь на брифинге не только обвинил США в «распространении теорий заговоров и дезинформации, таких как утечка из китайских лаборатории, подчеркивая, что подобных версий являются неуважением к работе ВОЗ, что грозит подрывом международной солидарности в борьбе с пандемией. Более того, представитель МИД КНР предложил американским властям в рамках расследования происхождения коронавируса COVID-19 обеспечить доступ специалистов ВОЗ на «военную базу в Форт-Детрик

[9] Байден велел разведке удвоить усилия по поиску источника COVID-19 // INTERFAX.RU, 26.05.2021. — URL: https://www.interfax.ru/world/769032 (дата обращения: 16.08.2021).

[10] Exclusive: Intel agencies scour reams of genetic data from Wuhan lab in Covid origins hunt // Katie Bo Williams, Zachary Cohen and Natasha Bertrand, CNN, 06.08.2021. — URL: https://edition.cnn.com/2021/08/05/politics/covid-origins-genetic-data-wuhan-lab/index.html (дата обращения: 16.08.2021).

как можно раньше, и биолаборатории, которыми располагают США по всему миру»[11].

Такая дипломатическая риторика и динамика американо-китайских «пикировок» на международной арене по вопросу появления короновирусной инфекции получившей официальное название COVID-19, а также ответственности за ее распространение по миру, убедительно свидетельствует о весьма длительной перспективе «COVID-дипломатии». Как США, так и КНР будут пытаться в этом процессе использовать свое влияние на ВОЗ и другие международные организации для достижения своих политических целей, которые окажут минимальное влияние на решение реальных вопросов в противодействии с пандемией.

Появление «вакцинной дипломатии» было обусловлено неожиданным для США и ЕС итогом развернувшейся на мировой арене «гонки» за разработку эффективной профилактической вакцины для противодействия пандемии COVID-19. Официальное появление 11 августа 2020 г. в России первой в мире зарегистрированной вакцины на основе хорошо изученной платформы вектора аденовируса человека[12], с одной стороны, ознаменовало научно-медицинский прорыв, осуществленный российскими учеными-вирусологами, а с другой предоставляло возможность мировому сообществу объединить усилия в противодействии распространения новой короновирусной пандемии. Однако инновационный препарат, который Российский фонд прямых ин-

---

[11] Пекин призвал США пустить к себе экспертов для расследования истоков COVID-// INTERFAX.RU, 26.05.2021 – URL: 19https://www.interfax.ru/world/768958 (дата обращения: 16.08.2021).

[12] Международное непатентованное или группировочное или химическое наименование: «Вакцина для профилактики новой коронавирусной инфекции (COVID-19)»; Торговое наименование лекарственного препарата: «Гам-КОВИД-Вак Комбинированная векторная вакцина для профилактики коронавирусной инфекции, вызываемой вирусом SARS-CoV-2». — URL: https://grls.rosminzdrav.ru/Grls_View_v2.aspx?routingGuid=962a4d42-1c47-4af4-b14d-86c6ce1421fd&t] (дата обращения: 16.08.2021).

вестиций (РФПИ), организуя экспорт «Спутника V» представлял «вакциной для всего человечества», стал целью «агрессивных информационных атак» в бурном потоке русофобской риторики в русле санкционной политики США и ЕС против России.

Фейковые информационные «страшилки» о побочных эффектах российской вакцины или ее дефиците существенно стремились замедлить как вакцинацию населения в России, так и экспорт препарата в зарубежные страны.

Аналитики Би-би-си, которые целенаправленно мониторили сообщения РФПИ, информационных агентств (РИА Новости, ТАСС, Интерфакс, Рейтер) о соглашениях на поставки «Спутника V», а также о заключенных контрактах на производство вакцины за рубежом в мае 2021 г. констатировали «экспансию» российского препарата в страны, совокупное население которых превышает больше половины населения мира[13].

Международная экспансия российской вакцины

[13] Дьяконова О., Козловский С. Экспансия «Спутника»: где производят и уже используют российскую вакцину от коронавируса. — URL: https://www.bbc.com/russian/features-56675724 (дата обращения: 16.08.2021).

Необходимо отметить, что западные СМИ и цифровые коммуникационные ресурсы их обеспечивающие, относительно достоверно отражают государственную стратегию России, которая нацелена чтобы отечественные медицинские производственные площадки обеспечивали населения страны. При этом, зарубежные публицисты, аналитики и эксперты не упускают возможности критиковать недостатки бюрократической административной системы ее реализуемой в отдельных регионах страны.

Основные информационные виртуальные ресурсы рубрики «вакцинной дипломатии» подвергают сомнению экспортные возможности России, обвиняя российские власти в необоснованной пропаганде противодействия пандемии на международной арене или невыполнении контрактных обязательств по поставкам вакцины в зарубежные страны.

Питательную почву для дезинформации представляется тот факт, что положительная динамика применения «Спутник V» в России и за рубежом, обеспечила регистрации вакцины к маю 2021 г. более чем 60 странах, из которых уже свыше 40 государств получили первые поставки препарата и начали его применение. С учетом этого, чтобы обеспечит экспорт вакцины РФПИ заключил соглашения на зарубежное производство «Спутник V» с 15 компаниями из 10 стран и переговоры с другими зарубежными компаниями и правительствами по этому вопросу продолжаются. О желании производить вакцину заявили власти Армении, Венесуэлы, Саудовской Аравии, ОАЭ, Алжира, Мексики и Бангладеш. В Италии и Швейцарии медицинские компании выразили готовность производить «Спутник V» после решения Европейского медицинского агентства (ЕМА), которое с 4 марта 2021 г. проводит процедуру экспертизы российской вакцины. в занимается одобрением вакцин для использования на европейском рынке. Этого решения ждут и другие европейские страны так как смогут беспрепятственно размещать заказы на «Спутник V» и организовывать его производство. Однако настораживает тот факт, что 7 апреля издание Financial Times

сообщило, что EMA проверяет соответствие испытаний вакцины принципам надлежащей клинической практики, а именно — «этическим стандартам».

Необходимо подчеркнуть, что если производство «Спутник V» в Беларуси, Казахстане, Иране, Аргентине, Турции, Египте, Сербии в первую очередь, нацелено на обеспечение потребностей этих стран, то производственные мощности Индии, Китая, Южная Кореи и, возможно, Бразилии имеют потенциал и должны стать основными поставщиками вакцины по экспортным контрактам России. Примечательно, что регистрацию и использование российской вакцины от коронавируса индийские власти экстренно одобрили 12 апреля 2021 г., когда ситуация в стране с заболеваемостью и смертностью от *COVID-19* побила мировые рекорды и стала катастрофической. РФПИ оперативно заключила контракты на суммарный объем производство в Индия уже с мая 2021 г. 426 млн комплектов доз «Спутника V» в год с пятью индийскими медицинскими компаниями.

На фоне первоначального дефицита профилактических вакцин от COVID-19 в странах ЕС, Венгрия и Словакия в условиях роста заболеваемости первыми подписали контракты на поставку российской вакцины, поставки которой начали поступать в страны уже в феврале–марте 2021 г. несмотря на отсутствие одобрения «Спутника V» европейским регулятором. Еще тогда глава МИД Венгрии Петер Сийярто в интервью Russia Today отметил, что власти страны «подверглись нападкам просто потому, что решили обратить свой взор на Восток, вместо того чтобы смотреть только на Запад».

Подобные претензии властных бюрократов ЕС к властям Словакии в рамках «вакцинной дипломатии» вызвали в стране политический скандал, что привело к отставке премьера И. Матовича. Первоначально для дискредитации решения словацкого премьера не согласные с ним представители коалиционного правительства 8 апреля 2021 г. бездоказательно заявили, что прибывшая в страну партия доз «Спутника V»

отличается от исследуемого EMA и не соответствует показателям исследования, которые опубликованы в журнале Lancet. Затем фейковую новость о «некачественной вакцине» руководитель словацкого МИДа заменил проатлантическим заявлением в духе холодной войны: премьер И. Матович поддался российскому «орудию гибридной войны» и поставил под сомнение работу Словакии с ЕС.

Яркими свидетельствами дезинформационной кампании, имеющей целью не допустить российскую вакцину на европейский и другие рынки, являются публикации с броскими провокационными названиями, например, «Русская рулетка» или триумф российской дипломатии? Нужна ли ЕС вакцина «Спутник», Вакцинация против ковида в ЕС — в чем проблема и при чем тут «Спутник» и др. По мнению представителя РФПИ особой активность отличилось немецкое издании Bild за короткое время опубликовала более 15 подобных статей, атакующих вакцину «Спутник V». Обобщая информационную шумиху, издание New York Times резюмировало, что «вакцинная дипломатия» стала «яблоком раздора» среди европейских стран. При этом в аналитической статьи иронично отметили, что «остается неясным, является ли «Спутника V» тем медицинским прорывом, который объявил в прошлом году В. В. Путин, но она уже доказала свою эффективность в распространении хаоса и раскола в Европе». Весьма показательно в американской газете (NY Times), которую трудно подозревать в политических симпатиях к России, автор утверждает, что «большинство экспертов уверены, в эффективности российской вакцины». Более того он признает, что единственная причина раскола и раздрая в Европе в связи со «Спутник V»— в том, что ее наотрез, резко, априори отвергают по политическим причинам антироссийски настроенные силы, политики и правительства. В целом, поддерживая американского публициста, хочу дополнить его выводы тем, что русофобская истерия подпитывается финансово-экономическими ресурсами бизнеса, имеющего выгоду от санкционной политики проводи-

мой коллективным западом и курируется политиками, которые по тем или иным причинам защищает их интересы. Об этом убедительно свидетельствует быстрый и категорический отказ от закупок «Спутник V» властными элитами Литвы, Украины, Польши, обвинивших практически хором Россию в использовании вакцинной дипломатии в как средство «гибридной войны» в геополитических целях.

Специфика финансово-экономического фактора вакцинной дипломатии состоит в том, что Россия впервые получила возможность вывести российскую фармацевтическую промышленность на международный рынок, который согласно источникам Би-би-си в фармпромышленности впервые оценен почти в 1 трлн долларов. Однако, по мнению руководителя научной экспертизы венчурного фармацевтического фонда Inbio Ventures И. Ясный, попытки *РФПИ* внедрится на международном рынке вакцин сильно ограничены пока «Спутник V» не одобрила ВОЗ и регулятор Евросоюз EMA. Этот процесс затянулся так как Россия, не являясь членом Международной конференции по гармонизации технических требований к регистрации лекарственных препаратов для человека (ICH), не имеет практики законодательного оформления должного качества для преодоления жестких барьеров, которые регулируют доступ новых лекарственных средств в странах ОЭСР. Деятельность участвующих пропагандируемой в западных СМИ «гонке вакцин» американских, английских и немецких фармкомпаний, которые спустя полгода вышли на международный рынок, подтверждает прогноз российского эксперта. Например, Европейское агентство лекарственных средств 21 декабря 2021 г. предоставило первое «условное разрешение»[14]

[14] Условное разрешение на продажу является одним из регулирующих механизмов ЕС для облегчения раннего доступа к лекарствам, удовлетворяющим неудовлетворенную медицинскую потребность, в том числе в чрезвычайных ситуациях, таких как нынешняя пандемия. — URL: https://www.ema.europa.eu/en/news/ema-recommends-first-covid-19-vaccine-authorisation-eu. (дата обращения: 16.08.2021).

Европейской комиссии на продажу в ЕС американо-немецкой вакцины Comirnaty, разработанная немецкой биотехнологической компанией BioNTech при сотрудничестве с американской Pfizer. Исполнительный директор EMA Э. Кук для успокоения европейцев заявила: «Мы будем продолжать собирать и анализировать данные о безопасности и эффективности этой вакцины, чтобы защитить людей, принимающих вакцину в ЕС»[15]. ВОЗ также весьма оперативно поддержала это решение EMA, одобрив применение данного препарата для использования в экстренных случаях уже 31 декабря того же года. Европейское агентство лекарственных средств в ускоренном темпе уже в начале марта 2021 г. подтвердило безопасность вакцины Moderna, а ВОЗ в конце апреля включила американский препарат в список рекомендованных вакцин для экстренного использования для профилактики коронавирусного вируса COVID-19.

«Экономическо-политическим» назвал решение экспертов в ходе закрытого заседания в онлайн-формате участников Всемирного конгресса вакцин (World Vaccine Congress Washington 2021) признать препарат производства американской компании Moderna лучшим среди вакцин от коронавируса директор Научно-исследовательского центра имени Гамалеи А. Гинцбург. Он отметил, что решалась «цена вопроса порядка 100 миллиардов долларов» и нельзя было «отдать эти деньги Российской Федерации» несмотря на более оптимальные параметры стоимость-качество-эффективность российской вакцины «Спутник V» или германо-американской Pfizer/BioNTech[16].

---

[15] EMA Recommends the First COVID-19 Vaccine Authorisation // European Mediacal Agency — URL: https://www.ema.europa.eu/en/news/ema-recommends-first-covid-19-vaccine-authorisation-eu. (дата обращения: 16.06.2021).

[16] Гинцбург прокомментировал выбор лучшей вакцины на Всемирном конгрессе // РИА–Новости, 06.05.2021. — URL: https://ria.ru/20210506/vaktsina-1731273945.html (дата обращения: 16.08.2021).

Однако волнообразное распространении короновирусной пандемии весной 2021 г. в Европе с высокими показателями смертности от нее в странах ЕС, вызывая беспокойство западноевропейцев, активизировали политический фактор «вакцинной дипломатии» как на межгосударственном уровне, так и с участием региональных властных структур, которые носили не всегда согласованный характер. Например, после заявления австралийских экспертов, специализирующихся на эпидемиологии и вирусологии, что использованию одной из самых лучших мировых вакцин «Спутник V» мешает политика[17] премьер-министр Австрии Себастьян Курц 7 февраля 2021 г. призвал ЕМА утвердить «все доступные вакцины как можно скорее»[18]. Еврокомиссар по внутренним рынкам Тьерри Бретон на пресс-конференции в Брюсселе 17 марта Еврокомиссар назвал «Спутник V» одним из кандидатом на применение в ЕС и заявил, что ЕС, «возможно, поможет России с производством вакцины»[19]. Госсекретарь по делам Европы при МИД Франции Клеман Бон 23 марта в эфире радиостанции France Info заявил, что не исключает Франция может начать применение российской вакцины от коронавируса «Спутник V» в июне, когда препарат пройдет экспертизу Европейского агентства по лекарственным средствам. «Но не нужно политизировать этот вопрос. Если вакцина полезна, если она имеется в наличии, то следует этим

[17] В Австралии заявили, что вакцина «Спутник V» лучшая, но политизированная // RuNews24, 10.08.2021. — URL: https://runews24.ru/society/10/08/2021/b25743s5fe46847bd023ecb326dcdd26 (дата обращения: 16.08.2021).

[18] Канцлер Австрии заявил о готовности привиться вакциной из России // РИА-Новости, 07.02.2021. — URL: https://ria.ru/20210207/vaktsina-1596353461.html (дата обращения: 16.08.2021).

[19] Еврокомиссар назвал «Спутник V» кандидатом на применение в ЕС // РБК, 17.03.2021. — URL: https://www.rbc.ru/politics/17/03/2021/605203139a794701ef2d1e62https://www.rbc.ru/politics/17/03/2021/605203139a794701ef2d1e62 (дата обращения: 16.08.2021).

воспользоваться», — сказал представитель французского МИД (цитата по ТАСС)[20].

Канцлер ФРГ Ангела Меркель по итогам совещания по вопросам вакцинации с главами немецких регионов 19 марта уверенно заявила, что Германия может самостоятельно закупить российскую вакцину «Спутник V», если Евросоюз после одобрения препарата регулятором не пойдет на централизованные поставки[21]. Со схожим заявлением выступил премьер-министр Италии Марио Драги. «Мы закажем «Спутник V» и посмотрим. Если общеевропейские усилия работать не будут — особенно в области здравоохранения, — мы должны быть готовы действовать самостоятельно. Я не единственный, кто так считает», — заявил он на первой пресс-конференции в должности главы правительства, отметив, что канцлер Германии придерживается такой же позиции[22].

На этом весьма продуктивном фоне противодействия короновирусной инфекции, газета Le Figaro 26 марта цитирует резонансное заявление президента Франции Э. Макрона: «Мы столкнулись с мировой войной нового типа, имея дело с действиями России и Китая, пытающихся через поставки вакцин получить влияние»[23]. В тот же день министр иностранных дел страны Ле Дриан в эфире France Info radio заявляет, что

[20] В МИД Франции назвали возможные сроки начала использования «Спутника V» // ТАСС, 23.03.2021 – URL: https://tass.ru/obschestvo/10970625 (дата обращения: 16.08.2021).

[21] Germany: Merkel, state leaders agree on strategy to jump-start vaccinations. — URL: https://www.dw.com/en/germany-merkel-state-leaders-agree-on-strategy-to-jump-start-vaccinations/a-56931483 (дата обращения: 16.08.2021).

[22] Европа опоздала на прививку // Коммерсант, 21.03.2021. — URL: https://www.kommersant.ru/doc/4740408 (дата обращения: 16.08.2021).

[23] COVID-19: Macron prédit «de nouvelles mesures» à prendre «dans les prochains jours et semaines» // Le Figaro, 26.03.2021. — URL: https://www.lefigaro.fr/sciences/en-direct-suivez-la-conference-de-presse-d-olivier-veran-20210325 (дата обращения: 16.08.2021).

«Вакцина „Спутник V“ используется скорее для пропаганды и агрессивной дипломатии, чем для медицинской помощи из солидарности»[24].

Такого рода синхронные нападки на Россию по актуальной проблеме международной жизни предвещали как минимум дипломатический скандал. Однако 30 марта 2021 г. пресс-служба Кремля сообщала, что по инициативе президента Франции Э. Макрона и канцлера ФРГ А. Меркель по телефону президент России В. В. Путин обсудил актуальные «задачи объединения усилий в борьбе с общей угрозой — пандемией коронавирусной инфекции» COVID-19, в частности, «перспективы регистрации в ЕС российской вакцины «Спутник V», а также возможных поставок и совместного производства этого препарата в странах ЕС»[25].

В условиях такого политического хаоса, когда перспектива ослабления короновирусной инфекции с помощью самой распространенной в Европе вакциной AstraZeneca становилась довольно призрачной на фоне наступающей третьей волны пандемии, в Германии и Франции стали проявляться признаки политического раскола относительно «Спутник V» между региональными и федеральными властями. В начале апреля премьер-министр Баварии Маркус Зёдер заявил, что заключен предварительный контракт на получение 2,5 млн доз российской вакцины при условии ее одобрения европейским регулятором, который позволит «помимо возможности импорта вакцины напрямую из России компании R-Pharm также создать соб-

[24] В МИД Франции назвали российскую вакцину от COVID-19 «средством пропаганды и агрессивной дипломатии» // 26.03.2021. — URL: https://nv.ua/world/geopolitics/franciya-raskritikovala-rossiyskuyu-vakcinu-ot-koronavirusa-poslednie-novosti-50150358.html (дата обращения: 16.08.2021).

[25] Путин обсудил с Меркель и Макроном перспективы «Спутника V» в ЕС // INTERFAX.RU, 30.03.2021. — URL: https://www.interfax.ru/world/758711 (дата обращения: 16.08.2021).

ственную производственную линию в Баварии»[26]. В середине апреля глава региона Прованс — Альпы — Лазурный берег Рено Мюзелье заявил, что сделал предзаказ на «Спутник» в количестве 500 тысяч доз. Во французском МИДе раскритиковали это решение и назвали его «безответственным», поскольку оно «создает риски неравенства в обеспечении регионов вакциной»[27].

Такие проявления в европейской политической жизни однозначно трактуются чиновниками ЕС, как следствие «российской вакцинной дипломатии «Спутника V», которая продемонстрирует свою невероятную эффективность в деле распространении разногласий и раскола в Европе, где политика Брюсселя не позволяет сдержать третью волну заболеваемости ковид[28]. На этом фоне включаются ресурсы публицистов, политологов, или отставных дипломатов типа А. Демаре (A. Demarais), которая вещая в британском 24-часовом новостном телеканале «Скай ньюс»[29] грозно предупреждала западноевропейцев, что «подписавшись на вакцины из России и Китая, ждите требований, которым не сможете отказать».

Таким образом, за лавиной распространяющихся в традиционных СМИ и цифровых коммуникационных виртуальных ресурсов информации о проводимой Россией и Китаем «ковид-дипломатии» и «вакцинной дипломатии» явно просма-

---

[26] Цит. по: Дьяконова О, Козловский С. Экспансия «Спутника»: где производят и уже используют российскую вакцину от коронавируса. — URL: https://www.bbc.com/russian/features-56675724. (дата обращения: 16.08.2021).

[27] Там же.

[28] Brussels is needled by Russia's Sputnik V vaccine diplomacy // News. The Times. — URL: https://www.thetimes.co.uk/article/brussels-is-needled-by-russias-sputnik-v-vaccine-diplomacy-3qp0cbg2r (дата обращения: 20.03.2021).

[29] Телеканал ходит в группу каналов организации BSkyB (British Sky Broadcasting), которая в свою очередь является частью корпорации News corporation Руперта Мердока. Канал осуществляет вещание в цифровом формате через сеть спутниковых приёмников.

тривается новое направление цифровой дипломатии, которое в условиях информационной войны развязанной США и странами ЕС направленной на дискредитацию политики России по противодействию короновирусной инфекции в партнерстве с международными организациями и государствами, которые оказывают реальную помощь в продвижении профилактических вакцин, включая весьма эффективный российский препарат «Спутника V».

Список использованных источников и литературы

1. Байден велел разведке удвоить усилия по поиску источника COVID-19 // INTERFAX.RU, 26.05.2021 — URL: https://www.interfax.ru/world/769032 (дата обращения: 16.08.2021).
2. В Австралии заявили, что вакцина «Спутник V» лучшая, но политизированная // RuNews24, 10.08.2021 — URL: https://runews24.ru/society/10/08/2021/b25743s5fe46847bd023ecb326dcdd26 (дата обращения: 16.08.2021).
3. В МИД Франции назвали возможные сроки начала использования «Спутника V» // ТАСС, 23.03.2021 — URL: https://tass.ru/obschestvo/10970625 (дата обращения: 16.08.2021).
4. В МИД Франции назвали российскую вакцину от COVID-19 «средством пропаганды и агрессивной дипломатии» // 26.03.2021 — URL: https://nv.ua/world/geopolitics/franciya-raskritikovala-rossiyskuyu-vakcinu-ot-koronavirusa-poslednie-novosti-50150358.html (дата обращения: 16.08.2021).
5. Гинцбург прокомментировал выбор лучшей вакцины на Всемирном конгрессе // РИА–Новости, 06.05.2021 — URL: https://ria.ru/20210506/vaktsina-1731273945.html (дата обращения: 16.08.2021).
6. Дьяконова О., Козловский С. Экспансия «Спутника»: где производят и уже используют российскую вакцину от коронавируса. — URL: https://www.bbc.com/russian/features-56675724 (дата обращения: 16.08.2021).
7. Европа опоздала на прививку // Коммерсант, 21.03.2021 — URL: https://www.kommersant.ru/doc/4740408 (дата обращения: 16.08.2021).
8. Канцлер Австрии заявил о готовности привиться вакциной из России // РИА-Новости, 07.02.2021 — URL https://ria.ru/20210207/vaktsina-1596353461.html (дата обращения: 16.08.2021).

9. Муртазаев А. Потерянные во времени: как мы переживаем коллективную травму от COVID-19 // Forbes, 02.08.2021 — URL: https://www.forbes.ru/forbeslife/436397-poteryannye-vo-vremeni-kak-my-perezhivaem-kollektivnuyu-travmu-ot-covid-19 (дата обращения: 16.08.2021).
10. Пекин призвал США пустить к себе экспертов для расследования истоков COVID-19 // INTERFAX.RU, 26.05.2021 — URL: https://www.interfax.ru/world/768958 (дата обращения: 16.08.2021).
11. Путин обсудил с Меркель и Макроном перспективы «Спутника V» в ЕС // INTERFAX.RU, 30.03.2021 — URL: https://www.interfax.ru/world/758711 (дата обращения: 16.08.2021).
12. Brussels is needled by Russia's Sputnik V vaccine diplomacy // News. The Times — URL: https://www.thetimes.co.uk/article/brussels-is-needled-by-russias-sputnik-v-vaccine-diplomacy-3qp0cbg2r (дата обращения — 20.03.2021).
13. COVID-19 : Macron prédit «de nouvelles mesures» à prendre «dans les prochains jours et semaines» // Le Figaro, 26.03.2021 — URL: https://www.lefigaro.fr/sciences/en-direct-suivez-la-conference-de-presse-d-olivier-veran-20210325 (дата обращения: 16.08.2021).
14. EMA Recommends the First COVID-19 Vaccine Authoriыation // European Mediacal Agency — URL: https://www.ema.europa.eu/en/news/ema-recommends-first-covid-19-vaccine-authorisation-eu. (дата обращения: 16.06.2021).
15. Exclusive: Intel agencies scour reams of genetic data from Wuhan lab in Covid origins hunt // Katie Bo Williams, Zachary Cohen and Natasha Bertrand, CNN, 06.08.2021 — URL: https://edition.cnn.com/2021/08/05/politics/covid-origins-genetic-data-wuhan-lab/index.html (дата обращения: 16.08.2021).
16. Germany: Merkel, state leaders agree on strategy to jump-start vaccinations — URL: https://www.dw.com/en/germany-merkel-state-leaders-agree-on-strategy-to-jump-start-vaccinations/a-56931483 (дата обращения: 16.08.2021).

И. О. Яникеева,
аспирантка МГИМО МИД России

КИБЕРСАНКЦИИ КАК ИНСТРУМЕНТ СДЕРЖИВАНИЯ ЦИФРОВОГО РАЗВИТИЯ

Аннотация: для обеспечения эффективности участия и вовлечения людей в экономическую, политическую и социальную жизнь не только отдельного государства, но и мирового сообщества в целом необходимым является доступ к современным ИКТ, которые становятся важнейшим ресурсом цифрового развития государств. Однако США и ЕС разработали механизмы киберсанкций, которые в настоящее время применяются в качестве инструмента сдерживания цифрового развития. Наиболее яркими примерами являются санкции, введенные США в отношении китайской компании «Huawei» и российской компании АО «Лаборатория Касперского». Существующие режимы киберсанкций препятствуют преодолению цифрового разрыва и наращиванию потенциала по защите национального киберпространства. Масштаб существующих киберугроз, цифровой разрыв, и тот факт, что киберпространство становится ареной межгосударственной конкуренции, актуализируют вопрос глобального регулирования цифровой среды. Представляется возможным международное сотрудничество в области помощи развитию в цифровом пространстве, разработка и реализация многосторонних программ, способствующих преодолению информационного неравенства, в условиях противодействия киберугрозам посредством разработки и применения международных киберсанкций, принимаемых на уровне Совета Безопасности ООН.

Ключевые слова: киберсанкции, российско-американские отношения, международная информационная безопасность, цифровое развитие, цифровой разрыв, ЕС, США.

В XXI веке особое значение приобрело взаимодействие между информационно-коммуникационными технологиями (ИКТ) и человеком. Для обеспечения эффективности участия и вовлечения людей в экономическую, политическую и социальную жизнь не только государства, но и мирового сообщества в целом необходимым является доступ к новым ИКТ, которые становятся важнейшим ресурсом цифрового развития государств.

С распространением ИКТ растет количество киберугроз, бороться с которыми государства пытаются своими силами, в том числе применяя односторонние экономические санкции для того, чтобы принудить другие страны или отдельные лица изменить свое поведение или чтобы нанести им ответный ущерб за их действия в цифровой среде (киберасанкции). В числе наиболее активных инициаторов подобных односторонних кибермер — Европейский союз (ЕС) и Соединенные Штаты Америки (США).

Киберсанкции являются новым феноменом, поскольку появились всего шесть лет назад с момента вступления в силу Указ президента США 13694[30]. Их появление было обусловлено ускоренным развитием ИКТ, ростом киберугроз и отсутствием глобального партнерства для решения проблем, связанных с цифровой средой.

Киберсанкции — это адресные ограничительные меры, вводимые государствами и организациями в отношении физических и юридических лиц за их деятельность в цифровой среде. Они включают в себя финансовые ограничения, заморозку активов, блокировку аккаунтов в социальных сетях, цифровую изоляцию, запрет на въезд. Однако могут быть использованы и другие инструменты внешней политики.

Цель киберсанкций — изменить нежелательное поведение физического и юридического лица; ограничить возможности для проявления нежелательного поведения и для выбора не-

[30] Presidential Documents. Executive Order 13694. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. 2015. — URL: https://home.treasury.gov/system/files/126/cyber_eo.pdf (дата обращения: 16.05.2021).

желательного для того или иного государства курса действий[31]. Кроме того, киберсанкции, используемые в одностороннем порядке, являются средством достижения политических целей, таких как сдерживание технологического, цифрового развития или достижения каких-либо преимуществ в цифровой среде.

В настоящее время киберсанкции применяются несмотря на тот факт, что в соответствии с положениями принятого консенсусом доклада Группы правительственных экспертов (ГПЭ) 2015 года и закрепившей его рекомендации в резолюции Генеральной Ассамблеи ООН №70/237, любые обвинения в организации и совершении преступных деяний, выдвигаемые в отношении государств, должны быть обоснованными[32].

Основным механизмом по введению киберсанкций является публичная атрибуция атак[33]. В основе этого механизма находится неподкрепленное юридически значимыми доказательствами обвинение любого физического или юридического лица, государства в осуществлении каких-либо злонамеренных действий в кибернетическом пространстве.

В соответствии с законами США, после публичной атрибуции атаки возможно применение всех доступных мер противодействия — от экономических ограничений до ответных кибератак[34].

---

[31] Смеетс М. Несовместимые цели: экономические санкции и ВТО // Россия в глобальной политике. // 2014. №4. Июль/Август. — URL: https://globalaffairs.ru/articles/nesovmestimye-czeli-ekonomicheskie-sankczii-i-vto/ (дата обращения: 16.05.2021).

[32] Резолюция, принятая Генеральной Ассамблеей 23 декабря 2015 года по докладу Первого комитета (A/70/455) 70/237. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. 2015. — URL: https://undocs.org/ru/A/RES/70/237 (дата обращения: 16.05.2021).

[33] Карасев П. Кибербои без правил // РСМД. 2019. — URL: https://russiancouncil.ru/analytics-and-comments/analytics/kiberboi-bez-pravil/?sphrase_id=56814264 (дата обращения: 16.05.2021).

[34] Presidential Documents. Executive Order 13757. Taking Addi-

Кроме того, санкции США являются экстерриториальными, то есть вводятся в отношении третьих лиц из третьих стран за их взаимодействие с подсанкционными лицами. Это способно оказать негативное влияние на цифровое развитие, поскольку государства, компании, физические лица из третьих стран могут отказаться и отказываются как-либо взаимодействовать с государствами, физическими и юридическими лицами, в отношении которых введены односторонние киберсанкции, которые, в свою очередь, с точки зрения международного права, являются нелегитимными, учитывая нерешенность проблемы атрибуции. Примерами являются киберсанкции в отношении российской компании АО «Лаборатория Касперского» и китайской компании «Huawei».

В отсутствии всеобщих международных универсальных правил поведения в киберпространстве любое государство может обвинить кого-угодно в кибератаках, в представлении киберугрозы национальной безопасности в соответствии со своими политическими интересами и ввести киберсанкции. В ответ на это могут быть введены ответные ограничительные меры, санкционная спираль начнет закручиваться, и эскалация конфликта будет неизбежна, что в свою очередь, негативно повлияет и на цифровое развитие в целом.

Масштаб существующих киберпроблем, включая цифровой

tional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities. 2016. — URL: https://home.treasury.gov/system/files/126/cyber2_eo.pdf (дата обращения: 16.05.2021); 31 CFR Part 578. Cyber-Related Sanctions Regulations. URL: https://clck.ru/VMTcM (дата обращения: 16.05.2021); Electronic Code of Federal Regulations. 80 FR 81752-15. Issuance of Cyber-Related Sanctions Regulations to implement Executive Order 13694. // 2020. URL: https://home.treasury.gov/system/files/126/fr80_81752.pdf (дата обращения: 16.05.2021); Department of the Treasury, Office of Foreign Assets Control. 31 CFR Part 578. Cyber-Related Sanctions Regulations. — 2015. — URL: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities (дата обращения: 16.05.2021).

разрыв, и тот факт, что киберпространство становится ареной межгосударственной конкуренции, актуализируют вопрос глобального регулирования цифровой среды. Международное взаимодействие и механизм санкций ООН по вопросам МИБ возможны и необходимы. В отличие от уже существующих киберсанкционных механизмов киберсанкции на уровне ООН не будут препятствовать цифровому развитию и наращиванию потенциала по защите национального киберпространства.

Список использованных источников и литературы

1. Карасев П. Кибербои без правил // РСМД. 2019. — URL: https://russiancouncil.ru/analytics-and-comments/analytics/kiberboi-bez-pravil/?sphrase_id=56814264 (дата обращения: 16.05.2021).
2. Резолюция, принятая Генеральной Ассамблеей 23 декабря 2015 года по докладу Первого комитета (A/70/455) 70/237. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. 2015. — URL: https://undocs.org/ru/A/RES/70/237 (дата обращения: 16.05.2021).
3. Смеетс М. Несовместимые цели: Экономические санкции и ВТО // Россия в глобальной политике. // 2014. №4. Июль/Август. — URL: https://globalaffairs.ru/articles/nesovmestimye-czeli-ekonomicheskie-sankczii-i-vto/ (дата обращения: 16.05.2021).
4. Department of the Treasury, Office of Foreign Assets Control. 31 CFR Part 578. Cyber-Related Sanctions Regulations. — 2015. — URL: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities (дата обращения: 16.05.2021).
5. Issuance of Cyber-Related Sanctions Regulations to implement Executive Order 13694. // 2020. — URL: https://home.treasury.gov/system/files/126/fr80_81752.pdf (дата обращения: 16.05.2021).
6. Presidential Documents. Executive Order 13757. Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities. 2016. — URL: https://home.treasury.gov/system/files/126/cyber2_eo.pdf (дата обращения: 16.05.2021).

Н. А. Цветкова,
д-р ист. наук, профессор,
заведующая кафедрой американских исследований СПбГУ

ДИПЛОМАТИЯ ДАННЫХ США: РЕЗУЛЬТАТЫ РЕАЛИЗАЦИИ ЦИФРОВЫХ ПРИЕМУЩЕСТВ

Аннотация: в статье рассматриваются проекты США в области дипломатии данных. В настоящее время в США создан аппарат дипломатии данных и сформировались региональные подходы к использованию данного внешнеполитического инструмента. Используя анализ больших данных, автор оценивает эффективность проектов США на примере Афганистана, Сирии и Венесуэлы.

Ключевые слова: США, дипломатия данных, анализ больших данных, социальные сети, Сирия, Венесуэла, Афганистан.

Процессы в системе международных отношений, которые связаны с известным феноменом цифровизации, можно разделить на несколько типов. Во-первых, это возникновение новых инструментов дипломатии и внешней политики — цифровой дипломатии и дипломатии данных. Во-вторых, это появление в повестке международных политических дискуссий вопросов глобального управления интернетом и обеспечения его суверенизации. В-третьих, это распространение цифровых политических технологий, таких как цифровое голосование и др. В данной статье мы рассмотрим только одно из направлений цифровой внешней политики США, которое является самым актуальным на современном этапе — дипломатию данных.

Под дипломатией данных понимают использование аналитики больших данных для реализации внешнеполитических задач. Данный инструмент появился в арсенале внешней политики США в 2019–2021 гг. и уже имеет новый аппарат, ведомства, законодательную базу, региональные направления, что позволяет

нам сделать выводы о реализации так называемого цифрового преимущества США в области внешней политики.

