УДК 327 Вестник СПбГУ. Международные отношения. 2024. Т. 17. Вып. 3

Международная информационная безопасность: от классической к сетевой дипломатии России

В. И. Булва

Министерство иностранных дел Российской Федерации,
Российская Федерация, 119002, Москва, Смоленский бул., 32/34

Для цитирования: Булва В. И. Международная информационная безопасность: от классической к сетевой дипломатии России // Вестник Санкт-Петербургского университета. Международные отношения. 2024. Т. 17. Вып. 3. С. 325–341. https://doi.org/10.21638/spbu06.2024.306

В статье рассмотрено становление новой области международных отношений — международной информационной безопасности, а также дальнейшее деление данной проблематики на три трека — безопасность в сфере использования ИКТ и самих ИКТ, противодействие информационной преступности, управление интернетом. Автор анализирует, каким образом трансформировалась модель дипломатического взаимодействия на примере сотрудничества на вышеназванных направлениях. Исследование позволяет сделать вывод, что международная информационная безопасность как одна из областей новых вызовов и угроз требует развития инструментов сетевой дипломатии в качестве вспомогательных элементов классической межгосударственной дипломатии. Такой формат позволяет привлечь, наряду с государствами, различные заинтересованные стороны, а гибкий подход к организационной структуре (отсутствие иерархии) — наладить контакты не только с полноправными членами, но и с внешними партнерами (Россия — АСЕАН, БРИКС+ и др.). Российская Федерация стремится сохранить ооноцентричную модель сотрудничества в сфере международной информационной безопасности, используя созданные по инициативе ООН площадки Рабочей группы открытого состава по безопасности в сфере использования ИКТ и самих ИКТ и Специального комитета открытого состава ООН по разработке универсальной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, а также Международного союза электросвязи. Одновременно активизируется сотрудничество России на региональном и трансрегиональном уровне с целью консолидации усилий мирового большинства, которое могло бы обеспечить продвижение на международной арене российских инициатив, ориентированных на предотвращение конфликтов в информационном пространстве и минимизацию ущерба от инцидентов в сфере использования ИКТ.

Ключевые слова: международная информационная безопасность, информационная преступность, информационно-коммуникационные технологии, сетевая дипломатия.

Дипломатия в области международной информационной безопасности (МИБ) начала развиваться в конце XX в., когда по инициативе России данная проблема была официально закреплена в повестке дня ООН после принятия резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Изначально ключевые разногласия выстраивались между двумя лагерями: Россия и ее союзники — США и их партнеры. Отличительная

© Санкт-Петербургский государственный университет, 2024

черта российского подхода заключалась в широкой трактовке понятия «международная информационная безопасность», которое включало как технические аспекты (безопасность инфраструктуры и информационных систем), так и вопросы контента (безопасность информации). На Западе, в свою очередь, при развитии международного сотрудничества акцент делался преимущественно на первой составляющей (кибербезопасность) [1, с. 150].

На уровне внешнеполитических ведомств в последнее время наблюдаются изменения как в России, так и в США. В РФ четко разграничиваются два направления обеспечения МИБ — проблема кибербезопасности (выработка норм и правил поведения для обеспечения физической безопасности инфраструктуры информационно-коммуникационных технологий (ИКТ)) входит в компетенцию Департамента международной информационной безопасности МИД России, а вопросы информационно-психологической безопасности — Департамента информации и печати МИД России.

В Соединенных Штатах, которые по-прежнему выступают против включения в глобальную повестку когнитивной составляющей информационного противоборства, эта тематика активно развивается на национальном уровне (отдел цифровых свобод Бюро по вопросам киберпространства и цифровой политики Госдепартамента США) и в рамках сотрудничества с партнерами (борьба с гибридными угрозами).

Так или иначе на рубеже XX–XXI вв. происходит закрепление данного направления в системе международных отношений в компромиссной формулировке «безопасность в сфере использования ИКТ и самих ИКТ». Именно такой термин используется в базовых резолюциях Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принимаемых ежегодно по инициативе Российской Федерации и соавторов.

Угрозы в сфере информационной безопасности относятся к категории новых вызовов и угроз, специфика которых состоит в их трансграничном характере и вовлеченности неконвенциональных акторов (террористических и преступных группировок). Изначально российская дипломатия на данном направлении представляла классический формат межгосударственного взаимодействия. Однако с течением времени в России, как и в большинстве государств мирового сообщества, происходило осознание необходимости привлечения к переговорному процессу и других участников — неправительственных сторон, которые разрабатывают информационные технологии и фактически контролируют информационную инфраструктуру (бизнес), а также обладают узкоспециализированными знаниями в сфере информационной безопасности (научно-исследовательские институты, аналитические центры). Таким образом, на примере международного сотрудничества в сфере информационной безопасности показано, каким образом новые области международных отношений способствуют трансформации форм дипломатии. Цель исследования заключается в определении роли классической и сетевой дипломатии в продвижении российский инициатив в сфере информационной безопасности.

В трудах таких зарубежных авторов, как Д. Белл [2], М. Постер [3], К. Шваб [4], Э. Тоффлер [5], М. Кастельс [6], акцент делается на изучении рисков, вызовов

и угроз цифровой трансформации общества. Наибольшее количество исследований в зарубежной литературе в сфере информационной безопасности посвящено анализу военно-политических угроз. Можно выделить таких авторов, как М. Либики [7], Р. Моландер [8] и А.Шафрански [9]. Российские эксперты затрагивают как военно-политические аспекты международной информационной безопасности, так и вопросы [10], связанные с рисками социально-гуманитарного характера и когнитивного противоборства [11–13].

Особое внимание как в России, так и за рубежом уделяется применимости международного права к информационному пространству. Необходимость адаптации международно-правовых норм с учетом специфики ИКТ обоснована в работах А. А. Стрельцова [14] и В. Н. Трофимова [15]. Западный подход к проблеме применимости международного права к ИКТ-среде отражен в «Таллинском руководстве» [16]. Вопросы применимости международного права, в частности международного гуманитарного права, к регулированию вооруженных конфликтов изучали Э. Тикк, К. Мики [17], К. Киттичайсари [18] и А. Робертс [19].

Несмотря на повышение заинтересованности со стороны научного сообщества к проблематике международной информационной безопасности, по-прежнему недостаточное внимание уделяется дипломатии как ключевому инструменту формирования системы МИБ, а также трансформации механизмов и форматов дипломатического взаимодействия с учетом укрепления роли новых акторов мировой политики и специфики угроз в сфере использования ИКТ.

