# МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ В ЦИФРОВУЮ ЭПОХУ

УДК 327.56, 327.57, 327.7, 327.8

## Система международной информационной безопасности в условиях политической турбулентности

*С. А. Себекин*

Иркутский государственный университет,
Российская Федерация, 664003, Иркутск, ул. Карла Маркса, 1

**Для цитирования:** *Себекин С. А.* Система международной информационной безопасности в условиях политической турбулентности // Вестник Санкт-Петербургского университета. Международные отношения. 2023. Т. 16. Вып. 2. С. 170–190. https://doi.org/10.21638/spbu06.2023.205

Статья посвящена рассмотрению основных изменений, происходящих в системе обеспечения международной информационной безопасности после начала специальной военной операции на Украине. Делается попытка спрогнозировать вызовы и риски, с которыми столкнется система обеспечения МИБ в перспективе. Первоочередные трансформации связаны с переговорным процессом в рамках ООН, который в условиях нарастания политического антагонизма между ключевыми субъектами диалога становится все более политизированным и начинает испытывать некоторые трудности. Предполагается, что в условиях новой политической реальности нерешенным останется вопрос о «всеобъемлющем» противодействии международной киберпреступности. Наблюдается некоторая фрагментация самой системы международной информационной безопасности, которая испытывает центробежные тенденции в условиях продвижения альтернативных друг другу подходов к решению ключевых вопросов в этой сфере. Наконец, можно ожидать, что Соединенные Штаты во взаимодействии с Россией более активно задействуют проактивную стратегию так называемой *упреждающей защиты,* которая должна осуществляться посредством концепции *постоянной вовлеченности.* Также рассмотрены предварительные выводы, которые продемонстрировали действия на Украине, касательно роли и места кибератак непосредственно в рамках вооруженного конфликта. Предполагается, что в ближайшем будущем кибератаки не будут рассматриваться как средство достижения реальных стратегических эффектов на поле боя, где доминирующую роль играют конвенциональные вооружения. Делается попытка дать некоторые рекомендации по сохранению определенной динамики развития системы МИБ.

*Ключевые слова:* международная информационная безопасность, РГОС ООН, *Программа действий*, киберпреступность, упреждающая защита.

24 февраля 2022 г. с началом российской специальной военной операции (СВО) на Украине мир вступил в новый международно-политический кризис. Нарастающие противоречия затронули и сферу киберполитики. В связи с этим сегодня существует определенный риск того, что в будущем можно будет наблюдать некоторую фрагментацию усилий по обеспечению глобальной информационной безопасности или даже изменения в архитектуре глобальной системы обеспечения международной информационной безопасности (МИБ), определенные признаки чего мы можем наблюдать уже сейчас.

В данной работе будет рассмотрено, каким образом политический конфликт на Украине повлиял на становление системы МИБ в глобальном масштабе — как в рамках главного переговорного формата ООН, так и во взаимодействии по киберповестке между двумя ключевыми бенефициарами международного переговорного процесса — Россией и Соединенными Штатами. Также кризис показал, какую роль кибератаки могут играть непосредственно в вооруженном конфликте, тем самым давая некоторые представления о том, в каком направлении система МИБ должна развиваться дальше.

## Вопросы терминологии

В данной работе используются как термин «информационный», так и термины с приставкой «кибер-». В то время как западная приставка «кибер-» подразумевает под собой сугубо технические аспекты воздействия (в отношении конкретных устройств, систем, сетей, технологических процессов, цифровой инфраструктуры), термин «информационный» — российского происхождения и носит амбивалентный характер: под ним понимаются как информационно-технические, так и информационно-психологические воздействия. Несмотря на то что термин «информационный» используется в России на официальном уровне (в том числе в документах), вместе с тем термины с приставкой «кибер-» также получили в российском публичном пространстве широкое использование, под ними подразумеваются чисто технические аспекты. В данной статье речь идет в основном о воздействиях технического характера — т. е. в отношении устройств, сайтов, технологических систем и т. д. В целом, когда речь идет о российском дискурсе по рассматриваемому вопросу, мы будем употреблять термин «информационный». Однако в тех случаях, когда подобное разграничение важно и нам надо подчеркнуть сугубо технический аспект воздействий, мы будем использовать термины с приставкой «кибер-».

## Что такое система международной информационной безопасности?

Можно говорить, что на сегодняшний день система МИБ находится на стадии своего становления, т. е. предпринимаются конкретные усилия по обеспечению МИБ и идут активные обсуждения данного вопроса, но нет общепризнанной, четкой и унифицированной международно-правовой базы. «Основы государственной политики Российской Федерации в области международной информационной безопасности», утвержденные указом президента РФ от 12 апреля 2021 г., определяют систему обеспечения МИБ как «совокупность международных и национальных институтов, регулирующих деятельность в глобальном информационном про-

странстве в целях предотвращения (минимизации) угроз международной информационной безопасности» [1]. Вместе с тем стоит отметить, что формирующаяся система обеспечения МИБ более многоаспектна и включает в себя не только непосредственно международные и национальные институты, но и широкий спектр акторов.

Во-первых, как уже было сказано, это сами международные институты, в рамках которых ведутся переговорные процессы по вопросу обеспечения МИБ, а также принимаемые в их рамках документы. Ключевые переговорные процессы проходят в ООН (об этом будет рассказано далее). Также профильные вопросы обсуждаются в рамках БРИКС (Рабочая группа экспертов государств по вопросам безопасности в сфере использования ИКТ), ШОС (Группа экспертов государств — членов ШОС по МИБ), Международного союза электросвязи, ЮНЕСКО, МАГАТЭ, ОДКБ, ОБСЕ, АТЭС, АСЕАН, НАТО (ранее вопросы МИБ обсуждались также в ходе диалога Россия — НАТО) и т. д.

