Vestnik RUDN. International Relations. ISSN 2313-0660 (print), ISSN 2313-0679 (online)
2022 Vol. 22 No. 2 342—351
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
http://journals.rudn.ru/international-relations

НАУЧНЫЕ ШКОЛЫ

SCIENTIFIC SCHOOLS

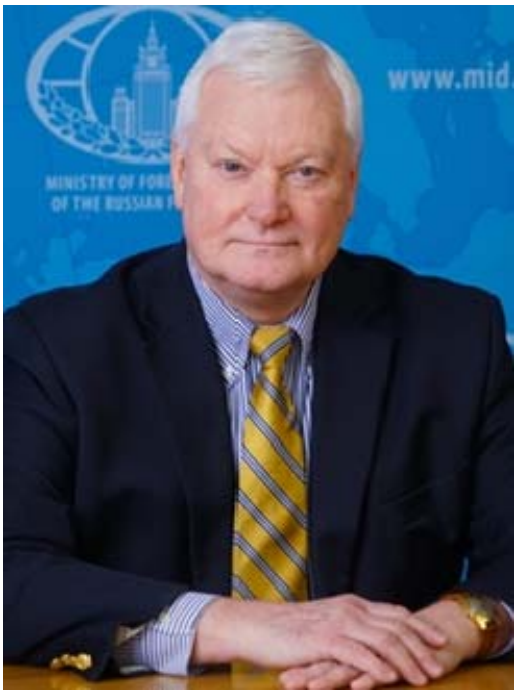
DOI: 10.22363/2313-0660-2022-22-2-342-351

Международная информационная безопасность: в поисках консолидированных подходов

Интервью с АНДРЕЕМ ВЛАДИМИРОВИЧЕМ КРУТСКИХ, Специальным представителем Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, Чрезвычайным и Полномочным Послом, директором Департамента международной информационной безопасности МИД России

Аннотация. Андрей Владимирович Крутских — Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности с 2014 г., ведущий эксперт в данной сфере в России и в мире. Он занимал должность председателя Группы правительственных экспертов ООН по достижениям в сфере информации и телекоммуникаций и Группы экспертов государств — членов ШОС по международной информационной безопасности (МИБ). С 2020 г. А.В. Крутских является директором Департамента международной информационной безопасности (ДМИБ) МИД России, с 2017 г. — директором Центра международной информационной безопасности и научно-технологической политики (ЦМИБ) МГИМО МИД России. Андрей Владимирович — автор фундаментальных работ, посвященных вопросам МИБ, научный редактор комплексного учебного пособия «Международная информационная безопасность: теория и практика» (в трех томах), подготовленного авторским коллективом ЦМИБ. В ходе интервью А.В. Крутских рассказал о подходах России в области МИБ, роли Российской Федерации в выработке правил ответственного поведения государств в глобальном информационном пространстве.

Ключевые слова: международная информационная безопасность, информационно-коммуникационные технологии, ООН, РФ, США, КНР



Для цитирования: *Крутских А. В.* Международная информационная безопасность: в поисках консолидированных подходов : интервью с Андреем Владимировичем Крутских, Специальным представителем Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности / интервью провел Д. А. Пискунов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 342—351. https://doi.org/10.22363/2313-0660-2022-22-2-342-351

International Information Security: In Search of Consolidated Approaches

Interview with ANDREY V. KRUTSKIKH,
Special Representative of the President of the Russian Federation
for International Cooperation in the Field of Information Security,
Ambassador Extraordinary and Plenipotentiary,
Acting Director of the Department of International Information Security
of the Russian Ministry of Foreign Affairs

Abstract. Andrey Vladimirovich Krutskikh is the Special Representative of the President of the Russian Federation for International Cooperation in the field of Information Security since 2014, and a leading expert in this field in Russia and around the world. He served as Chairman of the UN Panel of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the SCO Member States Panel of Experts on International Information Security (IIS). Since 2020, A.V. Krutskikh holds the position of Director of the Department for International Information Security (DIIS) of the Ministry of Foreign Affairs of Russia, since 2017 he is Director of the Center for International Information Security, Science and Technology Policy of MGIMO University. Andrey Vladimirovich is the author of fundamental works devoted to IIS issues, the scientific editor of the three volume comprehensive textbook "International Information Security: Theory and Practice," prepared by the CIIS team of authors. During the interview A.V. Krutskikh spoke about Russia's approaches to international information security, the role of our country in developing the rules of the responsible State behavior in the global information space.