При исследовании использовался системный подход, в разработку которого весомый вклад был внесен А. Д. Богатуровым. Данный подход позволяет рассматривать ландшафт международного сотрудничества в сфере информационной безопасности как группу элементов, связанных между собой сетью взаимодействий. В частности, автор уделяет внимание различным уровням многостороннего сотрудничества в сфере информационной безопасности — региональному, макрорегиональному и глобальному — с акцентом на перспективы использования инструментов сетевой дипломатии на каждом из вышеобозначенных треков. Учитываются внешние факторы сотрудничества и противоборства, обусловленные оппонирующими подходамив и альтернативными глобальными инициативами США и ЕС по безопасности в сфере ИКТ.

Проведению исторического анализа эволюции методов дипломатического взаимодействия способствовали хронологический метод и анализ официальных документов в сфере международной информационной безопасности. При этом основную часть источников составляют инициативы и проекты резолюций России в данной сфере, поскольку именно они внесли ключевой вклад в формирование институциональной (учреждение Рабочей группы открытого состава ООН по безопасности в сфере использования ИКТ и самих ИКТ (далее — РГОС) и Спецкомитета по информационной преступности) и концептуальной базы (повестка рабочих групп) международного сотрудничества по безопасности в сфере использования ИКТ и самих ИКТ. Одновременно с этим анализируются инициативы западных государств, ориентированные на продвижение альтернативных площадок взаимодействия в духе «избирательного партнерства».

Дипломатия в области международной информационной безопасности

Появление новой отрасли международного сотрудничества отражало тренд на секьюритизацию неклассических сфер безопасности. Если ранее поддержание безопасности подразумевало предотвращение и урегулирование военно-политических конфликтов, то с 1990-х годов в глобальной повестке появляется проблематика новых вызовов и угроз, одна из которых связана с использованием ИКТ. При этом выделяется ряд специфических особенностей данной категории угроз, что обуславливает невозможность борьбы с ними в рамках традиционной парадигмы военно-политической безопасности, основанной исключительно на межгосударственном сотрудничестве.

Во-первых, источниками новых вызовов и угроз, и в частности угроз в области использования ИКТ, становятся наряду с государствами неправительственные игроки — террористические, экстремистские, преступные группировки [20, с. 102]. В результате межгосударственное соперничество (использование ИКТ в военно-политических целях) дополняют другие компоненты «триады» — применение ИКТ в террористических и преступных целях. В этой связи классические инструменты, востребованные при урегулировании конфликтов между государствами, оказываются недостаточно эффективными при купировании угроз в информационном пространстве.

Во-вторых, потенциал государств в сфере контроля ИКТ-среды ограничен в силу того, что информационная инфраструктура создается с опорой на технологии частного сектора. Более того, укрепляется рынок крупных IT-компаний, которые отвечают как за техническую сторону (развитие критической информационной инфраструктуры), так и за содержательное наполнение информационного пространства (генерирование контента). Как следствие, выработка решения по обеспечению международной информационной безопасности становится невозможной без привлечения практического опыта и ресурсного потенциала бизнеса.

В-третьих, изучение такого предмета, как международная информационная безопасность, требует не только дипломатических навыков, но и отраслевых знаний, поэтому для развития сотрудничества на данном треке недостаточно использования исключительно политического уровня (т. е. традиционного канала дипломатии). Необходима экспертиза со стороны узкопрофильных специалистов, в том числе представителей научного, академического и экспертного сообществ, гражданского общества.

В-четвертых, как и другие новые вызовы и угрозы, противоправное использование ИКТ носит трансграничный характер, а в самом информационном пространстве отсутствуют четко выраженные границы. С учетом данного фактора для обеспечения информационной безопасности приоритетным становится объединение усилий максимально широкого числа участников в рамках единого переговорного процесса.

Итак, вышеперечисленные особенности международной информационной безопасности способствуют формированию многоуровневой системы дипломатии, включающей сотрудничество на глобальных, трансрегиональных, макрорегиональных и региональных площадках, а также в двустороннем формате. С появлением

новой отрасли в системе международных отношений меняется и модель дипломатического взаимодействия. На смену традиционной межгосударственной официальной дипломатии приходит сетевой принцип, отличительная черта которого заключается в отсутствии жесткой иерархии [21, с. 147]. В его основе лежит деятельность «гибких альянсов» [20, с. 121], объединяющих максимальное количество заинтересованных сторон.

В конце 1990-х годов прошла серия двусторонних российско-американских переговоров по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Однако из-за противоречий сторон, в первую очередь концептуальных (в отношении понятийного аппарата и предмета регулирования), выйти на практические договоренности не удалось. В этих условиях было принято решение о переносе тематики на глобальный уровень. Сначала рассматривалась площадка Международного союза электросвязи (МСЭ), но в итоге соответствующий пункт международной повестки был закреплен в резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 1998 г. [22].

Постепенно глобальная дипломатия в области международной информационной безопасности разделилась на три отдельных, но взаимосвязанных между собой трека: безопасность в сфере использования ИКТ и самих ИКТ (Группа правительственных экспертов, позже Рабочая группа открытого состава), противодействие информационной преступности (Специальный комитет по выработке всеобъемлющей конвенции по противодействию информационной преступности (далее Спецкомитет)), управление интернетом (Международный союз электросвязи). На двустороннем и региональном уровне эти вопросы обычно рассматриваются в связке друг с другом.

В поисках глобального переговорного формата: ООН vs «избирательные партнерства»

Институциональные основы международного сотрудничества в сфере информационной безопасности под эгидой ООН были заложены в 2001 г., когда в резолюции Генеральной Ассамблеи ООН было закреплено решение о формировании Группы правительственных экспертов (ГПЭ). Вплоть до 2017 г. именно этот переговорный механизм оставался основным и выполнял миссию координации подходов ключевых государств [23]. После 2017 г. на фоне провала попытки согласовать итоговый доклад ГПЭ активизировались дискуссии о необходимости совершенствования формата с учетом повышенного спроса на подключение к переговорам со стороны большого количества государств мирового сообщества. Часть из них принимали участие в работе Групп правительственных экспертов различных созывов, а некоторые — в деятельности трансрегиональных и региональных объединений, таких как БРИКС, ШОС, СНГ, ОДКБ.