Необходимо отметить, что дипломатия данных выросла из так называемой «цифровой дипломатии», которая развивалась администрацией Барака Обамы с 2010 г. Тогда цифровая дипломатия подразумевала использование социальных сетей как инструмента внешней политики или как части публичной дипломатии. Многие эксперты делали выводы о влиянии цифровой дипломатии на различные процессы в мировой политике, включая «арабскую весну», протестное движение в России, на пространстве СНГ и т.п. Сегодня цифровая дипломатия также активно развивается, но дипломаты все чаще используют «цифровые следы» пользователей сети интернет, а также преимущества феномена датафикации (*datalization*), который появился благодаря новому технологическому повороту.

Датафикация — это неконтролируемое распространение самых различных данных, фактов и информации и является основой для развития дипломатии данных. Отсутствие глобальных норм в использовании или рассекречивании цифровых следов создает возможности для использования самой разной информации в политических целях, а также в традиционной дипломатии. Известные кампании по рассекречиванию правительственных документов, переписки или личной жизни политиков (например, кампания против Хиллари Клинтон в августе 2016 г.) являются частью дипломатии данных, что вписывается в известную стратегию так называемых *disparage campaigns*[35].

Толчком для развития дипломатии данных США стал новый виток обострения в российско-американских отношениях, лоббирование политики необходимости информационного сдерживания России в странах Европейского Союза, а также внутрипо-

[35] Tsvetkova N. Russian Digital Diplomacy: A Rising Cyber Soft Power // Russia's Public Diplomacy: Evolution and Practice. Velikaya A. and Simons G. (Eds.). London, New York: Palgrave Macmillan, 2020, pp. 103–117.

литические проблемы, связанные с деятельностью администрации Д. Трампа. В 2018–2019 гг. аппарат публичной дипломатии и цифровой дипломатии было перестроен: ранее существующее ведомство под названием «Центр глобального взаимодействия» (Global Engagement Center), созданное в период администрации Барака Обамы для ведения информационного противостояния с экстремистской информацией ИГИЛ, полностью реорганизовал свою работу в сторону осуществления дипломатии данных. Были привлечены эксперты в области аналитики больших данных, искусственного интеллекта и пропаганды, которые сформировали основные структурные звенья для решения трех основных проблем в информационном сдерживании, связанных с Ираном, Россией и Китаем. Именно эти государства и их информационная политика обозначены как основное приложение дипломатии данных. Дипломатия данных США сдерживает информационные потоки, которые направлены из этих стран в другие целевые регионы. Российское направление подразумевает сдерживание реализации глобальных проектов России в цифровой сфере на Ближнем Востоке, Латинской Америке и Центральной Азии посредством взаимодействия с местной цифровой средой, а также посредством развития активной цифровой дипломатии и международного вещания США в странах этих регионов. Китайское направление подразумевает противодействие китайскому международному вещанию посредством создания эффективных контр-месседжей. Иранское направление подразумевает активное препятствование распространению пропаганды правительства Ирана как внутри страны, так и за ее пределами[36].

Более того, в Центре глобального взаимодействия были созданы уникальные по-своему функциональному предназначению отделы: отдел сбора данных (Data Collection), сотрудники

[36] Цветкова Н. А., Федорова И. В. Дипломатия данных США: цели, механизм, содержание. США и Канада: экономика, политика, культура, 51(1). С. 104–116.

которого занимаются получением данных из социальных сетей; отдел аналитики (Analytics and Research) — выявление ключевых блогеров и нарративов; отдел сотрудничества в области технологий (Technology Engagement) — обеспечение партнеров в зарубежных странах технологическими новинками (TechCamps); отдел контента (Content Team) — создание месседжей и антимесседжей; наконец, «отдел кадров» (Resources Team) — поиск нужных специалистов и блогеров в зарубежных странах.

По состоянию на 2021 г. данное ведомство является самым эффективным с точки зрения планов реализации цифровой дипломатии и дипломатии данных США, поскольку является основным центром сбора информации и соединяет в себе потребности традиционной дипломатии с возможностями цифровых технологий. Центр превращается в своеобразный пул взаимодействия между традиционными дипломатами и экспертами в области социальных сетей и больших данных. Аналитики больших данных не только формируют карту целевой аудитории в зарубежных странах для посольств и дипломатов США, но и пишут эффективные твиты, посты или ответы на комментарии пользователей в социальных сетях, что сокращает объем работы для дипломатов[37].

Чтобы посмотреть на первые результаты реализации дипломатии данных правительством США в «поле», были рассмотрено несколько государств, в которых просматривается деятельность США по данному направлению: Афганистан, Сирия, Венесуэла. Основные задачи исследования были связаны с выявлением активности США в местных социальных сетях, пониманием политических задач и определением эффективности цифровой дипломатии США. Методом исследования выступала аналитика больших данных. В самом кратком изложении — мы использовали

[37] Venezuela in U.S. Public Diplomacy, 1950s–2000s: the Cold War, Democratization, and the Digitalization of Politics / Tsvetkova N., Kheifets V., Sytnik A., Tsvetkov, I. // Cogent Social Sciences, 5(1), 2019. P. 1–15.

все посты и твиты относительно определенного хэштега и определенной геолокации. Многочисленные посты и твиты официальных аккаунтов правительства США были извлечены из баз при помощи специальной компьютерной программы и последующей машинной обработки твитов, постов, комментариев и т.д.[38].

Анализ постов институциональных аккаунтов США в социальных сетях Афганистана, например, показал, что активные пользователи позитивно реагируют на американские посты, которые связаны с проблемой развития и восстановления Афганистана, а также с проведением экономических реформ. Однако число пользователей в данной стране остается небольшим: лишь около 9–10 % населения используют интернет, что снижает эффективность цифровой дипломатии США. Более того, на эффективность действий США в афганском сегменте интернета оказывает влияние активная информационная политика местных групп талибов и внешних игроков. Как только «цифровые дипломаты» США, но каким-то причинам перестают создавать контент в социальных сетях или международное вещание США в Афганистане не распространяет привлекательных лозунгов, информационный вакуум быстро заполняется информацией, идущей от группы экстремистов, медиаджихадистов и т.п. Наконец, афганское интернет-пространство является конкурентным полем для цифровых дипломатов Великобритании, России и Китая. На современном этапе США не являются лидером информационного противоборства в Афганистане[39].

Цифровая дипломатия США в Сирийской Арабской Республике может служить еще одним примером ограниченности

[38] Цветкова Н. А. Феномен цифровой дипломатии в международных отношениях и методология его изучения // Вестник РГГУ. Серия: Политология. История. Международные отношения, 2, 2020. С. 37–47.

[39] Цветкова Н. А., Сытник А. Н. Публичная дипломатия в Афганистане, 2002–2018 гг.: влияние США на социальные сети, политическую систему и университеты // Вестник Санкт-Петербургского университета (Политология. Международные отношения), 11(4), 2018. С. 344–361.

влияния отдельной страны на интернет-пространство в зарубежном государстве. Мы ставили своей задачей выявить так называемых основных ифлюэнсеров в сирийском сегменте интернета и показать место и роль дипломатии данных США. Используя машинные методы получения больших данных из социальных сетей, мы сделали вывод, что ни США, ни Россия, ни страны Европейского Союза не оказывают такого существенного влияния на активных пользователей социальными сетями в Сирии как это делает Саудовская Аравия. Понятно, что данный региональный игрок преследует свои политические цели в Сирии, и, соответственно, содержание информации, поступающее от частных блогеров и официальных каналов международного вещания Саудовской Аравии значительно отличается от информации, которая поступают от ведущих игроков Европы, а также от США или России[40].

Наконец, пример Венесуэлы показывает еще одно интересное явление в области цифровой дипломатии. Политический кризис в Венесуэле активизировал информационную деятельность США в местных социальных сетях. До событий 2018–2019 гг., США активно поддерживали местные СМИ, блогеров, журналистов и, как известно, правительство Венесуэлы не препятствовало работе международного вещания США. Активная информационная политика США как в традиционном формате, так и в онлайне, должна была привести к завоеванию симпатий общественного мнения в Венесуэле. Однако наш анализ показал совершенно иную картину: огромное количество местных и цифровых СМИ самой разной политической окраски и активная цифровая политика действующего президента привели к вытеснению постов и твитов официальных аккаунтов публичной дипломатии США на вторые и третьи позиции в венесуэльском сегменте интернета. Присутствие США заметно в данном сег-

[40] Сытник А. Н. Информационное противоборство в Сирии // Азия и Африка сегодня. 2018. №2. С. 64–68.

менте, но не является ведущим. Первые роли играют местные СМИ и блогеры[41].

Заключая наш краткий обзор развития дипломатии данных США, можно сказать, что данный инструмент является эффективным только в случае постоянного плотного взаимодействия с местными блогерами и СМИ, которые готовы использовать американскую версию событий для распространения по своим каналам, а также при активном использовании искусственного интеллекта для создания убедительных месседжей и ответов на комментарии под постами в социальных сетях.

Список использованных источников и литературы

1. Сытник А. Н. Информационное противоборство в Сирии. Азия и Африка сегодня, 2, 2018. С. 64–68.
2. Цветкова Н. А. Феномен цифровой дипломатии в международных отношениях и методология его изучения. Вестник РГГУ. Серия: Политология. История. Международные отношения, 2, 2020. С. 37–47.
3. Цветкова Н. А., Сытник А. Н. Публичная дипломатия в Афганистане, 2002–2018 гг.: влияние США на социальные сети, политическую систему и университеты. Вестник Санкт-Петербургского университета (Политология. Международные отношения), 11 (4), 2018. С. 344–361.
4. Tsvetkova N. Russian Digital Diplomacy: A Rising Cyber Soft Power. Russia's Public Diplomacy: Evolution and Practice. Velikaya A. and Simons G. (Eds.). London, New York: Palgrave Macmillan, 2020, pp. 103–117.
5. Цветкова Н. А., Федорова И. В. Дипломатия данных США: цели, механизм, содержание. США и Канада: экономика, политика, культура, 51 (1). С. 104–116.
6. Tsvetkova N., Kheifets V., Sytnik A., Tsvetkov, I. Venezuela in U.S. Public Diplomacy, 1950s–2000s: the Cold War, Democratization, and the Digitalization of Politics. Cogent Social Sciences, 5 (1), 2019. P. 1–15.

[41] Venezuela in U.S. Public Diplomacy, 1950s–2000s: the Cold War, Democratization, and the Digitalization of Politics / Tsvetkova N., Kheifets V., Sytnik A., Tsvetkov, I. // Cogent Social Sciences, 5 (1), 2019. P. 1–15.

Р. В. Болгов,
канд. полит. наук, доцент кафедры мировой политики,
СПбГУ

ПРОБЛЕМА РАЗРЫВА В ЦИФРОВЫХ ПОТЕНЦИАЛАХ СТРАН НАТО

Аннотация: в статье рассмотрена проблема разрыва в цифровых потенциалах стран НАТО. Особое внимание уделено анализу того, насколько эффективно обеспечена совместность действий вооруженных сил НАТО с помощью информационных технологий. Также рассмотрены основные успехи и неудачи в сфере кибербезопасности на саммитах НАТО последних лет. Введены в научный оборот документы, регламентирующие вопросы кибербезопасности НАТО.

Ключевые слова: кибервойна, кибербезопасность, киберугроза, информационная война, цифровой разрыв, НАТО.

Сегодня не только отдельные страны, но и международные военно-политические блоки реализуют на практике концепции военного строительства с акцентом на информационные технологии. В частности, НАТО приравнивает готовность к кибервойне к противоракетной обороне и борьбе против терроризма. В соответствии с 5-й статьей Североатлантического пакта, атака на одного члена НАТО должна рассматриваться всеми членами альянса как нападение на всех. Применение данного принципа в отношении кибератак является сегодня основой политики кибербезопасности НАТО. Это должно повлечь за собой совместные действия, причём они включают в себя не только ответные кибератаки, но и возможность удара с помощью обычных вооружений. Особенно актуальным этот вопрос стал после принятия странами НАТО Стратегической концепции 1999 г., где предусматривалась возможность военных операций НАТО за пределами территории государств-членов альянса. Американский сенатор

Сьюзен Коллинз в 2010 г. заявила, что США рассматривают вопрос о приравнивании кибератаки к объявлению войны[42]. Пока что на практике этот принцип не был применён, однако само присутствие в политическом дискурсе таких рассуждений говорит о признании странами НАТО ключевой роли цифровой трансформации в военно-политической сфере, сопоставимой с ролью обычного и даже ядерного оружия. Но применение на практике данного принципа пока что затруднено слабой разработанностью международного права в области кибероружия.

Обеспечение совместности действий вооруженных сил НАТО с помощью ИКТ

Несмотря на актуальность вопросов кибербезопасности, основное внимание НАТО уделяет развитию ИКТ (информационно-коммуникационных технологий) для повышения возможностей обычных вооружений. И здесь ИКТ также не остаются в стороне, поскольку концепция совместности действий в рамках военной коалиции не может быть реализована без современных средств связи. Для обеспечения совместимости военных возможностей также требуется развитие оружия, основанного на информационных технологиях. Наконец, для борьбы с сетевыми структурами террористов, объявленной приоритетным направлением деятельности НАТО, необходимо развитие сетевых принципов организации и управления вооруженными силами в рамках альянса, что потребует внедрения ИКТ[43].

Серьезным препятствием реализации совместности действий в рамках НАТО является, как это ни странно, военно-технологическое лидерство США и связанное с ним значительное

[42] В Давосе обсудили вопросы кибербезопасности. Портал Security Lab, 01.02.2010. — URL: http://www.securitylab.ru/news/390311.php (дата обращения: 15.06.2021).

[43] Болгов Р. В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Дисс. канд. полит. наук. СПб., 2011.

отставание европейских членов НАТО от США. В связи с этим, в апреле 1999 г. на саммите НАТО в Вашингтоне была принята Инициатива об оборонном потенциале (ИОП), направленная на сокращение и в дальнейшем на устранение разрыва в военно-технической оснащенности вооруженных сил европейских стран-членов НАТО с США. ИОП предусматривала усиление военного потенциала европейских стран НАТО по пяти направлениям: мобильность войск, материально-техническое обеспечение, выживаемость, боеспособность, системы C4ISR[44]. Благодаря синергии вооруженных сил должна была быть увеличена не только согласованность вклада союзников в выполнение задач НАТО, но также должен возникнуть «эффект масштаба», т.е. общий эффект синергии действий должен был превысить эффект простой суммы потенциалов каждого отдельного партнера.

Однако данная инициатива показала недостаточную эффективность: в соответствии с выводами руководящей группы высокого уровня, созданной специально по данному вопросу, по 16 из 58 поставленных целей за трехлетний период работа почти не продвинулась. Основная причина — ограниченные военные бюджеты европейских членов НАТО. Необходимость противостояния негосударственным акторам с сетевой структурой, которая вышла на первый план после террористических атак 11 сентября 2001 г., также подтолкнула к разработке нового документа, который бы регламентировал развитие совместных действий вооруженных сил стран НАТО. Новая инициатива, принятая на саммите НАТО в ноябре 2002 г. (т.н. Пражское обязательство по потенциалу, ПРОП)[45], учитывает недостаточное

[44] Defence Capabilities Initiative. NATO Press Release NAC-S(99)69, 25 April 1999. — URL: http://www.nato.int/docu/pr/1999/p99s069e.htm (дата обращения: 15.06.2021).

[45] Prague Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002. — URL: https://cutt.ly/MmbbS1k (дата обращения: 15.06.2021).

по сравнению с США финансирование ВС европейских стран-членов НАТО. ПРОП ориентировано на небольшое количество сил и средств, которые играют решающую роль в выполнении всего спектра миссий НАТО. Одним из основных направлений обеспечения совместности названа разработка «совместимых средств связи в сопряженных системах командования, управления и информации, обеспечивающие эффективную связь во всех звеньях взаимодействующих воинских формирований разных стран»[46].

Однако отставание европейских стран-членов НАТО от США сохранялось, и дальнейшее развитие событий показало, что США в ходе военных операций в Афганистане и Ираке полагались на собственные силы, а не на совместные действия с союзниками по коалициям, многие из которых являются членами НАТО. Ряд экспертов полагает, что это было произошло именно из-за отсутствия у вооруженных сил европейских государств многих военных возможностей — высокоточных вооружений, БПЛА, приборов ночного видения, цифровых систем связи и т.д., необходимых для высокотехнологичных операций[47]. Также проблематичным было недостаточное взаимодействие внутри подразделений, состоящих из разных родов войск разных государств. Это дало корреспонденту ВВС Фрэнку Гарднеру повод сравнить совместные действия разных родов войск разных государств НАТО со строительством Вавилонской башни[48].

Стоит также отметить и неоднородную позицию внутри НАТО по вопросам кибербезопасности и информационно-

---

[46] Штоль В. Новые военные потенциалы НАТО. Обозреватель-Observer, 2003, № 10.

[47] Ek C. NATO's Prague Capabilities Commitment. CRS Report for Congress. Washington: Congress Research Service, 2007. — URL: http://www.fas.org/sgp/crs/row/RS21659.pdf (дата обращения: 15.06.2021).

[48] Gardner F. NATO's cyber defense warriors. BBC News, 3 February 2009. — URL: http://news.bbc.co.uk/2/hi/europe/7851292.stm (дата обращения: 15.06.2021).

технологической модернизации вооруженных сил. Так, европейские члены этой организации опасаются чрезмерного информационного превосходства США, и у них для этого есть повод в связи со скандалом, связанным с использованием США разведывательной сети «Эшелон» для несанкционированного сбора информации в странах НАТО. Позиция по этому вопросу также неоднородна в системе принятия решений в США. Позиция Президента, а также спецслужб и Госдепартамента состоит в том, что они выступают против спешки в данном вопросе, говоря о том, что вопрос международно-правового регулирования военно-политических аспектов информационной безопасности пока не приобрёл достаточной актуальности, считая необходимым сначала накопить достаточный практический опыт регулирования подобных проблем. Однако в интересах Министерства обороны — скорейшее приравнивание информационного противоборства к вооруженному конфликту и распространение норм права вооружённых конфликтов на кибервойны. Пока что большая часть полномочий в данном вопросе принадлежит спецслужбам, и в их интересах сохранение текущей ситуации, поскольку в случае признания информационного противоборства в качестве вооружённого конфликта значительная часть полномочий перейдёт к Министерству обороны.

Успехи и неудачи в сфере кибербезопасности на саммитах последних лет

Следует признать, что за последнее десятилетие был достигнут определенный прогресс. Так, между странами НАТО было налажено сотрудничество в плане объединения усилий в области производства высокоточного оружия. В частности, Нидерланды обладают технологиями преобразования обычных вооружений в высокоточное оружие. Германия управляет консорциумом, производящим коммуникационное оборудование для стратегических ВВС. Дания и Норвегия сосредоточились

на координации закупок вооружений для ВМФ[49]. Некоторые эксперты скептически относятся к этим инициативам, полагая, что наращивание военного потенциала в контексте войн с террористами и партизанами не имеет смысла, и данные инициативы служат в первую очередь интересам компаний-производителей информационно-технологичных вооружений[50].

В 2005 г. в документе NATO Defence Requirements Review было объявлено о начале реализации концепции «комплексных сетевых возможностей НАТО» (NATO Network Enabled Capabilities)[51]. В рамках этой концепции решаются вопросы синхронизации действий высокотехнологичных подразделений армий НАТО. Работа ведется по трем направлениям: внедрение современных систем связи, разработка перспективных систем C4ISR, а также реформирование организационных структур управления вооруженными силами, переподготовку личного состава, реформу доктринальной базы[52].

В рамках проблематики высокотехнологичных вооружений, из последующих саммитов НАТО следует отметить саммиты в Стамбуле (2004), Риге (2006), Лиссабоне (2010) и Чикаго (2012), хотя ни в Стамбуле, ни в Риге не были приняты новые столь же широкие инициативы в рассматриваемой сфере, как в Вашингтоне и Праге. На саммите в Стамбуле лидеры стран-членов НАТО договорились о дальнейшей трансформации боевых возможностей. На саммите в Риге было принято Всеобъемлющее политическое руководство, которое, среди прочего, касается развития совместных возможностей проведения информационных

---

[49] Ek C. NATO's Prague Capabilities Commitment. CRS Report for Congress. Washington: Congress Research Service, 2007. — URL: http://www.fas.org/sgp/crs/row/RS21659.pdf (дата обращения: 15.06.2021).

[50] Там же.

[51] Mission Task Analysis for the NATO Defence Requirements Review. Prepared by S. Armstrong (QinetiQ Ltd, UK). 1 February 2005. — URL: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA438925 (дата обращения: 15.06.2021).

[52] Там же.

операций, защиты от кибератак и внедрения сетевых принципов в организацию и управление вооруженными силами[53]. Руководящая группа высокого уровня пришла к выводу, что 70% из 460 обязательств стран-членов были полностью выполнены[54].

В Стратегической концепции НАТО, принятой на саммите в Лиссабоне в ноябре 2010 г., говорится, что кибератаки стали более частыми, более организованными и представляют серьезную угрозу для жизнеобеспечивающей инфраструктуры. Члены НАТО обязались координировать свои действия в данной сфере через единый орган кибероборонy, который должен быть создан[55], но кем, когда и кто несет ответственность, не уточняется. Отсутствие конкретики еще раз говорит об отсутствии консенсуса по этой проблеме внутри НАТО (между США и европейскими членами организации).

На саммите в Ньюпорте (2014) подтверждена применимость статьи 5 Североатлантического договора к киберпространству. На следующем саммите в Варшаве (2016) киберпространство было признано пятым измерением поля боя наряду с сушей, водой, воздухом и космосом. Было принято Обязательство по кибероборонe на 2017–2019 гг. (первый цикл), целью которого было объединить киберсистемы стран-членов. Был создан Комитет по кибероборонe, который должен заниматься мониторингом исполнения Плана действий НАТО по кибероборонe. Кроме того, проводятся ежегодные учения «Кибер Коалиция»

---

[53] Comprehensive Political Guidance. Endorsed by NATO Heads of State and Government on 29 November 2006. — URL: https://cutt.ly/8mbbJGE (дата обращения: 15.06.2021).

[54] Ek C. NATO's Prague Capabilities Commitment. CRS Report for Congress. Washington: Congress Research Service, 2007. — URL: http://www.fas.org/sgp/crs/row/RS21659.pdf (дата обращения: 15.06.2021).

[55] Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation. Adopted by Heads of State and Government in Lisbon, 19 November 2010. — URL: https://cutt.ly/vmbbGFm (дата обращения: 15.06.2021).

(CyberCoalition) и «Сомкнутые щиты» (Locked Shields). 2017–2018 годы были ознаменованы отходом НАТО от пассивной защиты к активным действиям в киберпространстве: была высказана идея создания Центра кибероперaций.

В последние годы НАТО уделяет большое внимание взаимодействию со странами-партнерами альянса в сфере кибербезопасности[56]. Именно эта сфера призвана «протестировать» амбиции стран-кандидатов в НАТО и показать, насколько глубоко возможна интеграция военных систем. Так, с Финляндией заключено Рамочное соглашение по кибероборoне. Со Швецией взаимодействие ведется в рамках Центра кибероборoны, расположенного в Таллине. Кроме того, НАТО оказывает техническую и консультативную помощь Украине, Молдове, Грузии, Иордании в сфере кибербезопасности. Взаимодействие с ЕС ведется по линии NCIRC — EU CERT (Computer Emergency Response Team).

Наиболее ярко проблема цифрового разрыва внутри НАТО проявляется в сфере искусственного интеллекта. Так, президентство Д. Трампа было ознаменовано политикой изоляционизма, отказом финансировать европейских партнеров и обвинениями их в нежелании «догонять» США. В то же время расходы на цифровую трансформацию армий европейских стран-членов НАТО не растут в той степени, какую ждут от них США. В частности, сегодня в Европе программы развития искусственного интеллекта рассчитаны на 10 лет, но США нужен результат здесь и сейчас. Еще одна проблема: технологии третьих стран. Около трети стран-членов НАТО используют китайские технологии наблюдения с использованием искусственного интеллекта, то есть имеет место тенденция к одновременному развертыванию американских и китайских технологий. Ведутся дебаты об участии Китая в создании европейских сетей 5G. В то же время, внутри

[56] Bolgov R., Filatova O., Yag'ya V. The United Nations and Russian initiatives on international information security. Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018. Pp. 31–38.

США тоже нет единой позиции по этому вопросу: и государство, и бизнес, и научные центры имеют здесь свои интересы, и их подходы отличаются.

Таким образом, дальнейшее развитие совместных возможностей ВС и оснащение войск НАТО информационно-технологичными вооружениями зависит от того, как будут развиваться события в местах, где воюют коалиционные силы, состоящие в т.ч. из сил членов НАТО. Растущие боевые возможности НАТО потребуют от её членов выделения дополнительных средств, найти которые смогут далеко не все члены Североатлантического альянса, поэтому военно-технологический разрыв между США и остальными членами НАТО будет сохраняться.

Список использованных источников и литературы

1. Болгов Р. В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Дисс. канд. полит.наук. СПб, 2011.
2. В Давосе обсудили вопросы кибербезопасности. Портал Security Lab, 01.02.2010 — URL: http://www.securitylab.ru/news/390311.php (дата обращения: 15.06.2021).
3. Штоль В. Новые военные потенциалы НАТО. Обозреватель-Observer, 2003, №10.
4. Bolgov R., Filatova O., Yag'ya V. The United Nations and Russian initiatives on international information security. Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018. Pp. 31–38.
5. Comprehensive Political Guidance. Endorsed by NATO Heads of State and Government on 29 November 2006. — URL: https://cutt.ly/8mbbJGE (дата обращения: 15.06.2021).
6. Defence Capabilities Initiative. NATO Press Release NAC-S(99)69, 25 April 1999. — URL: http://www.nato.int/docu/pr/ 1999/p99s069e.htm (дата обращения: 15.06.2021).
7. Ek C. NATO's Prague Capabilities Commitment. CRS Report for Congress. Washington: Congress Research Service, 2007. — URL: http://www.fas.org/sgp/crs/row/RS21659.pdf (дата обращения: 15.06.2021).

8. Gardner F. NATO's cyber defense warriors. BBC News, 3 February 2009. — URL: http://news.bbc.co.uk/2/hi/europe/7851292.stm (дата обращения: 15.06.2021).
9. Mission Task Analysis for the NATO Defence Requirements Review. Prepared by S. Armstrong (QinetiQ Ltd, UK). 1 February 2005. — URL: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA438925 (дата обращения: 15.06.2021).
10. Prague Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002. — URL: https://cutt.ly/MmbbS1k (дата обращения: 15.06.2021).
11. Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation. Adopted by Heads of State and Government in Lisbon, 19 November 2010. — URL: https://cutt.ly/vmbbGFm (дата обращения: 15.06.2021).

СЕКЦИЯ 3

«ПРИМЕНИМОСТЬ НОРМ МЕЖДУНАРОДНОГО ПРАВА К ИНФОРМАЦИОННОМУ ПРОСТРАНСТВУ»

А. А. Стрельцов,
член Президиума НАМИБ,
ведущий научный сотрудник факультета вычислительной
математики и кибернетики МГУ имени М. В. Ломоносова

ПРИМЕНЕНИЕ МЕЖДУНАРОДНОГО ПРАВА К ИНФОРМАЦИОННОМУ ПРОСТРАНСТВУ

Аннотация: международное право является основой системы поддержания безопасности и мира в условиях формирования информационного общества. Применение международного права к отношениям в области использования информационно-коммуникационных технологий сталкивается в рядом трудностей. Актуальным направлением преодоления трудностей на современном этапе развития международных отношений может стать сотрудничество в вопросах практического применения правил ответственного поведения в среде информационно-коммуникационных технологий.

Ключевые слова: информационно-коммуникационные технологии, суверенитет, правовой режим безопасности, международные споры, сила и угроза силой, международное гуманитарное право, правила ответственного поведения государств в ИКТ-среде.

Международное право занимает центральное место в системе средств регулирования отношений между государствами, включая и отношения в информационно-коммуникационных технологий (ИКТ-среде). В докладах Группы правительственных экспертов по достижениям в области информатизации и коммуникаций в контексте международной безопасности (далее — ГПЭ) эксперты пришли к выводу, что «международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет существенно важное значение для поддержания

мира и стабильности и создания открытой, безопасной, мирной и доступной ИКТ — среды»[1].

По мнению членов ГПЭ, соблюдение государствами международного права, в частности обязанностей по Уставу ООН, является основой определения правомерных действий в области использования ИКТ, направленных на создание открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. При этом «суверенитет государств, международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях»[2].

В международном праве под территорией государства понимается совокупность физических сред, в пределах которых государство осуществляет суверенитет, т.е. применяет свое правовое верховенство и юрисдикцию[3]. Территория государства обычно имеет признанные другими государствами границы. Признание границ государства достигается посредством заключения соответствующих договоров с соседними государствами, а также официальных заявлений по данному вопросу уполномоченных органов других государств.

ИКТ-среда является пространством международных отношений. Понятие «ИКТ-среда» в политических документах Российской Федерации и США в целом достаточно близки. Так, в российской политической доктрине понятие «ИКТ-среда» является синонимом «информационная сфера». Данная сфера определяется как «совокупность автоматизированных систем и объектов, использующих ИКТ для выполнения прикладных задач, а также информационной инфраструктуры, объединяющей технические устройства, системы и сети, функционирование которых обеспечивается организациями, находящимися в различных юрисдик-

[1] Доклады ГПЭ ООН (2013, 2015), A/68/98*, A/70/174.

[2] Доклады ГПЭ ООН (2015), A/70/174.

[3] Международное публичное право / Под ред. К. А. Бекяшева. М.: Проспект, 1998.

циях, на основе частно-государственного партнерства»[4]. В политической доктрине США близким аналогом понятия «ИКТ-среда» является понятие «информационная среда», которая раскрывается как совокупность индивидов, организаций и систем сбора, обработки, распространения и использования информации[5].

С точки зрения физической природы протекающих процессов ИКТ-среда представляет собой «киберпространство», которое может рассматриваться как глобальная составляющая информационной сферы, включающая как взаимосвязанные сети инфраструктур информационных технологий (сеть Интернет, телекоммуникационные сети, компьютерные системы, процессоры и контроллеры и т.п.), а также расположенную в них информацию в форме «данные»[6].

Новизна ИКТ-среды как пространства международного сотрудничества, а также виртуальность процесса применения ИКТ, не позволили пока государствам выработать единое толкование норм и принципов международного права и вытекающих из них обязательств государств в ИКТ-среде.

Во-первых, основу инфраструктуры ИКТ-среды составляют сети связи и глобальная сеть Интернет. Способность ИКТ-среды содействовать международному сотрудничеству в области использования ИКТ для передачи и обработки информации зависит от коммерческих организаций, действующих в различных юрисдикциях. Эти организации являются собственниками и владельцами технических устройств сетей связи и сети Интернет, оказывают услуги связи, обработки и распространения информации, удаленного доступа к требуемым данным.

---

[4] Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г., № 646.

[5] US Department of Defense, DOD Dictionary of Military and Associated Terms (JP 1–02) (June 2019), and Strategy for Operations in the Information Environment, (June 2016).

[6] US Department of Defense, DOD Dictionary of Military and Associated Terms (JP 1–02) (June 2019).

Обработка и передача информации в сети Интернет осуществляется с использованием глобальной системы цифровых идентификаторов (доменных имен, цифровых адресов). Работоспособность системы адресации и навигации поддерживается некоммерческой организацией «Международная корпорация адресов и доменных имен (ICANN, США)».

С учетом того, что США не принимали на себя международных обязательств по обеспечению устойчивости функционирования сети Интернет, а корпорация ICANN не является субъектом международного права и, соответственно, не обладает международной правоспособностью, дееспособностью и деликтоспособностью, возможность применения публичного международного права для обеспечения устойчивости функционирования и безопасности использования устройств и систем ИКТ-среды оказывается весьма ограниченной.

Во-вторых, реализация ИКТ автоматизации обработки и передачи информации на вычислительных и коммуникационных устройствах имеет виртуальный характер. Это существенно затрудняет получение достоверных свидетельств о факте инцидента в ИКТ-среде и определение субъектов международного права, причастных к его возникновению, а также о масштабе негативных последствий инцидента. В то же время участие свидетелей и независимых экспертов является одним из условий возможности разрешения международных споров с применением мирных средств, рекомендованных Уставом ООН — «переговоров, обследования, посредничества, примирения, арбитража, судебного разбирательства»[7], и других средств. Показательно, что за все время возникновения международных споров по поводу инцидентов в ИКТ-среде эти средства ни разу не применялись.

В-третьих, в ИКТ-среде отсутствуют признанные международным сообществом границы зон ответственности государств, т.е. остаются неопределенными пространственные пределы их

[7] Устав ООН. Ст. 33.

суверенитета. Решение этой проблемы посредством «привязки» национальных сегментов ИКТ-среды к территории («юрисдикция государств над ИКТ-инфраструктурой на их территории»[8]) требует конкретизации, обеспечивающей получение юридически надежной информации об инцидентах в ИКТ-среде и о государствах, вовлеченных в эти инциденты.

Ввиду данных обстоятельств международное право пока не стало инструментом, способным на основе международного сотрудничества предотвращать использование ИКТ для нанесения ущерба правам и свободам человека и гражданина, законным интересам коммерческих и некоммерческих организаций в области информационной деятельности, а также деятельности государственных органов по обеспечению безопасности использования информационной инфраструктуры, которая является общественным благом глобального характера[9].

Имеющиеся разногласия по вопросам применения международного права препятствуют повышению эффективности международного сотрудничества в области безопасности и мира.

Политической основой применения международного права является соблюдение основных принципов Устава ООН[10].

К числу основных принципов международного права, регулирующих отношения в ИКТ-среде, по мнению членов ГПЭ (2015 г.), относятся[11] следующие.

---

[8] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и коммуникации в контексте международной безопасности. 24 июня 2013 г. A/69/98*, п. 20.

[9] Шерстюк В. П., Стрельцов А. А. Ключевые проблемы правового обеспечения международной информационной безопасности // Сборник докладов участников четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Москва, 7–9 декабря 2020 г.

[10] Декларация о принципах международного права от 24.10.1970. № 2625. 25 сессия Генеральной ассамблеи ООН.

[11] Доклад ГПЭ ООН (2015), A/70/174.

Принцип суверенного равенства в ИКТ-среде, который означает юридическое равенство государств между собой, право каждого государства пользоваться правами, присущими полному суверенитету.

Как отмечено в итоговом докладе ГПЭ (2015 г.), государства обладают юрисдикцией над ИКТ-инфраструктурой, расположенной на их территории. Государства должны выполнять международные обязательства в отношении международно противоправных деяний, приписываемых им в соответствии с международным правом.

Вместе с тем приписывание государствам международно правовой ответственности за противоправные деяния в ИКТ-среде должно носить обоснованный характер и не ограничиваться только предположениями о том, что такие деяния осуществляются с территории или с объектов ИКТ — инфраструктуры государства.

В ответ на международно-противоправные деяния государства имеют право принимать меры, соответствующие международному праву и признанные в Уставе.

Неотъемлемым суверенным правом государства в области обеспечения безопасности является право государства на индивидуальную и коллективную самооборону. Это правомочие относится к случаям вооруженного нападения на члена ООН и существует до тех пор, пока Совет Безопасности не примет мер, необходимых для поддержания международного мира и безопасности. Во всех случаях использования силы государства должны соблюдать принципы международного права, в том числе принципы гуманности, необходимости, пропорциональности и индивидуализации силовых действий.

Принцип мирного разрешения международных споров в ИКТ-среде заключается в обязанности государств разрешать свои международные споры мирными средствами таким образом, чтобы не подвергать угрозе международный мир, безопасность и справедливость.

Мирные средства разрешения международных споров представляют собой международно-правовые способы, приемы, методы урегулирования споров между государствами без применения вооруженных сил.