Key words: international information security, information and communications technologies, United Nations, Russia, United States, China

For citation: Krutskikh, A. V. (2022). International information security: In search of consolidated approaches : Interview with Andrey V. Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security. Interviewed by D. A. Piskunov. *Vestnik RUDN. International Relations*, 22(2), 342—351. https://doi.org/10.22363/2313-0660-2022-22-2-342-351

— Уважаемый Андрей Владимирович, Россия стала инициатором процесса выработки норм, правил и принципов в сфере информационно-коммуникационных технологий (ИКТ) на площадке ООН в 1998 г. Значительные успехи на этом направлении были достигнуты при сотрудничестве с региональными объединениями, такими как СНГ, Организация Договора о коллективной безопасности (ОДКБ), Шанхайская организация сотрудничества (ШОС), БРИКС, Ассоциация государств Юго-Восточной Азии (АСЕАН), Лига арабских государств (ЛАГ), Африканский союз. Значит ли это, что Россия становится одним из лидеров в области разработки норм в сфере ИКТ?

— Россия стояла у истоков обсуждения проблематики обеспечения международной информационной безопасности (МИБ). В 1998 г. наша страна впервые внесла в Первом комитете Генеральной Ассамблеи ООН проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[1].

[1] Резолюция ГА ООН A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций

Предложенный РФ документ получил поддержку со стороны подавляющего большинства государств — членов Организации.

Профильный переговорный процесс развивался постепенно. В 2001 г. Россия инициировала создание Группы правительственных экспертов ООН (ГПЭ) — узкого по составу формата, в работе которого принимали участие представители 15—25 государств в личном качестве (Бирюков, Алборова, 2019). Цели этого механизма эволюционировали от изучения угроз в ИКТ-сфере до разработки элементов ее регулирования, прежде всего норм, правил и принципов ответственного поведения государств в информационном пространстве. Работа ГПЭ оказалась результативной: в итоговых докладах 2010, 2013 и 2015 гг.[2], принятых консенсусом, закреплены базовые принципы сотрудничества в области МИБ. В частности, 11 рекомендованных ГПЭ в 2015 г. добровольных правил включены в первоначальный свод международных правил, норм и принципов ответственного поведения государств, закрепленный российской резолюцией Генеральной Ассамблеи ООН № 73/27[3].

С течением времени круг государств, желающих участвовать и иметь право голоса в ооновской дискуссии по МИБ, расширялся. В ответ на запрос международного сообщества в 2018 г. Россия предложила создать качественно новый переговорный механизм — Рабочую группу ООН открытого состава (РГОС). Ее принципиальное отличие от ГПЭ — возможность всех без исключения государств — членов ООН «на равных» участвовать в процессе принятия конкретных решений в области МИБ и отстаивать интересы национальной безопасности. РГОС, известная как «Кибер-Генассамблея», является первым универсальным, инклюзивным, прозрачным и подлинно демократичным переговорным механизмом по проблематике МИБ в системе ООН (Зиновьева, 2020). Несмотря на трудности, обусловленные пандемией, РГОС успешно завершила свою деятельность в марте 2021 г. принятием итогового доклада консенсусом всех 193 государств — членов ООН[4].

31 декабря 2020 г. по инициативе России при поддержке внушительного большинства государств Генеральная Ассамблея ООН в ходе своей 75-й сессии одобрила российский проект резолюции, постановляющий созвать начиная с 2021 г. новую РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ на период 2021—2025 гг.[5] Такое решение служит подтверждением актуальности и необходимости обеспечения глобального переговорного процесса по вопросам МИБ. Следует отметить, что новая РГОС уполномочена обсуждать выдвигаемые государствами профильные предложения, вопросы наращивания потенциала, а также налаживания диалога стран (при их лидирующей роли) с

в контексте международной безопасности» // ООН. 04.01.1999. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 01.04.2022).

[2] См.: Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2010 г. (A/65/201) // ООН. 30.07.2010. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&referer=/english/&Lang=R (дата обращения: 01.04.2022); Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 г. (A/68/98) // ООН. 24.06.2013. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R (дата обращения: 01.04.2022); Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г. // ООН. 22.07.2015. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата обращения: 01.04.2022).

[3] Резолюция ГА ООН A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // ООН. 11.12.2018. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement (дата обращения: 01.04.2022).