Другим фактором, который учитывался при подготовке новой институциональной инициативы, выступал рост интереса неправительственных игроков (бизнеса, гражданского общества и научного сообщества), которые к тому времени уже получили опыт международного участия в консультативном статусе на площадках Международного союза электросвязи. За расширение прав негосударственных

субъектов в данной сфере активно выступили западные государства, но они, в отличие от России, настаивали на уравнивании в правах негосударственных и государственных представителей [24, с. 30]. Данное противоречие стало одним из ключевых при работе будущей Рабочей группы открытого состава, а также фигурировало в качестве центрального элемента многочисленных западных инициатив: «Парижский призыв к доверию и безопасности в киберпространстве» (2018 г., Франция), «Форум технологий будущего (2021 г., Великобритания), «Глобальная коалицию демократического технологического развития» (2021 г., США), «Декларация о будущем Интернета» (2022 г., США), «Международное агентство по мирному использованию киберпространства» — как альтернатива РГОС (2022 г., США) [25, с. 71].

Россия, в свою очередь, отстаивала принцип сохранения совещательной роли неправительственных сторон. В этой связи внимание российской дипломатии было сосредоточено на поиске формата многоуровневого общения, организованного в группе заинтересованных субъектов, который бы выходил за рамки традиционных, жестких, ирерархичных институтов [21, с. 146]. Такой подход нашел отражение в российских инициативах от 2018 г. об учреждении РГОС [26] и от 2019 г. о формировании Спецкомитета [27]. Обе переговорные площадки предусматривали участие всех государств — членов ООН, причем решения в форме итоговых докладов принимались на основе консенсуса, что обеспечивало сохранение принципа равноправия.

Сетевой принцип функционирования РГОС позволил интенсифицировать диалог с региональным объединениями (организациями, сетевыми институтами и интеграционными структурами). В соответствии с мандатом Рабочей группы, свои позиции могут представлять (а затем публиковать на официальном сайте РГОС в качестве вкладов) региональные организации. В ходе работы РГОС первого созыва объединения государств-членов, представляющих как западное сообщество (ЕС), так и развивающиеся страны (Движение неприсоединения, группа Африканских государств, Карибское сообщество (КАРИКОМ)), представили свои рекомендации по различным пунктам мандата группы [28].

Благодаря возможностям формата РГОС к глобальной дискуссии по вопросам безопасности в сфере использования ИКТ и самих ИКТ присоединились другие заинтересованные стороны (частный сектор, академическое, экспертное и научное сообщества, гражданское общество). Они получили право принимать участие в выработке совместных договоренностей в рамках политического процесса. В рамках нового пятилетнего мандата (2021–2025 гг.) Группа уполномочена рассматривать не только национальные инициативы, но и обсуждать проблемы институционализации переговоров со всеми заинтересованными сторонами во вспомогательных подгруппах по отдельным пунктам повестки дня РГОС, что сделает диалог более структурированным. Однако на практике ряд организаций столкнулся с препятствиями на пути подключения к полноценной работе РГОС по политическим мотивам. Так, представители большинства российских компаний и научно-исследовательских институтов не смогли получить не просто американские визы для участия в межсессионных встречах и неформальных консультациях с участием Председателя, но и даже аккредитацию на мероприятия по линии РГОС.

Несмотря на трудности переговорного процесса в РГОС, в данном формате удалось добиться определенных успехов. Деятельность РГОС первого созыва

завершилась принятием итогового доклада и Доклада Председателя (закрепившего спорные вопросы для будущих дискуссий), которые содержали положения по всем пунктам мандата группы — перечень существующих и потенциальных угроз в сфере использования ИКТ, применимость международного права к информационному пространству, меры по наращиванию потенциала, меры укрепления доверия, институционализация будущего диалога. Основным камнем преткновения остались вопросы необходимости адаптации международного права с учетом особенностей ИКТ, а также проблема атрибуции.

Усовершенствование механизма атрибуции с целью противодействия практике публичных необоснованных обвинений и для верификации порядка установления источника кибератаки стало приоритетной задачей дипломатии России на площадке РГОС нового созыва. В результате большинство государств поддержали предложение российской делегации о создании реестра контактных пунктов как меры доверия, что позволило наладить механизм обмена сведениями о совершаемых атаках между компетентными ведомствами [29].

Долгосрочная цель дипломатии России по безопасности в сфере использования ИКТ и самих ИКТ состоит в принятии всеобъемлющей конвенции, содержащей юридически обязательные нормы. В 2023 г. был представлен советующий обновленный проект универсальной Конвенции. Как и на этапе зарождения данной области дипломатии, безусловным приоритетом Российской Федерации остается предотвращение конфликтов в информационном пространстве (в отличие от курса западных стран на регулирование конфликтов в сфере использования ИКТ) и содействие использования ИКТ в мирных целях [30].

Во время деятельности РГОС второго созыва обострились дискуссии вокруг перспектив регулярного институционального диалога под эгидой ООН. Франция и Египет представили Программу действий по поощрению ответственного поведения государств при использовании ИКТ в контексте международной безопасности. Главная цель инициативы заключалась в учреждении нового глобального постояннодействующего механизма взамен существующей РГОС. Планировалось, что на новой площадке будут обсуждаться правила ответственного поведения добровольного характера, без адаптации международного права с учетом специфики ИКТ. Особое внимание было уделено повышению статуса неправительственных участников. Вместе с тем в содержательном плане инициатива не предполагала нововведений, она дублировала мандаты ГПЭ и РГОС.

По принципу сетевого взаимодействия построена работа другой площадки, созданной по инициативе России в соответствии с резолюцией Генеральной Ассамблеи ООН в 2019 г. — Специального комитета открытого состава по разработке универсальной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Как и в РГОС, сетевые инструменты сотрудничества дипломатии позволили запустить в рамках Спецкомитета наряду с межправительственным треком переговорный процесс по линии представителей различных компетентных ведомств (включая министерства юстиции и министерства цифрового развития). На неправительственном уровне к предметному обсуждению положений текста будущей конвенции привлекаются эксперты-юристы для того, чтобы в дальнейшем избежать правовых лакун. В качестве наблюдателей к сессиям Спецкомитета привлекаются неправительственные

организации, научные учреждения, IT-бизнес. При этом монопольное право на принятие окончательного решения на основе консенсуса сохраняется за государствами.