Мирные средства разрешения международных споров могут реализовываться в следующих формах:

— непосредственные переговоры (двусторонние, многосторонние или на международных конференциях);
— международная примирительная процедура (добрые услуги и посредничество; следственные или согласительные комиссии);
— международная арбитражная и судебная процедура (международный арбитраж; Международный суд ООН);
— разрешение споров в международных организациях. Выбор того или иного средства — это суверенная воля государства.

Государства должны разрешать международные споры на основе суверенного равенства и воздерживаться от любых действий, которые могут ухудшить положение настолько, что подвергнут угрозе поддержание международного мира и безопасности.

Принцип неприменения силы или угрозы силой в ИКТ-среде заключается в том, что государства воздерживаются в их международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо иным образом, несовместимым с Целями ООН[12]. Государства обязаны не побуждать, не поощрять и не оказывать содействие другим государствам в применении силы или угрозы силой, а также не должны использовать представителей для совершения международно противоправных деяний с использованием ИКТ и должны стремиться обеспечивать, чтобы их территория не использовалась негосударственными субъектами для совершения таких деяний.

[12] Устав ООН, ст. 2 п. 4.

Принцип уважения и защиты прав человека и основных свобод заключается в том, что государства и иные субъекты международного права должны уважать, в том числе в ИКТ-среде, права человека и основные свободы, включая свободу мысли, совести, религии и убеждения для всех без различия расы, пола, языка и религии, а также выполнять свои обязательства, как они установлены в международных декларациях и соглашениях в этой области.

Принцип невмешательства во внутренние дела в ИКТ-среде заключается в запрете государствам прямого или косвенного вмешательства по любым причинам во внутренние или внешние дела любого государства, в том числе и посредством использования ИКТ-среды.

Проявляя единство в понимании важности применения международного права к регулированию отношений в ИКТ-среде, члены международного сообщества существенно расходятся в представлениях о путях решения и этой задачи.

В этих условиях важным средством международного нормативного регулирования отношений в ИКТ-среде становятся добровольные, необязательные правила ответственного поведения государств.

Основными источниками правил являются рекомендации ГПЭ ООН (2015 г.), а также Резолюция 73-й сессии Генеральной Ассамблеи ООН, одобренная большинством участников обсуждения.

Правила ответственного поведения государств в ИКТ-среде являются новым инструментом регулирования международных отношений в рассматриваемой области. Создание правил позволяет, с одной стороны, удовлетворить объективную потребность международного сообщества в регулировании отношений между государствами по поводу использования ИКТ, а с другой — сохранить «свободу рук» в вопросах обеспечения национальной безопасности и безопасности информационной инфраструктуры.

С формальной точки зрения правила ответственного поведения государств в ИКТ-среде не являются ни правовыми нормами, ни нормами «мягкого права». Данные правила могут рассматриваться как средство привлечения дополнительного внимания международного сообщества к вопросам международного нормативного регулирования применения ИКТ. Опыт практического применения правил может помочь конкретизировать проблемы адаптации норм и принципов международного права и мер укрепления взаимного доверия в ИКТ-среде.

Обсуждение проблем формирования системы международной информационной безопасности на заседаниях сессий Генеральной Ассамблеи ООН, в ГПЭ ООН и Рабочей группе открытого состава[13] показывает единодушную поддержку международным сообществом применения правил ответственного поведения государств в ИКТ-среде.

Привлекательность правил как нового средства регулирования международных отношений в ИКТ-среде подтверждается и появлением новых инициатив, связанных с созданием дополнительных правил ответственного поведения государств в ИКТ-среде.

К их числу можно отнести предложения Глобальной комиссии по киберстабильности[14] и компании Майкрософт.

В международном сообществе сформировался консенсус в вопросе о необходимости проработки вопросов практического применения этих правил[15].

Практическое применение правил ответственного поведения государств предполагает их имплементацию в национальное законодательство. Для имплементации правил ответственно-

[13] Final Substantive report. Open-ended working group on developments in the field of information and telecommunications in the contest of international security. A/AC.290/2021/CR.P.2

[14] Advancing cyberstability. Global Commission on the Stability of Cyberspace. Final report. November 2019.

[15] Резолюция ГА ООН A/73/27 от 5 декабря 2018 г.

го поведения государств в ИКТ-среде представляется важным решение следующих вопросов[16].

а. Принятие государствами политического решения об имплементации правил в национальное законодательство, т.е. определение группы государств, готовых приступить к имплементации и принять определенный акт, закрепляющий политическое согласие в данном вопросе.
б. Выбор способа имплементации правил ответственного поведения государств в ИКТ-среде[17] (рецепция, трансформация, отсылка; инкорпорация).
в. Обеспечение согласованного толкования правил ответственного поведения государств в ИКТ-среде, обеспечивающего однообразное понимание их содержания и возможных процедур выполнения.
г. Формирование специального механизма мониторинга соблюдения правил ответственного поведения государств в ИКТ-среде и обсуждения спорных вопросов по поводу возможного нарушения правил.

В Российской Федерации, по существу, сформирована политическая и правовая основа для сотрудничества с другими государствами по вопросам имплементации правил ответственного поведения государств в ИКТ-среде.

После принятия согласованных политических решений по вопросам имплементации и накопления всеобщей практики применения эти правила могут трансформироваться в нормы «мягкого» или «твердого» международного права.

---

[16] Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды / Под ред. А. Стрельцова, Э. Тикк; Международный исследовательский консорциум. 2020. — URL: https://namib.online/ (дата обращения: 11.08.2021).

[17] Курносова Т. И. Понятие и способ имплементации норм международного права в национальное законодательство // Актуальные проблемы российского права. 2015. № 34. С. 203–209.

Список использованных источников и литературы

1. Декларация о принципах международного права от 24.10.1970. №2625. 25 сессия Генеральной ассамблеи ООН.
2. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и коммуникации в контексте международной безопасности. 24 июня 2013 г. A/69/98*, п. 20.
3. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г., № 646.
4. Курносова Т. И. Понятие и способ имплементации норм международного права в национальное законодательство // Актуальные проблемы российского права. 2015. № 34. С. 203–209.
5. Международное публичное право / Под ред. К. А. Бекяшева. М.: Проспект, 1998.
6. Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды / Под ред. А. Стрельцова, Э. Тикк; Международный исследовательский консорциум. 2020. — URL: https://namib.online/ (дата обращения: 11.08.2021).
7. Шерстюк В. П., Стрельцов А. А. Ключевые проблемы правового обеспечения международной информационной безопасности // Сборник докладов участников четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности. Москва, 7–9 декабря 2020 г.
8. Advancing cyberstability. Global Commission on the Stability of Cyberspace. Final report. November 2019.
9. Final Substantive report. Open-ended working group on developments in the field of information and telecommunications in the contest of international security. A/AC.290/2021/CR.P.2
10. US Department of Defense, DOD Dictionary of Military and Associated Terms (JP 1–02) (June 2019), and Strategy for Operations in the Information Environment, (June 2016).
11. US Department of Defense, DOD Dictionary of Military and Associated Terms (JP 1–02) (June 2019).

Т. А. Полякова,
д-р юрид. наук, профессор,
главный научный сотрудник, и.о. заведующего сектором
информационного права и международной информационной
безопасности Института государства и права РАН

ВЛИЯНИЕ ПАНДЕМИИ COVID-19 НА РАЗВИТИЕ СИСТЕМЫ ПРИНЦИПОВ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[18]

Аннотация: в статье рассматривается вопрос о влиянии на современном этапе пандемии covid-19 на развитие системы принципов обеспечения международной информационной безопасности в условиях цифровой трансформации. Проблема обеспечения международной безопасности информационной безопасности является одной из ключевых на повестке дня внутренней и внешней политики России на современном этапе развития государства, общества и международной политики в условиях мирового кризиса.

Ключевые слова: международная информационная безопасность, принципы, система, пандемия, инфодемия.

В условиях ускоряющихся процессов развития глобального информационного общества и перехода к цифровой цивилизации, характеризующихся не только трансформацией экономики (четвертой промышленной революции), возрастает международная политическая конфронтация, появляются новые риски, вызовы и угрозы в информационном пространстве.

Сегодня в эпоху активных процессов цифровой трансформации, мирового кризиса, связанного еще и с проблемами, об-

[18] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16012.

условленными мировой пандемией COVID-19, остро ощутимо их влияние и на систему права, как международного, так и национального. Очевидно, что внедрение в жизнь социума прорывных (сквозных) технологий, выполняющих роль своеобразного драйвера и динамика развития информационно-телекоммуникационной индустрии в мировой экономике влияет и на. благосостояние граждан и развитие России как демократического, федеративного, правового государства. При этом представляется особенно важным отметить, что в 2021 году, объявленным в России годом науки и технологий, на происходящие в мире процессы, связанные с развитием его научно-технологического потенциала, безусловно, влияет как на международном, так и национальном уровне возрастание новых рисков, вызовов и угроз информационной безопасности. В связи с этим в фокусе внимания находится определение и решение новых задач стратегического характера, направленных на укрепление системы международной информационной безопасности (далее — МИБ).

Знаковым событием стало утверждение Указом Президента РФ от 12 апреля 2021 г. № 213 новой редакции «Основ государственной политики Российской Федерации в области международной информационной безопасности», в которых одним из направлений реализации государственной политики в области МИБ определено содействие выработке с учетом специфики информационно-коммуникационных технологий новых принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве[19].

В этой связи особо важно отметить, ключевое значение новелл в Конституцию РФ (статьи 71 и 114) внесенных в 2020 г. в целях не только развития информационного общества и обеспечения информационной безопасности, а также напрямую связанных

[19] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Указом Президента РФ 12.04.2021 № 213 // Официальный сайт Совета безопасности РФ. URL: http://www.scrf.gov.ru (дата обращения: 21.05.2021).

с закреплением суверенитета государства и его территориальной целостности, как важнейших государственных задач, что напрямую связано с соблюдением ключевых принципов международного права, включая и информационную сферу.

Эти вопросы в настоящее время приобретают приоритетное значение, как правовое, так и политическое в условиях обострения противостояния и цивилизационного кризиса в мире для обеспечения стабильности. Для развития государственной политики в рассматриваемой сфере и развития системы МИБ особое значение имеет также новелла, включенная в ст. 79.1 Конституции РФ, где указывается, что: «Российская Федерация принимает меры по поддержанию и укреплению международного мира и безопасности, обеспечению мирного сосуществования государств и народов, недопущению вмешательства во внутренние дела государств»[20]. Внесенные в 2020 г. поправки в Конституцию РФ относят к ведению Российской Федерации обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных (ст. 71, пункт «м»). На обеспечение стабильности и устойчивого развития Российской Федерации, также направлены поправки, связанные с перераспределением отдельных полномочий между органами государственной власти и местного самоуправления, касающиеся формирования Президентом РФ Государственного Совета, а также Совета Безопасности Российской Федерации. Впервые также включены исходные положения обеспечения безопасности, использующиеся в непосредственной связи с безопасностью личности, общества и государства.

Тема обеспечения информационной безопасности как составляющей национальной безопасности, особенно в эпоху нового этапа информационной революции — «цифровой трансформа-

[20] Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 01.09.2020).

ции», занимает центральное место не только в стратегических документах, определяющих векторы государственной политики современного государства, но и отражается на развитии всей правовой системы, особенно это касается информационного права[21]. Такая цифровая трансформация, несомненно, повлияет и на изменение системы научных специальностей в праве. В краткосрочной, среднесрочной и долгосрочной перспективе прогнозируется дальнейшее нарастание вызовов, угроз и рисков в цифровой сфере, что подтверждается и особенно проявляется условиях пандемии COVID-19 в России и во всем мировом сообществе. Например, к ним сегодня можно отнести в эпоху короновирусной реальности «инфодемию», «кибердемию». Полагаем, что противодействие этим явлениям, учитывая их трансграничный характер, следует рассматривать как принципы обеспечения МИБ. Эти вопросы требуют межотраслевых исследований, включая и правовые[22].

В связи с этим Россия должна иметь необходимый научный потенциал, включая вопросы развития науки и образования, для формирования адекватной системы правового регулирования новых отношений, их институцинализации, статуса субъектов, современных подходов и моделей регулирования сквозных технологий, включая технологии искусственного интеллекта, робототехники[23].

[21] Полякова Т. А. Минбалеев А. В., Кроткова Н. В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75–87.

[22] Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / под общ. ред. д.ю.н., профессора Т. А. Поляковой. — Саратов: Амирит, 2020. — С. 229–231.

[23] Полякова Т. А. Роль России в формировании международной повестки правового обеспечения информационной безопасности в условиях больших вызовов. Третьи Бачиловские чтения. Цифровая трансформация:вызовы праву и векторы научных исследований: материалы Международной научно-практической конференции /отв. ред. Т. А. Полякова, А. В. Минбалеев. Москва: Проспект, 2020. — 312 с.

Информационная безопасность, являясь одной из ключевых составляющих национальной безопасности, представляет собой сложную, динамично развивающуюся систему, имеющую закономерные связи между ее элементами, процессами организации и самоорганизации, принципами функционирования и развития. Доктрина информационной безопасности (2016 г.) в связи с развитием конституционно-правовых основ, новыми вызовами и угрозами, требует научного, правового осмысления и выработки новых подходов, направленных на уточнение целей и задач, средств их реализации.

Переход к цифровой трансформации, ее возрастающее значение в государственном управлении, системе государственных услуг, в расширении пространства доверия, включая неурегулированность на законодательном уровне институтов идентификации и аутентификации, необходимость развития правового обеспечения критической информационной инфраструктуры, требует новых системных концептуальных подходов в целях защиты информационного пространства, а также защиты цифровых прав граждан, оборота цифровых данных, обеспечения неприкосновенности частной жизни, и защиты персональных данных граждан и т.д. Эти вопросы становятся приоритетными при формировании государственной политики.

По нашему мнению, в современных условиях особенно актуальными как в теоретическом, так и в практическом отношении, являются вопросы обеспечения национальной и международной информационной безопасности. Заслуживают внимания такие вопросы как соблюдение конституционных прав и свобод граждан, реализуемых в информационной сфере, деятельность общественных объединений в информационной сфере, направленная на насильственное изменение основ конституционного строя и нарушение целостности России, разжигание социальной, расовой, национальной и религиозной вражды, по распространению этих идей в средствах массовой информации.

Вместе с тем, отдельных исследований заслуживают вопросы, касающиеся отнесения к федеральному ведению информационных технологий и оборота цифровых данных. Безусловно, это положение является глубоким, требующим научных исследований и хорошо проработанных предложений по правовому регулированию. Принятие указанных поправок к Конституции РФ направлено на расширение функции государства при обеспечении информационной безопасности общества и личности. В этой связи положение статьи 71 коррелируется со статьей 24 Основного закона, в которой по сути ключевой является информационная безопасность личности, связанная со сбором, хранением, использованием и распространением информации о частной жизни гражданина и его персональных данных, а именно эти личные данные сегодня очень чувствительны и требуют усиления их правовой защиты.

Необходимо научное осмысление и обоснование развития использование различных моделей правового регулирования (саморегулирования, сорегулирования, гибридного регулирования), а также неправовых регуляторов (этических, технических, базовых принципов правового регулирования в информационной сфере). Среди них выделяются такие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации как неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без соответствующего согласия. Представляется, что требуют научного осмысления также правовые положения о Российской Федерации (государстве) как субъекте, обеспечивающем безопасность граждан и общества в целом при применении информационных технологий и обороте цифровых данных. Кроме того, в организационно-правовой системе обеспечения информационной безопасности в России расширяется роль соответствующих государственных органов в сфере надзора за оборотом персональных данных и обеспечения их защиты, правовой статус которых

должен быть закреплен в положениях государственных органов, обеспечивающих информационную безопасность личности, общества и государства. В целях развития конституционно-правовых основ в области информационной безопасности необходима новая концепция правового регулирования общественных отношений, обеспечивающих реализацию государственных мер в вопросах информационной безопасности личности и защиты граждан от современных цифровых угроз.

Новые конституциональные положения являются импульсом для доктринального развития системы правового регулирования обеспечения национальной системы информационной безопасности и совершенствования государственной политики в области международной информационной безопасности, международного сотрудничества в соответствии с новыми стратегическими задачами в этой сфере.

Эти вопросы относятся к правовому регулированию МИБ, представляющей собой такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства должно обеспечиваться поддержание международного мира, безопасности и стабильности. Система обеспечения МИБ в целях предотвращения или минимизации рассматриваемых угроз должна стать совокупностью международных и национальных институтов, регулирующих деятельность в глобальном информационном пространстве. На достижение этих целей направлена государственная политика России по предотвращению (урегулированию) межгосударственных конфликтов в глобальном информационном пространстве, а также учету национальных интересов России при формировании системы обеспечения МИБ[24].

[24] Полякова Т. А. Роль России в формировании международной повестки правового обеспечения информационной безопасности в условиях больших вызовов / Третьи Бачиловские чтения. Цифровая трансформация: вызовы праву и векторы научных исследований: материалы Между-

Для успешной реализации новых стратегических задач развития, как национальной информационной безопасности, так и системы МИБ сегодня необходимы не только фундаментальные междисциплинарные, правовые научные исследования, включая проблемы трансформации системы прав человека, принципов, но и, безусловно, продвижения российских инициатив в этой области в целях достижения консенсуса, а также возрастающей «морально-психологической мотивации востребованности научно-аналитической работы», как справедливо отмечает А. В. Зинченко[25]. Интеграция усилий должна быть направлена на комплексные научно-обоснованные исследования, связанные с обеспечением международной информационной безопасности.

Список использованных источников и литературы

1. Зинченко А. В. Архитектоника международной информационной безопасности. М.: Аспект-Пресс, 2021. — 160 с.
2. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения — 01.09.2020).
3. Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе:монография/ под общ.ред. д.ю.н., профессора Т. А. Поляковой. — Саратов: Амирит, 2020. — 254 с.
4. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Указом Президента РФ 12.04.2021 № 213 // Официальный сайт Совета безопасности РФ. URL: http://www.scrf.gov.ru (дата обращения: 21.05.2021).

народной научно-практической конференции; отв. ред. Т. А. Полякова, А. В. Минбалеев. Москва: Проспект, 2020. — С. 3–28.

[25] Зинченко А. В. Архитектоника международной информационной безопасности. М.: Аспект-Пресс, 2021. — С. 8.

5. Полякова Т. А. Минбалеев А. В., Кроткова Н.В Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75–87.
6. Полякова Т. А. Роль России в формировании международной повестки правового обеспечения информационной безопасности в условиях больших вызовов / Третьи Бачиловские чтения. Цифровая трансформация: вызовы праву и векторы научных исследований: материалы Международной научно-практической конференции; отв.ред. Т. А. Полякова, А. В. Минбалеев. Москва: Проспект, 2020. — 312 с.

А. К. Жарова,
д-р юрид. наук, доцент,
ст. науч. сотр., Институт государства и права РАН

СООТНОШЕНИЕ ТЕХНОЛОГИЧЕСКОГО И ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: обеспечение информационного суверенитета государства в эпоху развития цифрового пространства должно обеспечиваться взаимодействующей системой правовых и технических норм регулирования. В свою очередь государственная власть должна распространяться на контроль над распространением информации и используемыми информационными технологиями на своей территории, особенно прикладным программным обеспечением как основного технологического инструмента, предназначенного для выполнения различных задач пользователей — граждан государства.

Информационная безопасность — это этап обеспечения информационного суверенитета и требует первоочередного решения вопроса, касающегося технологической и программной безопасности информационных систем. В связи с этим необходимо разработать взаимодействующую нормативную систему, которая обяжет зарубежных разработчиков соблюдать российские стандарты информационной безопасности и требования законодательства об обеспечении информационной безопасности как составляющей технологического и информационного суверенитета.

Ключевые слова: информационная безопасность, информационный суверенитет, программное обеспечение, техническое регулирование.

Идея государственного суверенитета была сформулирована еще в XVI веке[26]. С развитием информационных технологий и вступлением мира в цифровую эпоху возник вопрос об обеспечении государственного суверенитета в цифровом пространстве — информационном суверенитете.

Понятие информационного суверенитета раскрывается в Указе Президента РФ «Об утверждении Концепции развития рынка ценных бумаг в Российской Федерации». Так, в соответствии с данным документом «обеспечение информационной безопасности России, включает обеспечение информационного суверенитета, то есть формирование и проведение политики исходя из интересов национальной безопасности России»[27]. Решением Совета глав правительств СНГ «О Стратегии обеспечения информационной безопасности государств — участников Содружества Независимых Государств» информационный суверенитет определен «как способность самостоятельно осуществлять функции государства в информационной сфере в целях соблюдения прав и свобод граждан, обеспечения национальной и коллективной безопасности»[28].

Таким образом, понимание информационного суверенитета только с позиции «государственной власти по контролю над распространением информации на своей территории»[29] явля-

[26] Дмитриева Г. К., Викторова Н. Н. Суверенитет государства в контексте привлечения иностранных инвестиций // Актуальные проблемы российского права. 2018. № 12. С. 26–38.

[27] Указ Президента РФ от 1 июля 1996 г. № 1008 «Об утверждении Концепции развития рынка ценных бумаг в Российской Федерации» // СЗ РФ 1996. № 28. Ст. 3356.

[28] Решение Совета глав правительств СНГ «О Стратегии обеспечения информационной безопасности государств — участников Содружества Независимых Государств» // Единый реестр правовых актов и других документов СНГ — URL: http://cis.minsk.by/ (дата обращения: 11.08.2021).

[29] Шахназаров Б. А. Территориальный принцип охраны интеллектуальной собственности и действие государственного суверенитета в цифровом пространстве // Lex russica. 2018. № 12. С. 132–144.

ется ограниченным, поскольку обеспечение информационного суверенитета включает одновременно обеспечение технологического суверенитета и цифрового суверенитета.

Анализ п. 8 Доктрины информационной безопасности Российской Федерации позволяет прийти к выводу, что в перечень национальных интересов нашего государства в информационной сфере включены обеспечение информационной безопасности человека и гражданина, государства и общества; обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, включая критическую информационную инфраструктуру Российской Федерации и единой сети электросвязи Российской Федерации; развитие отрасли информационных технологий и электронной промышленности; противодействие угрозам использования информационных технологий в деструктивных целях, а также защита суверенитета в информационном пространстве.

В целях обеспечения информационного суверенитета посредством обеспечения технологического суверенитета, с 2015 г. Российская Федерация взяла курс на импортозамещение информационных технологий. Вначале запрет касался допуска программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд[30]. В настоящее время импортозамещение информационных технологий коснулось всех отраслей экономики, общее количество нормативных правовых актов, направленных на импортозамещение данной области равно 49.

Технологический суверенитет может обеспечиваться созданием собственных технологических разработок, системы стандартов

[30] Постановление Правительства РФ от 16 ноября 2015 г. № 1236 (ред. от 30.03.2019) «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

информационной безопасности или принуждением зарубежных производителей соблюдать отечественные нормы технического регулирования, как это сделано в Китайской народной республике. Нельзя приуменьшать значимость системы норм технического регулирования и ориентации их на нормы технического регулирования, поскольку цифровое пространство функционирует на основе взаимодействующих информационных технологий их механизмов организации, управления и использования.

Импортозамещение, как один из этапов обеспечения технологического суверенитета требует создание разработанной и взаимодействующей системы нормативного (правового и технического) регулирования информационной безопасности.

Переход на отечественные технологии будет очень долгим, дорогостоящим и сложным процессом в плане технологической реализации. Так, эксперты выделяют большое количество сложностей, например, разработка комплексных архитектур и решений для замещения экосистем корпоративного программного обеспечения, совместимость технологий[31] и др.

Таким образом, одномоментно осуществить переход на отечественные технологии невозможно, но в течение данного периода необходимо обеспечить безопасность российских граждан, использующих в своих отношениях зарубежные аппаратно-программные комплексы. В данных отношениях немаловажную роль играют нормы технического регулирования.

В пользу необходимости формирования взаимодействующей системы нормативного (правового и технического) регулирования информационной безопасности, говорит и тот факт, что зарубежные производители программного обеспечения в соответствии с нашим законодательством не обязаны соблюдать российские стандарты.

---

[31] Главные проблемы и препятствия импортозамещения ИТ в России. — URL: https://www.tadviser.ru/index.php/%D0%A1%D1% (дата обращения: 11.08.2021).

Так, в соответствии с ч. 8. ст. 14 ФЗ «Об информации, информационных технологиях и о защите информации»[32] «технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании».

Однако сфера действия ФЗ «О техническом регулировании»[33] не распространяется на «… стандарты распространения, предоставления или раскрытия информации…». Кроме того, ФЗ «О техническом регулировании» не регулирует отношения, «связанные с разработкой, принятием, применением и исполнением … требований к безопасному использованию атомной энергии, в том числе требований безопасности объектов использования атомной энергии, требований безопасности деятельности в области использования атомной энергии, требований к осуществлению деятельности в области промышленной безопасности, безопасности технологических процессов на опасных производственных объектах, требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики, требований к обеспечению безопасности космической деятельности….».

Таким образом, можно отметить, что ни бытовые информационные технологии, ни критические информационные инфраструктуры не защищены требованиями законодательства от ошибок и закладок, заложенных в них.

Соответственно возникают предпосылки внедрения «закладок» в информационные технологии иностранного производства и их реализации в Российской Федерации, что в свою очередь может оказать деструктивное воздействие на функ-

[32] СЗ РФ 2006. № 31 (ч. 1). Ст. 3448.

[33] СЗ РФ 2002. № 52 (ч. 1). Ст. 5140.

ционирование российской информационной инфраструктуры. Например, приложения Google для операционной системы Android[34] контролируют своих пользователей и разработчики признали данный факт.

Обеспечение информационной безопасности как этапа обеспечения информационного суверенитета требует первоочередного решения вопроса, касающегося технологической и программной безопасности информационных систем, в том числе и критически важных объектов.[35]

Таким образом, разработка взаимодействующей системы норм правового и технического регулирования является решением обеспечения технологического суверенитета как составляющей обеспечения информационного государственного суверенитета. Внедрение отечественных технологических разработок, создание взаимодействующей системы нормативного регулирования информационной безопасности, а также целостности, доступности и устойчивого функционирования информационных инфраструктур позволит Российской Федерации обеспечить информационный суверенитет, в том числе и контроль над информационными потоками в цифровом пространстве Российской Федерации.

Список использованных источников и литературы

1. Дмитриева Г. К., Викторова Н. Н. Суверенитет государства в контексте привлечения иностранных инвестиций // Актуальные проблемы российского права. 2018. № 12. С. 26–38.
2. Решение Совета глав правительств СНГ «О Стратегии обеспечения информационной безопасности государств — участников Содружества Независимых Государств» // Единый реестр правовых актов и других документов СНГ — URL: http://cis.minsk.by/ (дата обращения: 11.08.2021).

[34] Программы Google вредоносны. — URL: https://www.gnu.org/proprietary/malware-google.ru.html (дата обращения: 11.08.2021).

[35] См.: Исаков В. Б., Сарьян В. К., Фокина А. А. Правовые аспекты внедрения интернета вещей // ИТ-Стандарт. 2015. № 4(5). С. 9–16.

3. Шахназаров Б. А. Территориальный принцип охраны интеллектуальной собственности и действие государственного суверенитета в цифровом пространстве // Lex russica. 2018. № 12. С. 132–144.
4. Главные проблемы и препятствия импортозамещения ИТ в России — URL: https://www.tadviser.ru/index.php/%D0%A1%D1% (дата обращения: 11.08.2021).
5. ФЗ «Об информации, информационных технологиях и о защите информации») // СЗ РФ 2006. № 31 (1 ч.). Ст. 3448.
6. ФЗ «О техническом регулировании» // СЗ РФ 2002. № 52 (ч. 1). Ст. 5140.
7. Программы Google вредоносны — URL: https://www.gnu.org/proprietary/malware-google.ru.html (дата обращения: 11.08.2021).
8. Исаков В. Б., Сарьян В. К., Фокина А. А. Правовые аспекты внедрения интернета вещей //ИТ-Стандарт. 2015. № 4(5). С. 9–16.
9. Указ Президента РФ от 1 июля 1996 г. № 1008 «Об утверждении Концепции развития рынка ценных бумаг в Российской Федерации» // СЗ РФ 1996. № 28. Ст. 3356.
10. Постановление Правительства РФ от 16 ноября 2015 г. № 1236 (ред. от 30.03.2019) «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

В. Н. Трофимов,
член Национальной ассоциации международной информационной безопасности, действительный член РАЕН

МЕЖДИСЦИПЛИНАРНЫЙ ПОДХОД К РЕГУЛИРОВАНИЮ ПОРЯДКА ИСПОЛЬЗОВАНИЯ КИБЕРПРОСТРАНСТВА

Аннотация: для установления стабильного порядка использования киберпространства представляется целесообразным использовать весь спектр доступных средств, а не только средства международного права (то есть применять междисциплинарный подход). При этом не всегда оправданно проводить линию на умиротворение оппонента и ограничиваться призывами к сотрудничеству и снижению напряженности. Такая линия подведения может оказаться контрпродуктивной. Междисциплинарный подход, учет силовых моделей поддержания порядка предполагают ясное доведение до другой стороны своих претензий на использование киберпространства.

Ключевые слова: киберпространство, междисциплинарный подход, международное право, политика силы, переговоры, санкции, кибератака.

Пока использование киберпространства лишь отчасти регулируется с помощью международного права. Существует Будапештская конвенция 2001 года, но она не носит универсального характера, в ней не участвуют Россия и Китай. Есть ряд региональных и двусторонних соглашений, в том числе, с участием РФ. В рамках ООН принято решение о разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, однако не исключено, что в ней не будут участвовать страны НАТО.

Таким образом, даже вопрос о пресечении использования киберпространства в преступных целях, в решении которого, казалось бы, заинтересованы все страны, до сих пор должным образом не урегулирован с помощью международно-правовых средств.

Каковы же перспективы в использовании киберпространства? Неужели, нет никакой надежды прийти к взаимоприемлемым согласованным правилам поведения, установить международный контроль, выработать универсальные ясно прописанные права и обязанности государств?

Если пытаться решать эту проблему только силами юристов-международников, то, действительно, перспективы вряд ли хорошие. Пока подобные усилия российских представителей в целом наталкивались на непонимание со стороны, например, США и их союзников. Как представляется, более перспективным является путь решения проблемы регулирования порядка использования киберпространства на междисциплинарной основе, используя не только возможности международного права, но и иные инструменты.

Другие страны, в частности США, используют киберпространство для ведения информационных войн, для вмешательства во внутренние дела других государств, для кибератак, в иных подобных целях. При этом широко используют двойные стандарты, обман. При этом они, видимо, исходят из того, что занимают доминирующее положение в киберпространстве, способны использовать его в собственных целях и при этом могут не допустить или ограничить такое его использование другими государствами. Соответственно, какие-либо международные соглашения, касающиеся глобальной сети, могут только ослабить их доминирующее положение.

Итак, возникло новое пространство (киберпространство), которое носит, в том числе, международный характер. При этом одни государства стремятся сохранить в нем доминирующее положение и одновременно пытаются сузить для других стран возможность использовать глобальную сеть. Средства, приме-

няемые при такой борьбе за киберпространство, подчас далеки от международно-правовых.

Надо полагать, что в условиях активной борьбы за киберпространство вряд ли легко добиться заключения международных соглашений, фиксирующих правила его использования. Наверное, единственное тут исключение, это противодействие киберпреступности и терроризму. Видимо, в таких условиях вряд ли оправданно ограничивать себя только международно-правовыми методами, надо использовать весь спектр доступных средств. Среди них выделим средства силового регулирования. В таком случае теоретически такой подход становится междисциплинарным, то есть и международно-правовым, и одновременно подчиняющимся теории использования силовых методов.

Вряд ли можно утверждать, что в мировой практике уже сформировалась какая-то единая теория применения силы, носящая универсальный характер. Однако видимо, можно все-таки попытаться выделить некоторые ее более или менее характерные особенности. В первую очередь речь идет о поддержании мирового порядка, в отличие от правопорядка. Такой порядок, то есть более или менее стабильное состояние, складывается в случае либо доминирования каких-то государств в определенном пространстве (в киберпространстве) в целом или в его части. Либо в случае, если в таком пространстве сложился более или менее устойчивый баланс сил. Если порядок сложился, стал устойчивым, можно рассчитывать, что в таком случае удастся зафиксировать правила поведения в виде международно-правовых норм.

А если порядок только складывается? Если идет непрерывная борьба и не прекращаются попытки поставить под вопрос объем влияния других сторон? Наверное, позволительно утверждать, что тут все происходит не совсем хаотично. Можно выделить определенную систему, позволяющую продвигаться к возникновению устойчивого порядка.

Общей характерной чертой такой системы является то, что участники борьбы за пространство все-таки в первую очередь

пытаются установить границы своего влияния с помощью минимальных усилий, не прибегая сразу к радикальным средствам, в том числе в виде применения силы. Возможно, тут даже складывается определенная иерархия действий.

Понятно, что там, где используются силовые методы, основным средством определить победителя является проба сил. Наверное, самая мирная проба сил происходит либо в форме переговоров, либо в форме обмена какими-то устными или письменными заявлениями. Из них каждая сторона пытается выяснить, насколько силен противник и насколько нужно считаться с его интересами? Или его следует еще подвинуть, сузить контролируемое им пространство? Например, США обвиняют Россию во вмешательстве во внутренние дела, во вмешательстве в процесс выборов президента. Конечно, такие обвинения носят устную форму. На них можно реагировать различными способами или даже игнорировать.

Допустим, в нашем конкретном примере США сочли, что реакция России не подтверждает ее претензий на право совершать определенные действия в киберпространстве. Тогда логично перейти к иной, более высокой степени пробы силы, уже с реальным, хотя пока и ограниченным применением силы. Например, речь идет о санкциях. Применяя санкции, США хотят убедиться, что Россия поняла, что не может безнаказанно вмешиваться во внутренние дела и больше никогда не будет это делать. То есть отступила и не претендует на использование киберпространства в таком виде.

Еще один этап применения пробы силы, это угроза применения силы. Например, США ясно заявляют, что могут осуществить кибератаку в отношении России, а также ее объектов или конкретных лиц. Это еще не применение силы, не сама кибератака. Но это, несомненно, угроза применения силы. На такие действия тоже возможны различные ответные действия.

Наконец, США осуществляют непосредственно кибератаку. Например, говорят, что точно проведут ее, но последствия ее бу-

дут заметны ограниченному кругу лиц. Иными словами, в этом случае идет речь все-таки об ограниченном применении силы. Тут не применяется сила в отношении объектов критической инфраструктуры.

Последняя стадия — применение силы в отношении объектов критической инфраструктуры. Например, удар по банковскому сектору, отключение российских банков от системы SWIFT. Итак, выше перечислены некоторые способы применить силу в киберпространстве, причем в определенной иерархии, по нарастанию степени применения силы. Пожалуй, на практике примерно так это и происходит. Важный вопрос: как именно надо реагировать на применение силы на каждом ее этапе? Какие методы реагирования приведут к стабилизации ситуации, к установлению порядка в использовании киберпространства? Какие методы позволят наиболее коротким путем достичь ситуации, когда порядок использования киберпространства можно зафиксировать в виде международного договора?

На практике нередко можно встретить подход, согласно которому лучше не разжигать страсти и не портить отношения с государством, которое пытается сузить чужие возможности использования киберпространства. То есть речь идет о сдержанной реакции, о попытке уговорить оппонента, что не следует превращать киберпространство в арену силовой борьбы.

Продуктивно ли такое увещевание? Оно имеет один существенный недостаток: не позволяет оппоненту убедиться, насколько силен противник. Призывы вести себя сдержанно могут оказаться контрпродуктивными. Соответствующее государство, применяя силу, хочет понять, в какой мере ему можно доминировать в киберпространстве, и насколько силен оппонент. Надо ли считаться с его интересами, а если считаться, то в какой мере? А ничем не подкрепленные призывы к миролюбию такой информации не несут.