Во-вторых, акторами, формирующими систему МИБ, являются государства и их правительства. Помимо инициатив, которые сами государства выдвигают в рамках ООН (о чем также будет рассказано далее), здесь можно выделить отдельные правительственные инициативы, выдвигаемые в «частном порядке». Заслуживает внимания инициатива Франции «Парижский призыв к доверию и безопасности в киберпространстве», представленная 12 ноября 2018 г. на Форуме по управлению интернетом. На настоящий момент к призыву присоединились не только 79 государств, но и 706 некоммерческих и коммерческих организаций, а также 391 организация гражданского общества[1]. Стоит упомянуть инициативу властей Швейцарии «Женевский диалог об ответственном поведении в киберпространстве» 2018 г., цель которой — определение ролей и зон ответственности различных субъектов в обеспечении глобальной кибербезопасности. Немаловажную роль в формировании и развитии системы международной информационной безопасности играет и частный сектор (компании). В 2018 г. по инициативе компании Microsoft был создан консорциум Cybersecurity Tech Accord с целью объединения усилий по противодействию киберугрозам и продвижения норм ответственного поведения в киберпространстве (на настоящий день к инициативе присоединилось более 150 компаний). 16 февраля 2018 г. на Мюнхенской конференции по безопасности девять компаний, среди которых Daimler, Airbus, IBM и др., подписали совместную «Хартию доверия» в сфере кибербезопасности, разработанную по инициативе Siemens.

Далее вклад в формирование системы МИБ вносят неправительственные, межправительственные и некоммерческие организации, область деятельности которых фокусируется на обсуждении вопросов информационной безопасности, предоставлении рекомендаций и публикации соответствующих отчетов и которые, в частности, вносят свои предложения в рамках переговорного процесса ООН на правах неформальных членов. Среди них можно выделить Институт кибермира (CyberPeace Institute), Глобальную комиссию по стабильности киберпространства (Global Commission on the Stability of Cyberspace, прекратила работу в декабре 2021 г.) и т. д. В общем и целом систему МИБ можно описать как деятельность

[1] По состоянию на 4 марта 2023 г.

и взаимодействие международных организаций, государств, негосударственных игроков с различной формой организации, других субъектов международных отношений, направленные на обеспечение МИБ, создание и разработку универсальных правил поведения в кибер-/информационном пространстве и предотвращение информационных угроз, также включающих в себя принятие соответствующих документов. Безусловно, важнейшей частью системы МИБ является также и двух- и многостороннее взаимодействие государств по киберповестке. Вместе с тем формирование системы МИБ предполагает не обособленную деятельность вышеуказанных субъектов, а общность их интересов и совместное участие в обсуждении проблем МИБ. Так, в переговорном процессе ООН принимают участие не только государства, но и представители частного сектора, НКО, академические сообщества, в том числе вышеупомянутые Cybersecurity Tech Accord, Институт кибермира, Глобальная комиссия по стабильности киберпространства и т. д. Однако в этом плане политический кризис на Украине дестабилизировал эту систему, замедлил процесс ее построения на открытых и инклюзивных началах, хотя главный переговорный процесс в ООН продолжается с переменным успехом.

## Состояние переговорного процесса по вопросу обеспечения международной информационной безопасности в рамках ООН

На сегодняшний день основу формирования системы МИБ составляет переговорный процесс в рамках Организации объединенных наций, так как именно здесь проходят ключевые обсуждения вопроса об установлении правил приемлемого поведения в киберпространстве. Однако несмотря на то что переговорный процесс по вопросу обеспечения международной информационной безопасности в рамках функционирующей с 2018 г. Рабочей группы открытого состава ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС ООН) с переменным успехом продолжается, украинский политический кризис в некоторой степени дестабилизировал его и нарушил связи между некоторыми участниками профильного диалога на высшем уровне — Россией и США (и их союзниками), с одной стороны, и между правительствами и представителями негосударственных игроков — с другой.

Впервые вопрос об обеспечении международной информационной безопасности был внесен в повестку дня Организации объединенных наций именно Россией, когда в 1998 г. она представила проект резолюции под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» на заседании Первого комитета Генеральной Ассамблеи. Этот документ — своего рода правила поведения для государств в киберпространстве [2, с. 33].

Также именно по инициативе России в 2004 г. была создана Группа правительственных экспертов ООН (ГПЭ ООН) в сфере информатизации и телекоммуникаций в контексте международной безопасности с целью решения проблем международной информационной безопасности. За все время по итогам работы ГПЭ было принято три доклада — Доклады ГПЭ ООН от 2010, 2013 и 2015 гг. [3, с. 60–61, 64, 67; 4]. В группу входили как Россия, так и США. В 2017 г. работа ГПЭ ООН в сфере информатизации и телекоммуникаций в контексте международной безопасности завершилась полным провалом.

Первая «поляризация» диалога по вопросам МИБ в рамках ООН произошла в 2018 г., когда на 73-й сессии Генеральной Ассамблеи ООН в Первом комитете по пункту 96 повестки дня Россия и США представили два конкурирующих проекта резолюции — российский A/C. 1/73/L. 27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (и его обновленную версию A/C. 1/73/L. 27/Rev.1) и американский A/RES/73/266 «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности». Оба проекта 9 ноября были одобрены Первым комитетом Генассамблеи ООН подавляющим большинством голосов, а 5 декабря приняты Генеральной Ассамблеей подавляющим большинством голосов [5; 6].

Ключевое отличие этих резолюций заключалось в том, что американская инициатива предусматривала «воссоздание» ГПЭ ООН с ограниченным числом участников, а российская инициатива предлагала создание кардинально новой *Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС ООН)* с более высоким статусом в рамках ООН и новым форматом работы, предусматривающим не только расширение состава государств-участников на их добровольной основе, но и *включение «предпринимательских кругов, неправительственных организаций и научного сообщества»*.

В итоге в конце 2018 г. в рамках ООН параллельно было создано сразу два переговорных формата по вопросу решения проблем международной информационной безопасности — РГОС ООН и ГПЭ ООН, что являлось отражением той поляризации, которую занимали по отношению друг к другу Россия и США в вопросе обеспечения глобальной информационной безопасности. По итогам работы двух групп были приняты соответствующие доклады — 10 марта 2021 г. приняла свой доклад РГОС ООН, а 14 июля 2021 г. — ГПЭ ООН.