[4] Доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2021 г. // ООН. 18.03.2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/74/PDF/N2106874.pdf?OpenElement (дата обращения: 01.04.2022).

[5] Резолюция Генеральной Ассамблеи ООН A/RES/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // ООН. 04.01.2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement (дата обращения: 01.04.2022).

бизнесом, неправительственными организациями и научно-академическим сообществом.

Успех Группы зависит от целой серии факторов, среди которых ключевой — ее субстантивное наполнение. Принципиально важно придать деятельности РГОС максимально прагматичный и практико-ориентированный характер, чтобы итогом ее работы стали прикладные нормы, рекомендации и программы помощи.

Безусловно, значительные успехи на этом направлении достигнуты при сотрудничестве с региональными объединениями. Россия активно взаимодействует с государствами СНГ, ОДКБ, ШОС, БРИКС, АСЕАН, Региональный форум АСЕАН (АРФ), ЛАГ, Африканского союза. Работа на данных площадках направлена на согласование конкретных решений по обеспечению МИБ. Выработка норм, правил и принципов ответственного поведения активно обсуждается в БРИКС и ШОС. Противодействие информационной преступности — один из ключевых аспектов дискуссии по линии ОДКБ, СНГ, АСЕАН, АРФ. В рамках АСЕАН идет разработка понятийного аппарата в сфере безопасного использования ИКТ. Россия также заключила целый ряд двусторонних межправительственных соглашений, которые позволяют углублять диалог с государствами-единомышленниками в сфере МИБ (Крутских, Бирюков, 2017).

Можно сказать, что Россия продолжает задавать тон международному сотрудничеству в данной области, добиваясь выработки правил ответственного поведения под эгидой ООН, которые должны базироваться на следующих принципах:

– суверенное равенство;

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

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

– уважение прав человека и основных свобод;

– невмешательство во внутренние дела других государств[6].

— Какие школы осмысления обеспечения МИБ, на ваш взгляд, сложились на сегодняшний день в мире? Какие исследовательские инициативы, а также каких авторитетных экспертов вы можете отметить в этой связи? Можно ли разделить их на группы в зависимости от подходов?

— В настоящее время важную роль в международном сотрудничестве играет публичная дипломатия. К обсуждению различных аспектов МИБ активно подключаются представители научно-академического сообщества. На базе МГИМО МИД России функционирует Центр международной информационной безопасности и научно-технологической политики (ЦМИБ), который непосредственно вовлечен в обсуждение вопросов использования ИКТ в рамках РГОС, а также на региональных и двусторонних площадках[7]. В марте 2022 г. сотрудники ЦМИБ приняли участие в неформальной онлайн-встрече председателя РГОС Б. Гафура с представителями заинтересованных негосударственных сторон, после чего был опубликован аналитический доклад ЦМИБ об основных подходах России по МИБ (International Information Security…, 2021). Помимо этого, сотрудники Центра на регулярной основе выступают на мероприятиях по линии СНГ, ОДКБ, ШОС, БРИКС, АРФ и АСЕАН.

ЦМИБ вносит важный вклад в подготовку профессиональных кадров. В 2019 г. был выпущен учебник в трех томах «Международная информационная безопасность: теория и практика» (2019), который в 2021 г. был переиздан и дополнен (Международная информационная безопасность: теория и практика,

[6] Резолюция Генеральной Ассамблеи ООН A/RES/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // ООН. 04.01.2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement (дата обращения: 01.04.2022).

[7] Центр международной информационной безопасности и научно-технологической политики // МГИМО МИД России. URL: https://mgimo.ru/about/structure/ucheb-nauch/ciis/ (дата обращения: 01.04.2022).

2021). Это первое в мире комплексное издание по данной теме, представляющее собой фактически научную онтологию по МИБ. На базе учебника был подготовлен инновационный цифровой образовательный комплекс «Международная информационная безопасность: теория и практика», который был выдвинут на премию Правительства России в области образования за 2021 г. и вошел в «короткий список» номинантов.

В рамках программы «Приоритет — 2030» ЦМИБ подготовил доклад «Международная информационная безопасность: подходы России», в котором в доступном для широкой аудитории формате представлены самые насущные проблемы МИБ, а также комплексно охарактеризованы подходы России к формированию международного режима в области безопасности ИКТ на глобальном, региональном и двустороннем уровнях (International Information Security: Russia's Approaches, 2021). Доклад был представлен на площадке ООН и получил широкое признание в академическом и дипломатическом сообществе.