Главным препятствием глобального сотрудничества в данной сфере служат концептуальные разногласия между западными странами, с одной стороны, а также Россией и ее союзниками — с другой. США и их партнеры приоритезирует тематику прав человека и гендерного равенства, отодвигая на второй план вопросы практического сотрудничества по борьбе с информационной преступностью. Более того, эта группа государств заинтересована в сохранении базового постулата Будапештской конвенции о компьютерных преступлениях от 2001 г. — ст. 32, которая разрешает трансграничный доступ к компьютерным данным, хранящимся на территории другой стороны, без ее предварительного согласия. Во избежание вмешательства во внутренние дела под предлогом противодействия информационной преступности Российская Федерации настаивает на включении в будущую Конвенцию статьи по защите суверенитета (ст. 3 проекта Конвенции). Данное положение предполагает сохранение полной юрисдикции государства на его территории и возможность осуществления действий в национальном пространстве только в рамках внутреннего права соответствующего государства.

Еще одним поводом для противоречий сторон выступает сфера охвата конвенции. Россия исходит из того, что криминализированы должны быть все преступления, совершаемые с использованием информационно-коммуникационных технологий, т. е. как компьютерные преступления, так и противоправные деяния, связанные с использованием информационных систем и сетей для распространения деструктивной идеологии, пропаганды, незаконной торговли и т. д. Запад, в свою очередь, продвигает идею узкой трактовки киберпреступности, ограничивая действие возможного документа (по аналогии с Будапештской конвенцией) преступлениями, совершаемые с помощью компьютерных технологий.

Несмотря на сохранение данных спорных моментов, работа Спецкомитета продолжается. США предпринимали попытку подмены формата Спекомитета путем создания «коалиций по интересам» с исключительным участием «демократических государств». В частности, они продвигали идею по формированию механизма борьбы с вымогателями (Ransomware Initiative), которая изначально была открыта только для ограниченного числа американских партнеров. Одновременно с этим США стремились сорвать запуск функционирования самого Спецкомитета (голосуя против соответствующей резолюции ООН и стремясь склонить союзников к отказу от поддержки российского проекта) и не допустить принятия конвенции ООН.

Вопреки попыткам США саботировать переговорный процесс под эгидой ООН, модальности работы Спецкомитета были согласованы, и данная площадка начала субстантивную работу в 2019 г. В этих условиях Соединенные Штаты сменили тактику, взяв курс на выхолащивание содержательной части документа, пытаясь подменить российский проект положениями Будапештской конвенции от 2001 г., содержащей ограниченный перечень преступлений в сфере компьютерной безопасности и фиксирующей право подписантов проводить следственные действия в чужой юрисдикции без согласия правоохранительных органов этой страны. Тем не менее благодаря поддержке со стороны мирового большинства — развивающихся государств, не прерывается обсуждение всеобъемлющей конвенции с учетом широкой палитры вопросов, обозначенных в российском проекте

данного документа. Планируется, что в 2024 г. будет согласован текст универсальной конвенции.

Помимо подмены повестки, создания искусственных препятствий для работы площадок ООН (РГОС, Спецкомитета и Международного союза электросвязи), вытеснения российских представителей из данных структур (представителей российских НПО в РГОС и Спецкомитете, а также российских официальных лиц в уставных органах МСЭ), западные государства стремятся создать площадки вне рамок ООН в духе так называемого порядка, основанного на правилах. Такие «избирательные партнерства» рассматриваются как альтернатива универсальному ооноцентричного международно-правовому режиму, многополярному миропорядку как в цифровой среде, так и в системе международных отношений в целом [31, с. 15]. Наиболее показательной в этой связи выступает флагманская инициатива США — саммит за демократию и формирование Альянса за будущее интернета.

На первом Саммите за демократию планировалось анонсировать создание Альянса за будущее интернета. В ходе встречи этого сделано не было, однако 28 апреля 2022 г. США и 60 государств и глобальных партнеров подписали «Декларацию о будущем интернета» [32], приняв на себя обязательства по продвижению свободного, открытого, глобального, функционально совместимого, надежного и безопасного интернета для всего мира, который «базируется на единых для всех правилах и демократических ценностях». Декларацию подписали США, все члены ЕС, Австралия, Великобритания, Грузия, Израиль, Канада, Сербия, Украина, Япония, а также Европейская комиссия и Тайвань.

В центре внимание лежит задача противодействия «цифровому авторитаризму», т. е «подавлению свободы выражений мнений, цензуру в отношении независимых новостных источников, вмешательство в выборы, распространение дезинформации и лишение граждан других прав со стороны отдельных государств (прежде всего, России и Китая)». Подобные действия, по мнению коллективного Запада, приводят к «фрагментации интернета». На практике фрагментация интернета проявляется в стремлении западных стран изолировать отдельные государства от участия в формировании «правил».

В числе основных принципов, прописанных в документе, значатся защита прав и свобод человека, содействие глобальному интернету со свободным потоком информации, развитие инклюзивной и доступной связи, стимулирование доверия к глобальной цифровой экосистеме, в том числе за счет защиты конфиденциальности и противодействия киберпреступлениям, укрепление многостороннего подхода к управлению интернетом. По содержанию это дублирует работу таких универсальных структур, как ООН, «Группа семи», «Группа двадцати», Организация экономического сотрудничества и развития, Всемирная торговая организация, Корпорация по управлению доменными именами и IP-адресами (ICANN).

Логическим продолжением вышеупомянутых инициатив является созыв второго Саммита за демократию в 2023 г. В ходе саммита прошли тематические сессии по вопросам, связанным с использованием ИКТ: «Противодействие неправомерному использованию технологий и росту цифрового авторитаризма», «Формирование новых технологий для обеспечения уважения прав человека и демократических принципов» [33]. США призвали сформировать «экосистему новых технологий в соответствии с демократическими принципами и правами человека» [34].

Безусловным приоритетом Соединенных Штатов является противостояние злоупотреблению технологиям для подавления контроля, разделения и лишения гражданских прав, а также распространения цифрового авторитаризма.