8 октября 2021 г. Россия и США внесли на рассмотрение Первого комитета 76-й Генеральной Ассамблеи ООН совместный проект резолюции A/C. 1/76/L. 13 об установлении универсальных правил поведения в киберпространстве, название которого было создано путем сложения названий предыдущих российской и американской инициатив от 2018 г. — «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере применения информационно-коммуникационных технологий». Принятая резолюция отмечает усилия, предпринятые в рамках РГОС (наравне с ГПЭ) по обеспечению международной информационной безопасности. 3 ноября 2021 г. на заседании Первого комитета резолюция была принята без голосования [7]. Совместная инициатива стала возможна благодаря договоренностям, достигнутым В. В. Путиным и Джо Байденом в ходе российско-американского саммита в Женеве в 2021 г. Важность этого события для рассматриваемого вопроса заключалась в следующем. Во-первых, согласно резолюции, с этого момента в ближайшем будущем РГОС становится единственным в ООН форматом, в рамках которого будут вестись основные обсуждения проблемы обеспечения международной информационной безопасности на самом высоком уровне. Во-вторых, это означает практически «автоматическое» признание проделанных в рамках РГОС усилий со стороны всех соавторов новой резолюции, среди которых помимо Рос-

сии оказались США и их союзники — Австралия, Франция, Германия, Великобритания, Япония, которые ранее были «по другую сторону окопа».

На сегодняшний день, как представляется, определенной кульминацией напряженности стало возвращение к своеобразной конкуренции в области продвижения глобальных инициатив и поляризации усилий — в октябре 2022 г. на 77-й сессии Генеральной Ассамблеи ООН по вопросу обеспечения МИБ вновь были представлены два конкурирующих проекта резолюций (как это было в 2018 г.). Первый — российский проект «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/C. 1/77/L. 23). Второй проект — инициатива Франции и Египта «Программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности» (A/C. 1/77/L. 73), выдвинутая в ООН еще осенью 2020 г. с целью создания в ООН единственного (взамен работавших тогда еще РГОС и ГПЭ) и постоянно действующего переговорного формата, которую теперь уже поддержали США. Несмотря на поддержку РГОС, резолюция предусматривает после окончания ее мандата в 2025 г. запуск нового в ООН формата — соответственно «Программы действий». 3 ноября 2022 г. Первый комитет Генеральной Ассамблеи ООН одобрил оба проекта резолюций [8].

Собственно, в данном случае риски фрагментации могут проявляться в том, что обсуждение вопросов МИБ вновь будет проходить в рамках двух конкурирующих форматов — РГОС и новой Программы действий. Сама резолюция о «Программе действий» очень положительно оценивает результаты, достигнутые в рамках РГОС, заявляя о ее «эволюционной основе», и даже поддерживает ее работу, позиционируя «Программу действий» в качестве не конкурирующего, а взаимодополняющего формата (пусть и полноценного). Резолюция России и ее партнеров предусматривает ведение переговорного процесса лишь в рамках РГОС как «единственного инклюзивного формата». Есть риски, что текущий политический кризис и, как следствие, институциональная поляризация могут вновь обнажить разногласия по некоторым ключевым вопросам обеспечения МИБ, которые долгое время являлись своего рода камнем преткновения между Россией и Соединенными Штатами. Одной из таких тем является вопрос о применимости международного права к киберконфликтам.

Так, в резолюции по «Программе действий», со ссылкой на предыдущие доклады ГПЭ по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (функционировала с 2004 по 2021 г.) и доклад РГОС, заявляется о применимости существующих норм международного права к информационным воздействиям. Вместе с тем «Программа действий» предусматривает возможную разработку в будущем дополнительных норм и имеющих силу обязательств с учетом особенностей ИКТ [9, с. 3], что может стать определенным шагом в сторону российского подхода и попыткой достижения консенсуса. Российская резолюция признает подход об универсальной применимости существующих норм как бы между строк, делая акцент в основном на разработке дополнительных норм с учетом особенностей ИКТ [10]. В целом можно считать, что в новых резолюциях вопрос о применимости существующих норм носит «компромиссный характер» и является их общей чертой.

Хочется отметить, что «Программа действий» во многих аспектах представляется конкурентоспособным форматом, так как несколько расширяет повестку

диалога — например, сокращение «гендерного цифрового разрыва», повышение жизнестойкости всех сообществ, секторов и сохранения подхода, ориентированного на интересы людей, а также предусматривает более институциональные, постоянные (и формальные) механизмы переговорного процесса, среди которых: периодический обзор прогресса, достигнутого в осуществлении программы действий; предоставление государствами обзоров о предпринимаемых на национальном уровне усилиях по применению правил ответственного поведения; механизмы отслеживания реализации согласованных норм и правил; разработка дополнительных норм и правил.

Так или иначе, инициатива о создании параллельного формата — «Программы действий» — может рассматриваться Россией как попытка если не «вытеснить», то уменьшить ее влияние в самом переговорном процессе по профильному вопросу, который был запущен именно ей в 1998 г. Переговорный процесс в ООН, по всей видимости, продолжится, но есть определенные риски того, что он может принять конкурентный характер. Скорее всего, в определенной степени Соединенные Штаты, Россия и их партнеры будут принимать участие в работе сразу в двух форматах, однако подобное участие может оказаться чисто формальным. Здесь стоит отметить, что по сравнению с 2018 г., когда Россией и США также были представлены две конкурирующие резолюции по вопросу обеспечения МИБ в рамках ООН, число соавторов российской резолюции значительно сократилось — с 34 в 2018 г. до 13 в 2022 г.

Далее текущий политический кризис поставил на повестку дня вопрос об истинной инклюзивности и транспарентности профильного диалога, так как представители частного сектора начали сталкиваться с определенными ограничениями касательно возможности участия в переговорах в рамках РГОС. Так, стороны несколько месяцев (с начала работы Первой субстантивной сессии в декабре 2021 г. вплоть до апреля 2022 г.) не могли согласовать модальности участия негосударственных акторов в переговорах. Позже аккредитацию на полноценное участие в работе третьей сессии РГОС (25–29 июля) не получили 32 организации — 27 западных, заблокированных Россией (среди которых активнейшие участники РГОС предыдущего созыва Microsoft и ассоциация Cybersecurity Tech Accord), и 5 российских, заблокированных Украиной (в том числе «Лаборатория Касперского»), — им осталось «довольствоваться» лишь правом неформального участия [11].