А если ответить жестко? Например, заявить, что поскольку США сами вмешиваются во внутренние дела России, то и она будет вынуждена действовать симметрично, то есть вмешиваться во

внутренние дела США? Приведет ли это к ухудшению отношений с этой страной? Тут есть два варианта. Если американская сторона не сочтет, что такой ответ подтвержден реальной решимостью совершать соответствующие действия, то произойдет эскалация напряженности, ухудшение отношений. Неубедительный ответ побудит противника перейти к следующей стадии пробы силы, например, к санкционному давлению. Видимо, для того, чтобы избежать ухудшения отношений, надо найти форму ответить так, чтобы у противника не возникло сомнений в решимости дать ему отпор. Если такая форма будет найдена, скорее всего, никакого ухудшения отношений не произойдет. Другая сторона получит то, что хотела — ясность по вопросу соотношения сил. А это прямой путь к установлению согласия, а дальше и вовсе порядка использования какого-то сегмента киберпространства или способа использования киберпространства.

Похоже, это правило жесткого ответа будет действовать на всех этапах, когда противник проверяет потенциальные возможности оппонента на деле и постепенно повышает давление. То есть лучше не бояться испортить отношения, а отвечать предельно ясно, может быть, даже предельно жестко, причем, чем раньше, тем лучше. Ведь противнику важна скорее определенность, чем форма действий другой стороны, якобы, способная его «обидеть».

А если все-таки попытаться увещевать противника, на каждом следующем этапе эскалации пытаться призывать к миру, к взаимопониманию, к дружбе? Скорее всего, такая политика будет контрпродуктивна. Она будет вынуждать оппонента переходить к все более высокой степени применения силы, пока не возникнет ясность, какими реальными возможностями обладает другая сторона, чтобы отстоять свои интересы. При этом речь может идти не только о возможностях, но и о решимости претендовать на какую-то часть киберпространства или на способ его использования. Ничем не подкрепленные увещевания и призывы к миру приведут к ровно противоположному результату, к войне на более высоком уровне.

Надо отметить, что Россия после довольно продолжительного противостояния с США в киберпространстве, возможно, готова отойти от политики умиротворения, в том числе применительно к угрозе отключения российских банков от системы SWIFT. Не исключено, что Президент России, обращаясь к Федеральному Собранию и говоря о красной черте, имел в виду в том числе и это. Что означает такая «красная черта»? Будет ли Россия рассматривать действия по пересечению такой черты как casus belli? Вряд ли. Но в любом случае ссылка на «красную черту» является какой-то формой ответного применения силы, а если точнее, то угрозой применения силы, хотя и довольно неопределенной по содержанию. Возможно, в результате удастся убедить США в своей решимости дать отпор и удержать от подобных силовых действий в киберпространстве.

Влияет ли пандемия COVID-19 на процесс установления общеприемлемого порядка использования киберпространства, на обеспечение безопасности в информационной среде? Фундаментальные основы установления такого порядка вряд ли изменятся. Конечно, с одной стороны, пандемия ставит человечество перед вопросом объединения усилий для выживания. С другой стороны, можно ожидать и обострения борьбы за ресурсы и жизненное пространство, в том числе и в рамках киберпространства.

Итак, междисциплинарный подход к регулированию порядка использования киберпространства предполагает использование не только международно-правовых средств, но и иных средств, в том числе и силовых. Правильная реакция на силовые действия другой стороны, позволяющая ясно определить соотношение силы, будет быстрее вести к стабильности в киберпространстве, а в конечном итоге и к заключению соответствующих международных договоров.

Список использованных источников и литературы

1. Трофимов В. Н. Применимость международного права к киберпространству: иллюзия или необходимость? М.: Юстицинформ, 2021 — 182 с.
2. Послание Президента Федеральному Собранию. — URL: http://www.kremlin.ru/events/president/transcripts/messages/ 65418 (дата обращения: 14.04.2021).

Н. П. Ромашкина,
канд. полит. наук,
руководитель подразделения проблем
информационной безопасности
ЦМБ ИМЭМО РАН

ИКТ-УГРОЗЫ МЕЖДУНАРОДНОМУ МИРУ, БЕЗОПАСНОСТИ И СТАБИЛЬНОСТИ: ГРАНИЦЫ НЕОБХОДИМОГО И ВОЗМОЖНОГО ДЛЯ МЕЖДУНАРОДНО-ПРАВОВОГО СОТРУДНИЧЕСТВА

Аннотация: в статье проводится анализ современных угроз международному миру, безопасности и стабильности, исходящих из пространства информационно-коммуникационных технологий (ИКТ). Проблема международно-правового сотрудничества для предотвращения таких угроз является одной из ключевых во внутренней и внешней политике Российской Федерации. Статья содержит предложения международных мер, необходимых для обеспечения безопасности в ИКТ-среде, а также прогноз возможности их реализации.

Ключевые слова: информационно-коммуникационные технологии (ИКТ), кибернетическое оружие, информационная угроза, киберугроза, кибератака, критически важные объекты государственной инфраструктуры, вмешательство во внутренние дела суверенных государств, международная безопасность, стратегическая стабильность, международные отношения, международно-правовое сотрудничество.

Становление новой системы международной безопасности в XXI веке характеризуется ускоренным ростом угроз миру на планете, исходящих из цифрового пространства и связанных с вредоносным применением информационно-коммуникаци-

онных технологий (ИКТ)[36]. Наиболее опасными являются информационные угрозы (ИКТ-угрозы, кибернетические угрозы) международному миру, безопасности и стабильности, которые носят глобальный, стратегический характер. В общем виде их можно разделить на три большие группы:

— применение вредоносных ИКТ в военно-политических целях для осуществления враждебных действий и актов агрессии, и, в первую очередь, негативное влияние вредоносных ИКТ на уровень стратегической стабильности;
— деструктивное ИКТ-воздействие на элементы критически важных объектов государственной инфраструктуры;
— вмешательство во внутренние дела суверенного государства, снижение общественной стабильности, разжигание межэтнической и межнациональной розни посредством ИКТ.

В современных условиях, когда международные отношения по-прежнему строятся на принципах взаимного вооруженного сдерживания и привержены политике с позиции силы, информационные угрозы добавляют неопределенности и могут способствовать эскалации конфликтов, что снижает уровень стратегической стабильности. Использование ИКТ в качестве важного инструмента разрешения межгосударственных споров становится все более значимой проблемой в процессе обеспечения международной безопасности. Таким образом, использование ИКТ превращается в один из важнейших элементов военно-политического потенциала государств, дополняющий, а иногда и заменяющий традиционные политико-дипломатические средства и вооружения. В условиях параллельно развивающихся процессов разрушения режима контроля над вооружениями и ухудшения отношений «великих держав» значение военной мощи, цифровых технологий военного и двойного назначения

[36] Андрей Крутских: Без международного сотрудничества проблему конфронтации в интернете не решить. 6 июня, 2021. — URL: https://eer.ru/article/v-mire/u751/2021/06/06/4226 (дата обращения 06.06.2021).

как одного из ключевых факторов соперничества и противоборства увеличивается.

Наличие этих факторов требует поиска дополнительных механизмов международного управления. Однако, несмотря на то, что Россия еще с конца прошлого века выступает за создание международных инструментов контроля над ИКТ-вооружениями под эгидой ООН, они до сих пор отсутствуют. При этом вероятность осуществления соответствующих угроз возрастает.

Так, в настоящее время для большинства стран мира стратегическое значение имеет защищенность ИКТ-систем, которые стали важным фактором обеспечения суверенитета, обороноспособности и безопасности государства. При этом речь сегодня идет об угрозе ускоренного развития (гонки) информационных вооружений. Все больше государств обладают наступательным кибернетическим оружием (кибероружием). ИКТ, таким образом, могут спровоцировать развязывание межгосударственного военного конфликта, в первую очередь, из-за возможности несоразмерного использования методов реагирования на ИКТ-угрозы и атаки: пострадавшая сторона может применить в ответ реальное оружие[37].

Кроме того, конфликт может возникнуть по ошибке, так как в настоящее время отсутствует универсальная методология идентификации нарушителей, не выработаны критерии отнесения кибератак к вооруженному нападению, не сформированы универсальные принципы расследования инцидентов. Эта угроза усиливается с учетом решения НАТО о применении Статьи 5 Устава Альянса в ответ на кибернападения. Напомню, что Статья 5 предполагает возможность применения всех имею-

[37] Ромашкина Н. П., Марков А. С., Стефанович Д. В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А. В. Загорский, Н. П. Ромашкина. — М.: ИМЭМО РАН, 2020. — URL: https://www.imemo.ru/files/File/ru/publ/2020/2020-017.pdf (дата обращения 06.06.2021). С. 71.

щихся сил и средств НАТО в том числе, и ядерного оружия (ЯО), в ответ на нападение на одного из членов Альянса[38].

Таким образом, ситуация в области стратегической стабильности может оцениваться как кризисная. В условиях существующих дестабилизирующих факторов, а также ускоренного развития вредоносных ИКТ существующих механизмов международного управления в этой области недостаточно.

В контексте обеспечения стратегической стабильности особого внимания требует безопасность ракетно-ядерных вооружений. Все ядерные державы модернизируют их, стремясь внедрять новые компьютерные технологии. Все больше компонентов военной ядерной инфраструктуры — от боеголовок и средств их доставки до систем управления и наведения, систем связи, командования и контроля над ядерными силами — зависят от сложного программного обеспечения, что делает их потенциальными мишенями для ИКТ-атак[39].

Таким образом, защита стратегических вооружений, систем предупреждения о ракетном нападении (СПРН), противовоздушной (ПВО) и противоракетной обороны (ПРО), связи, командования и контроля над ЯО от вредоносных ИКТ являются актуальными глобальными проблемами современности. При этом в дополнение или вместо принципа сдерживания за счет неминуемого ответного удара, растет интерес к сдерживанию путем блокирования использования наступательных средств («блокирование пуска» — «left of launch») с помощью ИКТ[40].

Одной из важнейших существующих угроз стратегического

---

[38] The North Atlantic Treaty. Washington D.C. 4 April 1949. — URL: https://www. nato.int/cps/en/natolive/official_texts_17120.htm (дата обращения 06.06.2021).

[39] Ромашкина Н. П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. — 2019. — № 1(29). — С. 2–9.

[40] Left of Launch. March 16, 2015. — URL: https://missiledefenseadvocacy.org/alert/3132/ (дата обращения 10.05.2021).

характера является развитие новейших противоспутниковых средств на основе ИКТ, позволяющих уничтожать спутники, а также влиять на работу не только искусственных спутников Земли мирного, но также двойного и военного назначения, включая элементы СПРН. Такие средства могут повлиять на эффективность работы спутников в рамках систем Ведения боевых действий в едином информационном пространстве, которые активно совершенствуются в развитых в военном отношении государствах. Это одна из самых серьезных угроз стратегической стабильности на современном этапе. Напомню, что в июне 2018 года впервые была озвучена информация о кибервмешательстве в работу американского спутника военного назначения, когда, по утверждению компании Symantec, внедрение «закладки» в ПО СУ позволило изменить орбиту спутника и перехватить чувствительные данные[41].

Снижение уровня стратегической стабильности, в первую очередь, обусловлено влиянием вредоносных ИКТ на рост вероятности:

— ошибочного санкционированного пуска БР, а также предотвращения (блокирования) пуска;
— получения ложной информации от СПРН о запуске БР со стороны противника из-за растущей изощренности ИКТ-атак;
— повреждения или разрушения каналов коммуникаций, создания помех в системе управления, командования и контроля ВС;
— снижения уверенности военных, принимающих решения, в работоспособности систем и восприятия каких-то действий в качестве начального этапа перехода к условиям гарантированного взаимного уничтожения.

Таким образом, все государства мира без исключения не могут чувствовать себя неуязвимыми, когда речь идет не о гипо-

[41] Symantec зафиксировала кибератаку на компании-операторы спутников в США и Азии // ТАСС. 2018. 20 июня. — URL: https://tass.ru/mezhdunarodnaya-panorama/5306217 (дата обращения 10.07.2020).

тетической, а об абсолютно реальной возможности нанесения ущерба стратегическим ядерным вооружениям с использованием ИКТ. Но максимальная опасность существует для ядерных держав, и максимальная ответственность лежит также на них, и, в первую очередь, на США и России, как на обладателях самыми существенными ядерными потенциалами. Эта угроза является общей, существует взаимная уязвимость. Следовательно, договоренности по снижению этой угрозы необходимы.

Важнейшей особенностью современного этапа является рост возможностей по расширению международно-правового сотрудничества в этой области. Много лет эксперты высказывали уверенность в том, что заявления лидеров стран о готовности вести конструктивный диалог и подписывать соответствующие документы, регулирующие опасную деятельность в цифровой сфере, могут сыграть важную инициирующую роль, способную положить начало переговорному процессу[42]. Именно такие заявления прозвучали от Президента РФ В. В. Путина в последние годы на различных площадках, в частности, в 2021 году на заседаниях Коллегии ФСБ и МВД, в Послании Президента Федеральному Собранию в 2021 году и других. Так, на Заседании Совета Безопасности России 26 марта 2021 года Президент подчеркнул: «*Считаем необходимым заключить универсальные международно-правовые договорённости, направленные на предупреждение конфликтов и выстраивание взаимовыгодного партнёрства в мировом информационном пространстве, на его максимальное использование для устойчивого развития каждого государства, на создание благоприятных условий для научного поиска, для быстрого внедрения самых передовых технологических решений при предотвращении потенциальных рисков. Важно сообща разработать и согласовать универсальные и справедливые для*

[42] Ромашкина Н. П. Новые технологии: вызовы международной безопасности и стабильности // Безопасные информационные технологии: сборник трудов Десятой международной научно-технической конференции. — М.: МГТУ им. Н. Э. Баумана, 2019. — С. 329–334.

всех правила ответственного поведения государств в информационном пространстве с чёткими и внятными критериями допустимых и недопустимых действий и придать им юридически обязательный характер. То есть каждая страна должна эти правила неукоснительно выполнять»[43].

Одним из ключевых документов в этом ряду является «Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности» от 25 сентября 2020 года[44], где указано, что «одним из основных стратегических вызовов современности является риск возникновения масштабной конфронтации в цифровой сфере. Особая ответственность за её предотвращение лежит на ключевых игроках в сфере международной информационной безопасности (МИБ)». В заявлении обосновывается актуальность и необходимость одобрения со стороны США «комплексной программы практических мер по перезагрузке наших отношений в сфере использования информационно коммуникационных технологий (ИКТ)». Предложенные конкретные шаги четко указывают на параллели с опытом создания режимов контроля за традиционными и ядерными вооружениями[45]. «*Данные меры направлены на повышение уровня доверия между нашими государствами…, станут весомым вкладом в построение глобального мира в информационном пространстве. Обращаясь*

---

[43] Заседание Совета Безопасности. 26 марта 2021 года. — URL: http://www.kremlin.ru/events/president/news/65231 (дата обращения 27.03.2021).

[44] Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. 25 сентября 2020 года. URL: http://www.kremlin.ru/events/president/news/64086 (дата обращения 26.09.2020).

[45] Колесниченко Александр. Андрей Крутских: с кибербезопасностью все так же, как с ядерным оружием // Аргументы и факты. 25.05.2017. — URL: https://aif.ru/society/safety/andrey_krutskih_s_kiberbezopasnostyu_vse_tak_zhe_kak_s_yadernym_oruzhiem (дата обращения: 10.05.2021).

ко всем странам, включая США, предлагаю выйти на заключение глобальной договорённости о принятии политического обязательства государствами о ненанесении первыми удара с использованием ИКТ друг против друга». Важнейшим ответом на эти предложения и взаимную обеспокоенность стал тот факт, что проблемы ИКТ-угроз впервые обсуждалась в контексте обеспечения стратегической стабильности на встрече президентов России и США 16 июня 2021 года[46]. Дальнейшие перспективы реализации возможностей по решению этой проблемы во многом зависит от профессионализма экспертов и дипломатов, которые будут готовить и проводить консультации и переговоры.

Проблема деструктивного ИКТ-воздействия на элементы критически важных объектов государственной инфраструктуры (КИ) также уже является частью глобальной проблемы обеспечения государственной и международной безопасности. Нарушение работы или уничтожение КИ может оказать необратимое негативное воздействие на национальную и экономическую безопасность, здравоохранение, правопорядок и т.д. Даже если эти объекты не подключены к интернету напрямую, устройства автоматизированной системы управления технологическим процессом (АСУ ТП), используемые для дистанционного контроля по защищенным коммуникационным линиям, могут быть взломаны в результате атаки на другие объекты, где функционируют АСУ ТП. При этом показатель опасности для АСУ ТП в настоящее время оценивается специалистами как критический или высокий. Вредоносные программы разрабатываются в настоящее время во многих странах, однако 83% всех площадок, используемых для распространения «зловредов», расположены всего в 10 государствах. Лидером этого рейтинга

[46] Biden — Putin Summit in Geneva: What prospects for a more peaceful and secure cyberspace? 17 JUNE 2021. — URL: https://ict4peace.org/activities/biden-putin-summit-in-geneva-what-prospects-for-a-more-peaceful-and-secure-cyberspace/ (дата обращения: 18.06.2021).

являются США[47]. Целями таких «вредоносов» могут быть органы государственной власти, банки, спутниковые, нефтегазовые и транспортные системы, электро- и атомные станции, коммуникационные системы, порты, аэропорты, военные объекты, что может привести к страшным последствиям как на государственном, так и на глобальном уровне. Таким образом, подобные вредоносные программы представляют собой перспективное стратегическое оружие, а растущая сложность оборудования и ПО КИ ведет к росту вероятности ошибок и уязвимостей. Таким образом, масштабные кибернетические и киберкинетические воздействия на КИ, на государственных лидеров и на социум с применением «мягкой, умной силы» с ИКТ, включающей финансовую, организационную, техническую, информационную и идеологическую деятельность, может привести к снижению боеготовности и боеспособности армии и флота в условиях разрушенной КИ, даже без применения военной силы со стороны воздействующей стороны, и, как следствие, к разрушению государства, на которое такое воздействие оказывается. Наибольшее беспокойство вызывают угрозы военным объектам, как части КИ, и, в первую очередь, угрозы системе командования и управления ядерным оружием.

Исходя из статистики кибернападений на КИ ведущих стран мира, эта проблема является максимально актуальной. При этом все развитые в цифровом отношении государства являются уязвимыми. Следовательно, международно-правовое сотрудничество в этой области отвечает интересам многих стран мира.

В отношении угрозы вмешательства во внутренние дела суверенных государств сегодня уже нельзя усомниться в глобальных возможностях ИКТ по подрыву политической, экономической и социальной систем, по психологическому воздействию на на-

[47] Путин заявил, что больше всего кибератак в мире идет с территории США. 16 июня 2021. — URL: https://tass.ru/politika/11667495 (дата обращения 17.06.2021).

селение для дестабилизации государства и общества. Кроме того, в последнее время некоторые из главных субъектов влияния, в первую очередь, США, не стесняется открыто говорить о своих действиях с применением цифрового пространства, в частности, интернета, социальных сетей и т.д. для «продвижения демократии», что неоднократно приводило к снижению общественной стабильности, разжиганию межэтнической и межнациональной розни посредством ИКТ и смене лидеров государств и правительства. Таким образом, речь и в этом случае идет о разрушении государства даже без применения военной силы. Для России эти факты вмешательства, являются максимально серьезной угрозой, т.к. они происходят на территориях бывшего СССР и / или в зонах интересов России. При этом, судя по лавинообразному потоку обвинений и санкций в адрес России со стороны коллективного Запада, они также рассматривают угрозу вмешательства во внутренние дела с использованием ИКТ в качестве максимально серьезной.

Следовательно, и эта угроза является общей, существует взаимная уязвимость. Следовательно, договоренности по снижению этой угрозы необходимы. При ответе на вопрос, насколько они возможны, необходимо учитывать главную проблему, связанную с тем, что самыми продвинутыми и уже хорошо опробованными технологиями для вмешательства обладает одно государство в мире — США.

В таких условиях, когда обеспечение безопасной ИКТ-среды стало частью системы глобальной международной безопасности, целесообразно ставить вопрос о необходимости разработки российской Стратегии информационной безопасности. Это обосновано, в частности, тем, что стратегические документы, на юридической основе определяющие направления и перспективы развития государства (а ИКТ являются одной из важнейших характеристик развития), играют особую роль на современном этапе и создают правовой фундамент инновационного развития, определяя основы государственной политики.

Важнейшими характеристиками стратегии в отличие от всех других видов документов, в частности, являются:

1) целевой подход к разработке, основанный на определении важнейшей цели и задач по ее достижению;
2) системный подход к реализации, предусматривающий решение указанных задач и, соответственно, максимальный охват всех основных направлений;
3) комплекс конкретных согласованных и взаимосвязанных мероприятий, средств и ресурсов, обеспечивающих достижение результатов;
4) действия по единому поэтапному плану с четко обозначенными целевыми индикаторами и показателями на каждом из этапов;
5) мониторинг за ходом реализации стратегии и применение системы мер юридического контроля за достижением конечных и промежуточных результатов.

Стратегия информационной безопасности России сможет стать фундаментом развития информационной сферы в стране, обеспечивающим организационные, законодательные и экономические условия, а также гарантии безопасного эволюционного процесса. Документ призван сформулировать цель и задачи развития, обеспечить защиту от угроз и рисков в информационном пространстве. Важной частью стратегии, как правило, является также четко прописанная система мониторинга и мер юридического контроля за достижением конечных и промежуточных результатов. Такой документ может сыграть важную роль в создании концепции сдерживания агрессивных действий в условиях новой эры стратегического ИКТ-противоборства, заложить фундамент режима контроля над ИКТ-вооружениями, позволяющего избежать информационной войны с глобальными разрушительными последствиями.

Кроме того, для обеспечения более безопасного и стабильного мира в условиях всеобъемлющего влияния цифрового пространства целесообразны международные действия с участием России:

1) разработка и внедрение новых ИКТ России, совершенствование соответствующих специальных гражданских и военных структур для обеспечения глобального баланса сил и средств;
2) включение вопросов обеспечения информационной безопасности в обсуждения и переговоры по ядерным вооружениям и стратегической стабильности на двусторонней (РФ-США) и многосторонней основе с участием России;
3) разработка на международном военно-политическом уровне конкретных мер по укреплению доверия, в частности, обмен данными об информационных угрозах, практическое межгосударственное сотрудничество и др. на многосторонней основе, в первую очередь, между РФ и США с целью выхода на подписание документа о безопасности военной деятельности в информационном пространстве;
4) активизация работы в государствах — обладателях ЯО по более эффективной подготовке персонала и защите программно-аппаратных средств военной инфраструктуры от различных ИКТ-нападений (в частности: унификация; территориальное распределение; дублирование обработки данных; создание «воздушной прослойки», т.е. отсутствие пересечения внутренних сетей критически важных объектов с глобальной информационной сетью; узкая специализация программного обеспечения и др.) для обеспечения как национальной, так и международной безопасности;
5) для более эффективного решения последней задачи целесообразно активизировать усилия по созданию исследовательской программы по ИКТ-стабильности военной сферы экспертами из ядерных держав;
6) выработка и фиксация общего для РФ и США понимания опасности ИКТ-угроз для международной безопасности и стабильности, дальнейшая деятельность по привлечению к этому процессу всех ядерных держав;
7) выработка общих подходов к оценке вероятности непреднамеренных и преднамеренных ИКТ-атак на СЯС;

8) четкая фиксация всеми ядерными державами вероятного ответа в случае обнаружения ИКТ-атак на СЯС в целях обеспечения сдерживания в применении ИКТ-вооружений.

Эти меры могут заложить основу для создания политики сдерживания в цифровой среде так, как это было сделано в период биполярности в отношении ядерных вооружений, стать фундаментом для более широких двусторонних и многосторонних соглашений о контроле над вооружениями в так называемом информационно-ядерном пространстве в будущем. При этом работа по оценке ИКТ-угроз находится на одном из первых этапов, и логично полагать, что деятельность экспертного сообщества сегодня может быть исключительно полезной для структур, принимающих государственные решения.

Параллельно целесообразно работать над созданием режима контроля над ИКТ-вооружениями, который мог бы включать:

— запрет на ИКТ-атаки на конкретные объекты, в первую очередь, в военной сфере (заявления, обязательства, соглашения, договоры);
— ограничение и/или отказ от наступательных ИКТ-возможностей;
— меры контроля за распространением ИКТ-вооружений;
— международные нормы в отношении средств и методов предотвращения и устранения киберконфликтов;
— разработку конвенции о запрещении вредоносного использования ИКТ в сфере ЯО.

Список использованных источников и литературы

1. Крутских А. В. Без международного сотрудничества проблему конфронтации в интернете не решить. 6 июня, 2021. — URL: https://eer.ru/article/v-mire/u751/2021/06/06/4226 (дата обращения 06.06.2021).
2. Заседание Совета Безопасности. 26 марта 2021 года. — URL: http://www.kremlin.ru/events/president/news/65231 (дата обращения 27.03.2021).
3. Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области

международной информационной безопасности. 25 сентября 2020 года. URL: http://www.kremlin.ru/events/president/news/64086 (дата обращения 26.09.2020).

4. Колесниченко А., Крутских А. В. С кибербезопасностью все так же, как с ядерным оружием // Аргументы и факты. 25.05.2017. — URL: https://aif.ru/society/safety/andrey_krutskih_s_kiberbezopasnostyu_vse_tak_zhe_kak_s_yadernym_oruzhiem (дата обращения: 10.05.2021).
5. Путин заявил, что больше всего кибератак в мире идет с территории США. 16 июня 2021. — URL: https://tass.ru/politika/11667495 (дата обращения 17.06.2021).
6. Ромашкина Н. П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. — 2019. — № 1 (29).
7. Ромашкина Н. П. Новые технологии: вызовы международной безопасности и стабильности // Безопасные информационные технологии: сборник трудов Десятой международной научно-технической конференции. — М.: МГТУ им. Н. Э. Баумана, 2019. — С. 329–334.
8. Ромашкина Н. П., Марков А. С., Стефанович Д. В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А. В. Загорский, Н. П. Ромашкина. — М.: ИМЭМО РАН, 2020. — URL: https://www.imemo.ru/files/File/ru/publ/2020/2020-017.pdf (дата обращения 06.06.2021).
9. Biden — Putin Summit in Geneva: What prospects for a more peaceful and secure cyberspace? 17 JUNE 2021. — URL: https://ict4peace.org/activities/biden-putin-summit-in-geneva-what-prospects-for-a-more-peaceful-and-secure-cyberspace/ (дата обращения 18.06.2021).
10. Left of Launch. March 16, 2015. — URL: https://missiledefenseadvocacy.org/alert/3132/ (дата обращения 10.05.2021).
11. Symantec зафиксировала кибератаку на компании-операторы спутников в США и Азии // ТАСС. 2018. 20 июня. — URL: https://tass.ru/mezhdunarodnaya-panorama/5306217 (дата обращения 10.07.2020).
12. The North Atlantic Treaty. Washington D.C. 4 April 1949. — URL: https://www.nato.int/cps/en/natolive/official_texts_17120.htm (дата обращения: 06.06.2021).

Д. Д. Штодина,
аспирантка кафедры международного права
МГИМО МИД России

МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ СОТРУДНИЧЕСТВА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: в настоящей работе на основе анализа международно-правовых актов, регулирующих деятельность субъектов международного права в киберпространстве, рассматриваются проблемы обеспечения международной информационной безопасности.

Ключевые слова: международная информационная безопасность, киберпространство, информационно-коммуникационные технологии, киберпреступность, кибербезопасность, международно-правовое сотрудничество, кибершпионаж, кибератака.

В современном международном праве рассматриваются следующие проблемы, связанные с регулированием киберпространства: предел распространения суверенитета государства в киберпространстве и возможности его ограничения, ведение кибервойн, кибертерроризм, проблема кибершпионажа, применимость действующих норм международного права к ИКТ.

Автором будут рассмотрены основные правовые источники в области ИКТ, существующие на сегодняшний день, проанализированы их недостатки и обозначены нерешенные вопросы в области международно-правового регулирования современного регулирования МИБ.

Так, В. М. Шумилов и Л. М. Крайнюкова предлагают разграничить преступления в информационной сфере (направлены против киберпространства и киберинфрастуктуры) от пре-

ступлений, совершаемых с помощью киберсредств (орудия преступления)[48]. Сложность состоит также в определении термина «кибертерроризм» и его отличии от термина «информационный терроризм». Правоведы предлагают рассматривать первый термин в более узком смысле, тогда как второму термину предлагается дать расширительное толкование, но даже в таком случае невозможно точно определить состав преступления «информационный терроризм». В любом случае подобные преступления следует отнести к преступлениям международного характера.

Основной вопрос на сегодняшний день состоит в уточнении международно-правовых норм, регулирующих деятельность, поведение государств и их лиц в киберпространстве. В науке доминирующее мнение состоит в презумпции распространения норм международного права, и, прежде всего, Устава ООН на эту новую среду человеческой деятельности. Все же и при таком подходе к регулированию остается вопрос об уникальности киберпространства как нового объекта международного права и, соответственно, о специфических способах нормативного регулирования в нем деятельности государств. Киберпространству не знакомо определение в нем каких-либо границ, действия государственного суверенитета и распространения на него национальной юрисдикции. Поэтому не вполне ясным остается вопрос, например, о применимости определения агрессии, существующем в современном международном праве, о неприменении силы в этом пространстве, а если поставить проблему шире, то вообще встает вопрос о допустимости распространения обязательств государств по общему международному праву к киберпространству в порядке mutatis mutandis.

Следует отметить, что на сегодняшний день не существует конвенции, которая бы всесторонне регулировала международно-

[48] Шумилов В. М., Крайнюкова Л. С. Роль ООН в нормативном противодействии практике транснациональных преступлений террористического характера в информационной сфере // МЖМП. 2020. №4. С. 23–37.

правовой режим киберпространства. По мнению А. Г. Волеводза[49], сотрудничество в этой области носит, скорее, фрагментарный характер (на уровне региональных организаций и интеграционных объединений), что также не способствует созданию единообразного регулирования киберпространства. Другая проблема состоит в том, что многие термины в киберпространстве необходимо, как и ЕКПЧ, толковать на основе «эволюционного подхода», т.е. с учетом развития информационно-коммуникационных технологий. Немаловажным остается вопрос, касающийся суверенитета государства и его нарушения в случае возникновения кибератаки.

Устав ООН, нормы которого имеют и договорный, и обычноправовой характер, составляет стержень современного международного права[50]. На уровне lex specialis в сфере международной информационной безопасности (далее — МИБ) существует не так много обязательных к исполнению норм международного права.

В связи с тем, что прогрессивное регулирование киберпространства чаще всего осуществляется именно на региональном уровне, следует рассмотреть сотрудничество государств на этом уровне.

1. *Региональный уровень*

   Значимыми международно-правовыми источниками в этой сфере можно считать следующие документы:

- Конвенция о компьютерных преступлениях (Будапештская конвенция, 23.11.2001)[51]

---

[49] Волеводз А. Г. Международно-правовые основы международного сотрудничества в обнаружении, отслеживании, сохранении и изъятии компьютерной информации // Международное публичное и частное право. — 2001. — № 4. — С. 28–41.

[50] Данельян А. А., Гуляева Е. Е. Международно-правовые аспекты кибербезопасности // Московский журнал международного права. 2020; (1):44–53.

[51] Конвенция о компьютерных преступлениях от 23.11.2001 г. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081580 (дата обращения: 09.05.21).

Данный документ принят в рамках Совета Европы, что отражает его «региональный характер». Неевропейские государства также участвуют в Конвенции, например, Израиль, Колумбия, Марокко, Коста-Рика, Перу, Панама, Япония и т.д.[52] В Конвенции содержатся основные определения — «компьютерная система», «компьютерные данные», «поставщик услуг», «данные о потоках».

Определены составы преступных деяний (неправомерный перехват; воздействие на данные; воздействие на функционирование системы; противозаконное использование устройств и т.д.).

Конвенция выступает своеобразным «кодексом поведения»: каждая Сторона обязана принимать меры по уголовному преследованию в сфере МИБ в перечисленных в статьях составах деяний, преследованию по другим уголовным преступлениям, совершаемым с использованием компьютерной системы, сбору доказательств в электронной форме.

Для ряда государств Конвенция является основанием для выдачи преступника в связи с совершением перечисленных в ней деяний. Для РФ, однако, в Конституции РФ предусмотрен запрет выдачи собственных граждан (ст. 61): «…Гражданин Российской Федерации не может быть выслан за пределы Российской Федерации или выдан другому государству…».

Согласно Конвенции, Стороны оказывают на взаимной основе правовую помощь для проведения расследований. Значимой составляющей в расследовании по «электронным уголовным делам» выступает возможность получения заинтересованной Стороной внеплановой информации, которая может помочь запрашивающей Стороне провести внутреннее расследование (при этом не требуется направлять предварительный запрос запрашиваемой Стороне).

---

[52] Официальный сайт Совета Европы: URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cLkq4WBO (дата обращения: 09.05.21).

К настоящему времени данная Конвенция остается первым многосторонним международным договором о преступлениях, совершаемых в киберпространстве. Вместе с тем, в Конвенции не дано четкого определения такого ключевого термина как «кибератака».

Российская Федерация не подписала и не ратифицировала Будапештскую конвенцию 2001 г. По состоянию на 2020 г. общее число ратификаций Конвенции составило 65[53]. Российская сторона убеждена в том, что отдельные положения данной Конвенции могли бы нарушить суверенитет государства в части получения беспрепятственного доступа к компьютерным данным другого государства.

Е. А. Архипова, В. Н. Додонов[54] к числу иных узконаправленных документов Совета Европы по вопросу регулирования преступности в киберпространстве относят также Конвенцию об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма (16.05.2005), Конвенцию ООН против транснациональной организованной преступности (15.11.2000), Протокол против незаконного ввоза мигрантов по суше, морю и воздуху, дополняющий Конвенцию ООН против транснациональной организованной преступности (15.11.2000).

С каждым годом технологические возможности влияния на общество и государство увеличиваются, а со времени принятия последней универсальной конвенции прошло 19 лет. Российская Федерация выразила обеспокоенность в связи с принятием положений ст. 32 Будапештской Конвенции, т.к. право без согла-

[53] Официальный сайт Совета Европы. URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185 (дата обращения: 09.05.21).

[54] Е. А. Архипова, В. Н. Додонов. Международно-правовые проблемы сотрудничества при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации // МЖМП. — 2020. — № 2. — С. 77–87.

сия другой Стороны получать доступ к компьютерным данным может нарушить принцип уважения суверенитета государства.

- Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, 16.06.2009 г. (вступило в силу для РФ 2.06.2011 г.)[55].

В Соглашении термин «информационная преступность» определен следующим образом: «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях через квалификацию деяния как противоправного». (Приложение 1. Перечень основных понятий в области обеспечения международной информационной безопасности). В тексте документа нет детальной расшифровки понятийного аппарата.

В Соглашении представлены следующие угрозы в сфере МИБ: информационное оружие, информационная война, информационный терроризм, информационная преступность, использование доминирующего положения в киберпространстве, распространение информации, наносящей вред всем сферам жизни общества и государства, угрозы функционированию национальных и глобальных инфраструктур, имеющие природный или техногенный характер.

Стороны разработали Приложение №2 к данному Соглашению, где определили источники и признаки каждой из угроз.

На двустороннем уровне Российская Федерация также заключила ряд соглашений в сфере МИБ.

Так, 05.04.2019 Россия и Туркменистан подписали Соглашение о сотрудничестве в сфере МИБ. Глава МИД России С. В. Лавров подчеркнул: «…Это первый документ, регулирующий отно-

[55] Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 г. URL: http://docs.cntd.ru/document/902289626 (дата обращения: 09.05.21).

шения в сфере МИБ между Россией и странами Центральной Азии»[56].

09.09.2018 было заключено Соглашение между Правительством Российской Федерации и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности[57].