В итоговой декларации второго Саммита за демократию подчеркивается, что международное право применимо в существующем виде к регулированию процессов в информационном пространстве. Тем самым исключается возможность выработки юридически обязательных норм с учетом специфики ИКТ. Вместо этого продолжается курс по формированию «правил», причем роль арбитра, следящего за их соблюдением, берут на себя западные кураторы. Акцент делается на важности преодоления цифрового неравенства путем поддержки проектов в области развития ИКТ-инфраструктуры. В этой связи обратим внимание на то, что участие западных государств в реализации мер по наращиванию потенциала исходит из принципа обусловленности. Речь идет о предоставлении технологической помощи развивающимся странам или содействии в подготовки профильных кадров в обмен на суверенитет этих стран.

На текущий момент в промежуточном докладе РГОС и резолюции ГА ООН именно за Рабочей группой был сохранен статус ключевой переговорной площадки по вопросам безопасности в сфере использования ИКТ и самих ИКТ до 2025 г. (до срока истечения ее мандата), вопрос о будущем формате должен быть решен в рамках РГОС на основе консенсуса государств.

Для России неприемлема подмена международно-правового режима с участием всех государств «порядком, основанным на правилах». В новой редакции Концепции внешней политики России от 2023 г. отмечается: «Испытанию на прочность подвергается международно-правовая система: узкая группа государств стремится подменить ее концепцией миропорядка, основанного на правилах (навязывание правил, стандартов и норм, при выработке которых не было обеспечено равноправное участие всех заинтересованных государств)» [35]. Это осложняет выработку коллективных ответов на транснациональные вызовы и угрозы и в конечном итоге приводит к снижению уровня доверия и предсказуемости в международных делах. В этих условиях повышается актуальность наращивания контактов на трансрегиональном и региональном уровнях, которые рассматриваются Россией как вспомогательный практикоориентированный канал взаимодействия, а не альтернатива ооноцентричной модели сотрудничества.

Трансрегиональные и региональные партнерства с участием России

В дипломатии России международное сотрудничество в сфере информационной безопасности на региональных и трансрегиональных площадках играло особую роль в периоды, когда стопорились переговоры на глобальном уровне в рамках Группы правительственных экспертов ООН. Так, в 2006 г. трек по безопасности в сфере использования ИКТ и самих ИКТ был запущен в ШОС, сформирована Группа экспертов по международной информационной безопасности. Примечательно, что после усиления контактов Российской Федерации с региональными партнерами, включая страны ШОС, у российских проектов резолюций появились соавторы: в 2006 г. — 10 государств, в 2007 г. — 17, в 2008 г. — 28, в 2009 г. — 29, в 2010 г. — 35.

Основные усилия государств — членов ШОС были направлены на согласование правил ответственного поведения стран в информационном пространстве. Интенсификация взаимодействия в рамках ШОС происходила на фоне сложных переговоров по данной проблематике в ГПЭ ООН. В результате к 2011 г. в ШОС завершилась работа над проектом добровольных правил ответственного поведения для передачи на рассмотрение в Генеральную Ассамблею ООН. Представители государств ШОС (Россия, Китай, Таджикистан и Узбекистан) направили на имя Генерального секретаря официальное письмо с данным «кодексом поведения» [36]. Главная особенность инициативы — ее мирный характер. Во-первых, в качестве одной из целей обозначено предотвращение конфликтов в цифровой среде. Во-вторых, в документе акцент делается на неприемлемости силового противодействия угрозам с использованием ИКТ, т. е. недопустимости милитаризации информационного пространства. Помимо резолюции ГА ООН наработки государств — членов ШОС, закрепленные в письмах на имя Генерального секретаря ООН от 2011 и 2015 гг., были учтены при подготовке итоговых докладов ГПЭ ООН от 2013 и 2015 гг.

Второй этап активизации сотрудничества в ШОС приходится на 2017–2018 гг., в это же время неудачно завершилась работа ГПЭ ООН шестого созыва (не был достигнут консенсус между участниками по итоговому докладу). Ключевые противоречия между Россией и западным лагерем развернулись по поводу угрозы гонки вооружений в информационном пространстве и его превращения в арену для новых войн. В этой связи главной задачей российской дипломатии в ШОС стала адаптация правил ответственного поведения как ключевого инструмента предотвращения конфликтов в сфере использования ИКТ и обеспечения уважения национального суверенитета государств. В 2018 г. государства ШОС выступили с совместной инициативой, предложив обновленный «кодекс поведения» стран. Предложенные 13 правил были инкорпорированы в резолюцию Генеральной Ассамблеи ООН от 5 декабря 2018 г. [26]. Они отражали российский подход к международной информационной безопасности в целом и ориентировали на необходимость преодоления технологического дисбаланса между странами.

На современном этапе региональные форматы дипломатии России в сфере международной информационной безопасности продолжают развиваться в рамках классических международных организаций с использованием инструментов сетевого взаимодействия (СНГ, ОДКБ, ШОС). При этом особенно актуальным становится укрепление потенциала гибких институтов сетевой дипломатии (Региональный форум АСЕАН по безопасности, БРИКС). Если миссия региональных организаций заключается в выстраивании практикоориентированного сотрудничества и координации позиции сторон, то сетевые структуры все большое значение приобретают как платформы для выработки решений с целью их апробации в кругу заинтересованных участников при возможном переносе на глобальный уровень в будущем.

В АРФ АСЕАН с 2018 г. функционируют два трека. Один связан с выработкой профильной терминологии. Тематические семинары по данной тематике проходят с привлечением к дискуссии экспертов, представляющих научное сообщество. Учитывая отсутствие общепринятого понятийного аппарата в сфере информационной безопасности на глобальном уровне, данное направление сотрудничества крайне

востребовано для повышения эффективности совместного противодействия угрозам в области ИКТ и ликвидации последствий киберинцидентов.

Второй трек АРФ АСЕАН — борьба с информационной преступностью. Важно отметить, что подобные мероприятия предполагают возможность участия Председателя Спецкомитета ООН по разработке всеобъемлющей универсальной конвенции по противодействию использованию ИКТ в преступных целях. Так, в марте 2022 г. в работе семинара принял участие Председатель Спецкомитета Ф. Мебарки [37]. Таким образом, площадка АСЕАН рассматривается как вспомогательный инструмент согласования параметров глобальной юридической конвенции по информационной преступности.