Инклюзивность переговорного процесса находится под угрозой и по причине конфронтации между правительствами некоторых стран и компаниями, вызванной в первую очередь политическими мотивами. Еще 25 марта 2022 г. Федеральная комиссия по связи США признала «Лабораторию Касперского» — единственную отечественную компанию, принявшую активное участие в работе РГОС первого созыва 2019–2021 гг., — потенциальной угрозой национальной безопасности США [12]. Антироссийскую позицию после февраля 2022 г. заняла компания Microsoft, которая 22 июня 2022 г. опубликовала доклад о предполагаемых кибервоздействиях в отношении информационной инфраструктуры Украины, что вызвало ответную реакцию МИД РФ и обвинение Microsoft в политизированности и «исполнении заказа Пентагона».

Нарастание антагонизма может привести к тому, что Россия в дальнейшем будет предвзято относиться к участию западных компаний в переговорном про-

цессе, ссылаясь на их стремление доминировать в информационном пространстве. В свою очередь, страны Запада и западные корпорации не будут видеть в российском правительстве ответственного участника переговорного процесса, обвиняя Россию в деструктивном поведении в киберпространстве и осуществлении кибервоздействий на инфраструктуру Украины. Западные компании могут оказаться фрустрированными негативным опытом отказа в аккредитации на полноценное участие в работе третьей сессии РГОС второго созыва, а также существующим антагонизмом между ними и российским правительством.

В перспективе такая ситуация способна поставить под вопрос саму идею инклюзивности и создать определенные риски для по-настоящему эффективного участия стейкхолдеров — как российских, так и зарубежных, — которое негласно может оказаться нежелательным и будет подвергаться формальным ограничениям, в том числе по причине приписываемого некоторым из них осуществления вредоносной деятельности, что особенно актуально в свете взятого странами курса на суверенизацию и отказ от программного обеспечения недружественных стран. Так или иначе, но блокирование участия различных компаний — лидеров отрасли (как российских, так и зарубежных) по политическим мотивам приведет не только к объективному торможению переговорного процесса, но и к снижению эффективности противодействия кибер-/информационным угрозам. Если говорить о ближайших перспективах диалога, то, возможно, Россия столкнется с противодействием в рамках ключевого для нее переговорного процесса ООН по обсуждению вопросов кибербезопасности — РГОС ООН, мандат которой действует до 2025 г. Переговорный процесс в ООН скорее всего продолжится, но он может существенно замедлиться.

Долгое время больной темой во взаимодействии Москвы и Вашингтона также оставалось отсутствие консенсуса в подходах к обеспечению МИБ, что нашло отражение в создании в 2018 г. и параллельном функционировании двух площадок — РГОС и ГПЭ. Проблемными вопросами являлись применимость международного права к киберконфликтам, использование информационно-коммуникационных технологий (ИКТ) в военных целях, распространение национального суверенитета на ИКТ-инфраструктуру, необходимость регулирования интернета на национальном уровне и т. д. С объединением в 2021 г. усилий России и США в рамках одной РГОС появилась надежда на то, что стороны будут разделять общие подходы к решению рассматриваемого вопроса. Однако сейчас, несмотря на то что переговорный процесс на данный момент идет полностью в рамках РГОС, возможно усиление поляризации в подходах к обеспечению международной кибербезопасности в контексте одного формата. Главный вопрос состоит в том, что западные страны глубоко убеждены в осуществлении Россией ряда кибератак в отношении Украины в процессе конфликта, в том числе и тех, которые якобы вызвали непреднамеренный эффект в европейских странах [13]. Это усугубляет риски торможения диалога и его поляризации — в рамках как ООН, так и двусторонних форматов.

## Вызовы в сфере борьбы с киберпреступностью

Еще одна составляющая системы МИБ — противодействие киберпреступности. Здесь диалог также сталкивается с рисками поляризации подходов из-за политизированности и противоречий, обнажившихся в новых политических условиях.

Еще в 2001 г. была принята Будапештская конвенция, или Конвенция Совета Европы о киберпреступности. Россия — единственная на тот момент страна — член Совета Европы, которая не подписала ее по причине потенциальной возможности нарушения суверенитета, заложенного в 32-й статье документа [14]. Так или иначе, но с тех пор ландшафт киберугроз и самого информационного пространства сильно изменился.

В связи с этим 27 июля 2021 г. Россия внесла на рассмотрение ООН проект Конвенции о противодействии использованию ИКТ в преступных целях в качестве альтернативы Будапештской конвенции, цель которой — расширить сферу международного сотрудничества по вопросу противодействия киберпреступности с учетом вызовов и угроз в сфере международной информационной безопасности. В 2022 г. рамках ООН уже прошли три субстантивные сессии Специального межправительственного комитета ООН по разработке данной Конвенции, по результатам которых запущен соответствующий диалог между правоохранительными органами стран-участниц.

Однако 12 мая 2022 г. был открыт для подписания второй дополнительный протокол к Будапештской конвенции, который подписали 22 страны. Представляется, что данный факт «обновления» документа если и не призван формально деактуализировать обсуждения российской инициативы в рамках ООН в условиях текущей политической ситуации, то по факту способен нивелировать дальнейшие усилия России по продвижению искомой российской Конвенции. Можно предположить, что процесс международного противодействия киберпреступности также приобретет несколько фрагментированный характер, так как страны — участницы Будапештской конвенции (а это преобладающая часть международного сообщества) будут взаимодействовать в рамках привычного для них формата и вряд ли захотят примкнуть к в конкурирующей инициативе, а Россия в свою очередь вряд ли присоединится к документу Совета Европы и далее будет продвигать свой проект Конвенции, пытаясь заручиться поддержкой стран-партнеров в рамках ООН.