Кроме того, на площадке МГИМО проходят конференции, форумы, семинары и круглые столы, в ходе которых обсуждаются актуальные аспекты цифровой повестки дня 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 данной области.

Можно сказать, что вокруг ЦМИБ сформировалась уникальная научная школа МГИМО в области исследования международной информационной безопасности и научно-технологической политики. Центр отстаивает национальные интересы Российской Федерации и оказывает экспертную поддержку экспертам страны в данной сфере. Научные труды ЦМИБ широко цитируются российскими и зарубежными учеными и задают направление для дальнейшей проработки этих вопросов и подготовки нового поколения исследователей. Сотрудники Центра активно публикуют статьи в научных изданиях, за их авторством выходят монографии, учебная и методическая литература.

Практико-ориентированное направление научных исследований в области МИБ формируется на базе созданной в 2018 г. Национальной Ассоциации международной информационной безопасности (НАМИБ)[8]. Президентом Ассоциации является советник секретаря Совета Безопасности РФ В.П. Шерстюк, члены Ассоциации — ведущие эксперты страны в области МИБ. Наблюдательный совет НАМИБ возглавляет заместитель секретаря Совета Безопасности РФ О.В. Храмов. Согласно Уставу Ассоциации, одной из основных ее целей является содействие продвижению российских инициатив в области обеспечения МИБ с проработкой в упреждающем режиме проблемных вопросов в интересах формирования переговорных позиций государственных органов. При обсуждении проекта «Основ государственной политики Российской Федерации в области международной информационной безопасности» 26 марта 2021 г. президент России В.В. Путин особо подчеркнул роль НАМИБ в реализации государственной политики России на данном направлении[9].

Действительно, в условиях, когда коллективный Запад развязал против России агрессивную кибервойну, взаимодействие по линии научно-академического сообщества имеет особое значение, поскольку многие контакты с Россией на государственном уровне по обеспечению МИБ прерваны. Углубленный экспертный разговор на полуторном треке — уникальный источник идейной «подпитки» усилий России на международной арене и в то же время объективного и нетривиального взгляда на перспективы многосторонней дискуссии.

[8] Национальная Ассоциация Международной Информационной Безопасности (НАМИБ). URL: https://namib.online/ (дата обращения: 01.04.2022).

[9] Президент провел в режиме видеоконференции заседание Совета Безопасности, в ходе которого рассматривался проект «Основ государственной политики Российской Федерации в области международной информационной безопасности» // Совет Безопасности РФ. 26.03.2021. URL: http://www.scrf.gov.ru/news/speeches/2952/ (дата обращения: 01.04.2022).

НАМИБ, в свою очередь, обладает богатым опытом проведения международных форумов и конференций, в том числе в Гватемале, Германии, Китае, на Кубе и т. д. В условиях пандемии Ассоциацией организован форум «Партнерство государства, бизнеса и гражданского общества при обеспечении МИБ», выпущены сборники докладов, а также аналитические, научные и методические работы[10].

Молодые исследователи также вовлекаются в научное осмысление МИБ и переговорную деятельность на данном направлении. Локомотивом для продвижения молодежных инициатив служит Школа международной информационной безопасности Дипломатической академии МИД России, которая регулярно проводит на своей площадке открытые лекции по актуальным аспектам МИБ, участвует в научных конференциях, семинарах и круглых столах по профильной тематике[11].

Проблематика обеспечения МИБ интересует и зарубежных исследователей. Нельзя не отметить ведущие научные центры КНР, которые занимаются изучением данного направления и прикладной работой. Прежде всего, речь идет об Ассоциации Интернета Китая[12], Китайской ассоциации безопасности киберпространства[13], Комитете федерации промышленности и торговли по эксплуатации и обслуживанию больших данных[14], Центре безопасности «360»[15]. Значительное внимание китайское научно-академическое сообщество уделяет изучению глобального управления Интернетом. Янь Сюэтун, директор Института современных международных отношений Университета Цинхуа, главный редактор «Китайского журнала о международной политике», рассматривает киберпространство в качестве ключевого драйвера развития мировой политики и международных отношений. Он выделяет глобальное управление киберпространством в качестве стратегической области противостояния США и КНР (Yan Xuetong, 2020). Кроме того, особое место в литературе КНР занимает проблематика технологической конкуренции США и КНР и ее последствий для глобального управления Интернетом (Li Zhi & Tang Runhua, 2020). Ряд авторов рассматривают китайский подход к глобальному управлению Интернетом в контексте национальной безопасности и цифрового суверенитета (Xu Peixi, 2021; Wang Zheng, 2020).