Одной из наиболее актуальных современных проблем, обсуждаемых на всех глобальных площадках (РГОС, МСЭ и в меньшей степени в Спецкомитете), выступает наращивание цифрового потенциала государств. Предполагается, что сокращение разрыва между технологически развитыми государствами и развивающимися странами приведет к повышению общей устойчивости мирового сообщества, сталкивающегося с угрозой постоянного экспоненциального роста инцидентов в информационном пространстве. Красной нитью всех глобальных дискуссий по этому поводу проходит вопрос об условиях предоставления такой помощи. Западные страны руководствуются стратегией «продажи» технологий в обмен на доступ к инфраструктуре, что в большинстве развивающихся стран воспринимается как новая форма колониализма. Россия подчеркивает важность учета реальных потребностей государств-реципиентов при реализации мер по наращиванию потенциала.

Потенциальной площадкой для укрепления данного направления международного сотрудничества России с развивающимся миром может стать форум БРИКС, в частности форматы «БРИКС аутрич» и «БРИКС+». Вопросы международной информационной безопасности в повестке БРИКС фигурируют с 2011 г. В Саньянской декларации от 2011 г. они рассматривались в связке с проблемой терроризма [38], а с 2013 г., после принятия Этеквинской декларации, фигурируют как отдельный вектор деятельности БРИКС [39].

Особое значение государства БРИКС отводят укреплению информационного потенциала с целью содействия благоприятному социальному и экономическому развитию. С 2018 г. страны реализуют программы в сфере научно-исследовательских и опытно-конструкторских работ (НИОКР) на базе функционирующего в рамках БРИКС научно-исследовательского института. Кроме того, по линии академических и экспертных кругов осуществляется обмен передовыми практиками в области безопасности использования ИКТ [40]. Крайне важным при этом является общность позиции всех государств-членов в отношении необходимости уважения национального суверенитета государств.

* * *

Таким образом, появление новой сферы международных отношений — международной информационной безопасности — послужило толчком для развития новой формы дипломатического взаимодействия — сетевой дипломатии. Использование сетевых инструментов (рабочие группы, гибкие институты) позволяет привлечь к переговорному процессу широкий круг участников из числа как государств

мирового сообщества, так и заинтересованных неправительственных сторон (бизнес, гражданское общество, научное сообщество). При этом возникают противоречия в отношении модальности участия негосударственных игроков и сохранения центральной роли государств.

Российская Федерация стремится использовать потенциал сетевой дипломатии для углубления сотрудничества в сфере международной информационной безопасности как на глобальном уровне (на площадках Рабочей группы открытого состава ООН по безопасности в сфере использования ИКТ и самих ИКТ, Специального комитета открытого состава ООН по разработке универсальной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, Международного союза электросвязи), так и в рамках региональных партнерств (региональных организаций и сетевых структур). Основой российского подхода остается курс на формирование всеобъемлющей многоуровневой системы международной безопасности при сохранении центральной роли в принятии решений за государствами.

Магистральная задача российской дипломатии заключается в консолидации усилий мирового большинства вокруг ооноцентричных структур с целью недопущения создания «порядка, основанного на правилах» в кругу избранных государств. Инклюзивное сотрудничество на основе уважения интересов всех государств, их равноправия и национального суверенитета — единственно возможный путь предотвращения конфликтов в информационном пространстве, минимизации ущерба от информационной преступности и максимально полного использования преимуществ цифрового развития.

Литература

1. Цветкова, Н. А. и Стадник, И. Т. (2018), Политика кибербезопасности США. Эволюция восприятия угроз, *Международные процессы*, т. 16, № 3, с. 147–169.

2. Белл, Д. (1999), *Грядущее постиндустриальное общество: опыт социального прогнозирования*, пер. с англ., М.: Academia.

3. Шваб, К. (2020), *Четвертая промышленная революция*, М.: Эксмо.

4. Poster, M. (1995), *The second media age*, New York: Willey Blackwellp.

5. Toffler, A. (1990), *Powershift: Knowledge, Wealth, and Violence in the 21st Century*, New York: Bantam Booksp.

6. Castells, M. (2007), Communication, Power and Counter-power in the Network Society, *International Journal of Communication*, no. 1, pp. 238–266.

7. Libicki, M. (2018), Expectations of cyber deterrence, *Strategic Studies Quarterly*, no. 4, pp. 44–57.

8. Molander, R., Riddile, A. and Wilson, P. (1996), *Strategic Information Warfare: A New Face of War*, Santa Monica: Rand.

9. Szafranski, R. (1995), A Theory of Information Warfare: Preparing for 2020, *Airpower Journal*, no. 1.

10. Зинченко, А. В. (2021), *Архитектоника международной информационной безопасности*, М.: Аспект Пресс.

11. Алборова, М. Б. и Бирюков, А. В. (2021), *Социально-гуманитарные риски информационного общества и международная информационная безопасность*, М.: Аспект Пресс.

12. Багдасарян, В. Э. (2016), Когнитивное оружие как инструмент десуверенизации, *Центр научной политической мысли и идеологии им. Сулакшина*. URL: https://rusrand.ru/docconf/kognitivnoe-orujie-kak-instrument-desuverenizacii (дата обращения: 21.05.2023).

13. Манойло, А. В. (2023), Объекты и субъекты информационного противоборства, *Пси фактор*. URL: http://psyfactor.org/lib/psywar24.htm (дата обращения: 05.05.2023).

14. Стрельцов, А. А. (2014), Международное право и проблема обеспечения международной информационной безопасности, *Международная жизнь*, № 11, с. 20–34.

15. Трофимов, В. Н. (2021), *Применимость международного права к киберпространству: иллюзия или реальность?* М.: Юстицинформ.

16. *The Tallinn Manual* (2017), 2nd ed., New York: Cambridge University Press; Tallinn: Cooperative Cyber Defence Centre of Excellence.

17. Eneken Tikk, E. and Kerttunen, M. (eds) (2020), *Routledge Handbook of International Cybersecurity*, London: Routledge.

18. Kriangsak Kittichaisaree (2017), *Public International Law of Cyberspace*, Cham: Springer International Publishing.

19. Roberts, A. (1995), The Laws of War: Problems of Implementation in Contemporary Conflicts, *Duke Journal of Comparative & International Law*, 6, pp. 11–78.

20. Бурганова, И. Н. (2016), Феномен сетевой дипломатии в системе международных отношений (на примере Российской Федерации), *Международный научно-исследовательский журнал*, № 6-1 (48), с. 120–123.

21. Morozov, V. M. (2021), Network Diplomacy: Approaches to the Israel-Palestinian conflict, *Вестник ВолГУ. Серия 4: История. Религоведение. Международные отношения*, т. 26, № 1, с. 145–155.