Поляризация в подходах наблюдается и на уровне самих документов. Так, в российской конвенции делается акцент на применении к информационному пространству принципа суверенитета и «осуществления юрисдикции в отношении “национального” информационного пространства», в то время как Конвенция Совета Европы в определенной степени предполагает «трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным» [15; 16]. Данное ключевое противоречие является еще одним фактором взаимного «неприсоединения» к данным инициативам России и ее партнеров — с одной стороны, и США и ее союзников — с другой.

## Политика США в отношении России в сфере киберповестки

Важнейшим элементом формирующейся системы МИБ является взаимодействие двух ключевых бенефициаров международного переговорного процесса по киберповестке — России и Соединенных Штатов, которое также утратило свою динамику и дальнейшие перспективы на нормализацию. Взаимодействие России и Соединенных Штатов по киберповестке насчитывает уже два десятилетия, однако пиком стало заключение во время двусторонней встречи Владимира Путина

и Барака Обамы в 2013 г. на саммите G8 в Северной Ирландии соглашений «О мерах укрепления доверия в сфере использования ИКТ». Однако достигнутые тогда результаты были перечеркнуты политическим кризисом на Украине 2013–2014 гг., а после окончательно провалены взломами серверов Национального комитета Демократической партии США во время предвыборной кампании 2016 г. и возложением ответственности за них на Россию, после чего на Москву посыпались систематические обвинения в осуществлении кибератак на США.

Решение возобновить взаимодействие на позитивных началах было принято в ходе российско-американского саммита в Женеве, состоявшегося 16 июня 2021 г., когда стороны достигли соглашения начать двусторонние консультации по киберповестке. Вскоре была образована соответствующая рабочая группа по проблемам обеспечения безопасности в сфере информационно-коммуникационных технологий, которая успела провести несколько раундов консультаций.

Однако в начале апреля 2022 г. США заявили о прекращении взаимодействия с Россией по вопросу обеспечения кибербезопасности и закрытии этой группы [17]. В условиях краха консультационных механизмов, созданных по итогам женевского саммита, которые должны были сдерживать конкуренцию между Россией и США и сделать ее более контролируемой, государства рискуют вновь быть ввергнутыми в пучину неконтролируемой конкуренции в сфере киберполитки.

Чтобы успешно конкурировать и обеспечить себе стратегическое превосходство в киберпространстве, Соединенные Штаты еще при Д. Трампе приняли на вооружение стратегию *упреждающей защиты* (от англ. defend forward) [18; 19; 20, с. 111, 137, 162], которая должна осуществляться посредством концепции *постоянной вовлеченности* (от англ. persistent engagement) и представляет собой проведение упреждающих кибероперaций в сетях противника и в случае необходимости выведение из строя систем и серверов противника еще до того, как он осуществит кибератаки [19, с. 6, 24, 25, 28–30; 21–25], в то время как постоянная вовлеченность подразумевает, что эти упреждающие кибероперации будут осуществляться на *постоянной основе* в режиме реального времени против потенциальных противников как можно ближе к источнику предполагаемой агрессии с целью навязать им дополнительные стратегические затраты, оспорить их превосходство и в то же время подтвердить стратегическое превосходство США в киберпространстве [21; 22, с. 105–106; 26, с. 381, 382, 388, 389; 27, с. 11–13, 22, 23; 28, с. 15, 20; 29, с. 13; 30]. Важная особенность постоянной вовлеченности — кибероперации не должны достигать уровня вооруженного конфликта. Цель этой стратегии — оспорить превосходство противников и одновременно подтвердить стратегическое превосходство Соединенных Штатов в киберпространстве.

Данный подход был сформулирован в стратегическом документе Кибернетического командования США «Достижение и поддержание превосходства в киберпространстве: Руководство для Киберкомандования США» от 23 марта 2018 г. и «Киберстратегии Министерства обороны США» от сентября 2018 г., «Национальной киберстратегии США» от 21 сентября 2018 г. Сам Джо Байден, еще будучи кандидатом в президенты, выразил желание продолжить эту политику с условием ее должного анализа, так как данная стратегия «может иметь непредвиденные последствия, выходящие за рамки киберпространства» [31]. Данного подхода было предложено придерживаться с условием его пересмотра и доработки и в опубли-

кованном в январе 2021 г. «Руководстве для новой администрации Байдена: Белая книга Комиссии по киберпространству "Солярий" № 5», которое представляет собой пакет рекомендаций по обеспечению кибербезопасности для новой на тот момент администрации Белого дома.

Помимо этого, созданной еще в 2019 г. Комиссией по киберпространству «Солярий» была предложена стратегия многоуровневого киберсдерживания [20, с. 1, 2, 7, 23–30] (от англ. layered cyber deterrence), которая включает в себя три уровня: 1) продвижение международных норм с целью формирования ответственного поведения и поощрения сдержанности в киберпространстве; 2) лишение выгод, достигаемое посредством улучшения обороны с целью минимизации получаемых агрессором преимуществ; 3) наложение издержек путем осуществления соразмерных ответных мер. По замыслу Комиссии, стратегия упреждающей защиты должна являться частью многоуровневого киберсдерживания и быть интегрирована в национальную киберстратегию США с использованием всех инструментов власти. Цель такого подхода — обеспечить защиту от кибератак разного уровня. Так, если наложение издержек и лишение выгод представляется эффективным против серьезных кибератак, которые можно квалифицировать как акт агрессии, то упреждающая защита посредством постоянной вовлеченности вполне подходит для «ежедневной конкуренции», для противодействия в режиме реального времени киберугрозам, которые не достигают уровня вооруженного конфликта. И если в наложении издержек может не быть необходимости (на сегодняшний день не было столь разрушительных кибератак, которые могут потребовать серьезных ответных мер), то упреждающая защита посредством постоянной вовлеченности — та стратегия, к которой Соединенные Штаты смогут прибегать на постоянной основе.