Исследованием проблематики кибербезопасности и роли КНР в ее обеспечении занимается Лаборатория Лейденского университета под руководством Р. Кримерса в рамках проекта *China's Role in Cyber Security*[16]. Р. Кримерс, профессор Лейденского университета, соучредитель проекта *DigiChina*, исследует регулирование КНР в области цифровых технологий, а также политику Китая в глобальном управлении Интернетом (Creemers, 2022).

Двусторонние отношения России и Китая носят характер всеобъемлющего стратегического партнерства. Наши страны придерживаются схожих взглядов в области обеспечения МИБ, поддерживают выработку под эгидой ООН правил ответственного поведения государств в информпространстве.

Подходы западных стран отличаются от продвигаемых Россией и Китаем. Главным достижением научной школы коллективного

[10] Программа XV международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении МИБ» // НАМИБ. 24.09.2021. URL: https://namib.online/2021/09/programma-xvmezhdunarodnogo-foruma-partnerstvo-gosudarstva-biznesa-i-grazhdanskogo-obshhestva-pri-obespechenii-mezhdunarodnoj-informacionnoj-bezopasnosti/ (дата обращения: 01.04.2022).

[11] Школа МИБ // Дипломатическая академия МИД России. URL: https://www.dipacademy.ru/special-projects/mib-school/ (дата обращения: 01.04.2022).

[12] Zhongguo hulianwang xiehui [Интернет-сообщество Китая]. URL: https://www.isc.org.cn (accessed: 01.04.2022). (На китайском языке).

[13] Zhongguo wangluo kongjian anquan xiehui [Ассоциация кибербезопасности Китая]. URL: https://www.cybersac.cn (accessed: 01.04.2022). (На китайском языке).

[14] Zhonghua quanguo gongshangye lianhehui [Всекитайская федерация промышленности и торговли]. URL: https://www.acfic.org.cn/zzjg_327/zmwyh/2021_wlaqwyh/2021_wlaqwyh_md (accessed: 01.04.2022). (На китайском языке).

[15] 360 qiye anquan hui [Ассоциация корпоративной безопасности «360»]. URL: https://www.360.cn (accessed: 01.04.2022). (На китайском языке).

[16] China's Role in Cyber Security // Leiden Asia Centre. URL: https://leidenasiacentre.nl/chinas-role-in-cyber-security/ (accessed: 01.04.2022).

Запада в области МИБ (следует отметить, что в западном научном дискурсе чаще используется термин «кибербезопасность») считается публикация Таллиннского руководства и Таллиннского руководства 2.0 о применимости международного права к конфликтам и войнам в информационной сфере, подготовленного сотрудниками Центра киберзащиты НАТО в Таллинне под руководством профессора права М. Шмидта[17]. Данное издание — академический научный труд, не имеющий обязательной юридической силы, но претендующий на продвижение западной переговорной позиции по МИБ, по сути допускающей использование ИКТ в военных целях. Следует также отметить, что внутри западной научной школы в данной области имеют место существенные содержательные и идеологические расколы.

В этом контексте хотелось бы отметить, что Россия выступает за более активное вовлечение бизнеса, неправительственных организаций и научно-академического сообщества в глобальную дискуссию по вопросам обеспечения информбезопасности. На наш взгляд, специфика ИКТ такова, что представители негосударственных субъектов могут внести весомый содержательный вклад в решение задач, стоящих перед международным сообществом.

— В 2020 г. китайские компании China Mobile и Huawei при поддержке заинтересованных министерств выдвинули предложение в рабочей группе МСЭ о разработке новых протоколов IP-адресов, способствующих дальнейшему развитию передовых технологий, в том числе 5G. Как вы считаете, могут ли предложенные стандарты стать альтернативой существующим протоколам сети Интернет, созданным по запросам Запада?

— Ключевую роль в управлении Сетью играют Корпорация по управлению доменными именами и IP-адресами (ICANN)[18] и ее дочерняя структура — Организация по открытым техническим идентификаторам (PTI)[19]. Несмотря на то, что ICANN формально является независимой некоммерческой организацией, фактически контроль над распределением имен и адресов Интернета осуществляет правительство США. Негосударственный статус ICANN выступает в роли «ширмы», призванной прикрыть американскую гегемонию США.