В ст. 1 данного соглашения содержится перечень основных угроз для МИБ, таких как использование технологий для осуществления актов, направленных на вмешательство в государственный суверенитет, нарушение территориальной целостности другого государства, нанесение экономического ущерба, терроризм, совершение преступлений в ИКТ и т.д. Координирующими Сторонами Соглашения были определены от России: Совет Безопасности РФ; от Вьетнама — Министерство общественной безопасности страны.

04.09.2017 подписано Соглашение между Правительством РФ и Правительством ЮАР о сотрудничестве в области международной информационной безопасности[58]. Данный документ позволяет координировать деятельность двух государств в рассматриваемой области, в т.ч. и с точки зрения их соответствующих правовых позиций в рамках ООН, БРИКС и Международного союза электросвязи.

---

[56] Официальный сайт новостной компании «МИР 24». URL: https://mir24.tv/news/16355700/rossiya-i-turkmenistan-podpisali-soglashenie-o-sotrudnichestve-po-informacionnoi-bezopasnosti (дата обращения: 09.05.2021).

[57] Соглашение между Правительством Российской Федерации и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности от 09.09.2018 г. URL: http://docs.cntd.ru/document/554398783 (дата обращения: 09.05.2021).

[58] Соглашение между Правительством РФ и Правительством ЮАР о сотрудничестве в области международной информационной безопасности от 04.09.2017 г. URL: https://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/2854430 (дата обращения: 09.05.2021).

10.07.2014 подписано Соглашение между Правительством РФ и Правительством Республики Куба о сотрудничестве в области обеспечения в области международной информационной безопасности[59]. В Приложении к Соглашению Стороны определили основные термины в области ИКТ.

25.12.2013 аналогичное Соглашение было подписано с Правительством Республики Беларусь, к которому также принято Приложение № 1 («Термины»). В Приложении № 2 к Соглашению приводится «Перечень основных угроз в области международной информационной безопасности, их источников и признаков».

Отметим, что в другом международном договоре РФ — Соглашении между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности 2009 г., также определены источники угроз и их признаки. В 2018 г. участниками ШОС было принято решение о мониторинге террористических киберугроз в рамках Совета региональной антитеррористической структуры (РАТС).

Можно также отметить региональное соглашение стран СНГ от 20.11.2013. Его полное название — Соглашение о сотрудничестве государств — участников СНГ в области обеспечения МИБ[60]. В ст. 2 документа «трансграничная передача информации» определена как «Передача информации оператором через государственные границы государств — участников СНГ органу власти, физическому или юридическому лицу государства».

---

[59] Соглашение между Правительством РФ и Правительством Республики Куба о сотрудничестве в области обеспечения в области международной информационной безопасности от 10.07.2014 г. URL: https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3339607 (дата обращения: 09.05.2021).

[60] Соглашение о сотрудничестве государств — участников СНГ в области обеспечения МИБ от 20.11.2013 г. URL: http://docs.cntd.ru/document/420278452 (дата обращения: 09.05.2021).

В 2001 г. было заключено Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями с сфере компьютерной информации (01.06.2001 г.)[61]. В данном документе были закреплены четыре состава уголовных преступлений в сфере ИКТ: 1) неправомерный доступ к охраняемой законом информации, 2) создание, использование, распространение вредоносных программ, 3) нарушение эксплуатационных правил работы с ЭВМ, 4) незаконное использование программ для ЭВМ и баз данных с нарушением авторских прав. Согласно мнению некоторых правоведов, к недостаткам данного источника можно отнести отсутствие четкого представления о природе подобных киберпреступлений, компетентных органах, уполномоченных рассматривать данные дела, нерешенность вопроса о суверенитете государства в этом пространстве.

Еще одним важным аспектом регулирования деятельности государств в киберсреде является проблема кибершпионажа. В 2013 г. при поддержке специалистов из НАТО и МККК было разработано Таллинское руководство по международному праву, применимому к кибервооружениям[62]. Расширенная версия была принята в 2017 г. Данное издание не имеет обязательной силы, но примечательно то, что впервые была дана попытка кодифицировать кибернормы в области международного гуманитарного права. Однако в Руководстве не была учтена «природа» киберсреды. Например, в документе предлагается разграничить кибершпиона и разведчика. Если первый, на основании действующих норм международного гуманитарного права, лишается во время вооруженного конфликта международного характера статуса военнопленного, т.к. скрывает свою принадлежность к вооруженным силам государства, то второй не скрывает свою принадлежность к вооруженным силам государства и может пользоваться стату-

[61] Соглашение о сотрудничестве государств — участников СНГ в борьбе с преступлениями с сфере компьютерной информации от 01.06.2001. URL: http://base.garant.ru/12123778/ (дата обращения: 09.05.2021).

[62] The Tallin Manual, 2017. URL: https://ccdcoe.org/research/tallinn-manual/ (дата обращения: 09.05.2021).

сом военнопленного. Проблема состоит в том, что разработчикам необходимо было учитывать анонимность пользователей сети, которая приводит к невозможности на практике отличить шпиона от разведчика[63]. Кибершпионаж описывается как « любой акт, совершенный тайно или под ложными предлогами (в процессе осуществления которого) используются кибернетические возможности для сбора (или попытки сбора) информации с намерением передать ее противной стороне». Отметим, что шпионаж стал явлением, характеризующем и немеждународные вооруженные конфликты, однако в Руководстве действия по шпионажу ограничены именно международными вооруженными конфликтами. В данном документе дается характеристика кибершпионажа, отличающего его от шпионажа в МГП — скорость получения информации, получение удаленного доступа к информации, отсутствие физического присутствия в государстве-жертве.

2. *Универсальный уровень*

Хотя информационная безопасность играет растущую роль в международной безопасности XXI века, в рамках ООН нет соответствующей универсальной конвенции и нет перспектив согласования таковой. Что касается многочисленных резолюций Генеральной Ассамблеи ООН, то они относятся к вспомогательным источникам международного права.

Вместе с тем по состоянию на 2021 г. существует ряд концепций Конвенций ООН по МИБ. Например, Концепция Конвенции об обеспечении международной информационной безопасности, разработанная в рамках ООН 22.09.2011 года[64]. В ст. 1 Конвенции дается ряд ссылок на особую роль международного права для обеспечения поддержания международного

[63] С. Ю. Гаркуша-Божко. Проблема кибершпионажа в международном гуманитарном праве // МЖМП. — 2021. — № 1. — С. 70–80.

[64] Концепция Конвенции об обеспечении международной информационной безопасности от 22.09.2011. URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 09.05.2021).

мира и безопасности в информационной среде. В ст. 3 предложено исключить применение Конвенции, если деяние носит сугубо внутригосударственный, а не международный характер.

Более поздняя концепция соответствующей Конвенции ООН (Конвенции безопасного функционирования и развития сети Интернет) была разработана 27.07.2017; в ней также были предложены определения МИБ.

Россия активно участвует в подготовке проектов Конвенций, направленных на борьбу с кибертерроризмом. Так, в 2011 г. в ООН был представлен проект документа, разработанный РФ, а именно «Конвенция об обеспечении международной информационной безопасности», а в 2017 г. был разработан проект «Конвенции ООН по безопасному интернету»[65].

РФ выступает за установление контроля над национальным сегментом интернета, что соответствует сложившейся практике т.н. «третьего этапа концепции суверенитета государств в киберпространстве», предполагающей подчинение ИКТ юрисдикции того государства, где они находятся[66].

Принято более двух десятков резолюций ГА ООН по данной проблематике.

Первая такая Резолюция ГА ООН — резолюция А/53/70 («Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности») была принята 04.12.1998[67].

---

[65] Концепция конвенции ООН по безопасному интернету от 2017 г. URL: https://docplayer.ru/57676899-Koncepciya-konvencii-oon-ili-koncepciya-bezopasnogo-funkcionirovaniya-i-razvitiya-seti-internet.html (дата обращения: 09.05.2021).

[66] Ефремов А. А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. — 2017. — № 1. — С. 201–215.

[67] Международная информационная безопасность: теория и практика. В трех томах. Том 2: учебник для вузов / Под общ. ред. А. В. Крутских. — М.: Аспект Пресс, 2019.

Резолюция ГА ООН A/73/27 («Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности») была принята 05.12.2018 года[68]. В соответствии с резолюцией, государства-члены ООН должны принимать во внимание рекомендации Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и информировать Генерального секретаря ООН о текущем состоянии информационной безопасности на своей территории. Важным положением резолюции стало формирование Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС).

12.12.2019 ГА ООН приняла резолюцию A/74/28 («Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности»). Документ призывает государства — члены ООН включить в повестку дня 75-й сессии ГА ООН пункт «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».Предусмотрено продолжение сотрудничества в обозначенной сфере.

12.12.2019 ГА ООН приняла резолюцию A/74/29 («Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»). Согласно документу, особо подчеркнуты возросшие риски наращивания военного потенциала в сфере ИКТ для военных целей; использования информационных технологий для создания и провоцирования конфликтов, использование таких технологий в преступных и террористических целях. Переговорный процесс для реагирования на такие риски должен быть запущен посредством РГОС.

В 2020 г. РГОС представит доклад Генеральной Ассамблее ООН. Соответствующие переговоры сфокусированы на вопросах соблюдения норм применимого международного права.

[68] Резолюция Генеральной Ассамблеи ООН A/73/27 от 5.12.2018 г. URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27 (дата обращения: 09.05.2021).

Основная проблема состоит в выявлении того, каков должен быть согласованный механизм деятельности в информационной среде, как решать вопрос о соответствии внутригосударственных норм об ИКТ применимыми нормами международного права. Для решения этих задач РГОС предлагает изначально вырабатывать т.н. «guidance notes» (рекомендации).

На 75-й сессии ГА ООН Генеральный Комитет ООН представил повестку заседания (первый доклад Генерального комитета от 16.09.2020 г. A/75/250[69]), где в п. 98 особо подчеркивалась необходимость развития в сфере информационных технологий и телекоммуникаций с целью обеспечения международной безопасности.

В повестке дня рассматривается влияние информационных потоков и технологий на распространение наркоторговли и терроризма (см. п. 111–113). В документе ООН дается также ссылка на роль информационно-коммуникационных технологий в целях устойчивого развития (резолюция ГА ООН 74/197[70]). В документе, принятом 19.12.2019 году[71], указывается на существующее в мире «неравенство» в сфере цифровых технологий и широкополосной связи между развитыми и развивающимися государствами и внутри этих стран. Согласно документу, в сфере ИКТ сохраняется и проблема гендерного неравенства среди пользователей ИКТ. Доля женщин, пользующихся интернетом, на 17 процентов ниже, чем доля мужского населения; в наименее развитых странах — на 43 процента ниже. В том же документе дается ссылка на резолюции ГА ООН от 13.12. 2019 г. A-B/74/92[72] по вопросам, касающимся информации, где говорится о роли информации «на службе человечества».

---

[69] Первый доклад Генерального комитета от 16.09.2020г. A/75/250. URL: https://www.un.org/en/ga/75/agenda/ (дата обращения: 09.05.2021).

[70] Резолюция Генеральной Ассамблеи ООН от 10.01.2020 г. URL: https://undocs.org/en/A/RES/74/197 (дата обращения: 09.05.2021).

[71] Там же.

[72] Резолюция Генеральной Ассамблеи ООН от 26.12.2019 г. URL: https://undocs.org/ru/A/RES/74/92a-b (дата обращения: 09.05.2021).

Генеральный секретарь ООН Антониу Гутерриш в 2018 г. выразил обеспокоенность тем, что до сих пор нет консенсуса относительно того, применяются ли положения Женевских конвенций 1949 г. по гуманитарному праву к ИКТ: «Episodes of cyber warfare between states already exist. What is worse is that there is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it»[73]. Также остается вопрос об обеспечении применения норм международного права к сфере ИКТ, хотя сегодня уже не вызывает сомнений необходимость в применении этих норм для обеспечения международной информационной безопасности.

В заключении необходимо отметить, что регулирование киберпространства на международно-правовом уровне оставляет желать лучшего. Основная проблема состоит в том, что сам термин «киберпространство» необходимо толковать «эволюционно», т.е. с учетом развития информационно-коммуникационных технологий. Особенностью киберпространства следует считать его распространение на практически все отрасли современного международного права — космическое право, воздушное право, морское право, гуманитарное право и т.д. Сложился отдельный режим эфемерного киберпространства, который требует регулирования со стороны первичных субъектов международного права — государств.

Затруднительным представляется сам процесс кодификации кибернорм, т.к. государства, как правило, сотрудничают фрагментарно и в достаточно узких сферах МИБ, например — в сфере обеспечения и гарантирования прав и свобод человека, обеспечении государственной тайны, хранении данных. Итогом правотворчества государств стало принятие большого количества норм, которые нередко противоречат друг другу и не заполняют «правовых лакун» в области регулирования и использования ИКТ.

---

[73] Geneva Internet Platform. URL: https://dig.watch/processes/un-gge (дата обращения: 09.05.2021).

Основным источником регулирования киберпространства по-прежнему остается Будапештская конвенция, однако она была принята в далеком 2001 г. и носит региональный характер. Вместе с тем, в данный момент сотрудничество государств наиболее плодотворно происходит именно на региональном уровне, что позволяет учитывать интересы государств-членов определенной региональной международной организации. На универсальном уровне достичь согласия государствам не удается в силу различия правовых позиций и взглядов, в частности, в вопросе о возможности ограничения государственного суверенитета в киберсреде и установлении контроля над национальным сегментом интернета. Все вышеизложенное не содействует выработки обязательных международно-правовых норм в области ИКТ, но ведет к принятию норм «мягкого права», которые не всегда могут заменить жесткое регулирование деятельности государств в ИКТ.

Безусловно, следует признать, что положения Устава ООН применимы и к киберсреде, но это пространство не может регулироваться без учета его качественных специфических характеристик — анонимности, отсутствия границ, свобода входа, эфемерности и т.д.

Список использованных источников и литературы

1. Архипова Е. А., Додонов В. Н. Международно-правовые проблемы сотрудничества при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации // МЖМП. — 2020. — №2. — С. 77–87.
2. Волеводз А. Г. Международно-правовые основы международного сотрудничества в обнаружении, отслеживании, сохранении и изъятии компьютерной информации // Международное публичное и частное право. — 2001. — №4. — С. 28–41.
3. Гаркуша-Божко С. Ю. Проблема кибершпионажа в международном гуманитарном праве // МЖМП. — 2021. — №1. — С. 70–80.

4. Данельян А. А., Гуляева Е. Е. Международно-правовые аспекты кибербезопасности // Московский журнал международного права. 2020;(1):44-53. URL: https://doi.org/10.24833/0869-0049-2020-1-44-53
5. Данельян А. А. Киберпространство и международное право // Международный правовой курьер. — 2019. — №4–5 (33–34). — С. 5–12.
6. Доктрина информационной безопасности Российской федерации: принята указом Президента РФ от 5.12.2016 г. URL: http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ (дата обращения: 09.05.2021).
7. Ефремов А. А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. — 2017. — №1. — С. 201–215.
8. Конвенция о компьютерных преступлениях от 23.11.2001 г. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081580 (дата обращения: 09.05.2021).
9. Концепция Конвенции об обеспечении международной информационной безопасности от 22.09.2011 г. URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения — 09.05.2021).
10. Концепция конвенции ООН по безопасному интернету от 2017 г. URL: https://docplayer.ru/57676899-Koncepciya-konvencii-oon-ili-koncepciya-bezopasnogo-funkcionirovaniya-i-razvitiya-seti-internet.html (дата обращения: 09.05.2021).
11. Международная информационная безопасность. Теория и практика. В трех томах. Том 1: учебник для вузов / Под общ. ред. А. В. Крутских. — М.: Аспект Пресс, 2019. — 384 с.
12. Официальный сайт новостной компании «МИР 24». URL: https://mir24.tv/news/16355700/rossiya-i-turkmenistan-podpisali-soglashenie-o-sotrudnichestve-po-informacionnoi-bezopasnosti (дата обращения: 09.05.2021).
13. Официальный сайт ООН. URL: https://www.un.org/counterterrorism/cybersecurity (дата обращения: 09.05.2021).
14. Официальный сайт Совета Европы. URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185 (дата обращения: 09.05.2021).

15. Официальный сайт Совета Европы: URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cLkq4WBO (дата обращения: 09.05.2021).
16. Резолюция Генеральной Ассамблеи ООН A/73/27 от 5.12.2018. URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27 (дата обращения: 09.05.2021).
17. Резолюция Генеральной Ассамблеи ООН от 10.01.2020. URL: https://undocs.org/en/A/RES/74/197 (дата обращения: 09.05.2021).
18. Резолюция Генеральной Ассамблеи ООН от 26.12.2019. URL: https://undocs.org/ru/A/RES/74/92a-b (дата обращения: 09.05.2021).
19. Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009. URL: http://docs.cntd.ru/document/902289626 (дата обращения: 09.05.2021).
20. Соглашение между Правительством Российской Федерации и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности от 09.09.2018. URL: http://docs.cntd.ru/document/554398783 (дата обращения: 09.05.2021).
21. Соглашение между Правительством РФ и Правительством Республики Куба о сотрудничестве в области обеспечения в области международной информационной безопасности от 10.07.2014 г. URL: https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3339607 (дата обращения: 09.05.2021).
22. Соглашение между Правительством РФ и Правительством ЮАР о сотрудничестве в области международной информационной безопасности от 04.09.2017. URL: https://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/2854430 (дата обращения: 09.05.2021).
23. Соглашение о сотрудничестве в борьбе с преступлениями в сфере информационных технологий от 28.09.2018. URL: https://www.cisatc.org/1289/135/152/9034 (дата обращения: 09.05.2021).
24. Соглашение о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. URL: http://base.garant.ru/12123778/ (дата обращения: 09.05.2021).

25. Шумилов В. М., Крайнюкова Л. С. Роль ООН в нормативном противодействии практике транснациональных преступлений террористического характера в информационной сфере // МЖМП. — 2020. — № 4. — С.23–37.
26. Geneva Internet Platform. URL: https://dig.watch/processes/un-gge (дата обращения: 09.05.2021).
27. Geneva Internet Platform. URL: https://dig.watch/processes/un-gge (дата обращения: 09.05.2021).
28. The Tallin Manual, 2017. URL: https://ccdcoe.org/research/tallinn-manual/ (дата обращения: 09.05.2021).

Ю. А. Юдина,
эксперт Центра международной
информационной безопасности
и научно-технологической политики МГИМО МИД России

ПРОБЛЕМА ОПРЕДЕЛЕНИЯ СТАТУСА ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: в статье рассматривается проблема определения статуса информационного пространства в контексте обеспечения международной информационной безопасности. Данная проблема сформирована несколькими ключевыми составляющими: недоговоренность по поводу понятийного аппарата в рассматриваемой сфере, а также расширение географии субъектов, влияющих на развитие и информационного пространства.

Ключевые слова: международная информационная безопасность, информационное пространство, правовой статус, информационно-коммуникационная операция.

В основе нерешенности вопроса об определении правового статуса информационного пространства в контексте МИБ лежит два важных аспекта: расхождение России и США в понимании и определении МИБ, в выработке универсального термина, а также в увеличении числа ключевых игроков в рассматриваемой области.

После распада СССР становление однополярного мира происходило на фоне начальной стадии экономической глобализации и общественной информатизации с сильным американским акцентом. Это обусловлено резким ростом мощи и влияния США, ставших единственной сверхдержавой. Неудивительно, что США выступают в качестве гегемона в международной информаци-

онной среде, активно культивируют политику силы, агрессивно продвигают свои идеи и навязывают свою волю остальным членам международного сообщества, с целью понижения их конкурентоспособности и мощи в сфере использования ИКТ.

Статус сверхдержавы США обрели, оседлав глобальную информационную революцию и став родиной современных информационных и коммуникационных технологий, в том числе интернета, которые сыграли роль драйвера общественного мнения.

Именно из США ИКТ начали распространяться по странам мира, став транснациональным феноменом. В самих же США появление этих технологий было обусловлено изначально нуждами Министерства обороны, которое, оценив военные перспективы информационной инновации, пошло навстречу гражданским потребностям и целям. Впоследствии технологии утратили исключительно военный статус, став коммерческим продуктом, а потому стало характерным усиление противостояния американского экспортного контроля и транснационального высокотехнологичного бизнеса. Именно бизнес самым активным образом вмешался в судьбу информационных и коммуникационных технологий. В связи с тем, что ИКТ стали глобальны по своей сути, они требуют глобального подхода[74].

В этой связи для обеспечения безопасности в информационном пространстве возникают межгосударственные альянсы. Их образование хоть и базируется на различных информационно-коммуникационных интересах, но имеет единую политическую цель.

В 2000 г. была принята Хартия глобального информационного общества. Авторы Хартии закрепили в ней основополагающие принципы функционирования и развития ГИО, в том числе равную доступность ИКТ всему населению планеты, а также сведение к минимуму цифрового разрыва.

---

[74] Окинавская хартия глобального информационного общества (Принята на о. Окинава 22.07.2000) // Дипломатический вестник. 2000. № 8. С. 51–56.

Документ умещает в себе и довольно амбициозные идеи. Так, Хартия призывает активно инвестировать в людей, осуществлять взаимовыгодное сотрудничество государственного и частного секторов, создавать синергию развивающихся и развитых стран, а равно и международного сообщества.

Для претворения в жизнь вышеперечисленных положений были проложены конкретные маршруты деятельности:

1) проведение экономических и структурных реформ в целях создания обстановки открытости, эффективности, конкуренции и использования нововведений, которые дополнялись бы мерами по адаптации на рынках труда, развитию людских ресурсов и обеспечению социального согласия;
2) рациональное управление макроэкономикой, способствующее более точному планированию со стороны деловых кругов и потребителей, и использование преимуществ новых информационных технологий;
3) разработка информационных сетей, обеспечивающих быстрый, безопасный и экономичный доступ с помощью конкурентных рыночных условий и соответствующих нововведений к сетевым технологиям, их обслуживанию и применению;
4) развитие людских ресурсов, способных отвечать требованиям века информации, посредством образования и пожизненного обучения и обслуживания растущих запросов на специалистов в области ИКТ во многих секторах экономики;
5) активное использование ИКТ в государственном секторе и содействие предоставлению в режиме реального времени услуг, необходимых для повышения уровня доступности власти для всех граждан.

Документ сформулировал «правила игры», безусловно, выгодные для высокотехнологичного бизнеса. Этот бизнес, как известно, процветает в развитых странах Запада; что лишний раз указывает на то, что Окинавская хартия принималась в условиях однополярного мироустройства и американского доминирования в глобальном информационном пространстве. Это обусловило

успешную адаптацию к процессам информатизации развитых стран, большинство из которых являются союзниками и партнерами США, в то время как очень многие из развивающихся стран, так и не смогли за десять лет преодолеть цифровой разрыв[75].

В 2002 г. в Марракеше (Марокко) прошла Полномочная конференция МСЭ, на которой были утверждены принципы построения глобального информационного общества. В их число вошли: укрепление международного сотрудничества и повышение безопасности информационных и телекоммуникационных сетей, содействие универсальному доступу к информации и знаниям по приемлемым расценкам, и, в первую очередь, обеспечение права доступа к ним. Накануне саммита состоялись региональные конференции с целью обсуждения глобального информационного общества. Таким образом, мировое сообщество весьма скрупулёзно подготовилось к Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО).

Встреча способствовала некоторому сближению основных игроков в цифровой сфере и позволила достичь некоторых позитивных сдвигов: так, развитые страны сохранили за собой право на охрану своей интеллектуальной собственности, а развивающиеся, в свою очередь, отстояли право на доступ к ИКТ.

Развитие информационного общества неизбежно столкнулось с возникновением ряда опасностей и угроз своему эффективному функционированию. В этой связи в международном сообществе в конце 90-х гг. прошлого столетия начались дискуссии на тему МИБ. Для всеобъемлющего и полного анализа МИБ и правовых механизмов ее регулирования и определения на основе такого анализа проблемы определения правового статуса информационного пространства, необходимо обратиться к рассмотрению понятийного аппарата МИБ, а также изучить позиции ведущих в данной направлении.

---

[75] Бирюков А. В. Современные международные научно-технологические отношения. — М.: РосНОУ, 2014. — С. 353.

Примечательно, что ни в международном сообществе, ни в среде научных деятелей до конца не сложилось единого мнения насчет ключевых понятий, относящихся к МИБ, что так же связано с противостоянием ключевых игроков на глобальной политической арене.

Первой попыткой дать определение основным понятиям в сфере МИБ стал один из ранних докладов Российской Федерации Генеральному секретарю ООН в области инновационных угроз, привнесенных внедрением цифровых технологий в ИКТ в современные международные отношения от 1999 года. Российская Федерация выделила пять ключевых понятий в области МИБ, среди которых особое место занимает «международная информационная безопасность»[76].

Обращает на себя внимание то, что используется термин «международная информационная безопасность», а не «кибербезопасность». Для этого существуют различные причины. «Кибербезопасность» сужает рассматриваемую область до технологической составляющей, исключая вопросы контента, в том числе пропаганду. По сути, информационная безопасность и кибербезопасность соотносятся как общее с частным, хотя мнения исследователей в данном вопросе могут расходиться.

Свое особое мнение по вопросу разграничения информационной безопасности и кибербезопасности высказывают специалисты в сфере технического (программного) обеспечения безопасности. Так, бизнес-консультант по безопасности компании Cisco А. В. Лукацкий настаивает на том, что термин «информационная безопасность» следует трактовать узко, исходя исключительно из одной ее составляющей — защиты информации. МИБ, в том значении, в котором она представлена в различных нормативных правовых актах, по его мнению, является

[76] Резолюция ГА ООН 54/49 от 01.12.1999 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://undocs.org/ru/A/54/PV.69 (дата обращения: 05.05.2021).

абсолютно контентной и расширяет понятие безопасности от обеспечения доступа к информации до борьбы с негативной информацией и цифрового суверенитета.

В противовес Лукацкому выступает технический директор компании Positive Technologies С. В. Гордейчик, отмечая, что безопасность представляет собой более обширное поле деятельности, нежели просто сохранение данных в секрете»[77]. Его мнение также поддерживает специалист по расследованию инцидентов ИБ Group-IB Д. Захаров. Он возмущенно отмечает, что кибербезопасность представляет собой кальку с англицизма, который можно сопоставить разве что с цифровой безопасностью, сводящейся к защите цифровых активов, защите серверов. Напротив, ИБ, заострил внимание Захаров, является всеобъемлющим термином, включающим самые разнообразные аспекты обеспечения безопасности: от технических до правовых[78].

Любопытно, что доктрины и стратегии США в период с 70-х по 90-е гг. прошлого века включали в себя именно термин «информационная безопасность», но как только вопрос о безопасности был включен в повестку дня ООН по инициативе РФ, Запад предпочел оставить за собой право обладать всеми информационными потоками, влияющими на мыслительную активность и социальную деятельность населения, продвигая на международной арене исключительно термин «кибербезопасность».

Нельзя не заметить, что США заинтересованы, в первую очередь, в защите данных в электронных инфраструктурах. Американские специалисты не считают, что безопасность информации тем направлением, которому присущи цензурирование,

---

[77] Документальный фильм «Завтра не умрет никогда. Поле битвы: интернет» — URL: https://www.youtube.com/watch?v=r1gzhR4D1rU (дата обращения: 05.05.2021)

[78] Захаров Д., Зива С. Материалы специального курса «Прикладные вопросы информационной безопасности» / Факультет вычислительной математики и кибернетики МГУ им. М. В. Ломоносова и международной компании Group-IB. 2021.

контроль информационного потока на население. В качестве подтверждения приведем цитату американского исследователя Г. Лассуэлла: «Пропаганда — это инструмент тотальной политики… Политическая пропаганда — это использование средств массовых коммуникаций в интересах власти»[79]. Из этого следует, что отечественные исследователи подчеркивают, что безопасность информации обязательно должна включать не только техническое (кибернетическое) измерение, но еще духовное и социальное[80], а западные политики, настаивая на узкой трактовке рассматриваемого вопроса, потенциально желают создать новые территории информационного контроля и придать идеи национального государства характер иллюзорности.

Для сглаживания разногласий в двусторонних отношениях РФ и США используется нейтральный термин — «безопасность при использовании информационно-коммуникационных технологий (ИКТ)». Впрочем, даже такой термин при переводе с английского языка может иметь различные переводы на русский язык, в том числе и такие вариации, как информационные и коммуникационные технологии. С точки зрения лингвистики, использование некоторых знаков пунктуации или союза, союзных слов и выражений влияет на семантику словосочетания, меняет наполнение, смысловую нагрузку и контекст.

Отсутствие консенсуса по поводу ключевого термина тесно связано с идейными течениями, пропагандируемыми различными субъектами секъюритизации, что отражается в их политической линии в глобальном масштабе. Безусловно, условия,

---

[79] Арбатов Г. А. Идеологическая борьба в современных международных отношениях. — М., 1970. С. 170; Окинавская хартия глобального информационного общества (Принята на о. Окинава 22.07.2000) // Дипломатический вестник. 2000. № 8. С. 51–56.

[80] Rauscher K. F., Yaschenko V. The Russia — U.S. Bilateral on Cybersecurity. Critical Terminology Foundations; Karl Frederick Rauscher, Valery Yaschenko EastWest Inst. Information Security Inst. of Moscow State Univ. 2011. April. Iss. 1. C. 18–41.

в которых государства и неправительственные акторы взаимодействуют и сотрудничают по вопросам цифровизации, имеют характер проблемный и требующий скорейшего разрешения.

Очевидно, что повсеместное внедрение ИКТ меняет характер социума, усиливает рост затрат с целью противодействия угрозам в сфере ИБ. Государства принимают и реализуют стратегии информационной безопасности. Также эксперты отмечают стремительный рост новых видов вооружения, в основе которого лежат информационно-коммуникационные технологии. Довольно давно государства разрабатывают программное обеспечение и иные средства, направленные против критической инфраструктуры других государств. Именно государства, в первую очередь, относятся к основным субъектам МИБ, что, разумеется, обусловлено тем, что именно государства, обладающие суверенитетом и исключительным правом на принятие норм, согласно теории международного публичного права являются субъектами международного публичного права и международных отношений.

В международных отношениях, сформированных в процессе производства, распределения, обмена и использования ИКТ принимают участие не только правительственные акторы — государства, государственные органы, но межгосударственные организации, бизнес-структуры, транснациональные корпорации: разработчики и поставщики новых видов ИКТ, компании, регистрирующие домены, разрабатывающие системы защиты бизнеса, государственных критических инфраструктур и частных пользователей средствами коммуникации, мессенджерами и проч., а также физические лица, причем в контексте обеспечения или нарушения безопасности данного типа взаимоотношений физлица часто фигурируют в качестве хакеров.

Повышение роли бизнеса, крупных компаний и транснациональных корпораций в экономическом обороте ИКТ-сферы влечет за собой и увеличение значения мнения таких акторов в аспектах обеспечения безопасности, в частности, потому что

бизнес-структуры подвергаются информационным атакам с той же частотой и масштабностью, как и государственно значимые объекты и структуры. В этой связи привлечение представителей бизнеса, транснациональных корпораций в переговорный процесс по выработке эффективных действенных норм регулирования МИБ могло бы значительно ускорить и упростить данный процесс. Кроме того, польза консолидации и совместной деятельности в области обеспечения МИБ правительственных акторов и бизнеса становится очевидной при оценке эффективности мер, которые разрабатывают и используют сами бизнес-структуры для защиты своих данных, безопасности своих клиентов и своей деятельности в целом.

Как уже сказано выше, к субъектам правоотношений в области ИКТ, относятся физические лица. В контексте вопроса МИБ следует остановиться именно на их отдельных представителях — хакерах.

Необходимо отметить, что хакерство представляет собой высокоинтеллектуальный вид деятельности, целью которой является изучение вопросов защищенности информационных систем, поиск ошибок, пробелов и уязвимостей, выстраивание и внедрение мер технического обеспечения безопасности, а равно и неправомерное вмешательство в такие системы, в том числе с деструктивными, преступными целями. Хакеры могут решать как общественно полезные задачи, например, тестировать системы безопасности, так и использовать ИКТ из корыстных побуждений для кражи данных или из хулиганских мотивов в отношении отдельной общественной группы. Кроме того, в связи со стремлением государств развивать свой киберпотенциал, многие хакеры активно привлекаются правительствами, в том числе для взлома систем и осуществления атак в отношении государств-конкурентов или «вражеских» государств. Такая ситуация представляется довольно спорной и неоднозначной, ввиду того, что немало хакеров, фактически состоящих на государственной службе, еще вчера могли пособничать террористам, преступным

группировкам. «Пограничное» положение хакеров осложняет возможность определить, могут ли они участвовать в формировании режима МИБ и готовы ли вообще идти на переговоры.

Объективной проблемой определения статуса информационного пространства является нежелание западными государствами признавать глобальность ИКТ и тенденцию цифровизации все большего числа обществ и государств. Несмотря на незначительные уступки США и их сателлитов в диджитал-сфере и появление различных межгосударственных альянсов ключевые противоречия остаются актуальными и по сей день: отсутствие консенсуса по вопросам аккумуляции единого понятийного аппарата, применение международного права к информационному пространству, роль международных организаций, в частности, ООН в формировании режима МИБ.

В силу отсутствия единообразия мнения и подходов к определению изучаемой темы и ее ключевых аспектов, также представляется сложным процессом, отягченным зародившимся противоборством субъектов секъюритизации в ИКТ-сфере, в том числе и в военно-политической области, тормозит определение статуса информационного пространства.

В результате формирования новой среды, столпом которой является использование цифровых технологий, возрастает риск образования новых угроз глобальной безопасности и безопасности отдельных государств. Вместе с секъюритизацией данной сферы происходит усиление контроля государствами отдельных направлений использования ИКТ, а также происходит создание и укрепление цифрового суверенитета государств. Также для исследуемой темы характерна активная деятельность неправительственных акторов: бизнес-структур, научного сообщества, но кроме того выгоды использования новых технологий для себя также открывают преступные сообщества и террористические группировки. Условия развития информационного пространства и формирования режима его безопасности эволюционирует параллельно с все усложняющимися вызовами и рисками.

Можно заметить, как на фоне глобальной информатизации меняется ландшафт общей системы международных отношений, к изменению которого стремятся приложить руку не только субъекты международного права, но и другие действующие стороны, деятельность которых может быть направлена, как на формирование перспективного, безопасного и экономически полезного взаимодействия, так и на деструктивное, всепоглощающее, бесконтрольное, а зачастую преступное поведение, что затрудняет разрешение проблемы определения статуса информационного пространства в контексте МИБ.

Список использованной литературы

1. Арбатов Г. А. Идеологическая борьба в современных международных отношениях — М., 1970. С. 170.
2. Бирюков А. В. Современные международные научно-технологические отношения — М.: РосНОУ, 2014. С. 353.
3. Документальный фильм «Завтра не умрет никогда. Поле битвы: Интернет» — URL: https://www.youtube.com/watch?v=r1gzhR4D1rU (дата обращения: 05.05.2021)
4. Захаров Д., Зива С. Материалы специального курса «Прикладные вопросы информационной безопасности» / Факультет вычислительной математики и кибернетики МГУ им. М. В. Ломоносова и международной компании Group-IB. 2021.
5. Окинавская хартия глобального информационного общества (Принята на о. Окинава 22.07.2000) // Дипломатический вестник. 2000. № 8. С. 51–56.
6. Резолюция ГА ООН 54/49 от 01.12.1999 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» — URL: https://undocs.org/ru/A/54/PV.69 (дата обращения: 05.05.2021).
7. Rauscher K.F., Yaschenko V. The Russia — U.S. Bilateral on Cybersecurity. Critical Terminology Foundations; Karl Frederick Rauscher, Valery Yaschenko EastWest Inst. Information Security Inst. of Moscow State Univ. 2011. April. Iss. 1. C. 18–41.