По заявлениям Киберкомандования США, этот подход уже был применен на практике против России в 2018 г., когда удалось предотвратить предполагаемое вмешательство Москвы в «промежуточные выборы» США 6 ноября 2018 г. и вследствие проведенной кибероперации заблокировать доступ в интернет так называемой «Фабрике троллей» (или «Агентству интернет-исследований») [32, с. 4; 33–35], деятельность которой, по мнению Соединенных Штатов, направлена на подрыв процесса демократических выборов в США[2]. По словам американских высокопоставленных лиц, данная кибероперация — всего лишь часть общей *постоянной киберкампании* против «российского вмешательства».

Можно предполагать, что особенно актуальным данный подход для США стал в ситуации текущего политического кризиса. Летом 2022 г. глава Киберкомандования США Пол Накасоне заявил, что США проводили серию наступательных, оборонительных и информационных операций в отношении России в поддержку Украины [36]. Более того, в недавнем заявлении Киберкомандования США от 25 октября 2022 г. подтверждается, что партнерские отношения и оказание помощи являются неотъемлемым компонентом постоянной вовлеченности, в рамках которой США по приглашению стран-партнеров проводят так называемые операции «превентивной охоты», суть которой заключается в совместном противодействии противнику [37]. По заявлению самих США, конфликт на Украине стал площадкой

[2] «Агентство интернет-исследований» было обвинено Министерством юстиции США во вмешательстве в выборы американского президента в 2016 г. по результатам расследований спецпрокурора США Роберта Мюллера.

для апробации концепции «киберзонта» — концепции коллективной кибероборо-ны, которую они планируют применять в дальнейшем — например, в случае пред-полагаемого вторжения Китая в Тайвань.

Таким образом, можно ожидать, что в условиях краха очередных консульта-тивных механизмов Вашингтон в том или ином виде задействует описанную стра-тегию против России либо будет делать декларативные заявления о ее применении. Сам Белый дом уже неоднократно заявлял о готовности отвечать на российские кибератаки пропорциональными средствами с использованием всех инструментов национальной власти. Также США могут вернуться к планированию операций по осуществлению ответных мер.

## Украинский киберфронт: первые выводы и их значение для формирования системы МИБ

Рассмотрение предварительных выводов, которые можно сделать о роли и ме-сте кибератак непосредственно в ходе вооруженного конфликта, важно для поним-ания того, в каком направлении должна развиваться система обеспечения МИБ в будущем и на чем необходимо сосредоточиться при дальнейших обсуждениях этого вопроса.

Конфликт на Украине и развернувшиеся в его рамках кибератаки создали пре-цедент, который дал некоторые представления о месте и роли кибервоздействий в общем стратегическом контексте, их стратегическом потенциале для достижения определенных эффектов во время вооруженного конфликта. Этот прецедент также стал своего рода полем эмпирической проверки некоторых стратегических поло-жений.

Первое, что показали конфликт на Украине и имевшие место кибервоздей-ствия, — на данном этапе кибератаки, несмотря на то что они рассматривались как «сопутствующие» современному конфликту, не создали непосредственно на-блюдаемых стратегических эффектов и не принесли никаких непосредственных преимуществ (мы не наблюдали масштабных киберэффектов и разрушения ин-фраструктуры с применением кибероружия), носили во многом спорадический и в некотором смысле хаотичный характер.

В этом контексте важно иметь в виду следующее — если полностью абстра-гироваться от возможности осуществления кибероперaций самими государствен-ными институтами конфликтующих сторон с целью достижения стратегических эффектов в текущем конфликте, мы увидим, что имевшие место кибервоздействия проводятся большей частью хактивистами, занявшими ту или иную сторону [38]. Более того, можно наблюдать, что конфликт на Украине стал своего рода полем для проверки киберпотенциала хакерских группировок в рамках идущей между ними киберконкуренции [39; 40]. Их кибератаки в большинстве своем преследова-ли цели поразить системы и сети какой-либо конкретной организации или струк-туры, не преследуя стратегических задач и не имея прямой «оперативной связки» с военными операциями на поле боя.

При этом, если российская сторона отрицает аффилированность с какими бы то ни было хакерскими группировками в случае осуществления последними кибе-ратак, то украинская сторона открыто обнародовала тот факт, что правительство

Украины поддерживает хакерское движение в конфликте, в самом его начале обратившись к хакерскому сообществу с призывом объединиться и начать проводить кибероперации по обороне украинских сетей и осуществлению кибершпионажа [41]. В условиях, когда подобные хакерские группировки действительно не имеют связи с правительством [42], может наблюдаться «молчаливое одобрение» их действий. Однако, согласно имеющимся разработкам в области применения международного права к киберконфликтам [43, с. 94], случай Украины показывает, что, когда одна сторона признает действия негосударственных акторов в качестве своих (что фактически произошло со стороны Украины в самом начале конфликта), их действия могут быть приписаны правительству.

В этом плане конфликт на Украине продемонстрировал, что государства не склонны полагаться на кибероперации как мощный инструмент решения стратегических задач. Кибератаки проводятся в основном негосударственными акторами с «молчаливого одобрения» государств в «серой зоне» конфликта и не попадают под правовое регулирование в полном смысле слова. Такие кибервоздействия являются «удобными» и перспективными с точки зрения создания своего рода фонового шума традиционного конфликта и определенных неудобств, а не достижения стратегических целей с учетом их невысокой эффективности и хаотичности, что позволяет избежать правовой ответственности самим хакерским группировкам. Стоит также отметить и тот факт, что имевшие место кибератаки в условиях традиционного конфликта оказались неэффективны в качестве инструмента принуждения или даже реторсии[3].

Так или иначе, но вопрос о роли кибервоздействий и их стратегической значимости в условиях традиционного вооруженного конфликта на данный момент остается дискуссионным. Можно предполагать, что на текущий момент кибератаки останутся инструментом достижения оперативных эффектов в рамках стратегической конкуренции в мирное время или в рамках гибридной войны (как это было в случае с кибератакой вируса Stuxnet на иранский ядерный завод в Нетензе в 2010 г.) и будут проводиться в «серой зоне» международного права, не достигая уровня акта агрессии и вооруженного конфликта.