22. *Резолюция ГА ООН A/RES/53/70 от 4 декабря 1998 г.* URL: https://undocs.org/ru/A/RES/53/70 (дата обращения: 20.12.2023).

23. Бойко, С. М. (2016), Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее, *Международная жизнь*, № 8, 54–71.

24. Исмаилов, Р. (2022), Почему для США так важно возглавить Международный союз электросвязи?, *Международная жизнь*, спецвыпуск, с. 29–32.

25. Смирнов, А. И. и Булва, В. И. (2023), «Киберправила» коллективного Запада в обход ООН и других универсальных структур — путь к подрыву миропорядка, *Международная жизнь*, № 5, с. 70–77.

26. *Резолюция ГА ООН A/73/PV.45 от 05 декабря 2018 г.* URL: https://undocs.org/ru/A/RES/73/27 (дата обращения: 20.12.2023).

27. *Резолюция ГА ООН A/RES/74/247 от 27 декабря 2019 г.* URL: https://undocs.org/ru/A/RES/74/247 (дата обращения: 20.12.2023).

28. *Open-ended Working Group: официальный сайт*. URL: https://www.un.org/disarmament/open-ended-working-group/ (дата обращения: 20.12.2023).

29. *Мера укрепления доверия № 1 о формировании глобального межправительственного реестра контактных пунктов, Проект РФ от 10.03.2023*. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_CBM1_on_PoCs__Directory_Proposal_of_the_Russian_Federation.pdf (дата обращения: 20.12.2023).

30. *Обновленная Концепция Конвенции ООН об обеспечении международной информационной безопасности, Проект России от 07.03.2023*. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation_0.pdf (дата обращения: 20.12.2023).

31. Лебедева, О. В. (2023), Приоритеты современной российской дипломатии: между ООН и «порядком, основанным на правилах», *Международная жизнь*, № 3, с. 10–19.

32. *A Declaration for the Future of the Internet*, 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (дата обращения: 20.12.2023).

33. *Summit for Democracy, 2023*. URL: https://www.state.gov/summit-for-democracy-2023/#Official-Events (дата обращения: 20.12.2023).

34. *United States: Advancing Technology for Democracy, Summit for Democracy*, 2023. URL: https://www.youtube.com/watch?v=gN6lJI4EflE (дата обращения: 20.12.2023).

35. *Концепция внешней политики России от 2023 г.* URL: https://www.mid.ru/ru/foreign_policy/official_documents/1860586/ (дата обращения: 20.12.2023).

36. *Письмо постоянных представителей Китая, РФ, Таджикистана и Узбекистана при ООН на имя Генерального секретаря от 12.09.2011*. URL: https://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf (дата обращения: 20.12.2023).

37. *Об итогах проведения семинара Регионального форума АСЕАН по безопасности по тематике противодействия использованию ИКТ в преступных целях*, 2023. URL: https://www.mid.ru/ru/detail-material-page/1804709/ (дата обращения: 20.12.2023).

38. *Саньянская декларация БРИКС от 14 апреля 2011 г.* URL: http://www.kremlin.ru/supplement/907 (дата обращения: 20.12.2023).

39. *Этеквинская декларация БРИКС от 27 марта 2013 г.* URL: http://nkibrics.ru/pages/summit-docs (дата обращения: 20.12.2023).

40. *Йоханнесбургская декларация БРИКС от 26 июля 2018* г. URL: http://nkibrics.ru/pages/summit-docs (дата обращения: 20.12.2023).

Статья поступила в редакцию 10 апреля 2024 г.;
рекомендована к печати 15 мая 2024 г.

Контактная информация:

Булва Валерия Игоревна — канд. ист. наук; va.i.bulva@my.mgimo.ru

International information security: From classical towards network diplomacy in Russia

V. I. Bulva

Ministry of Foreign Affairs of the Russian Federation,
32/34 Smolensky bul., Moscow, 119002, Russian Federation

For citation: Bulva V. I. International information security: From classical towards network diplomacy in Russia. *Vestnik of Saint Petersburg University. International Relations*, 2024, vol. 17, issue 3, pp. 325–341. https://doi.org/10.21638/spbu06.2024.306 (In Russian)

The article examines the formation of a new area of international relations — international information security, as well as its further division into three tracks — security in the use of ICTs and ICTs themselves, combating information crime, Internet governance. The author analyzes the way the model of diplomatic interaction has been transformed based on the example of cooperation in the above areas. The study shows that international information security, one of the areas of new threats and challenges, requires the development of network diplomacy tools as auxiliary elements of classical interstate diplomacy. This format makes it possible to attract various stakeholders along with states, and a flexible approach to the organizational structure (the absence of hierarchy) allows one to establish contacts not only with full members, but also with external partners (Russia-ASEAN, BRICS+ etc.). The Russian Federation strives to preserve the UN-centric model of cooperation in the field of international information security, using the platforms created on its initiative — the Open Working Group on Security in the use of ICTs and ICTs themselves and the UN Ad Hoc Open-ended Committee on the development of a universal Convention against the use of information and communication technologies for criminal purposes, as well as the International Telecommunication Union. At the same time, Russia intensifies cooperation at the regional and transregional level in order to consolidate the efforts of the world majority, which could ensure the promotion of Russian initiatives in the international arena aimed at preventing conflicts in the information space and minimizing the damage from incidents in the use of ICTs.

Keywords: international information security, information crime, information and communication technologies, network diplomacy.

References

1. Tsvetkova, N. A. and Stadnik, I. T. (2018), US Cybersecurity Policy. The evolution of threat perception, *Mezdunarodnye protsessy*, vol. 16, no. 3, pp. 147–169. (In Russian)

2. Bell, D. (1999), *The coming post-industrial society: The experience of social forecasting*, transl. from English, Moscow: Academia Publ. (In Russian)

3. Schwab, K. (2020), *The Fourth Industrial Revolution*, Moscow: Eksmo Publ. (In Russian)

4. Poster, M. (1995), *The second media age*, New York: Willey Blackwellp.

5. Toffler, A. (1990), *Powershift: Knowledge, Wealth, and Violence in the 21st Century*, New York: Bantam Booksp.

6. Castells, M. (2007), Communication, Power and Counter-power in the Network Society, *International Journal of Communication*, no. 1, pp. 238–266.