СЕКЦИЯ 4

«ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ИНДУСТРИИ 4.0: РОЛЬ БИЗНЕСА»

О. А. Мельникова,
канд. полит. наук, начальник отдела Департамента
международной информационной безопасности МИД России

ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: в то время как на международной арене разворачиваются острые дискуссии по различным аспектам международной информационной безопасности, бизнес продолжает терять колоссальные средства из-за вредоносной деятельности в сфере ИКТ. В статье изложен авторский взгляд вопрос, каким образом снизить остроту этой проблемы и то, какую роль в этом процессе может сыграть бизнес.

Ключевые слова: информационная безопасность, ИКТ-среда, кибератака, переговорный процесс, государственно-частное партнерство, бизнес-структуры, защита информационных ресурсов бизнес-сообщества.

Сегодня информационно-коммуникационные технологии (ИКТ) оказывают такое же решающее значение для национального и глобального развития, определяют статус государства на международной арене, как в 40-е годы прошлого века ядерные технологии, а с 1950-х до 1970-х годов — ракетно-космические.

Географические факторы и военно-политическая мощь государства уступают место доминирующим ныне ИКТ и цифровым ресурсам. По этой причине любое, даже самое небольшое, но обладающее современными кибертехнологиями государство способно стать крупным игроком глобального цифрового пространства.

Сегодня арена геополитического противостояния переместилась в сферу ИКТ. В этой связи важно ослабить уязвимость от их вредоносного использования. И уж тем более — не допустить перерастания угроз в цифровой сфере в серьезный вооруженный конфликт.

Необходимость договариваться об общепринятых правилах, нормах и принципах поведения в киберпространстве настолько же актуальна, как и потребность в создании эффективного механизма государственно-частного партнерства.

Интересы государства и бизнеса в вопросах международной информационной безопасности (МИБ) являются сегодня взаимодополняемыми. Построение новой модели взаимодействия, при которой государства создают стабильную и безопасную среду для деловой активности, а корпорации не подменяют государства и не размывают их суверенитет, становится наиболее актуальной задачей.

В то же время, обеспечение гарантий безопасности для бизнеса и создания ему условий для выхода на внешние рынки является залогом поступательного развития экономики в целом.

Традиционные методы оказания содействия бизнесу, предпринимаемые со стороны государств, применительно к сфере безопасного использования ИКТ, в силу объективных факторов не могут быть в достаточной степени эффективными.

Мировой бизнес уже давно и прочно встал на цифровые рельсы: управление бизнесом, финансовыми потоками, логистика, промышленное производство, все виды транспорта осуществляется при широком использовании ИКТ. Во многие сферы бизнеса начинается внедрение технологий искусственного интеллекта.

В силу этого бизнес продолжает терять колоссальные средства от вредоносного использования ИКТ и кибератак на свои активы. С каждым годом восполнить эти потери ему все сложнее в силу возрастающего количества киберпреступлений.

Пандемия коронавируса усугубила ситуацию, поскольку вызвала лавинообразное увеличение пользователей цифровых инструментов, и, как следствие, активизацию кибермошенников и увеличение злонамеренных актов в ИКТ-среде. Зафиксирован колоссальный рост преступности в информационном пространстве, увеличилось число кибератак, существенно возрос экономический ущерб от подобных противоправных акций.

Сервисы компаний по всему миру в период пандемии стали более уязвимыми. Основная причина — вынужденный переход на удаленный режим работы, что повысило риски взлома корпоративных сетей и вынужденные финансовые расходы на информационную безопасность.

Большинство кибератак исходит от преступных группировок и имеет своей целью банальное вымогательство денег. Целями могут выступать как финансовые гиганты, так и любая компания среднего звена и даже с весьма скромным оборотом средств, например, осуществляющие крупные контейнерные перевозки (датская компания Moller-Maersk, потерявшая в 2017 г. из-за атаки вируса-шифровальщика 300 млн долларов, или отель Romantik Seehotel Jaegerwirt /Австрия/, где злоумышленники дистанционно заблокировали входные двери в номера). Руководству отеля пришлось выплатить преступникам €1,5 тыс. в биткойнах для освобождения своих постояльцев.

Или совсем свежий пример с крупнейшим в США нефтепроводом Colonial Pipeline, перекачивающим примерно 45% потребляемого в Восточном побережье США топлива (2,5 млн баррелей в день из Техаса вдоль восточного побережья до Нью-Йорка), который из-за кибератаки, произошедшей 7 мая с.г., был остановлен на несколько дней. По экспертным оценкам кибератаку, которая стала одной из самых дорогих для экономики страны, осуществила преступная группировка.

Ущерб мировому бизнесу только от кибератак увеличивается из года в год: в 2016 г. — 445 млрд долл., в 2017 г. достигал 1 трлн долл., в 2018 г. — 1,5 трлн долл., в 2019 год — более 2,5 трлн долл., а 2022 году, по прогнозу Всемирного экономического форума, сумма может вырасти до 8 трлн долларов. Даже по этим цифрам видим, что рост более 50%.

Бизнес вкладывает колоссальные средства в техническое обеспечение собственной безопасности, но при этом продолжает терять огромные финансовые ресурсы. С каждым годом все большее число бизнес-структур отчетливо понимают, что

задача построения защиты, которую нельзя взломать, утопична по своей сути. Бизнес все больше осознает собственную объективную уязвимость перед злонамеренными действиями в отношении своих активов.

Очевидно, что бизнес не способен самостоятельно и эффективно себя защитить. Поэтому он объективно может стать союзником наших подходов. Условия для такого союза уже созданы.

Все это лишний раз указывает на необходимость активнее вовлекать бизнес-структуры в переговорный процесс по МИБ для выработки четких, действенных и юридически закрепленных «правил игры» в киберпространстве, а также на переход к созданию эффективного механизма государственно-частного партнерства.

В рамках глобального переговорного процесса по вопросам МИБ появилась возможность интенсивнее вовлекать в международные дискуссии бизнес-сообщество, как наиболее заинтересованных участников цифровизации, испытывающих серьезный экономический ущерб от противоправных действий в киберсфере.

Это позволит, с одной стороны, привлечь на свою сторону бизнес, с другой — вырабатывать новые формы государственно-частного партнерства в области МИБ.

В условиях всеобщей и объективно необходимой цифровизации экономики прагматичная, взвешенная позиция бизнеса, составляющего основу экономического потенциала современных государств, может способствовать выработке понятных базовых правил и норм поведения в киберсреде.

Бизнес объективно станет тем локомотивом, который подтолкнет государства к выработке четких «правил игры» в киберпространстве.

Механизм вовлечения бизнеса в ооновский переговорный процесс по тематике МИБ уже запущен. В январе 2021 г. (по инициативе России) в рамках ООН была учреждена новая Рабочая группа открытого состава по вопросам безопасности в сфере

использования ИКТ и самых ИКТ (РГОС) на 5-летний срок. Группа в рамках своего мандата уполномочена рассматривать национальные инициативы в области МИБ, а также вопросы институционализации диалога участников РГОС с другими заинтересованными сторонами — бизнесом, НПО и научным сообществом. 1–2 июня в Нью-Йорке будет проведена организационная сессия новой РГОС на период 2021–2025.

Для вовлечения бизнес в переговоры по МИБ сейчас самая подходящая ситуация, а переговоры представителей мирового бизнеса на площадке единственной международной организации — ООН — повысят степень доверия со стороны бизнеса к государственным институтам.

Важно также диверсифицировать процесс подключения бизнеса к переговорному формату, задействовав этот механизм на такие статусные площадки, как БРИКС, ШОС, АСЕАН и др.

Страны-участницы АСЕАН в последнее время неоднократно высказывали заинтересованность в широком вовлечении бизнес-структур в переговорный процесс по МИБ.

Осознают важность данных подходов и наши китайские партнеры, которые в таких значимых региональных структурах как ШОС, АРФ начинают продвигать свои концепции цифровой экономики для защиты бизнеса и с его участием.

Продолжим практику по включению в состав российских делегаций и рабочих групп на международных мероприятий (переговорах, конференциях, семинарах и др.) по вопросам МИБ представителей российских уполномоченных бизнес-структур. Для привлечения внимания к российским разработкам в области высоких технологий «на полях» профильных международных мероприятий за рубежом намечаем организацию выставок, презентаций, тренингов и др.

Рассчитываем на имеющиеся наработки, идеи и предложения в сфере информационной безопасности крупных компаний и экспертов, которые активно задействуют инструменты государственно-частного партнерства и, по нашему мнению,

способны внести ощутимый интеллектуальный вклад в международные дискуссии по МИБ.

В русле наших национальных интересов создание благоприятных условий для продвижения на мировой рынок российских производителей цифровых технологий, которые имеют все шансы стать хорошей альтернативой западным образцам. Это будет способствовать его переориентации на отечественные высокотехнологичные продукты и соответствующее техническое сопровождение. Это также позволит наглядно продемонстрировать всему миру преимущества российских ИКТ и предоставит широкие возможности для их дальнейшего развития.

Ведем активную работу по укреплению международно-правовой базы сотрудничества с зарубежными партнерами и подписанию соответствующих межправительственных соглашений, создавая надежную юридическую «платформу» для государственно-частного партнерства.

Задача по формированию условий для повышения эффективности государственно-частного партнерства в сфере информационной безопасности, содействие участию национальных коммерческих организаций-производителей товаров и услуг в сфере информационной безопасности в международном сотрудничестве в интересах укрепления информационной безопасности России и формирования системы обеспечения МИБ, которая определена «Основами государственной политики Российской Федерации в области международной информационной безопасности» (утверждены Указом Президента от 12 апреля 2021 г. №213)[1], представляется не только объективной и важной, но и требующей скорейшей масштабной реализации.

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности / утв. Указом Президента Российской Федерации от 12 апреля 2021 года № 213. — URL: http://www.publication.pravo.gov.ru/Document/View/0001202104120050/ (дата обращения: 11.05.2021).

Список использованных источников и литературы

1. Киселев С. Сбербанк оценил потери мировой экономики от кибератак // Независимая газета. 2019. 26 апреля. URL: https://www.ng.ru/economics/2019-04-26/100_2604191901.html/ (дата обращения: 22.04.2021).
2. Крутских А. В. Мирная киберстратегия России // Внешнеэкономические связи. 2021. №39. URL: https://eer.ru/article/gosudarstvo/u1283/2021/04/19/4044// (дата обращения 19.04. 2021).
3. Основы государственной политики Российской Федерации в области международной информационной безопасности / утв. Указом Президента Российской Федерации от 12 апреля 2021 года № 213. — URL: http://www.publication.pravo.gov.ru/Document/View/0001202104120050/ (дата обращения: 11.05.2021).
4. Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности». URL: https://www.garant.ru/products/ipo/prime/doc/400473497/ (дата обращения: 20.04.2021).
5. Group-IB опубликовала прогнозы по киберугрозам, с которыми мир столкнется в новом году. URL: https://www.group-ib.ru/media/gib-report-2020/ (дата обращения: 27.04.2021).

С. А. Семедов,
д-р филос. наук, профессор, заведующий кафедрой
Международного сотрудничества
Института управления и регионального развития РАНХиГС

В. А. Сухарева,
канд. филол. наук, преподаватель кафедры
Международного сотрудничества
Института управления и регионального развития РАНХиГС

ДИПЛОМАТИЧЕСКИЕ И САНКЦИОННЫЕ ВОЙНЫ КАК МЕТОДЫ ВЛИЯНИЯ НА МЕЖДУНАРОДНОЕ ЭКОНОМИЧЕСКОЕ СОТРУДНИЧЕСТВО

Аннотация: в статье рассматриваются проблемы взаимосвязи экономического инструментария, дипломатических методов и их влияние на международные экономические отношения. Современное информационное пространство стало полем не только сотрудничества и взаимодействия, но также и источником новых угроз. В трансформации мирового порядка информационные технологии выходят на передний план как инструменты для укрепления своих позиций участниками мировой политики. Основная угроза международной информационной безопасности — возможность применения информационно-коммуникационных технологий в целях, несовместимых с задачами обеспечения международной стабильности, прежде всего на уровне государств в отношении информационных инфраструктур другого государства в политических, в том числе военных целях.

Ключевые слова: международная информационная безопасность, киберугрозы, дипломатия, санкции, международное сотрудничество, преступность в киберпространстве, интернет, информационные войны, «спин-терапия», «черный пиар».

Информационное пространство представляет собой новую сферу международных отношений, одно из «новых неразделенных пространств», за раздел которого идет борьба между различными акторами мировой политики. Технологический прогресс в конце XX — начале XXI века создал новую сферу цифровых коммуникаций, которая стала полем не только сотрудничества и взаимодействия, но также и новых угроз. «Зависимость всех современных обществ от информационных технологий заставляет искать методы противодействия различным киберугрозам и… способы ведения наступательных операций против возможных противников»[2]. Можно говорить не только о возможностях, но и о реальных фактах противоборства государств в киберпространстве.

Фактически впервые со времен появления ядерного оружия появилась принципиально новая сфера применения силы в международных отношениях. Информационная безопасность выходит на передний план международной повестки дня вследствие осознания возрастающей зависимости всех сфер жизни личности, общества и государства от информационных инфраструктур и их уязвимости, в том числе физической. Подтверждение тому — атаки вирусов Stuxnet против АЭС в Иране, публикация конфиденциальной дипломатической переписки сайтом WikiLeaks, действия хакерского движения Anonimous, массовая волна протестов в странах арабского Востока, получившая в прессе название «Twitter-революции», «феномен Сноудена», кибератаки в период президентских выборов в США в 2016 и в 2020 гг.

Основная угроза международной информационной безопасности — возможность применения ИКТ в целях, несовместимых с задачами обеспечения международной стабильности, прежде

[2] Тренин Д. В. Традиционные и новые вызовы безопасности в международных отношениях // Современная наука о международных отношениях за рубежом: хрестоматия. В 3 т. Т. 2 / Под общ. ред. И. С. Иванова. — М.: НП РСМД, 2015. С. 139.

всего на уровне государств в отношении информационных инфраструктур другого государства в политических, в том числе военных целях; преступная и террористическая деятельность в киберпространстве. Это сделало технически решаемой проблему управления информационным пространством. Управление интернетом означает установление контроля над ключевыми ресурсами (доменные имена, IP-адреса, интернет-протоколы, система корневых серверов), контентом, регистрационными операциями и системой присвоения доменов и адресов. В начале 1990-х гг возникли международное сообщество IETF (Internet Engineering Task Force) и международная профессиональная организация ISOC (Internet Society). В 1998 году ведущие функции перешли к ICAN[3].

В настоящее время управление интернетом в значительной степени находится под контролем США. Техническая координация интернета, управление пространством имен и адресов сети осуществляется некоммерческой негосударственной организацией ICANN (Internet Corporation for Assigned Names and Numbers — Корпорация по присвоению имен и адресом интернета), зарегистрированной в штате Калифорния и зависящей в принятии решений от министерства торговли США. Сложившаяся ситуация создает ряд политических и экономических преимуществ для США, предоставляя возможность управления развитием и использованием интернета. Россия выступает за интернационализацию управления интернетом, при этом наша страна создала свой домен интернета — Рунет. Россия также выступает за необходимость контроля государствами собственного сегмента глобального информационного пространства и невмешательство во внутренние дела посредством использования ИКТ. Китай, страны Азиатско-Тихоокеанского региона и Афри-

[3] Мегатренды: основные траектории эволюции мирового порядка в XXI веке: учебник / под ред. Т. А. Шаклеиной, А. А. Байкова. — М.: Аспект Пресс, 2013. — 321 с.

ки выступают за передачу функций технической координации к Международному союзу электросвязи (специализированной организации ООН). Управление интернетом на основе межправительственного подхода в рамках Международного союза электросвязи (МСЭ) позволит защитить государственный суверенитет во Всемирной сети.

Таким образом, складываются новые форматы регулирования международной среды, изменившейся под воздействием инновационного развития, научно-технического прогресса и ряда других факторов. Нам кажется важным отметить особенность современных международных отношений — это использование дипломатических войн (несочетаемое «война» и «дипломатия») с информационным давлением, информационной войной. Создается устойчивое мнение в мировом информационном пространстве, что Россия нарушает элементарные правила на международной «шахматной доске»: шпионаж под дипломатическим прикрытием, «государственный терроризм» («дело Скрипалей» — Солсбери, Чехия — взрывы на военных складах…), нарушение Венских конвенций 1961 и 1963 года, использование Россией международных организаций для разведывательной и иной, несовместимой с дипломатическим статусом деятельностью (высылка 12 сотрудников Представительства РФ в ООН в 2018 году), Россия «нарушает международные соглашения» (инициирование США выхода из ДРСМД, ДОН…) и т.п. В пересмотре и трансформации мирового порядка информационные технологии выходят на передний план как инструменты для укрепления своих позиций участниками мировой политики.

Санкции и «дипломатические войны» становятся в современном мире частью информационных войн, причем эффективность применения санкций кратно возрастает при использовании новых технологий. К примеру, отключение России от международной финансовой трансакционной системы SWIFT (СВИФТ) создаст огромные проблемы не только государственной системе, но и экономике, дипломатии, каждому отдельно-

му гражданину. Вспомним печально известную швейцарскую фирму «Нога», по иску которой были заблокированы счета российских частных и государственных учреждений, в том числе и дипломатических представительств в нескольких европейских странах. К России за последние годы широко применяются такие информационные технологии, как «спин-терапия» (методика информационного управления событием. Например, политика России в Арктике, политика РФ в Сирии…), «черный пиар». Мне кажется, наша отечественная политология уделяет мало внимания «информационной агрессии», которая часто замаскирована под «общечеловеческие интересы».

Нужно отметить, что современные международные отношения во многом определяются тем образом, тем имиджем, который государство, общество создает в глазах мирового сообщества. А национальный брендинг во многом зависит от технологического информационного развития государства. Думаю, что РТ как информационная система, Большой театр, бренд «Сделано в России» играют громадную роль в формировании имиджа России. Наибольшую прибыль в информационную эпоху приносят информация и знания, информационные технологии и информационная продукция.

Хотелось бы уточнить некоторые философские основы понятия *«информационные технологии»*. Естественно, информационные технологии — это *Глобальная паутина*, производство и использование информационных технологий в политике, экономике, дипломатии. Однако информационная эпоха характеризуется тем, что информационные технологии воздействуют на психику, на сознание, в том числе на массовое сознание. Проблема информационных технологий — это проблема сегодня психоанализа, социальной психологии, социальной философии. Психозы и неврозы в современном киберпространстве, психологические аспекты влияния киберпространства (точнее, информации в к-пространстве) на принятие внешнеполитических решений, информационные технологии в исторической памяти,

в ее формировании (символов, героев, знаков…)… — это лишь небольшая часть тех проблем, на которые нам следует обращать внимание. Иначе, мы будем опять формировать свое видение мира через работы зарубежных авторов, таких как Ной Харари, Шошан Зубофф.

Впервые публично заявил о целесообразности проекта глобальной информационной инфраструктуры вице-президент США Альберт Гор еще в далеких 90-х гг. В 1996 в ЮАР состоялась международная межправительственная конференция «Информационное общество и развитие», с которой началась история глобального информационного общества (ГИО). Лидерство в формировании повестки принадлежало «Группе восьми», которая на Окинаве в 2000 г. приняла Хартию глобального информационного общества. Дискуссии о создании международно-правового режима управления интернетом начались еще в конце 90-х гг. в 2002 году вслед за хартией «Глобального информационного общества» последовала программная резолюция ГА ООН № 57/53, которая указала на недопустимость использования информационно-телекоммуникационных технологий и средств для оказания негативного воздействия на инфраструктуру государств. На Международном саммите по проблемам информационного общества в Женеве (2003 г.) Генеральному секретарю ООН было поручено создать Рабочую группу для выработки определения «управление интернетом» и подготовки отчета к Тунисскому саммиту 2005 года. На этом саммите был учрежден *Форум по управлению интернетом*, предназначенный для ведения многостороннего политического диалога по вопросам управления интернетом, действующего под эгидой ООН и на основании мандата ООН. Форум не вмешивается в вопросы повседневной эксплуатации или технического обслуживания интернета. Форум не осуществляет никаких надзорных функций и не подменяет существующие структуры, механизмы, институты или организации, но в тоже время привлекает их к своей работе и использует их опыт. Он действует на постоян-

ной основе посредством регулярных всемирных встреч, совещаний, которые могут проводиться одновременно с крупными конференциями ООН по соответствующим вопросам. Решения, принятые Форумом, носят рекомендательный характер.

К числу важнейших проблем правового регулирования и регламентирования информационных технологий применительно к интернету можно отнести:

— определение международно-правовых основ функционирования и дальнейшего развития интернета, что относится к управлению интернетом;
— уточнение правового статуса субъектов правовых отношений, связанных с использованием интернета, с учетом того факта, что такие отношения, как правило, осложнены иностранным элементом;
— установление правового режима объектов, являющихся предметом указанных выше отношений и относящихся к самым разным уровням инфраструктуры, применяемой для оказания услуг с использованием информационных технологий (сайты, сетевые серверы, компьютерные серверы, оборудование для передачи информации на магистральном и абонентском уровне и т.д.), а также применяемые в интернете средства адресации и идентификации;
— международно-правовые средства предотвращения использования интернета в противоправных целях;
— выявление оптимальной модели «управления интернетом», фиксация соответствующих ей прав и обязанностей государств в международно-правовых нормативных актах[4].

Объект и предмет регулирования правовых отношений, связанных с использованием интернета, однозначно определить невозможно, т.к. интернет — это многоуровневая технологиче-

[4] Международное право : учебник для вузов / отв. ред. С. А. Егоров. — М.: Статут, 2016. — 848 с. Гл. 26. Международное право и информационныне технологии. — С. 811–812.

ская информационная сеть, функционирование которой осуществляется в трансграничном масштабе[5].

За первые 20 лет XXI в. активно заработал механизм всемирных встреч на высшем уровне по вопросам Информационного общества. Но проблема «цифрового разрыва» усугубилась и, более того, высказывавшиеся надежды на «выравнивание игрового поля» в опоре на ИКТ оказались несостоятельными. Несправедливость имеет социально-экономическую, а не технологическую природу. В результате в связи с ГИО (Глобальное информационное общество) углубились противоречия между развитыми и развивающимися странами. Одновременно обострились противоречия вокруг интернета и его по существу единоличного контроля со стороны США. Проблема интернационализации Всемирной паутины стала предметом серьезной дискуссии в мировом сообществе, носящей как технологический, так и политический характер.

Если говорить про возможности глобального информационного общества, широкое использование информационных технологий дало возможность правительствам в режиме реального времени обращаться ко всем гражданам государства, выходить практически на неограниченную международную аудиторию, таким образом, внешняя политика начала работать в режиме онлайн, постоянно находясь в фокусе СМИ. Так же, развитие глобального информационного общества в первую очередь оказали глубокое трансформирующее воздействие на все сферы жизни общества — культурную, экономическую, социальную. Глобализация — одна из наиболее значимых тенденций современного мира, в значительной степени была обусловлена развитием и внедрением трансграничных по своей природе новейших научно-технических достижений, в том числе

[5] Касенова М. Б. Международно-правовое регулирование интернета. — СПб., 2012; Касенова М. Б., Якушев М. В. Управление интернетом: Документы и материалы. — СПБ, 2013.

информационных технологий и интернета. В формирующуюся глобальную технологическую и информационную среду уже переносятся ключевые составляющие международной, политической, торгово-экономической, культурной деятельности. Быстро развивается сектор электронной коммерции, многие виды бизнеса переносятся в онлайн-среду, появляются новые продукты и услуги. По сути, идет процесс реализации научно-технической демократии и становление единого международного научно-технического пространства, в рамках которого развиваются сотрудничество и обмен знаниями. Например, как единое информационное пространство — совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающих информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей.

Что касается противоречия формирования глобального информационного общества, то так как в современном мире, в его информационном аспекте, информационное пространство в связи с развитием технических каналов коммуникации стало практически безграничным, то есть в нем неэффективны практически все традиционные ограничения физического пространства — океаны, государственные границы, горы, географическая удаленность. Информационное пространство стирает границы, однако все же информационное пространство имеет свои рамки, обусловленные официальными ограничениями. Эти ограничения бывают конвенциональными — обязывающими соблюдать коммерческую тайну, обеспечивающими право человека на неприкосновенность частной жизни, и институциональными, связанными с государственной и военной тайной.

Поскольку структура информационного пространства обусловлена наличием связи между субъектами и объектами, кото-

рыми эти субъекты оперируют. Субъекты и объекты с течением времени изменяются, переходят из одних множеств в другие, образуя новые связи и разрушая старые — это обусловливает динамику информационного пространства. Основная проблема заключается в том, что в информационном пространстве структуры фрагментарны, а связи локальны, поэтому субъект информационного пространства иногда может даже не подозревать о существовании другого субъекта, информационно удаленного от него. Эта проблема решается транзитивным замыканием информационного пространства путем добавления к существующему информационному пространству информационной системы, которая содержит глобальную информацию и делает ее доступной всем субъектам информационного пространства, которые могут привести к нанесению ущерба чьим-либо интересам либо суверенитету, создавая предпосылки для властных манипуляций со стороны тех или иных акторов мировой политики.

Информационные средства воздействия становятся важным элементом военного потенциала государств, эффективно дополняющим традиционные средства ведения вооруженных конфликтов и способным в ряде случаев полностью заменить их. В структуре вооруженных сил появляются специальные подразделения, основная задача которых — ведение информационного противоборства и отражение информационных атак (в США с 2009 г. действует киберкомандование Cybercom, созданы аналогичные структуры в России и в Китае). Международные организации, прежде всего действующие в сфере безопасности, также координируют действия государств в данной сфере (так, действует Центр передового опыта по совместной киберзащите НАТО, в рамках ОДКБ проводятся операции по противодействию киберпреступности ПРОКСИ). При этом обеспечение информационной безопасности на международном уровне имеет определенную специфику по сравнению с иными вызовами и угрозами. Россия стала первым государ-

ством, поднявшим на международном уровне вопрос о появлении принципиально новых — информационных — угроз национальной и международной безопасности в XXI веке. С 1998 г. по инициативе России резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» принималась Генеральной Ассамблеей ООН ежегодно. Россия ориентирует международное сообщество на исследование угроз в сфере информационной безопасности и принятия необходимых совместных мер по их устранению, в том числе создание международно-правового режима, ограничивающего возможности использования ИКТ во враждебных целях. Москва рассматривает обеспечение международной информационной безопасности в рамках «триады» угроз: преступной, террористической и военно-политической». Кроме того, Россия инициирует обсуждение проблемы информационной безопасности на региональном уровне, в рамках таких организаций и форумов, как ШОС, АТЭС, БРИКС, ОБСЕ, ОДКБ. Растут противоречия между мировым лидерами — США, Китаем и Россией в сфере обеспечения информационной безопасности. Эти государства предлагают различные видения на проблемы обеспечения информационной безопасности. Если Китай, как и Россия, выступает за государственное регулирование информационной сферы и обеспечение информационной безопасности на основании международных договоров, то США предпочитают частную модель регулирования. В настоящее время Соединенные Штаты признают наличие военно-политических угроз международной информационной безопасности, при этом делают акцент на право регулирующем, а не предотвращающем подходе. В то время как Россия выступает за исключение интернет-пространства из военных действий (что нашло, в частности, выражение в проекте «Правил поведения в информационном пространстве», предложенном государствами ШОС для принятия в качестве неофициального документа ООН), США предлагают распро-

странить данную сферу нормы и принципы международного гуманитарного права. Признание информационной сферы в качестве объекта регулирования международного гуманитарного права легитимизирует возможность информационных войн, подчиняя их, однако, определенным правовым ограничениям (недопущение атак на объекты гражданской инфраструктуры и пр.). «Хотя мир не вел тотальных кибервойн, но эксперты по киберпространству и военные стратеги ожидают развертывания настоящего межгосударственного киберсражения уже в ближайшие годы.

Особую тревогу вызывает слабая система регулирования и контроля в этой области перед лицом растущей угрозы»[6]. Эксперты ставят вопрос о правомочности в международных отношениях коллективного наказания инициаторов кибератак, т.е. распространения на киберпространство концепции «гуманитарного вмешательства».

Важнейшей угрозой мировому порядку и вызовом мировому сообществу являются киберпреступления, количество которых растет в геометрической прогрессии. Ее размах впечатляет. По данным Allianz Global Corporate and Specialty, в 2016 году общий ущерб от интернет-преступности для мировой экономики превысил 575 млрд долл. Это около 1% мирового ВВП (к 2021 году размер ущерба от киберпреступлений вырос в несколько раз). За последние 4 года произошло десятикратное увеличение количества неизвестных программ, атакующих организации. Компьютерные атаки стали широко «использоваться в качестве инструмента политической борьбы, добычи компромата, межгосударственного противостояния»[7]. Книга «Взломанный мировой порядок» («The Hacked World Order»)

[6] Рекс Хьюз. Договор по киберпространству / Современная наука о международных отношениях за рубежом: хрестоматия. В 3 т. Т. 2 / Под общ. ред. И. С. Иванова. — М.: НП РСМД, 2015. С. 155.

[7] Грамматиков А., Вандышева О. Идет кибервойна народная // Эксперт. № 5. 2017. С. 13–14.

Адама Сигала, директора программы по политике в цифровом и киберпространстве при Совете по международным отношениям, была опубликована в начале 2016 г. и представляет собой одну из самых последних попыток охватить все события, разворачивающиеся в киберпространстве[8].

Киберпространство — относительно новая и неосвоенная сфера международных отношений и мировой политики, над которой не тяготеет груз наследия холодной войны. Именно поэтому кибердиалог может стать одной из самых перспективных платформ для развития международного сотрудничества. Киберпространство — уникальная, не знающая равных в новейшей истории человечества среда, способствующая индивидуальному развитию, однако важные решения по-прежнему принимаются странами с наиболее развитыми сферами технологий и инноваций. Это единственный шанс для всех стран начать содержательный и долгий диалог о том, в каком именно мировом порядке организации киберпространства они хотят жить.

Таким образом, становится очевидным факт, что высокие технологии представляют собой важный властный ресурс, который имеет экономическую и политическую ценность и может дать одной стране политические и технологические преимущества по сравнению с другими. В связи с этим научно-техническое соперничество занимает ключевое место в современной системе международных отношений и оказывает существенное воздействие на изменение в шкале индикаторов совокупного могущества страны. В результате чего нужно отметить, что страна, которая занимает лидирующее место в области научно-технических инноваций, имеет все основания для доминирующего положения в международном сообществе. Информационные технологии становятся фактором совокупной мощи государств. Традиционная межгосударственная система находит свое отра-

[8] Адам Сигал. Взломанный мировой порядок. — Public Affairs, 2016 (на англ. яз.).

жение в интернете, появляется новый термин «информационная геополитика». Это подтверждает также быстрое развитие так называемой дипломатии Web 2.0 в США, Китае, России, Израиле, особенно, в Швеции и ряде других стран.

Современные информационные технологии используются в международной политической борьбе (гонка вооружений, в центре — ракетно-ядерные и космические технологии):

1. Сегодня можно утверждать, что ядерную угрозу сменяет информационная опасность, которую несут вызовы, связанные с использованием ИКТ против других государств. История с Wikileaks, Э. Сноуденом, *информационные атаки* на Россию отражают попытку дестабилизировать различные международные ситуации плюс информационные войны, которые уже стали реальностью современного мира и серьезной угрозой национальной безопасности.
2. Проблемы создают также высокотехнологичный терроризм и преступность. В этой связи возрастает значение обеспечения *международной информационной безопасности*, ставшей важнейшим направлением противостояния в современной системе МО.
3. НТР оказывает воздействие на экономику и политику государств. Формируются новые виды коммерческой деятельности, требующие высокого уровня образования, что влияет на международную академическую мобильность, и, скорее всего, вызовет новую *масштабную волну миграции населения* Земли. Но «творческое разрушение» станет особенностью не только бизнеса. Существенно изменится «игровое поле» и в политической области. Возникнут новые механизмы управления обществом, появятся новые политические игроки, а также формы взаимодействия граждан и выражения ими мнений и влияния на власть.
4. Необходимо постоянное совершенствование методов и принципов построения и реализации государственной информационной политики. В противном случае «выжи-

вание на геополитической арене такого духовно мощного и самобытного государства, как Россия может стать проблематичным».

5. Проблемы информационного пространства, киберпространства, киберпреступности становятся в отношениях между ведущими участниками международных отношений основными.

Список использованных источников и литературы

1. Адам Сигал. Взломанный мировой порядок. — PublicAffairs, 2016 (на англ. яз.).
2. Грамматиков А., Вандышева О. Идет кибервойна народная // Эксперт. 2017. № 5. С. 11–19.
3. Касенова М. Б. Международно-правовое регулирование интернета. — СПб., 2012; Касенова М. Б., Якушев М. В. Управление интернетом: документы и материалы. — СПБ, 2013.
4. Мегатренды: основные траектории эволюции мирового порядка в XXI веке: учебник / под ред. Т. А. Шаклеиной, А. А. Байкова. — М.: Аспект Пресс, 2013. — 321 с.
5. Международное право: учебник для вузов / отв. ред. С. А. Егоров. — М.: Статут, 2016. — 848 с. Гл. 26.
6. Международное право и информационныне технологии. — С. 809–840.
7. Рекс Хьюз. Договор по киберпространству/ Современная наука о международных отношениях за рубежом: хрестоматия. В 3 т. Т. 2 / под общ. ред. И. С. Иванова. — М.: НП РСМД, 2015. С.155.
8. Тренин Д. В. Традиционные и новые вызовы безопасности в международных отношениях // Современная наука о международных отношениях за рубежом: хрестоматия. В 3 т. Т. 2 / под общ. ред. И. С. Иванова. — М.: НП РСМД, 2015. С. 139.

А. Ю. Толстухина,
канд. полит. наук,
программный менеджер и редактор сайта РСМД

РЕГУЛИРОВАНИЕ ГЛОБАЛЬНЫХ IT-КОМПАНИЙ: ОСНОВНЫЕ ТЕНДЕНЦИИ И ПРОБЛЕМЫ

Аннотация: в статье рассматривается проблема регулирования глобальных технологических корпораций и реакция последних на действия регуляторов. Акцент сделан на американских IT-корпорациях, но не упущен из вида и опыт Китая, где также отчетливо себя проявляет тренд на регулирование крупного бизнеса.

Ключевые слова: регулирование IT-корпораций, Big Tech, Microsoft, Apple, Alphabet, Amazon, Facebook, монополизация рынка, защита персональных данных, борьба с опасным контентом, информационныя безопасность.

В современном цифровом мире IT-корпорациям известно о нас абсолютно все — начиная от местоположения, совершенных покупок заканчивая музыкальными предпочтениями и политическими взглядами. Но самое главное, интернет-гиганты не просто собирают и анализируют полученные массивы данных, но и непосредственным образом влияют на наше сознание и формируют желания при помощи технологий искусственного интеллекта и таргетированной рекламы. Эксперты и политики уже начали говорить о цифровой диктатуре со стороны Big Tech. Так, канцлер Германии А. Меркель, выступая на площадке IGF в 2019 г., заявила о повышении опасности того, что «глобальные компании могут создавать параллельные миры со своими собственными правилами и стандартами и навязывать их пользователям»[9]. На эконо-

[9] Speech by Federal Chancellor Dr Angela Merkel opening the 14th Annual Meeting of the Internet Governance Forum in Berlin on 26 November 2019 — URL: https://www.bundesregierung.de/breg-en/news/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-

мическом форуме в Давосе в 2021 г. Президент России В. В. Путин отметил, что «ИТ-корпорации — это уже не просто какие-то экономические гиганты, по отдельным направлениям они де-факто конкурируют с государствами». Он также заострил внимание на том, что «глобальный бизнес может легко перейти ту грань, когда он сможет по своему усмотрению управлять обществом, подменять легитимные демократические институты, по сути, узурпировать или ограничивать естественное право человека самому решать, как жить, что выбирать, какую позицию свободно высказывать»[10].