Также эффективным может стать кибершпионаж. В условиях вооруженного конфликта в ближайшем будущем кибератаки вряд ли будут использоваться для достижения стратегических результатов и рассматриваться как «крайнее» средство, поскольку достичь нужных последствий эффективнее, быстрее и проще можно при помощи конвенциональных вооружений. Показательно, что кибератаки преимущественно осуществлялись на сети, системы и сайты гражданских учреждений — государственных структур, министерств и ведомств, СМИ, сферы бизнеса. Согласно открытым источникам, Украина зафиксировала воздействия в отношении телекоммуникационных провайдеров, объектов энергетической инфраструктуры, сайтов государственных институтов. В России целями кибервоздействий стали платежная система «Мир», сайт «Госуслуги», системы Росавиации, система онлайн-голосования, сайт «Роскосмоса», сайты образовательных учреждений во время приемной кампа-

[3] Реторсия (от лат. retorsio — обратное действие) — в международном праве правомерные принудительные действия государства, совершаемые в ответ на недружественный акт другого государства, не составляющий международного правонарушения — ни одна из сторон и негосударственных акторов не пошла на какие-либо уступки [44, с. 424–427].

нии 2022 г., сайты различных СМИ, информационные ресурсы компании «Мираторг» и т. д. Также в контексте вооруженного конфликта цифровые технологии будут гораздо успешнее использоваться для ведения информационно-психологического воздействия, закрепления повестки дня и получения данных.

Таким образом, дальнейшее формирование системы МИБ должно быть сосредоточено прежде всего на тех кибервоздействиях, которые угрожают критической информационной инфраструктуре — даже в период горячей фазы конфликта уязвимыми оказываются в первую очередь гражданские и административные сети. Необходимо сфокусироваться на воздействиях из «серой зоны», которые не вызывают серьезных кинетических эффектов — кибервоздействиях, происходящих в зоне так называемой конкуренции, в которой кибератаки не достигают уровня вооруженного нападения.

## Киберповестка в условиях мировой политической турбулентности: что делать?

В текущих условиях политизированности переговорного процесса достижение каких-либо весомых результатов в формировании полноценной системы обеспечения МИБ будет довольно проблематичным. В свете сложившихся обстоятельств для России существенно возрастают перспективы переговорного процесса по вопросу обеспечения МИБ в рамках таких форматов, как Шанхайская организация сотрудничества, БРИКС, ОДКБ, регионального партнерства Россия — АСЕАН и т. д. Здесь уже достигнут определенный прогресс в этом направлении и уже функционируют рабочие группы экспертов по профильному вопросу. Более того, именно при активном участии стран — членов ШОС, БРИКС и ОДКБ (главные из которых — Россия и Китай) предлагались ключевые инициативы для ООН в сфере обеспечения кибербезопасности, в том числе и инициатива о создании инклюзивной РГОС. В этом свете имеются определенные перспективы касательно экстраполяции некоторого функционала, заложенного в РГОС, на существующие рабочие группы. Важно расширить мандат соответствующих групп перечисленных организаций, сделать диалог в них более институциональным, инклюзивным и транспарентным. При этом представляется необходимым вовлечение в обсуждение вопросов кибербезопасности всех заинтересованных сторон — частного сектора, академических кругов, представителей гражданского общества.

Несмотря на нарастающую политизированность диалога, в будущем основным переговорным форматом по профильному вопросу должна остаться ООН. Достичь компромиссов будет трудно. Вместе с тем существует ряд ключевых вопросов, которые государствам необходимо обсуждать дальше — к примеру, возможный запрет на осуществление воздействий против определенных объектов критической инфраструктуры, нарушение в работе которых может привести к угрозе жизни и здоровью людей, экологической катастрофе и т. д.; табу может налагаться на определенные типы эффектов от информационных атак [45, с. 146; 46, с. 91; 47–49].

Также, несмотря на будущую институциональную поляризацию, РГОС и «Программа действий» имеют шансы стать взаимодополняемыми форматами, а российская и американская резолюции демонстрируют определенный консенсус по некоторым вопросам обеспечения МИБ, например по вопросу участия в пере-

говорном процессе всех заинтересованных сторон, что отражено в обеих резолюциях. В этом свете важным будет создать более эффективный механизм согласования модальностей участия стейкхолдеров — допуск хотя бы их ограниченного числа к обсуждениям в рамках обоих форматов может стать шагом к достижению определенного доверия. Странам важно не зацикливаться на работе лишь в «своих» форматах и тем более не отвергать «чужие», а постараться двигаться по направлению к достижению компромиссов. Что касается двустороннего взаимодействия с Соединенными Штатами, то здесь в ближайшем будущем не предвидится перспектив нормализации отношений по вопросу киберповестки. В этих условиях в качестве возможного варианта можно рассматривать переход к точечным механизмам взаимодействия — это могут быть консультации «по необходимости» с той целью, чтобы не допустить еще большей эскалации в цифровой среде и возникновения реального политического конфликта из-за киберпровокаций. Также необходимо в одностороннем порядке установить так называемые красные линии, которые в двустороннем соперничестве в киберпространстве лучше не пересекать, чтобы стратегическая киберконкуренция не перешла в реальный политический конфликт.

## Заключение

Так или иначе, но политический кризис на Украине дестабилизировал формирование полноценной системы МИБ. Сегодня вновь наблюдается поляризация переговорного процесса по вопросу обеспечения глобальной информационной безопасности, дифференциация в подходах между ключевыми игроками этого процесса. Несмотря на то что переговорный процесс в рамках ООН продолжится, он будет испытывать трудности, а сам диалог будет сильно политизирован. Что касается двустороннего взаимодействия с Соединенными Штатами, то здесь в ближайшем будущем не предвидится перспектив нормализации отношений по вопросу киберповестки. Также украинский конфликт продемонстрировал, что, скорее всего, в ближнесрочной перспективе кибератаки не будут рассматриваться как действенное средство достижения стратегических и тем более физических эффектов в ходе вооруженных конфликтов, в период которых гораздо более эффективными будут информационно-психологическое воздействие и кибершпионаж. В этом свете формирование системы МИБ должно быть сосредоточено на создании своего рода системы «табу» в отношении объектов критической инфраструктуры и, конечно же, в отношении возможных эффектов от кибератак. Вместе с тем стоит помнить, что политические риски, связанные с ухудшением отношений из-за кибератак, сохраняются и будут становиться все актуальнее. Заложниками политических разногласий будут оставаться, в частности, киберповестка и взаимодействие стран по вопросу киберполитики.