7. Libicki, M. (2018), Expectations of cyber deterrence, *Strategic Studies Quarterly*, no. 4, pp. 44–57.

8. Molander, R., Riddile, A. and Wilson, P. (1996), *Strategic Information Warfare: A New Face of War*, Santa Monica, CA: Rand.

9. Szafranski, R. (1995), A Theory of Information Warfare: Preparing for 2020, *Airpower Journal*, no. 1.

10. Zinchenko, A. V. (2021), *Architectonics of international information security*, Moscow: Aspekt Press. (In Russian)

11. Alborova, M. B. and Biryukov, A. V. (2021), *Social and humanitarian risks of the information society and international information security*, Moscow: Aspekt Press. (In Russian)

12. Bagdasaryan, V. E. (2016), *Cognitive weapons as a tool of desovereignization. Sulakshin Center for Scientific Political Thought and Ideology*. Available at: https://rusrand.ru/docconf/kognitivnoe-orujie-kak-instrument-desuverenizacii (accessed: 21.05.2023). (In Russian)

13. Manoilo, A. V. (2023), Objects and subjects of information warfare, *Psi faktor*. Available at: http://psyfactor.org/lib/psywar24.htm (accessed: 05.05.2023). (In Russian)

14. Streltsov, A. A. (2014), International law and the problem of ensuring international information security, *Mezhdunarodnaia zhizn*', no. 11, pp. 20–34. (In Russian)

15. Trofimov, V. N. (2021), *Applicability of international law to cyberspace: illusion or reality?*, Moscow: Iustitsinform Publ. (In Russian)

16. *The Tallinn Manual* (2017), 2nd ed., New York: Cambridge University Press; Tallinn: Cooperative Cyber Defence Centre of Excellence.

17. Eneken Tikk, E. and Kerttunen, M. (eds) (2020), *Routledge Handbook of International Cybersecurity*, London: Routledge.

18. Kriangsak Kittichaisaree (2017), *Public International Law of Cyberspace*, Cham: Springer International Publishing.

19. Roberts, A. (1995), The Laws of War: Problems of Implementation in Contemporary Conflicts. *Duke Journal of Comparative & International Law*, 6, pp. 11–78.

20. Burganova, I. N. (2016), The phenomenon of network diplomacy in the system of international relations (on the example of the Russian Federation), *Mezhdunarodnyi nauchno-issledovatel'skii zhurnal*, no. 6-1 (48), pp. 120–123. (In Russian)

21. Morozov, V. M. (2021), Network Diplomacy: Approaches to the Israel-Palestinian conflict, *Vestnik VolGU. Seriia 4: Istoriia. Religiovedenie. Mezhdunarodnye otnosheniia*, vol. 26, no. 1, pp. 145–155.

22. *UNGA Resolution A/RES/53/70 of December 4, 1998*. Available at: https://undocs.org/ru/A/RES/53/70 (accessed: 20.12.2023).

23. Boyko, S. M. (2016), UN Group of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security: A Look from the Past to the Future, *International Affairs*, no. 8, pp. 54–71. (In Russian)

24. Ismailov, R. (2022), Why is it so important for the United States to lead the International Telecommunication Union?, *Mezhdunarodnaia zhizn', Special Issue,* p. 29–32. (In Russian)

25. Smirnov, A. I. and Bulva, V. I. (2023), "Cyber rules" of the collective West, bypassing the UN and other universal structures — the path to undermining the world order, *Mezhdunarodnaia zhizn*', no. 5, pp. 70–77. (In Russian)

26. *UN General Assembly Resolution A/73/PV.45 of December 5, 2018*. Available at: https://undocs.org/ru/A/RES/73/27 (accessed: 20.12.2023). (In Russian)

27. *UN General Assembly Resolution A/RES/74/247 of December 27, 2019*. Available at: https://undocs.org/ru/A/RES/74/247 (accessed: 20.12.2023). (In Russian)

28. *Open-ended Working Group: official website*. Available at: https://www.un.org/disarmament/open-ended-working-group/ (accessed: 20.12.2023).

29. *Confidence-building measure No. 1 on the formation of a global intergovernmental register of contact points, Draft of the Russian Federation dated March 10, 2023*. Available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_CBM1_on_PoCs__Directory_Proposal_of_the_Russian_Federation.pdf (accessed: 20.12.2023). (In Russian)

30. *Updated Concept of the UN Convention on International Information Security, Russian Project dated 03/07/2023*. Available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation_0.pdf (accessed: 20.12.2023). (In Russian)

31. Lebedeva, O. V. (2023), Priorities of modern Russian diplomacy: Between the UN and the "rules-based order", *Mezhdunarodnaia zhizn'*, no. 3, pp. 10–19. (In Russian)

32. *A Declaration for the Future of the Internet, 2022*. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (accessed: 20.12.2023).

33. *Summit for Democracy, 2023*. Available at: https://www.state.gov/summit-for-democracy-2023/#-OfficialEvents (accessed: 20.12.2023).

34. *United States: Advancing Technology for Democracy, Summit for Democracy, 2023*. Available at: https://www.youtube.com/watch?v=gN6lJI4EflE (accessed 20.12.2023).

35. *Concept of Russian foreign policy of 2023*. Available at: https://www.mid.ru/ru/foreign_policy/official_documents/1860586/ (accessed: 20.12.2023). (In Russian)

36. *Letter from the permanent representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the UN addressed to the Secretary General dated 09.12.2011*. Available at: https://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf (accessed: 20.12.2023). (In Russian)

37. *On the results of the seminar of the ASEAN Regional Security Forum on the topic of countering the use of ICT for criminal purposes, 2023*. Available at: https://www.mid.ru/ru/detail-material-page/1804709/ (accessed: 20.12.2023). (In Russian)

38. *BRICS Sanyang Declaration of April 14, 2011*. Available at: http://www.kremlin.ru/supplement/907 (accessed: 20.12.2023). (In Russian)

39. *BRICS eThekwini Declaration of March 27, 2013*. Available at: http://nkibrics.ru/pages/summit-docs (accessed: 20.12.2023). (In Russian)

40. *Johannesburg BRICS Declaration of July 26, 2018*. Available at: http://nkibrics.ru/pages/summit-docs (accessed: 20.12.2023). (In Russian)

Received: April 10, 2024
Accepted: May 15, 2024

Author's information:

Valeria I. Bulva — PhD in History; va.i.bulva@my.mgimo.ru