Что касается Международного союза электросвязи (МСЭ)[20], то данная специализированная структура ООН ни юридически, ни политически не вовлечена в управление Интернетом, поскольку ее участие в данном процессе открыто саботируют США и их партнеры. Россия уже давно выступает за передачу прерогатив по управлению Интернетом МСЭ, который обладает необходимой экспертизой и легитимностью в данных вопросах (Зиновьева, 2009). Естественно, такие предложения противоречат принципиальным подходам США по сохранению контроля над Сетью.

Россия и Китай последовательно выступают за интернационализацию управления глобальной сетью Интернет, повышение роли государств в этом процессе, а также сохранение их суверенного права регулировать национальный сегмент Интернета (International Information Security…, 2021). Китай также активно участвует в принятии универсальных стандартов в области сетей связи пятого поколения 5G. Со стороны Китая и китайских компаний ведется работа по разработке новых протоколов IP-адресов. Все эти действия в конечном итоге направлены на интернационализацию международного управления Интернетом и повышение роли глобального сообщества в данном процессе в целях

[17] Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence / ed. by M.N. Schmitt. Cambridge ; New York : Cambridge University Press, 2013. URL: https://assets.cambridge.org/97811070/24434/frontmatter/9781107024434_frontmatter.pdf (accessed: 01.04.2022).

[18] The Internet Corporation for Assigned Names and Numbers (ICANN). URL: https://www.icann.org/en (accessed: 01.04.2022).

[19] Public Technical Identifiers (PTI). URL: https://pti.icann.org/ (accessed: 01.04.2022).

[20] International Telecommunication Union. URL: https://www.itu.int/ru/Pages/default.aspx (accessed: 01.04.2022).

придать ему инклюзивный и демократичный характер (Routledge Handbook of International Cybersecurity, 2020). Повторю, оптимальной институциональной базой для этого является МСЭ.

— США заморозили сотрудничество с Россией по вопросам кибербезопасности. Страны Запада на сессии Рабочей группы ООН открытого состава обвинили Россию во вредоносной деятельности в информпространстве. Как дальше будет развиваться диалог между Россией и Западом в многостороннем и двустороннем форматах по выработке конвенции об обеспечении МИБ?

— Россия и США — страны, которые несут особую ответственность за поддержание глобального мира и безопасности. Наше взаимодействие выстраивалось по-разному, но с неизменным настроем России на достижение практических результатов.

25 сентября 2020 г. президент Российской Федерации В.В. Путин выступил с комплексной программой практических мер по восстановлению российско-американского сотрудничества в области МИБ[21]. Программа была ориентирована на повышение уровня доверия, перезагрузку отношений с США в целях недопущения масштабной конфронтации в цифровой среде и включала в себя следующие направления:

1) восстановление полномасштабного двустороннего регулярного межведомственного диалога по ключевым вопросам обеспечения МИБ на высоком уровне;

2) поддержание непрерывной и эффективной работы каналов связи между компетентными ведомствами наших стран по линии Центров по уменьшению ядерной опасности, Групп оперативного реагирования на компьютерные инциденты и должностных лиц высокого уровня, курирующих эту проблематику в рамках структур, связанных с вопросами обеспечения национальной, в том числе информационной, безопасности;

3) совместная разработка и заключение двустороннего межправительственного соглашения о предотвращении инцидентов в информационном пространстве по аналогии с действующим советско-американским Соглашением о предотвращении инцидентов в открытом море и воздушном пространстве над ним от 25 мая 1972 г.;

4) обмен во взаимоприемлемой форме гарантиями невмешательства во внутренние дела друг друга, включая избирательные процессы, в том числе с использованием ИКТ и других высокотехнологичных методов.

Кроме того, президентом Российской Федерации В.В. Путиным было предложено выйти на заключение глобальной договоренности о принятии государствами политического обязательства о ненанесении первыми удара с использованием ИКТ. Предметной реакции на российское предложение не последовало.