Мощь IT-корпораций, которая лишь усилилась в период глобального социального дистанцирования, неоспорима. Их уже называют квазигосударствами, и это не удивительно — в сумме капитализация Microsoft, Apple, Alphabet, Amazon и Facebook — достигла в 2020 году 7 трлн долл. (это больше, чем ВВП большинства стран G20)[11]. Глобальные корпорации получили власть — они монополизировали рынок цифровых технологий, препятствуют развитию локальных компаний, усугубляя цифровой разрыв между странами, посягают на цифровой суверенитет государств, провоцируют поляризацию общества ввиду особенностей работы алгоритмов.

В этой связи, не удивительно, что сегодня проблема регулирования IT-гигантов активно обсуждается на различных международных форумах — Всемирном экономическом форуме в Давосе, Форуме по управлению интернетом (IGF) и т.д.

Попытки регулирования технологических гигантов особенно активно начали предприниматься с 2018 года. Главным образом

---

the-internet-governance-forum-in-berlin-on-26-november-2019-1701494 (дата обращения: 11.08.2021).

[10] Сессия онлайн-форума «Давосская повестка дня 2021» // сайт Президента России — URL: http://www.kremlin.ru/events/president/news/64938 (дата обращения: 11.08.2021).

[11] Стоимость пяти IT-гигантов США — $7 трлн. Больше, чем ВВП 16 стран G20 // РБК. Август, 2020. — URL: https://quote.rbc.ru/news/article/5f4363819a79479d6cdb08a1 (дата обращения: 11.08.2021).

оно наблюдается в области защиты данных и борьбы с опасным контентом. Определенный успех уже достигнут. Назовем несколько примеров: Крайстчерчский призыв к действию по искоренению террористического и насильственного экстремистского контента в интернете (Christchurch Call), согласно которому интернет-компании обязались немедленно изымать информацию террористического толка, а также действующий с 2018 года в ЕС закон о защите персональных данных (General Data Protection Regulation, GDPR)[12]. Интересно, что лишь за один год своего существования GDPR заставил корпорации заплатить штрафы на сумму более 56 млн евро[13].

Кроме того, в Евросоюзе есть еще одна законодательная инициатива, состоящая из двух пакетов — Закон о цифровых услугах Digital Services Act, DSA, 2020 г. (это новое законодательство в отношении незаконного контента, прозрачной рекламы и дезинформации) и Закон о цифровых рынках DMA (должен наложить каскад ограничений на доминирующих игроков, которые угрожают свободной конкуренции[14].

Интересно, что в США, где расположены главные офисы большинства интернет-гигантов, также всерьез озаботились проблемой регулирования технологических корпораций, хотя в этой стране предпочитают придерживаться так называемой

---

[12] Благодаря принятию GDPR пользователи были наделены определенными правами в отношении их персональных данных, а у компаний появились соответствующие обязанности. Например, для сбора данных компаниям необходимо получить согласие пользователей.

[13] Gil Press. Facebook, Google, Apple, Other Data-Driven Firms, Defy The Global Move To Strong Privacy Regulations. Forbes. June 26, 2019. — URL: https://www.forbes.com/sites/gilpress/2019/06/26/facebook-google-apple-other-data-driven-firms-defy-the-global-move-to-strong-privacy-regulations/?sh=6a9261e71ae0 (дата обращения: 11.08.2021).

[14] Европейская комиссия представила проект нового «цифрового законодательства» // Seldon news. Декабрь, 2019. — URL: https://news.myseldon.com/ru/news/index/242447002 (дата обращения: 11.08.2021).

калифорнийской модели управления, согласно которой корпорациям предоставляется максимальная свобода действий. Например, в Калифорнии появился свой аналог GDPR — это Закон о защите конфиденциальности потребителей (California Consumer Privacy Act, CCPA), вступивший в силу в 2020 г. Также в Америке всерьез обеспокоились контентом в социальных сетях. Президент США Джо Байден, не большой поклонник Facebook, грозится удалить статью 230 из текста «Акта о пристойности в телекоммуникациях», согласно которой такие платформы как Facebook и Twitter не являются «издателями» информации (publishers), а потому не несут ответственности за высказывания третьих лиц, использующих их услуги[15]. И еще один интересный факт — 7 мая США присоединились к Крайстчерчскому призыву, хотя изначально отказывались это делать, подчеркивая приверженность свободе слова в сети[16].

В России также выступают за регулирование деятельности IT-гигантов, которые зачастую уклоняются от уплаты налогов, не предоставляют никаких отчетов и игнорируют решения судов. В частности, звучат призывы к легализации крупных игроков в национальном правовом поле и налаживании каналов связи между сторонами для выстраивания эффективного диалога, а важнейшим шагом в этом направлении должно стать открытие их официальных представительств[17]. Кроме того, в начале 2021 года были внесены изменения в Федеральный закон «Об

---

[15] Bryan Pietsch, Isobel Asher Hamilton, Katie Canales. What you need to know about Big Tech's Section 230 shield, the internet law that Trump hated and Biden might reform// Insider. July 8, 2021. — URL: https://www.businessinsider.com/what-is-section-230-internet-law-communications-decency-act-explained-2020-5 (дата обращения: 11.08.2021).

[16] США заявили, что присоединятся к международной инициативе по борьбе с экстремизмом в сети // ТАСС. Май, 2021. — URL: https://tass.ru/mezhdunarodnaya-panorama/11326177 (дата обращения: 11.08.2021).

[17] Материалы RIGF. 8 апреля 2021. — URL: https://rigf.ru/press/?p=video&vid=b7zokhEq_uw (дата обращения: 11.08.2021).

информации, информационных технологиях и о защите информации»[18]. Госдума обязала социальные сети с 1 февраля 2021 г. самостоятельно выявлять и блокировать запрещенный контент, в том числе детскую порнографию и экстремистские материалы. Также принят закон о штрафах за отказ удалять противоправную информацию[19].

Важно несколько слов сказать и о Китае. В этой стране существует своя цифровая экосистема со своими технологическими гигантами, успешно вышедшими на глобальный рынок — Alibaba, Huawei, Tencent и пр. Однако даже при китайской модели управления не наблюдается безоблачных отношений между крупным бизнесом и правительством. Например, в апреле этого года власти Китая оштрафовали Alibaba на рекордные 2,8 млрд долл. Компанию обвинили в нарушении антимонопольного законодательства. Регулятор посчитал, что действия IT-гиганта негативно повлияли на конкуренцию на рынке электронной коммерции[20]. Еще один пример регулирования крупных игроков — обнародование в октябре 2020 г. законопроекта о защите персональных данных, который, как ожидается, вступит в силу в 2021 г. Закон должен будет ограничивать возможности интернет-платформ собирать и использовать данные потребителей в своих целях[21].

Интересно, что технологические компании в целом поддерживают тренд на регулирование. Более того, многие из них

---

[18] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». — URL: https://sozd.duma.gov.ru/bill/223849-7 (дата обращения: 11.08.2021).

[19] Штраф за треш // Российская газета. Декабрь 2020. — URL: https://rg.ru/2020/12/23/socseti-s-1-fevralia-obiazali-blokirovat-zapreshchennyj-kontent.html (дата обращения: 11.08.2021).

[20] Власти Китая оштрафовали Alibaba на рекордные $2,8 млрд // РБК. Апрель 2021. — URL: https://www.rbc.ru/business/10/04/2021/607105959a79474ed9ff1073 (дата обращения: 11.08.2021).

[21] Winston Ma. Breaking the Big Tech Monopoly.Winter 2021. No. 18. P. 166–179.

выступили с собственными инициативами: Microsoft предложил Цифровую женевскую конвенцию и Технологическое соглашение по кибербезопасности (Cybersecurity Tech Accord), Siemens — Хартию доверия (Charter of Trust), Facebook — документ по регулированию контента (Charting the Way Forward: Online Content Regulation), Google — предложение по Модернизации стандартов трансграничного правительственного доступа в облачную эпоху (Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era) и т.д. Кроме того, многие транснациональные IT-компании, включая Microsoft, Huawei, Kaspersky Lab, Siemens, Google и другие активно принимают участие в Женевском Диалоге (Geneva Dialogue), запущенном весной 2018 г. На этой площадке обсуждают роли и обязанности стейкхолдеров в киберпространстве, а также построение стабильной и безопасной системы защиты в области киберпространства.

Причина такого изобилия инициатив по регулированию интернета со стороны крупного бизнеса понятна — бесконечные иски, скандалы, давление со стороны правительств, падение доверия пользователей.

Очевидно, что вопрос регулирования для IT-гигантов весьма чувствительный, особенно в том, что касается вопроса сохранения их status quo на рынке. Никто не хочет терять свое влияние и многомиллиардные прибыли.

Итак, сегодня мы наблюдаем глобальный тренд принятия регуляторами мер, направленных на сдерживание крупных IT-корпораций и их регулирование. В ближайшей перспективе можно спрогнозировать нешуточную борьбу между государствами и компаниями. Проблема усугубляется тем, что отсутствует эффективный механизм разрешения споров по линии государство — крупный бизнес.

В заключении стоит отметить, что глобальный бизнес действительно находится на грани, когда может своими действиями нарушить хрупкий баланс цифровой экосистемы. В погоне

за прибылью под удар ставится суверенитет государств, права человека, нарушаются условия свободной конкуренции. Как на правительственном уровне, так и на уровне обычных пользователей такая угроза ощущается. Нельзя забывать, что основная цель бизнеса — получение прибыли. Это указано в уставе любого предприятия. Поэтому регулирование цифрового пространства только технологическими корпорациями не допустимо. И в вопросах регулирование должны принимать равное участие все заинтересованные стороны. Бизнес-модель цифровых компаний должна меняться, стать более человекоцентричной и транспарентной, также должен быть соблюден трудный баланс между privacy и security, между свободой слова и опасным контентом.

Список использованных источников и литературы

1. Власти Китая оштрафовали Alibaba на рекордные $2,8 млрд // РБК. Апрель 2021. — URL: https://www.rbc.ru/business/10/04/2021/607105959a79474ed9ff1073 (дата обращения: 11.08.2021).
2. Европейская комиссия представила проект нового «цифрового законодательства» // Seldon news. Декабрь, 2019. — URL: https://news.myseldon.com/ru/news/index/242447002 (дата обращения: 11.08.2021).
3. Материалы RIGF. 8 апреля 2021. — URL: https://rigf.ru/press/?p=video&vid=b7zokhEq_uw (дата обращения: 11.08.2021).
4. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». — URL: https://sozd.duma.gov.ru/bill/223849-7 (дата обращения: 11.08.2021).
5. Сессия онлайн-форума «Давосская повестка дня 2021» // сайт Президента России — URL: http://www.kremlin.ru/events/president/news/64938 (дата обращения: 11.08.2021).
6. Стоимость пяти IT-гигантов США — $7 трлн. Больше, чем ВВП 16 стран G20 // РБК. Август, 2020. — URL: https://quote.rbc.ru/news/article/5f4363819a79479d6cdb08a1 (дата обращения: 11.08.2021).
7. США заявили, что присоединятся к международной инициативе по борьбе с экстремизмом в сети // ТАСС. 2021. Май. — URL: https://tass.ru/mezhdunarodnaya-panorama/11326177 (дата обращения: 11.08.2021).

8. Штраф за треш // Российская газета. Декабрь 2020. — URL: https://rg.ru/2020/12/23/socseti-s-1-fevralia-obiazali-blokirovat-zapreshchennyj-kontent.html (дата обращения: 11.08.2021).
9. Bryan Pietsch, Isobel Asher Hamilton, Katie Canales. What you need to know about Big Tech's Section 230 shield, the internet law that Trump hated and Biden might reform// Insider. Jul 8, 2021 — URL: https://www.businessinsider.com/what-is-section-230-internet-law-communications-decency-act-explained-2020-5 (дата обращения: 11.08.2021).
10. Gil Press. Facebook, Google, Apple, Other Data-Driven Firms, Defy The Global Move To Strong Privacy Regulations. Forbes. June 26, 2019 — URL: https://www.forbes.com/sites/gilpress/2019/06/26/facebook-google-apple-other-data-driven-firms-defy-the-global-move-to-strong-privacy-regulations/?sh=6a9261e71ae0 (дата обращения: 11.08.2021).
11. Speech by Federal Chancellor Dr Angela Merkel opening the 14th Annual Meeting of the Internet Governance Forum in Berlin on 26 November 2019 — URL: https://www.bundesregierung.de/breg-en/news/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-the-internet-governance-forum-in-berlin-on-26-november-2019-1701494 (дата обращения: 11.08.2021).
12. Winston Ma. Breaking the Big Tech Monopoly.Winter 2021. No. 18. P. 166–179.

А. В. Бирюков,
канд. ист. наук, ведущий научный сотрудник,
ведущий эксперт Центра международной информационной
безопасности и научно-технологической политики
МГИМО МИД России

ТЕХНОГУМАНИТАРНЫЙ ДИСБАЛАНС КАК УГРОЗА ЦИФРОВОЙ ЭПОХИ

Аннотация: статья посвящена анализу рисков техногуманитарного дисбаланса и основным угрозам, которые возникают при значительном разрыве между техническим процессом и низком уровне развития нравственного потенциала человечества. Рассматривается также вопрос создания суперинтеллекта и вызовов, связанных с этим явлением.

Именно сейчас в условиях развития цифровой эпохи происходит целый каскад глобальных процессов, связанных с экономической глобализацией и общественной информатизацией и возрастающим воздействием человека на гомеостаз биосферы Земли. На современном этапе наука анализирует формирование информационно-кибернетического пространства, лавинообразный рост информационного потока, быстрый рост «суммы цифровых технологий», и как следствие, становление гибридного мира в результате симбиоза реального и виртуального. К числу серьезных вызовов относится и рост геополитической напряженности на международном и региональном уровне, обусловленный множественными противоречиями, все более развивающимися в условиях расширения новых угроз и вызовов.

Ключевые слова: научно-технический прогресс, искусственный интеллект, технологическая сингулярность, социально-психологические проблемы.

Открывая юбилейную 75-ю сессию Генеральной ассамблеи ООН, генеральный секретарь этой организации Антониу Гутер-

риш перечислил основные угрозы международному сообществу на современном этапе, назвав их всадниками Апокалипсиса. К их числу им были отнесены и «темные стороны цифровых технологий»[22]. Понятно, этой метафорой Антониу Гутерриш обозначил негативные аспекты технологического прорыва, которые неоднократно проявлялись в контексте НТП. Однако риски и угрозы данного типа в основном обусловливались не природой технологий, а неадекватными действиями человека, который их создал. Именно от воли человека зависело, как будет использован потенциал технологии, будет она служить делу добра или превратиться в орудие сил зла. В этой связи в центре внимания постоянно находилась проблема ограждения технологий от «недобрых рук». Опыт функционирования МАГАТЭ, специализированной организации ООН, и неформального режима контроля за ракетными технологиями указывает на то, что проблема нераспространения двойных технологий и соблюдения норм и правил их адекватного использования требует внимания всего международного сообщества и должна регулироваться обязывающими международно-правовыми документами.

Всадником Апокалипсиса названы не просто негативные последствия НТП, о которых широко заговорили в связи с тем, что достижения науки, овеществленные в технологиях, время от времени попадают не адекватным людям. Оправданную озабоченность вызывает то, что в мире науки рождаются идеи, которые могут привести к появлению опасных неконтролируемых человеком технологий, чреватых масштабной гибелью людей. Например, в последние годы развивается технология генетического редактирования эмбрионов человека. Самую жесткую оценку этому технологическому феномену дал представитель

[22] UN chief outlines solutions to defeat 'four horsemen' threatening our global future // UN News. 22.01.2020. — URL: https://news.un.org/en/story/2020/01/1055791 (дата обращения: 12.08.2021).

американских спецслужб. Бывший директор Национальной разведки США Джеймс Клэппер в отчете 2016 года сравнил технологию геномного редактирования с «оружием массового уничтожения и распространения». Особенно его впечатлила опасность этой технологии в сочетании с её дешевизной[23]. Думается, что эта оценка перекликается с идеей опасной неконтролируемой технологии, которая может навлечь беду на человечество.

В чем суть идеи? Её изложил Ник Бостром, создатель Института будущего человечества Оксфордского университета и автор бестселлера «Супер-интеллект». Он выдвинул концепцию «черных технологических шаров в уязвимом мире», предложив уподобить человеческую историю процессу извлечения шаров из урны. В течение истории человечество извлекло очень много шаров в подавляющем большинстве белых, но можно вспомнить несколько случаев извлечения серых шаров типа ядерных технологий. Изучая, какие шары извлекались в процессе всемирной истории, нельзя не заметить, что человечество ни разу не получало «по жеребьевке» по-настоящему черный шар, который содержал бы технологию, безальтернативно и по умолчанию, разрушающую цивилизацию. Здесь важно обратить внимание на вроде бы неприметное словосочетание — по умолчанию. По логике шар с ядерной энергией дает возможность уничтожить человеческую цивилизацию. Но это не может произойти по умолчанию. Кто-то должен начать глобальную войну. А человеческая история показывает, что даже в самых критических ситуациях политическим лидерами хватало осторожности не запускать машину судного дня. Настоящий черный шар — это технология, которая сама по себе, в рамках саморазвития, незаметно, вследствие усилий различных не связанных между собой групп и команд, преследующих свои собственные интересы, способна до основания или в основном разрушить цивилиза-

[23] Елена Ларина, Владимир Овчинский. Черный шар и глобальная инквизиция Ника Бострома // Наш современник. 2019. № 2. С. 138.

цию. Технологии черного шара — это всегда технологии, каждый шаг развития которых сам по себе воспринимается обществом как достаточно безопасный. Однако, накапливаясь, эти шаги приводят к качественному скачку, переходу на другой уровень, который несет с собой экзистенциональные риски и смертельные угрозы.

Вспомнили о «черном технологическом шаре» в связи с тем, что человечество семимильными шагами движется в направлении технологической сингулярности, которая станет реальностью, по оценке компетентных специалистов, уже во второй половине XXI века. Превалирует точка зрения, что социально-экономический и научно-технический прогресс приобретает такую насыщенность и скорость, что человечество будет не в состоянии самостоятельно управлять этим процессом традиционным образом. Потребуется опора на искусственный супер-интеллект. Другая трактовка в смысловом отношении близка этому пониманию. Технологическая сингулярность обозначает точку в будущем, когда эволюция в результате развития искусственного интеллекта ускорится настолько, что дальнейшие изменения приведут к возникновению разума с гораздо более высоким уровнем быстродействия и новым качеством мышления. В связи с такой перспективой невольно возникает вопрос о том, что «черный технологический шар» возникнет в условиях технологической сингулярности и может быть связан с активностью искусственного интеллекта.

Западные эксперты исходят из того, что в XXI веке разум человека намного отстанет от искусственного интеллекта. Это верная оценка с точки зрения умения просчитывать варианты с помощью алгоритмов. В этом смысле прогноз Рэя Курцвейла о том, что искусственный интеллект усилит человека является правильным. Однако вряд ли искусственный интеллект заменит нас, несмотря на многочисленные и интересные публикации на эту тему. Более того вовсе не исключено, что гегемония искусственного интеллекта может стать главной угрозой человече-

ству[24]. В любом случае — произойдут радикальные открытия поведения и мышления человека с последующей разработкой высоких технологий или человечество втянется в реальности технологической сингулярности на основе искусственного интеллекта — подобные прогнозы означают, что человечество должно хорошенько подготовиться к апофеозу доминирования технологий в гибридном мире цифровой эпохи. На наш взгляд, именно в этом контексте будет происходить формирование адекватной паутины смыслов, в которой важное место может занять трансформация техногуманитарного дисбаланса в техногуманитарную гармонию. О чем идет речь?

Феномен многоаспектен. Фундаментальным фактором стала информационная лавина, накрывшая человечество. Накапливаются и обрабатываются большие данные, которые все чаще рассматриваются в качестве важнейшего сырья XXI века. Эффективно работать с таким массивом информации можно только с опорой на мощный искусственный интеллект. В этом контексте возникло явление информационного парадокса, когда в огромном объеме информации крайне сложно найти качественные объективные данные, востребованные человеком. Выросло целое поколение людей, не обладающих долговременной памятью[25]. Между тем творческие процессы базируются именно на долговременной памяти.

Международной проблемой стала цифровая зависимость людей. В цифровую эпоху они переходят от опоры на аналитическое системное мышление к восприятию информации с помощью главным образом зрительных образов. Такой переход обусловлен сбережением энергии мозга, который включается

[24] Nick Bostrom. Superintelligence: Paths, Dangers, Strategies. — URL: www.amazon.com (дата обращения: 11.08.2021).

[25] Курпатов А. Современный человек страдает от информационного ожирения // Вместе-РФ, 12.02.2020. — URL: https://vmeste-rf.tv/news/joyce-brothers-here-a-modern-person-is-suffering-from-information-obesity/ (дата обращения: 05.10.2020).

при решении сложных задач, а в остальных случаях «простаивает». Отсюда с неизбежностью следует задача примитивизации информации, доставляемой потребителю. В результате мозг «впадает в спячку». Формируется особенный способ поверхностного восприятия окружающего мира — клиповое мышление, которое становится инструментом легкой внушаемости и зависимости человека. Мир захватила эпидемия цифрового аутизма, то есть состояния, при котором молодые люди не могут поддерживать длительный психологический контакт друг с другом и нередко просто не интересуются внутренним миром другого человека. Среди людей распространяются болезненные состояния, именуемые цифровое слабоумие и информационное оглупление[26]. Перечисленные социально-психологические недуги людей информационного общества лечатся в условиях социализации, образования и воспитания, а также идеологии, основанной прежде всего на национальной истории и культуре. И в то же время они являются признаками деградации, которую необходимо преодолевать самым решительным образом.

Однако заметное влияние на человека оказывает и международная среда. В мире растет понимание, что основным источником прогрессивного движения является социально активный и ответственный человек, ориентированный на знания и инновации и являющийся членом коллектива, понимающий, что индивидуальный интерес играет подчиненную роль. При этом такой человек должен быть ответственным и перед самим собой, понимая, что его ценность связана с духовным богатством, которое в сочетании с интеллектом формирует целостную личность. Именно духовный подъем, эмоции и чувства, способность творить со страстью — делают человека человеком

[26] Подробно см.: Андрей Курпатов. Четвертая мировая война. Будущее уже рядом! СПБ: ООО «Дом Печати Издательства Книготорговли „Капитал“», 2019. С. 294–309.

и выходят за рамки возможностей всесильного искусственного интеллекта. Не случайно, Клаус Шваб значительную часть своих рассуждений о четвертой промышленной революции посвящает человеку, возрастающей роли общественных ценностей, важности постановки социально-гуманитарных интересов на первое место по сравнению с другими факторами развития. При этом мы понимаем, что взгляды К. Шваба далеки от марксизма.

Другой аспект обусловлен способом производства, в основе которого лежит не максимизация прибыли, а удовлетворение потребностей человека в гармонии с окружающей средой. Звучит как давно забытая социалистическая константа. Однако, думается, такая идея уже появилась при описании контекста индустрии 5.0. На первое место в ней выдвигаются оптимальное сочетание экономического развития с социальной и экологической задачами.

В рамках дискуссии на нашей секции можно высказать следующие соображения:

— Технологическая угроза реальна, а отношение к ней требует не только солидарности, но и консолидации действий государственных органов, представителей гражданского общества, ученых, деловых людей и лиц, отягощенных общественной деятельностью. Опыт РГОС в этом смысле имеет большое значение.
— Представители бизнеса обязаны держать в поле зрения возможность появления «черного технологического шара» и поддерживать контакт по этому вопросу с компетентными правительственными экспертами.
— Мощное акцентирование искусственного интеллекта в условиях технологической сингулярности происходит на фоне того, что современная наука не изучила мозг человека, его разум и сознание до такой степени, чтобы делать однозначную ставку только на искусственный интеллект. Потенциал человеческого разума не раскрыт и нет ясности его возможностей с точки зрения развития человечества.

— Благотворительное финансирование исследований в области человеческого интеллекта внесет вклад в развитие отечественной науки на этом самом перспективном направлении научных исследований.
— Признаки гуманитарной деградация имеют место. Этот вызов необходимо учитывать. Поэтому подготовка творческих кадров превращается в общественную заботу. В частности, на корпоративном уровне востребованы программы преодоления упомянутых болезненных состояний.
— Весь комплекс общественных отношений должен развиваться с опорой на социально активного, знающего, ориентированного на инновации и высокоморального человека. Альтернативой такому человеку могут стать киборги. Вряд ли такая перспектива устроит человечество…

Список использованных источников и литературы

1. Алборова М. Б. Человек в условиях киберНЕстабильности / М. Б. Алборова // Специальный выпуск журнала «Международная жизнь». Международная конференция «Киберстабильность: подходы, перспективы, вызовы». — Москва, 16–17 декабря 2019.
2. Бирюков, А. В. Международные научно-технологические отношения в цифровую эпоху. М.: Аспект Пресс, 2020. — 224 с.
3. Глазьев, С. Ю. Без восстановления справедливости распределения национального богатства Россию ждут деморализация и деградация производственного потенциала // Военно-промышленный курьер. 15.09.2020. — URL: https://www.vpk-news.ru/articles/58661 (дата обращения: 02.10.2020)
4. Голубев В. С. Человековедение — главная наука XXI века и ее значение для социогуманитарного просвещения // Производство, наука, образование: системный подход. М.: ИНИР им. Витте, 2018.
5. Емелин В. А. Идентичность в информационном обществе. М.: КАНОН, 2018. — 360 с.
6. Ильин И. Россия. Путь к возрождению / Под ред. Крыловой Е. // Рипол-Классик, 2017. — 768 с.

7. Климович А. Вопросы философии Больших данных // Инновации в науке. 2018. № 8 (84). — URL: https://cyberleninka.ru/article/n/voprosy-filosofii-bolshih-dannyh/viewer (дата обращения: 05.10.2020) .
8. Курпатов А. Четвертая мировая война. Будущее уже рядом! СПБ.: ООО «Дом Печати Издательства Книготорговли „Капитал“», 2019. — 158 с.
9. Ларина Елена, Овчинский Владимир. Чёрный шар и глобальная инквизиция Ника Бострома // Наш современник. 2019. Февраль. — URL: https://reading-hall.ru/publication.php?id=24905 (дата обращения: 05.10.2020).
10. UN chief outlines solutions to defeat 'four horsemen' threatening our global future // UN News, 22.01.2020 — URL: https://news.un.org/en/story/2020/01/1055791 (дата обращения: 12.08.2021).

М. Б. Алборова,
канд. ист. наук, ведущий эксперт
Центра международной информационной безопасности
и научно-технологической политики
МГИМО МИД России

ЦИФРОВИЗАЦИЯ ОБЩЕСТВА 5.0 — СОЦИОГУМАНИТАРНЫЕ И ЭКОНОМИЧЕСКИЕ РИСКИ

Аннотация: в статье рассматриваются особенности вызовов и рисков цифровой трансформации современного общества. Автор анализирует современные проблемы становления и развития информационного общества. Особое внимание уделено социально-экономическим рискам, которые оказывают многостороннее влияние на изменения в различных сферах общества XXI века.

Ключевые слова: цифровое общество 5.0, инновационное развитие, трансформация общественных отношений, цифровые разрывы, постиндустриальное общество.

Современное постиндустриальное общество сформировало новые направления развития всех сфер деятельности человека. Активно внедряющиеся инновации и распространение механизмов цифровой экономики сформировали основы для становления информационной цивилизации. Процесс информатизации общества — закономерное следствие глобального развития человечества, который обусловлен целым рядом объективных факторов. Постепенно формируется и новое цифровое общество 5.0., которое акцентирует внимание на создании инновационно мыслящего поколения. Фактически складываются условия для глобальной трансформации социально-экономических основ посредством использования

цифровых технологий, таких, как Big Data, интернет вещей или искусственный интеллект[27].

Именно сегодня ускоряется и возрастает сложность искусственно создаваемой человеком среды своего обитания — техносферы, при этом мы видим не только усложнение системы, но и ее ненадежность, поскольку риски и вызовы современной цивилизации увеличились многократно. На этом фоне все больше человечество сталкивается с проблемой истощения природных ресурсов мира, в связи с этим сильнее возрастает необходимость отказа от господствующей длительное время тенденции экстенсивного развития цивилизации и перехода к новому инновационному типу развития. Исчерпание ресурсов и усложнение эффективного использования интеллектуального и физического человеческого потенциала приводит к потребности пересмотра цивилизационного подхода и выработке новых направлений устойчивого и безопасного развития человечества[28]. Активное применение научных технологий и инноваций может позволить сформировать новые условия для обновления экономической инфраструктуры, решения многих ресурсных и экологических вопросов.

Но при переходе к новому формату инновационного общества, необходимо решить накопленные проблемы, переосмыслить и принять решения для реагирования на риски. К таким рискам относятся:

— снижение уровня образования основной массы населения;
— неспособность использовать и обслуживать новые эффективные технологии;
— экономическая отсталость многих стран, резкая стратификация и маргинализация населения;
— низкий уровень здравоохранения и высокая смертность населения;

[27] Бирюков А. В. Международные научно-технологические отношения в цифровую эпоху. М.: Аспект Пресс, 2020.

[28] Елена Ларина, Владимир Овчинский. Чёрный шар и глобальная инквизиция Ника Бострома // Наш современник. 2019.

— снижение уровня рождаемости в ведущих технологических странах.

Все эти риски необходимо учитывать при активном построении нового человекоцентичного общества. Сегодня человечество с одной стороны сталкивается со значительными рисками, с другой стороны, получает большие возможности и от того, как оно распорядится этими возможностями будет зависеть будущее всего человечества. Поэтому столь актуальны вопросы нового технологического социально-ориентированного развития.

Глобальные изменения коснуться всех сфер жизни и будут формировать новую ступень развития цивилизации. Цифровая экономика, способствующая ускоренному развитию многих процессов, формирует основания и для становления общества 5.0. Вместе с тем, современный мир технологий — это и вопрос резкого увеличения рисков, и обострение проблемы обеспечения безопасности как нашей страны, так и мира в целом.

Эффективная политическая система, ориентированная на достижение национального интереса, приоритетно должна быть сконцентрирована на развитии технической сферы и повышении уровня образования национальных кадров России, которая за собой поведет и эволюцию всех систем общественных отношений.

На современном этапе, а особенно в условиях кризиса 2021 года инвестиции в новый технологический капитал необходимы. В рамках подобного подхода к развитию общества эксперты все активнее говорят о необходимости срочного создания новых центров сверхиндустриализации, инвестиций в фундаментальную науку, расширения активных малых и средних предприятий, такие инвестиции могут совмещать в себе и силу государства, и возможности предпринимательства, создавая условия для расширения государственно-частного партнерства.

Все большее распространение технократического подхода свидетельствует об объективном вовлечении человека в инновационную технологическую эру, объективное развитие техники

имеет активный, стремительный, отчасти агрессивный характер. Новая цивилизация диктует и новые требования к интеллектуализации всего общества. Базой для современной и будущей информационной экономической системы становятся накопленные знания или интеллектуально-информационный ресурс.

Важно еще раз акцентировать внимание на реализации значимых слагаемых развития инновационного общества:

— разработке и внедрении передовых информационных технологий с одновременным обеспечением безопасности;
— создании новых рабочих мест в сфере инновационных технологий;
— повышении уровня конкурентоспособности на международной арене;
— анализе социальных преобразований и формирования стратегических предложений для повышения жизненного уровня граждан страны;
— формировании условий для реализации возможностей человека, повышении его образования, воплощения его творческих замыслов.

Современная цифровая трансформация — это внедрение цифровых технологий как в государственные управленческие процессы, так и в бизнес-структуры социально-экономических систем всех уровней. Этот подход подразумевает фундаментальные изменения в подходах к управлению, корпоративной культуре, внешних коммуникациях. В результате изменяются многие аспекты развития общества, создаются условия для повышения эффективности каждого. Таким образом, цифровая трансформация предполагает фундаментальное переосмысление того, как работает общество, какие новые возможности будут реализованы, как создать условия для подготовки кадров и повышения уровня конкурентоспособности.

Социальные последствия глобального научно-технического прогресса, который заложен в основании современных изменений, неоднозначны. Сегодня запущены механизмы форми-

рования мирового технологического пространства, которые придали ускорение изменениям во всех сферах деятельности человека. Исследование процессов влияния этих изменений на общество может позволить человечеству сформировать условия для эффективного перехода к устойчивому развитию общества, даст время для определения стратегических перспектив.

Список использованных источников и литературы

1. Алборова М. Б. Человек в условиях киберНЕстабильности / М. Б. Алборова // Специальный выпуск журнала «Международная жизнь». Международная конференция «Киберстабильность: подходы, перспективы, вызовы». — Москва, 16–17 декабря 2019.
2. Бирюков А. В., Алборова М. Б. Переход от техногуманитарного дисбаланса к техногуманитарной гармонии как вызов информационного общества / А. В. Бирюков, М. Б. Алборова // Журнал «Глобальный научный потенциал». — № 12 (117). 2020.
3. Бирюков А. В. К вопросу о влиянии научно-технического прогресса на международные отношения в цифровую эпоху. // Ежегодник ИМИ, 2015, № 3. М.: ИМИ МГИМО МИД России, 2015.
4. Булва В. И. Манипулирование общественным сознанием — вызов информационного общества // Международная информационная безопасность: новая геополитическая реальность / Под ред. Е. С. Зиновьевой, М. Б. Алборовой — М.: Издательство «Аспект Пресс», 2021.
5. Зиновьева Е. С. Цифровая дипломатия, международная безопасность и возможности для России // Индекс безопасности. № 1 (104). — Том 19. — с. 217 — URL: http://www.pircenter.org/media/content/files/10/13559069820.pdf (дата обращения: 25.03.2021).
6. Зинченко А. В. «Архитектоника международной информационной безопасности» М..Издательство «Аспект-Пресс». 2021. — 160с.
7. Цыганов В. В., Бирюков А. В. Этический императив международных научно-технологических отношений: взгляд из России / Труды 18-й межд. конф. Цивилизация знаний: российские реалии. М.: РосНоУ, 2017.

С. Ю. Перцева,
канд. экон. наук, доцент кафедры международных финансов
МГИМО МИД России

ГЛОБАЛЬНАЯ ЦИФРОВАЯ ВАЛЮТА: ВОЗМОЖНОСТИ И УГРОЗЫ

Аннотация: в статье рассматриваются теоретические аспекты цифровой трансформации мировой валютной системы. Автор анализирует современные проблемы глобальных финансовых отношений, предпосылки и необходимость реформирования международных валютно-кредитных отношений. Особое внимание уделено реализации проекта создания цифровой наднациональной валюты на основе анализа возможностей и угроз. Изучен Доклад Совета по финансовой стабильности о регулировании, управлении и надзоре за мероприятиями по подготовке к внедрению глобального стейблкойна.

Ключевые слова: мировая валютная системы, цифровая валюта центрального банка, глобальный стейблкойн.

Научное и экспертное сообщество сегодня все чаще говорит о необходимости реформирования мировой валютной системы. Основной причиной этого являются имеющиеся противоречия современных международных валютно-финансовых отношений, к которым можно отнести:

1) неспособность СДР, вследствие особенностей расчёта этой счетной единицы на основе корзины валют и эмиссии, выполнять роль резервного актива;
2) неустойчивость плавающих курсов вследствие трансграничного движения спекулятивного капитала («горячих денег»);
3) фактическое сохранение за золотом роли резервного актива.

Следует отметить, что в течение более 70 лет роль наиболее используемой валюты в международных расчетах принадлежит доллару США, который признается мировой валютой. То есть

валютой, используемой в мировом обороте и выполняющей функции интернациональной меры стоимости (валюты цены в контракте), международного платежного средства (при международных расчетах), международного резервного средства (при формировании резервов и накоплений). Для признания валюты мировой, необходимо соблюдение таких условий, как участие в мировом торговом обороте, осуществление сделок финансового сектора и включение в структуру частных и официальных резервных активов иностранных государств.