После июльского саммита в 2021 г. в Женеве между Россией и США был запущен профильный экспертный диалог в формате «Кремль — Белый дом» под эгидой аппарата Совета Безопасности Российской Федерации и Совета национальной безопасности США[22]. Был налажен обмен оперативной информацией по киберпреступлениям, увеличен объем и качество информации о компьютерных инцидентах, передаваемой между Национальным координационным центром по компьютерным инцидентам России и Агентством кибербезопасности и защиты инфраструктуры США. Активизировалось двустороннее взаимодействие Генеральной прокуратуры Российской Федерации с Министерством юстиции США. Тем не менее, несмотря на опыт позитивного взаимодействия в данной сфере, весной 2022 г. Белый дом в одностороннем порядке вышел из единственного постоянно действующего канала связи с Кремлем. Кроме того, Вашингтон отказался от дальнейшего обсуждения вопросов безопасности

[21] Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности // Президент России. 25.09.2020. URL: http://kremlin.ru/events/president/news/64086 (дата обращения: 01.04.2022).

[22] Белый дом и Кремль согласились, что диалог — лучший способ деэскалации // Интерфакс. 31.12.2021. URL: https://www.interfax.ru/world/813561 (дата обращения: 01.04.2022).

объектов критической информационной инфраструктуры. Была остановлена и вся совместная работа по пресечению деятельности киберпреступников. США отказались от российского предложения деанонимизировать Интернет и принудили своих союзников не поддерживать нашу инициативу о принятии международного юридически обязывающего документа, регулирующего деятельность государств в информпространстве.

Вследствие односторонней и деструктивной позиции коллективного Запада снижается общий уровень информационной безопасности в мире. Количество кибератак последние годы растет. С начала 2022 г. западные страны многократно нарастили атаки на нашу страну — до миллиона в неделю.

20 мая 2022 г. под председательством президента Российской Федерации В.В. Путина состоялось заседание Совета Безопасности Российской Федерации, в ходе которого обсуждались вопросы информационной безопасности[23]. Президент России отметил, что в настоящее время предпринимаются целенаправленные попытки вывести из строя интернет-ресурсы объектов критической информационной инфраструктуры России[24]. В первую очередь под ударом оказались средства массовой информации, финансовые учреждения, социально значимые порталы. Кроме того, инструментом санкционного давления на Россию со стороны Запада стали ограничения на зарубежные информационные технологии, программы и продукты. Многие западные поставщики в одностороннем порядке прекратили техническую поддержку своего оборудования в России. Участились случаи ограничения работы или даже блокировки программ после их обновления. Однако уже сегодня можно сказать, что кибератрессия против России, как и в целом санкционный наскок на нашу страну, провалилась. В целом мы были готовы к этой атаке, и это результат той системной работы, которая велась все последние годы[25].

Вне зависимости от геополитической обстановки Россия остается открытой к диалогу и сотрудничеству на принципах взаимного доверия и уважения национальных интересов со всеми государствами, и США в этом смысле не исключение.

Что касается Конвенции об обеспечении МИБ, то впервые идея была озвучена Российской Федерацией в Екатеринбурге в 2011 г. на встрече высоких представителей, курирующих вопросы безопасности. Соавторами российского проекта тогда выступили 52 государства[26]. Обновленный проект Конвенции Россия представила в 2021 г. Сегодня ключевой площадкой для обсуждения положений будущей Конвенции об обеспечении МИБ является РГОС. В целях поддержания стратегической стабильности и обеспечения защиты от киберугроз недостаточно норм, которые носят добровольный и рекомендательный характер, требуется юридическое закрепление «правил дорожного движения» в ИКТ-среде.

— Как вы считаете, ускорится ли в перспективе процесс технологического разъединения на Запад, придерживающийся своей парадигмы кибербезопасности, и не-Запад, отстаивающий концепцию международной информационной безопасности и суверенное управление внутренним сегментом сети Интернет?

— Тенденции последних лет и тем более месяцев свидетельствуют о том, что раскол мирового сообщества на Запад и не-Запад продолжается.

Цель США и стран НАТО — восстановить и навеки закрепить свое доминирование в международных делах, чтобы решать собственные узкокорыстные задачи в ущерб национальным интересам других членов международного сообщества. Они противопоставляют пресловутый «миропорядок,

[23] Под председательством Владимира Путина в режиме видеоконференции состоялось заседание Совета Безопасности Российской Федерации // Совет Безопасности РФ. 20.05.2022. URL: http://www.scrf.gov.ru/news/allnews/3240/ (дата обращения: 21.05.2022).

[24] Там же.

[25] Заседание Совета Безопасности // Президент России. 20.05.2022. URL: http://kremlin.ru/events/president/news/68451 (дата обращения: 21.05.2022).

[26] Россия указала выход для интернета // Коммерсантъ. 23.09.2011. URL: https://www.kommersant.ru/doc/1779208 (дата обращения: 01.04.2022).

основанный на правилах», который на практике означает закрепление права сильного в мировых делах, традиционному пониманию системы международных отношений, основанной на международном праве.

Россия и ее единомышленники выступают за развитие всеобъемлющего сотрудничества в области МИБ с учетом интересов всех государств. Первостепенная задача — выработка международно-правовых основ деятельности стран, а также неправительственных субъектов в сфере ИКТ.

Текущая обстановка на глобальной арене едва ли располагает к оптимистическим прогнозам. Тем не менее безопасность в киберсфере требует международных договоренностей. Ставки слишком высоки, чтобы полагаться на игру без правил.

Невозможно существование кибермира, в котором отдельные государства стремятся укрепить свою безопасность за счет безопасности других. Необходимо всем мировым сообществом работать над предотвращением конфликтов в информационном пространстве, продвижением мирного использования ИКТ, недопущением их применения в преступных и террористических целях, а также продолжением профильных переговоров при центральной роли ООН. Иначе, как заявил С.В. Лавров, миру грозит киберанархия[27].

[27] Выступление Министра иностранных дел Российской Федерации С.В. Лаврова на пленарной сессии «Международные отношения в условиях цифровизации общественной жизни» международной научно-практической конференции «Цифровые международные отношения 2022», Москва, 14 апреля 2022 года // МИД России. 14.04.2022. URL: https://www.mid.ru/ru/foreign_policy/news/1809294/ (дата обращения: 01.05.2022).

Интервью провел Д.А. Пискунов / Interviewed by D.A. Piskunov

Поступила в редакцию / Received: 10.05.2022

Библиографический список

Бирюков А. В., Алборова М. Б. Социально-гуманитарное измерение международной информационной безопасности. Москва : Аспект Пресс, 2019.

Зиновьева Е. С. Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества. Москва : МГИМО, 2020.

Зиновьева Е. С. Международное управление интернетом: конфликт и сотрудничество. Москва : МГИМО, 2009.

Крутских А., Бирюков А. Новая геополитика международных научно-технологических отношений // Международные процессы. 2017. № 2. С. 6—26.

Международная информационная безопасность: теория и практика : в 3 т. / под общ. ред. А. В. Крутских. Москва : Аспект Пресс, 2019.

Международная информационная безопасность: теория и практика : в 3 т. / под общ. ред. А. В. Крутских. Москва : Аспект Пресс, 2021.

Creemers R. China's Cybersecurity Regime: Securing the Smart State. Leiden University, 2022. P. 1—38. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4070682 (accessed: 01.04.2022).

International Information Security: Russia's Approaches / ed. by A. Krutskikh, E. Zinovieva. Moscow, 2021.

Li Zhi, Tang Runhua. Duo li yi you guan fang mo shi : gou jian quan qiu hu lian wang zhi li ti xi de lu jing yan jiu [Многосторонняя модель: путь к созданию глобальной системы управления Интернетом] // Chuan mei guan cha [Медиа обозреватель]. 2020. Vol. 444, no. 12. P. 21—28. (На китайском языке).

Routledge Handbook of International Cybersecurity / ed. by E. Tikk, M. Kerttunen. Routledge, 2020.

Wang Zheng. Lian he guo "shuang gui zhi" xia quan qiu wang luo kong jian gui ze zhi ding xin tai shi [Глобальное управление Интернетом на пути к цифровой холодной войне или цифровому достоянию] // Zhong guo xin xi an quan [Информационная безопасность Китая]. 2020. Vol. 20, no. 1. P. 40—43. (На китайском языке).

Xu Peixi. 2020 shu zi leng zhan yuan nian: wang luo kong jian quan qiu zhi li de liang zhong lu xian zhi zheng [Год цифровой холодной войны 2020: битва двух путей глобального управления в киберпространстве] // Xin xi an quan yu tong xin bao mi [Информационная безопасность и конфиденциальность связи]. 2021. Vol. 21, no. 3. P. 16—23. (На китайском языке).

Yan Xuetong. Bipolar Rivalry in the Early Digital Age // The Chinese Journal of International Politics. 2020. Vol. 13, no. 3. P. 313—341. https://doi.org/10.1093/cjip/poaa007