Роль доллара США в текущий момент можно охарактеризовать следующим образом:

— основные объемы операций в мировой торговле, на мировом рынке FOREX осуществляются в долларах;
— доллар остается относительно стабильным в периоды кризисных явлений в мировой экономике в 2000–2002 гг. и в 2007–2008 гг., в 2020 г.;
— доллар широко используется в качестве резервного актива резидентами стран с переходной экономикой и развивающихся стран;
— долларизация приводит к росту эмиссионного дохода (сеньоража), получаемого США.

Следует обратить внимание на факторы, которые могут привести к неустойчивости доллара в среднесрочной перспективе:

— дефицит торгового баланса США (–63,9 млрд долл. на 01.10.2020)[29];
— дефицит федерального бюджета США (3 трлн долл.)[30];
— рост государственного и частного долга США (80 трлн долл.)[31];
— тенденция к расширению использования евро (на 01.11.2020 доля евро составила 37,82%, доля доллара — 37, 64%)[32];
— диджитализация валютно-финансовых отношений.

[29] U.S. Bureau of Economic Analysis
[30] BEA. Federal Reserve
[31] IIF
[32] SWIFT

Переход к наднациональной валюте предполагает потерю национальными государствами важной части суверенитета, — проведения денежно-кредитной политики в целях стимулирования экономического роста и повышения занятости.

Опыт европейских стран, в частности, Италии, Испании, Португалии, Греции показывает: утрата возможности проведения национальной денежно-кредитной политики лишает государства основного инструмента преодоления кризисных явлений в экономике.

А. Гринспен предложил ряд критериев для придания валюте статуса резервной (полагаем, что данные критерии верны и для наднациональной валюты)[33]:

1) устойчивость валюты и предсказуемость ее курса в кратко, — средне и долгосрочной перспективах;
2) открытость и развитость финансовой системы: финансовых рынков, инфраструктуры, эффективных и безопасных платежных систем;
3) эмитент валюты должен обладать сильной, конкурентной экономикой, открытой для совершения значительного числа международных транзакций, что повышает ее ликвидность.

В научной литературе под наднациональной валютой принято понимать денежную единицу, не являющуюся национальной валютой какой-либо страны, предназначенную для международных расчетов, использования в качестве резервного средства и для операций на финансовом рынке, эмитируемую наднациональным институтом.

Научный поиск в направлении создания и внедрения наднациональной валюты ведется достаточно активно. Правительства разных стран заявляют о необходимости проведения политики глобальной дедолларизации. В настоящее время, в эпоху стремительного развития цифровых технологий и их проникнове-

[33] Greenspan A. The Euro as an International Currency. Remarks Before the Euro 50 Group Roundtable. — Washington, D.C., 2001, November 30.

ния в финансовую сферу появляются идеи создания глобальной виртуальной валюты, основанной на технологии блокчейн.

Активно ведутся исследования по разработке центральными банками стран мира цифровых валют. По данным Банка международных расчетов 80% центробанков изучают и прорабатывают механизмы внедрения национальных цифровых валют. Пилотные проекты были запущены центральными банками Швеции, Уругвая, Канады, Китая. На стадии исследования и общественного обсуждения данные проекты находятся в России, Еврозоне, США.

Согласно Банку международных расчетов, цифровые валюты центральных банков (CBDC — Central Bank Digital Currency) — это электронное обязательство монетарного регулятора, номинированное в национальной счетной единице и выполняющее функции денег.

В научной литературе, выделяют преимущества CBDC (табл. 1).

Наряду с преимуществами цифровых валют центральных банков у данных проектов имеются и существенные недостатки, к которым можно отнести:

— значительную капиталоемкость, обусловливающую высокие затраты на инфраструктуру, новые технологии и защиту от киберрисков;
— необходимость трансформации традиционных для банков бизнес-моделей в отношении работы с клиентами, предоставления отчетности и взаимодействия с регулятором и др.

Высокий уровень внимания со стороны стран обусловлен проводимыми исследованиями в сфере внедрения национальных цифровых валют. Можно выделить два основных аспекта деятельности государств в данном направлении: масштаб исследований и реализация проектов, в том числе в тестовом режиме.

По данным Банка международных расчетов, в конце первого полугодия 2020 г. 36 центральных банков мира опубликовали работы, в которых рассматриваются розничные или оптовые

Таблица 1

Преимущества реализации проектов цифровых валют центральных банков

№	Преимущество	Характеристика
1.	Повышение стабильности и конкуренции в финансовой сфере	Усилится соперничество банков с технологическими компаниями, в том числе с глобальными игроками — BigTech, а также виртуальными валютами, широко представленными на криптовалютном рынке (более 4000 наименований) [9]
2.	Увеличение финансовой инклюзивности	Возрастет вовлеченность субъектов экономики в финансовую систему путем роста ее доступности, в том числе за счет внедрения платежной инфраструктуры с меньшими затратами на денежные переводы. Кроме того, монетарные власти получат дополнительные возможности для усиления прозрачности и контроля за операциями
3.	Расширение инструментов фискальной политики	Программируемость, прогнозируемость и прозрачность национальных цифровых валют обусловит усиление контроля за денежно-кредитной системой, увеличит прозрачность информационных потоков
4.	Стимулирование использования национальной цифровой валюты для розничных и оптовых платежей	Правительства стран получат дополнительную возможность эффективно реализовать политику дедолларизации

№	Преимущество	Характеристика
5.	Внедрение коммерческих CBDC (только для банков)	Позволит снизить расчетные риски, обеспечить круглосуточный доступ к ликвидности для банков и сократить издержки при трансграничных переводах

Источник: составлено автором на основе: https://forklog.com/chto-takoe-tsifrovaya-valyuta-tsentrobankov-cbdc/

цифровые валюты. При этом три страны (Уругвай, Эквадор и Украина) завершили пилотные проекты розничных цифровых валют. Аналогичные пилотные проекты реализуются в Швеции, Южной Корее, Восточно-Карибском валютном союзе, на Багамских Островах, в КНР и в Камбодже.

Стоит отметить, что идея получения стейблкоином статуса наднациональной валюты серьёзно рассматривается экспертным и научным сообществом. Так, 13 октября 2020 г. вышел документ с отчётом и рекомендациями Совета по финансовой стабильности G20 «Регулирование, управление и надзор за мероприятиями по подготовке к появлению «глобального стэйблкоина» (англ. «Regulation, Supervision and Oversight of «Global Stablecoin» Arrangements»), в котором стейблкоин рассматривается в качестве потенциальной наднациональной валюты.

Совет по финансовой стабильности предложил свое видение места стейблкоинов в системе международных финансов. Позиция авторов документа сводится к следующему: стейблкоины (stablecoins) признаны видом цифровых активов (digital assets), а глобальные стейблкоины (global stablecoins), в свою очередь, являются видом стейблкоинов. От иных видов цифровых активов (к примеру, криптовалют) стейблкоин отличают особые стабилизационные механизмы, которые позволяют снизить волатильность данного актива.

Эксперты G20 отмечают две возможные разновидности стабилизации. Первая — это «привязка» стейблкоинов к базовому

активу (например, к национальной фиатной валюте, к товарам, к другим видам цифровых активов). Вторая — алгоритмическая стабилизация через применение специальных протоколов, которые при изменении спроса/предложения обеспечивают поддержание их стоимости.

Нужно подчеркнуть, что на данном этапе глобальным стэйблкоином называется не повсеместно используемый стэйблкоин, а лишь тот, который потенциально имеет шансы приобрести существенный вес в мировой финансовой системе. В соответствии с документом, к возможным критериям, определяющим глобальный стэйблкоин относятся:

1) число и классификация пользователей;
2) стоимость и объём транзакций;
3) качество и объём резервных активов;
4) суммарная стоимость стэйблкоинов в обращении;
5) доля рынка в международных платежах и переводах;
6) количество юрисдикций, признающих использование данной валюты;
7) доля рынка, приходящаяся на каждую юрисдикцию;
8) взаимосвязь с финансовыми институтами и компаниями BigTech;
9) интеграция с цифровыми сервисами и платформами;
10) структурная и операционная сложность и др.

В документе «Регулирование, управление и надзор за мероприятиями по подготовке к появлению «глобального стэйблкоина» рассматриваются потенциальные риски. Можно предположить, что полностью избавиться от волатильности стейблкоина вряд ли удастся. Следовательно, в случае превращения такого актива в массовое средство сбережения, любое колебание его стоимости будет существенно отражаться на благосостоянии пользователей. Также необходимо обратить внимание на «проблему доверия» не только к самому активу, но и к финансовой системе в целом, ввиду наличия технологических и инфраструктурных рисков эмиссии и оборота стейблкоинов.

«Глобальности» стейблкоинам добавляет значительный объем выпуска, влияющий на их способность обращаться в нескольких юрисдикциях. К этой трактовке можно придраться, поскольку невещественный характер стейблкоинов и их присутствие в информационных сетях сами по себе предполагают, что данное цифровое средство априори имеет все шансы для беспрепятственного выхода за пределы национальных юрисдикций. В этом контексте глобальность важна, в первую очередь, для обозначения рисков, с которыми в очередной раз странам придется справляться общими усилиями.

Таким образом, превращение стейблкоина в широко применяемое средство обмена или сбережения несет в себе риски в области защиты прав инвесторов и потребителей, защиты данных, противодействия отмыванию денег и финансированию терроризма. В целом, это весьма типичный «набор» побочных эффектов, характерный для любого финансового инструмента эпохи 4.0.

Так, согласно документу, можно выделить следующие трудности принятия единой виртуальной валюты.

1. Единство регулирования на мировом уровне (необходимость поиска компромисса).
2. Кто будет эмитировать? Где?
3. К какому/им активу/ам привязывать?
4. Каким образом будет обеспечиваться стабильность, с помощью какого механизма: алгоритма/ привязки к активу?
5. Как классифицировать: средство платежа/ сберегательный актив? Под какие нормы регулирования относить, чтобы все функции оказались законодательно утвержденными?
6. Единая классификация на международном уровне.
7. Организация регулирования и контроля на национальном уровне и др.

В рекомендациях по регулированию «глобальных стейблкойнов», опубликованных 13.10.2020 показано, что на сегодняшний день в различных юрисдикциях предложено для стейблкойнов

13 правовых режимов от признания криптовалютой, до финансового инструмента и цифрового актива.

Согласно документу «Регулирование, управление и надзор за мероприятиями по подготовке к появлению «глобального стэйблкоина», глобальные стейблкоины отличают три ключевые характеристики: огромное число пользователей, участие в их выпуске компаний BigTech (Google, Apple, Amazon, Facebook) и широкое использование в международных платежах и переводах.

Международное сотрудничество в данной сфере необходимо для минимизации рисков и создания более совершенного и эффективного механизма регулирования глобальной цифровой валюты.

В качестве рисков, связанных с принятием глобального стейблкоина, в документе рассматривались следующие+

1. Связанные с организацией контроля: мошенничество и конфликт интересов управляющих структур; недостаток закреплённых договорённостей между ними; неопределённость, связанная с трудностями классификации и определением соответствующих контролирующих структур; неподходящие государственная форма классификации и подход к регулированию; отсутствие центрального ответственного института.
2. Связанные с выпуском и изъятием валюты: невозможность резкого «погашения» валюты в сжатые сроки; при алгоритмической системе изменения количества стейблкоинов — сбои в работе алгоритма, которые могут сказаться на ценности валюты.
3. Связанные с управлением резервными активами: резкое падение цены или ликвидности резервного/х актива/ов; недостаточная прозрачность резервных активов; мошенничество или ненадлежащее управление резервными активами; инвестирование в неликвидные активы; значительно увеличение волатильности резервных активов.

4. Связанные с ответственным хранением резервных активов: мошенничество, межстрановая организация, неясность в отношении прав на резервные активы (в особенности, когда сталкиваются правовые системы нескольких стран).
5. Связанные с организацией инфраструктуры: сбои в системе, которые могут повлиять на ценность стейблкоина (кибератака); неясность относительно возможности отзыва операции.
6. Связанные с признанием действительности операций: несколько узлов валидации и их сопряженность.
7. Связанные с хранением ключей доступа к валюте (цифровые кошельки): кража/ взлом, потеря в результате киберинцидента; непосредственная утеря ключей.
8. Связанные с обменом, торговлей, перепродажей и рыночной оценкой валюты: киберинциденты, мошенничество, сбои в работе системы, несанкционированные операции, манипуляция рынком и т.д.

Стоит отметить, что в документе не приводятся преимущества стейблкоина по сравнению с обычными валютами. Однако даются рекомендации правительствам стран по принятию необходимых мер в общем виде: обеспечить всесторонний контроль; определить ответственные институты; функции, попадающие в сферу контроля одного института, передать в его ведение, законодательно это оформить; выявить новые функции стейблкоина, не попадающие под юрисдикцию уже существующих институтов, обеспечить их регуляцию; определить в каких сферах происходит наложение одних правовых норм на другие, приводя к противоречиям и предоставлению возможности для мошенничества; усилить взаимодействие всех контролирующих органов. Эти рекомендации предписываются наднациональным институтам. На международном уровне необходимо прийти к взаимопониманию, разработать единые нормы и классификацию, заключить соответствующие соглашения.

В пользу того, что наднациональная виртуальная валюта вполне реальна, говорит тот факт, что наднациональные инсти-

туты начинают работу по её изучению, проработке механизмов контроля, подготовке рекомендаций. Так, согласно анализируемого документа, разработана дорожная карта проекта.

1. К декабрю 2021 г. такие организации, как Комитет по платежам и рыночным инфраструктурам, Группа разработки финансовых мер борьбы с отмыванием денег и финансированием терроризма, Международная организация комиссий по ценным бумагам, Базельский комитет по банковскому надзору, должны завершить пересмотр существующих стандартов и принципов и предоставить дальнейшие указания по их дополнению в случае необходимости.

К тому же сроку национальным правительствам рекомендуется принять или дополнить меры и механизмы регулирования глобальных стейблкоинов с ориентацией на те стейблкоины, которые имеют потенциал стать глобальными.

2. К июлю 2022 г. предполагается, что национальные стандарты будут изменены уже в соответствии с новыми рекомендациями Совета по финансовой стабильности, международными стандартами и указаниями наднациональных институтов.
3. с января 2022 г. по июль 2023 г. будут проводиться обсуждения Совета по финансовой стабильности с другими институтами касательно выявленных нерегулируемых аспектов применения глобального стейблкоина, будет рассматриваться возможность применения уже существующих механизмов. В случае необходимости будет произведено обновление ранее изданных рекомендаций.

Примиряя между собой различные подходы и взгляды, Совет описал несколько базовых ориентиров, которым национальным регуляторам стоило бы следовать. Действительно, при выработке единого подхода в области регулирования стейблкоинов было бы полезно создать адекватную рискам регуляторную среду; учесть стандарты авторитетных международных организаций (BCBS, FATF, IOSCO и др.); а также дать потенциальным обла-

дателям данного криптоактива полную информацию, как он функционирует и каким образом обеспечивается стабильность его цены. Для этого правительства должны досконально разобраться в цифровой сущности стейблкоина, не отрицая, но и не переоценивая его потенциал. Вероятно, только гибкость и готовность финансовых регуляторов к изменениям помогут им развенчать мифы и примириться с новой реальностью, в которой есть место не только наднациональной виртуальной валюте, но и еще более прогрессивным финансовым явлениям.

Таким образом, мировая валютная система подвержена значительным изменениям. Глобальная цифровизация неминуемо движется, хотя и не быстрыми, но весьма уверенными темпами. Процесс запущен, и вряд ли будет остановлен.

Список использованных источников и литературы

1. Международные финансы: учебник и практикум для вузов / В. Д. Миловидов и др.; отв.ред. В. Д. Миловидов, К. Е. Мануйлов. — Москва: Юрайт, 2020.
2. Перцева С. Ю. Криптоиндустрия и платежные системы / С. Ю. Перцева // Государственный советник. 2019. №2 (26).
3. Платежные системы в условиях цифровой экономики: учебное пособие // С. Ю. Перцева— Москва: МГИМО–Университет, 2019.
4. Greenspan A. The Euro as an International Currency. Remarks Before the Euro 50 Group Roundtable. — Washington, D.C., 2001, November 30.

В. Н. Осташкин,
д-р ист. наук, профессор, преподаватель
кафедры №19 (педагогики) Военного университета

НЕКОТОРЫЕ АСПЕКТЫ ВОСПИТАТЕЛЬНОЙ РАБОТЫ С ВОЕННОСЛУЖАЩИМИ АРМИИ И ФЛОТА В УСЛОВИЯХ СОВРЕМЕННОЙ ГИБРИДНОЙ ВОЙНЫ

Аннотация: в статье рассматривается значимость памятных исторических дат, необходимость приобщения молодежи к истории и традициям нашего народа, его духовно-нравственным корням в социальном обустройстве и организации хозяйственной жизни в условиях современной гибридной войны.

Ключевые слова: противостояние мировых держав, информационное пространство, информационное воздействие на военнослужащих Вооруженных Сил РФ.

США переходят от тактики сдерживания гибридных атак
к наступательным действиям во всех сферах: военной,
дипломатической, информационной, экономической.
Волна мирового хаоса может перехлестнуть наши
границы и разрушить Российское государство.

Андрей Ильницкий,
советник министра обороны РФ

2021 год достаточно богат историческими датами и юбилеями. Это 800-летие со дня рождения Александра Невского, 160-летие отмены крепостного права в России, 80-летие начала Великой Отечественной войны и много других важных дат в жизни Российской Федерации. Особое место в этой связи занимает исторический опыт общественного развития страны. Автор исходит из непреходящей значимости памятных исторических дат, необходимости приобщения современной

российской молодежи к истории и традициям нашего народа, его духовно-нравственным корням в социальном обустройстве и организации хозяйственной жизни.

В рамках международного военно-технического форума «Армия — 2020» совместно с представителями Минобороны России и экспертного сообщества были обсуждены вопросы психологической обороны в условиях современной гибридной войны, а также необходимость сохранения исторической правды прошлого нашего государства в ходе круглого стола «Психологическая оборона. Борьба за историю — борьба за будущее». На этом форуме был определен образ Вооруженных Сил РФ в современном обществе нашего Отечества, а также принята резолюция круглого стола, которая должна определить дальнейшие направления деятельности по продвижению нашей правды в российском обществе и за рубежом.

Необходимо подчеркнуть, что первый замминистра обороны России Руслан Цаликов констатировал, что сегодня против России идет информационная борьба, хотя нет ни одного аргумента, который можно было бы представить на суд широкой общественности. «Наши успехи и есть предмет атаки наших оппонентов. Причем мы себе такое поведение не позволяем, — подчеркнул он, — хотим мы того или не хотим, но невозможно не признать, что за последние годы сформировался позитивный образ армии в обществе. Об этом говорят цифры. Народ в свою армию поверил».

Вместе с тем, по мнению автора, вышеназванные памятные исторические даты станут объектом критики и лжи со стороны западных СМИ, и не только в текущем году. Это прогнозируемая автором тематика для современной гибридной войны, во многом основанной на русофобии, все чаще реализуемой в западном мире.

Особое значение для россиян и Вооруженных Сил РФ имеет 80-летие начала Великой Отечественной войны, уроки которой не потеряли своего значения и для современной военно-политической обстановки.

Анализ отношений между Россией и странами Запада — членами блока НАТО показывает, что мы находимся не просто в очень сложных отношениях, а практически в состоянии относительно нового вида войны — войны гибридной, которая во многом может заложить основы для полноценного противостояния на мировой арене.

13 апреля 2021 г. замглавы МИД России Сергей Рябков впервые за всю постсоветскую историю назвал США противником России: «США являются нашим противником, делают все для того, чтобы подорвать позиции России на международной арене, других элементов в их подходе к нам мы не видим».

Противник — военный термин, который используется для обозначения противостоящего в военных действиях государства или союза государств и его сил. Раз так, то нам надо руководствоваться известным выражением: «alager com alager» (на войне как на войне).

С чего, по мнению автора, необходимо начать воспитательную работу в Вооруженных Силах, которые являются частью российского общества?

Во-первых, необходимо признать серьёзность ситуации. Против нас системно, последовательно и настойчиво работает противник, имеющий свою пятую колонну и агентов влияния и внутри нашей страны. Его агрессивные информационно-гибридные действия прежде всего направлены на:

— институты государственной власти России, Президента РФ, а точнее на Владимира Путина персонально;
— срыв или дискредитацию выборных кампаний различного уровня в единый день голосования 19 сентября, включая выборы депутатов Государственной Думы, 12 глав субъектов Федерации (9 прямых, а также 3 через голосование) и выборы депутатов законодательных органов государственной власти в 39 субъектах РФ;
— Вооруженные Силы и силовые структуры России в целом и на их руководство персонально;

— традиционные религии, находящиеся на территории России;
— межнациональное общение народов РФ;
— российскую молодёжь.

Автор разделяет точку зрения исследователей, о том, что по выборам, молодёжи, церкви, силовым структурам и Президенту системная атака уже ведётся, а действия против Вооруженных Сил России только разворачиваются.

Во-вторых, в информационной войне существует только одна тактика победы — это наступление. Для отражения агрессивных атак на наше государство необходимо сбить повестку врагов и перехватить инициативу.

В этом плане напрашивается историческая аналогия с Великой Отечественной войной 1941–1945 гг., которая началась 80 лет назад. А если сегодня ведутся военные действия, пусть и в гибридной войне, то, по мнению автора, мы находимся в полушаге от «горячей» войны и тут возникает достаточно много вопросов.

Россия находится в жестокой конфронтации с США. Угрозы нашей стране будут носить экзистенциальный характер. И не случайно в феврале 2021 года о возможности ядерной войны с Россией или Китаем заявил глава Стратегического командования США адмирал Чарльз Ричард. Он отметил, что впервые после распада СССР Пентагон рассматривает вероятность прямого конфликта и военного столкновения с ядерной державой. «Китай представляет растущий вызов, Россия является угрозой на многих фронтах…», — заявил адмирал — помощник министра обороны США Джон Кирби.

В-третьих, необходимо определиться: что это за война, какие цели преследует противник, на каком этапе войны мы находимся.

По мнению автора, сейчас происходит первый этап Второй Великой Отечественной войны. Этот этап современной, пока ещё гибридной, войны удивительно совпадает с первым этапом Великой Отечественной войны 1941–1945 гг., когда РККА отступала. Сегодня мы тоже не только отступаем в гибридной войне, но и фактически отдали инициативу в руки противника.

В этом плане показателен опыт советско-финской войны, которая была короткой, но далеко не такой победоносной, как хотелось бы, но она была очень важной, т.к. многому научила политическое и военное руководство СССР. Эта война помогла избавиться от иллюзий, что «Красная армия всех сильней», появилась политическая воля для начала активной работы по подготовке к войне с фашизмом и нацизмом. Но есть малое замечание по сегодняшнему дню: у РФ нет времени «на раскачку», как это было в 1940–1941 гг., т.к. время стало важным фактором ведения современной войны.

У каждого из противников есть свои особенности, специфика, которую надо учитывать в гибридной войне. Против России активно действуют и США, они уверенно занимают первое место не только по экономическим возможностям, но и по военному потенциалу.

По мнению автора, мы уже опаздываем в определении США как «империи лжи и насилия». Необходимо исправить это отставание и подкрепить другими аспектами информационной войны. На современном этапе распространение фейковой информации, направленной на дискредитацию нашей страны, имеет лавинообразный характер.

За свою 230-летнюю историю США применяли военную силу более 240 раз — т.е. чаще, чем ежегодно[34]. Неудивительно, что американские военные, политики и дипломаты в вопросах «войны и мира» неоднократно применяли систему подмены понятий, причем делали это вполне сознательно.

5 февраля 2003 г. тогдашний Госсекретарь США Колин Пауэлл[35] выступил в Совете Безопасности ООН с обоснованием

[34] Алексей Зыков. URL: https:// vk.com/away.php?to=https%3A%2F%2Friafan.ru%2Fp%2F997502&post =93976686_1914&cc_key=z (дата обращения: 11.08.2021).

[35] Американский политический деятель и генерал армии США, Государственный секретарь в период первого срока президентства Джорджа Уокера Буша. В 1987–1989 годах был советником по национальной безопасности в администрации президента Рональда Рейгана,

необходимости начала новой войны против Ирака. В своей речи он сослался на «полученную из первых рук информацию о заводах на колесах и на рельсах по производству биологического оружия», добавив, что источник является свидетелем, так как он «сам руководил одним из таких предприятий».

Во время этого выступления Пауэлл потрясал знаменитой «пробиркой с белым порошком». По его словам, она была эквивалентна количеству спор сибирской язвы, с помощью которых можно убить небольшой город. Впоследствии Пауэлл назовет эту пробирку «полемическим приемом в выступлении» и скажет, что в ней, конечно же, был инертное и безопасное вещество. Это яркий и незабываемый пример того, как «Большая американская ложь» может начать и временно оправдать любую войну. Но, как показывает практика, с ней невозможно жить вечно.

Но вернемся к событиям внутри России.

По мнению автора, необходимо в кратчайшие сроки:

— вернуться к той системе воспитания молодого поколения в средних учебных заведениях и вузах, остатки которой были ещё в начале XXI в., когда существовала структура, занимающаяся воспитанием подрастающего поколения и которая вдруг стала ненужной для современной России. При этом необходимо четко увидеть причины такого преступного решения для дела воспитания подрастающего поколения, в результате которого, по мнению автора, выросло целое поколение не разделяющих идей патриотизма;
— требуется реализовать грамотный подход преподавания в старших классах средней школы и в вузах основ борьбы с идеями фашизма и нацизма. При это не бояться показывать, почему носителями этих идей стали миллионы, но обязательно показывать человеконенавистническую сущность этих идей, их идейные слабости и объяснять, почему они потерпели поражение

а в 1989–1993 годах — председателем Объединённого комитета начальников штабов. — *Примеч. автора.*

Схема существовавшей структуры воспитательной работы в России в начале XXI века

и объявлены вредоносными после окончания Второй мировой войны. Показывать, почему и с чей помощью возродились идеи фашизма и нацизма на территориях бывших республик СССР.

Сегодня, по мнению автора, активная подмена понятий и толерантность господствуют в российском обществе только в одном направлении. Они фактически размывают национальное самосознание россиян, которое крайне необходимо для формирования боевой активности у военнослужащих армии и флота РФ.

Для противостояние гибридным войнам, которые ведутся на современном этапе, необходимо значительно пересмотреть систему качественной подготовки воспитания в стране и уделить внимание как глобальному технологическому обновлению, так и усилению нравственных основ российского общества.

Список использованных источников и литературы

1. Сталин И. В. Приказ Народного комиссара обороны СССР 23 февраля 1942 года № 55 // Сталин И. В. Сочинения. — Т. 15. — М.: Писатель, 1997. — С. 93–98.
2. Чингиз Айтматов. Буранный полустанок (И дольше века длится день). — М., 1981. — С. 106–107.

М. М. Базлуцкая,
редактор RT Deutsch

ВЗАИМОЗАВИСИМОСТЬ СМИ И ГОСУДАРСТВЕННЫХ СТРУКТУР ПРИ ВЕДЕНИИ ЦИФРОВОЙ ДИПЛОМАТИИ

Аннотация: в статье рассматривается феномен цифровой дипломатии с точки зрения распространения сообщений через средства массовой информации. Автор отмечает важную роль СМИ для увеличения охвата аудитории на страницах государственных структур и официальных лиц. В работе также указываются причины взаимозависимости цифровой дипломатии и новостных агентств.

Ключевые слова: СМИ, цифровая дипломатия, новости, социальные сети, информация, источники информации.

С каждым днем человечество производит все больше информации. Только в 2020 году, согласно исследованию аналитической платформы DOMO, ежеминутно создавалось более 41,5 миллиона сообщений в WhatsApp, 2704 пользователя скачивали TikTok, а Amazon отправлял 6 659 посылок своим клиентам. В апреле того же года интернет стал доступен более 4,5 миллиардам человек — это на 6 процентов больше, чем было в начале 2019[36]. Пандемия COVID-19 укорила процесс цифровизации и приобщения населения к новым технологиям. В свою очередь, скорость предоставления информации пользователям окончательно стала основным конкурентным показателем для средств массовой информации на любой

[36] Аналитическая платформа domo.com. Инфографика Data Never Sleeps 8.0, 2020. — URL: https://web-assets.domo.com/blog/wp-content/uploads/2020/08/20-data-never-sleeps-8-final-01-Resize.jpg (дата обращения: 30.08.2021).

из существующих платформ — будь то телевидение, радио, социальные сети или мессенджеры.

Сегодня рассказать о событии спустя день или два для СМИ значит потерять своих клиентов и аудиторию. Журналисты работают по принципу «здесь и сейчас» и стремятся получить максимум информации из доступных источников. Поэтому в моменты срочного выпуска новостей редакторы зачастую обращаются к обычным пользователям и высоко ценят, если государственные структуры вовремя обновляют информацию на своих сайтах и в социальных сетях. Именно в этот момент цифровая дипломатия становится очень важным и влиятельным ресурсом в руках политики.

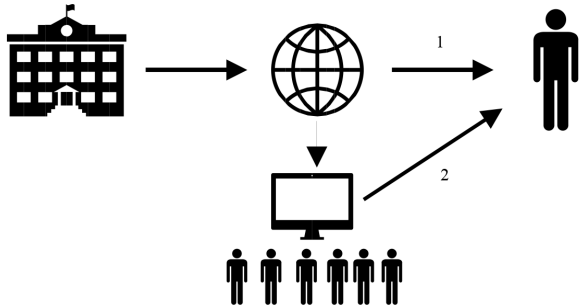
В данной статье мы обратимся к самому широкому определению цифровой дипломатии (далее — ЦД) профессора Школы коммуникаций Американского университета Прийи Доши, которая понимает под ЦД все, что входит в сферу взаимодействия правительственных учреждений с иностранными гражданами посредством новых коммуникационных сетей[37]. В этом случае, мы сможем более полно проанализировать роли государственных органов, СМИ и обычных пользователей в процессе обмена информацией.

Рассмотрим этот процесс с двух позиций, где в первом случае отсутствует роль СМИ как посредника между первичным источником информации и пользователем, а во втором такой посредник появляется.

Исходя из схемы, кажется, что быстрее информация дойдет до пользователя по пути номер 1. Однако на самом деле меньше всего времени будет затрачено человеком на получение информации из вторичного источника — по пути 2. Рассмотрим причины этого феномена.

---

[37] Doshi P. Digital diplomacy: Changing The World Through Communication. February 2016. — URL: https://www.american.edu/soc/news/digital-diplomacy-q-a.cfm (дата обращения: 30.08.2021).



Во-первых, в Сети активно огромное количество государственных учреждений, а также политиков, каждый из которых выдает собственные новости и делает публикации на различных сайтах и страницах. Таких страниц может быть неограниченное количество. У одного только Министерства иностранных дел России их более 100, включая аккаунты всех дипломатических представительств, и не считая личные страницы официальных представителей министерства[38]. И на всех из них может выдаваться контент, который не повторяется где-либо еще. При этом ни в одной стране еще не создано единой платформы-агрегатора для передачи сообщений всех источников одновременно. Эту функцию выполняют новостные агентства, такие как российское агентство ТАСС, американские CNN и Associated Press, немецкое dpa и другие.

Во-вторых, существует языковой барьер, который зачастую препятствует пользователю при обработке появляющейся информации. Сегодня в Twitter необходимо знать минимум английский язык, чтобы прочитать сообщения, опубликованные госорганами и официальными представителями страны. Одним из примеров может служить аккаунт Министерства иностран-

[38] Официальный сайт МИД России. — URL: https://www.mid.ru/ru/press_service/ social_accounts (дата обращения: 30.08.2021).

ных дел Ирана на английском[39], который дублирует и/или дополняет канал на персидском языке[40]. Так, гражданам, не владеющим этими языками придется прибегать к помощи переводчиков (в том числе и автоматических онлайн-переводчиков) либо новостных агентств. Что вновь возвращает нас к тому, что пользователь, который захочет узнать о происходящем в стране, на языке которой он не говорит, вероятно пойдет искать информацию о событиях в новостных лентах СМИ.

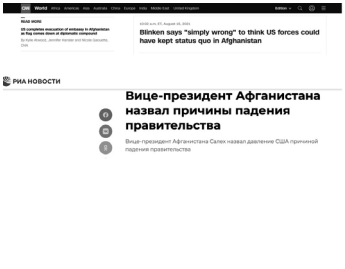
В-третьих, публикации государственных органов не дают контекста происходящего и часто лишь констатируют факт произошедшего события без анализа. Это не создает у пользователя полноценной картины ситуации. Эту проблему также решают СМИ, которые привлекают к анализу экспертов. Тем не менее картина мира пользователя после знакомства с мнением эксперта может отличаться, в зависимости от взглядов приглашенного специалиста.

Так, вопрос окончательного вывода войск НАТО из Афганистана поддерживался в американских СМИ и подвергался критике и / или сомнению в российских медиа.

---

[39] Официальный аккаунт Министерства иностранных дел Исламской Республики Иран в Твиттере на английском языке. — URL: https://twitter.com/IRIMFA_EN (дата обращения: 30.08.2021).

[40] Официальный аккаунт Министерства иностранных дел Исламской Республики Иран в Твиттере на персидском языке. — URL: https://twitter.com/IRIMFA(дата обращения: 30.08.2021).



Несмотря на то, насколько СМИ важны государственным органам и официальным лицам для донесения сообщений, настолько же важны эти же самые сообщения для журналистов.

Практически ни один новостной материал — за исключением, пожалуй, верифицированных видеоматериалов — не может обойтись без комментариев официальных представителей министерств и ведомств. Именно эти комментарии дают контекст ситуации, сообщают детали произошедшего, и / или являются ответной реакцией на предыдущий комментарий оппонента.

В данном случае, чем быстрее выйдет такой комментарий онлайн, а еще лучше на одном из языков Организации Объединенных Наций, тем больше вероятность, что он создаст вокруг себя новостной повод и его распространят с высокой скоростью мировые СМИ.

Таким образом, можно заключить, что публикации государственных организаций в рамках цифровой дипломатии направлены в первую очередь для их последующего анализа, обработки и трансляции в медиапространстве. При этом сами средства массовой информации стимулируют мировых игроков регистрироваться на различных платформах, чтобы сообщения от их лица или от имени государственной структуры были быстрее растиражированы.

Список использованных источников и литературы

1. Аналитическая платформа domo.com. Инфографика Data Never Sleeps 8.0, 2020. — URL: https://web-assets.domo.com/blog/wp-content/uploads/2020/08/20-data-never-sleeps-8- final-01-Resize.jpg (дата обращения: 30.08.2021).

2. Официальный аккаунт Министерства иностранных дел Исламской Республики Иран в Твиттере на английском языке. — URL: https://twitter.com/IRIMFA_EN (дата обращения: 30.08.2021).
3. Официальный аккаунт Министерства иностранных дел Исламской Республики Иран в Твиттере на персидском языке. — URL: https://twitter.com/IRIMFA(дата обращения: 30.08.2021).
4. Официальный сайт МИД России. — URL: https://www.mid.ru/ru/press_service/social_accounts (дата обращения: 30.08.2021).
5. Doshi P. Digital diplomacy: Changing The World Through Communication, February 2016. — URL: https://www.american.edu/soc/news/digital-diplomacy-q-a.cfm (дата обращения: 30.08.2021).

Научное издание

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ:
ВЛИЯНИЕ ПАНДЕМИИ COVID-19»

Сборник докладов
международной научной конференции
(Москва, 20 мая 2021 года)

Согласно Федеральному закону РФ от 29.12.2010 № 436-ФЗ
данная продукция не подлежит маркировке

Компьютерная верстка *А. С. Туманова*
Художественное оформление *Е. С. Игнатова*

Подписано в печать 11.10.2021. Формат 60x84 1/16.
Усл. печ. л. 19,6. Уч.-изд. л. 14,2. Заказ №

Издательство «МГИМО–Университет»
119454, Москва, пр. Вернадского, 76

Отпечатано в отделе оперативной полиграфии
и множительной техники МГИМО МИД России
119454, Москва, пр. Вернадского, 76