## Литература

1. Основы государственной политики Российской Федерации в области международной информационной безопасности. Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213 (2021), *Совет Безопасности Российской Федерации*. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 25.02.2023).

2. Sebekin, S. A. (2016), Russian Cyberdiplomacy in International Institutions: Providing international Information Security, в: *Россия — XXI век: IX Междунар. науч.-практ. конф.*, Владивосток, 28–31 окт. 2016 г.: мат-лы, ред. Сонин, В. В., Смирнов, В. П., Панов, В. В. и др., Владивосток: Дальневосточный федеральный ун-т.

3. Бойко, С. (2018), Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее, *Международная жизнь*, № 8, с. 54–71.

4. Зинченко, А. В. и Толстухина, А. Ю. (2018), Мир или война в киберпространстве? *Международная жизнь*, № 9, с. 82–90.

5. Россия предложила учредить в ООН рабочую группу по кибербезопасности (2018), *ТАСС*, 27 октября. URL: https://tass.ru/politika/5727314 (дата обращения: 09.01.2023).

6. Черненко, Е. В. (2018), Россия и США перетягивают всемирную паутину, *Коммерсант*, 12 ноября. URL: https://www.kommersant.ru/doc/3797617 (дата обращения: 09.01.2023).

7. Черненко, Е. В. (2021), Комитет Генассамблеи ООН одобрил российско-американскую резолюцию по кибербезопасности, *Коммерсант*, 3 ноября. URL: https://www.kommersant.ru/doc/5062751 (дата обращения: 09.01.2023).

8. Approving 15 Texts, First Committee Spotlights Impact of Illicit Weapons Trade on Women, Value of Gender Perspective in Reducing Armed Conflict, United Nations (2022), *United Nations*, November 3. URL: https://press.un.org/en/2022/gadis3705.doc.htm (дата обращения: 08.01.2023).

9. *Программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности: Проект резолюции A/C. 1/77/L. 73, Генеральная Ассамблея ООН: Семьдесят седьмая сессия. Первый комитет. Пункт 94 повестки дня. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности*, 13 октября 2022. URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N22/632/23/PDF/N2263223.pdf?OpenElement (дата обращения: 29.10.2022).

10. *Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Пересмотренный проект резолюции A/C. 1/77/L. 23/Rev.1, Генеральная Ассамблея ООН: Семьдесят седьмая сессия. Первый комитет. Пункт 94 повестки дня. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности*, 20 октября 2022. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/655/81/PDF/N2265581.pdf?OpenElement (дата обращения: 29.10.2022).

11. Черненко, Е. и Исакова, Т. (2022), Мины на информационном поле, *Коммерсант*, 25 июля. URL: https://www.kommersant.ru/doc/5480485 (дата обращения: 23.10.2022).

12. Shields, T. (2022), Kaspersky Named First Russian Company on Security Risk List, *Bloomberg*, March 6. URL: https://www.bloomberg.com/news/articles/2022–03–25/fcc-calls-kaspersky-china-telecom-china-mobile-security-risks (дата обращения: 22.10.2022).

13. KA-SAT Network cyber attack overview (2022), *Viasat*, March 30. URL: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview (дата обращения: 08.01.2023).

14. Арсентьев, А. (2008), Путин отказался подписать Конвенцию о киберпреступниках, *CNews*, 27 марта. URL: http://safe.cnews.ru/news/top/putin_otkazalsya_podpisat_konventsiyu (дата обращения: 03.11.2022).

15. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях: Проект конвенции (2021), *Коммерсант*, 29 июня. URL: https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_R.pdf (дата обращения: 23.10.2022).

16. *Конвенция о преступности в сфере компьютерной информации ETS N 185*, Будапешт, 23 ноября, 2001. URL: https://base.garant.ru/4089723/d78e49c48a908b41f776c768d5f3dc38/ (дата обращения: 23.10.2022).

17. Егоров, И. (2022), Совбез РФ: Белый дом закрыл единственный официальный канал связи с Кремлем, *RG.ru,* 7 апреля. URL: https://rg.ru/2022/04/07/sovbez-rf-belyj-dom-zakryl-edinstvennyj-oficialnyj-kanal-sviazi-s-kremlem.html (дата обращения: 23.10.2022).

18. Nakasone, P. M. and Sulmeyer, M. (2020), How to Compete in Cyberspace, *Foreign Affairs,* August 25. URL: https://www.foreignaffairs.com/articles/united-states/2020–08–25/cybersecurity (дата обращения: 27.02.2023).

19. Goldsmith, J. (2022), *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*, Oxford: Oxford University Press.

20. The United States of America Cyberspace Solarium Commission: Legislative Proposals, *Cyberspace Solarium Commission*. URL: https://www.solarium.gov/report (дата обращения: 28.02.2023).

21. Fischerkeller, M. P., Goldman, E. O. and Harknett, R. J. (2022), *Cyber Persistence Theory: Redefining National Security in Cyberspace,* Oxford: Oxford University Press.

22. Себекин, С. А. (2020), Постоянная вовлеченность в киберпространстве новая стратегия США и ее соотношение с киберсдерживанием, *Международные процессы*, т. 18, № 3 (62), с. 96–125.

23. Jasper, S. (2017), *Strategic Cyber Deterrence: The Active Cyber Defense Option,* New York: Rowman & Littlefield.

24. Sulmeyer, M. (2018), How the U. S. Can Play Cyber-Offense: Deterrence Isn't Enough, *Foreign Affairs*. URL: https://www.foreignaffairs.com/articles/world/2018–03–22/how-us-can-play-cyber-offense (дата обращения: 27.02.2023).

25. The Department of Defense Cyber Strategy 2018: Summary (2018), *U. S. Department of Defense*. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.pdf (дата обращения: 28.02.2023).

26. Fischerkeller, M. P. and Harknett, R. J. (2017), Deterrence is Not a Credible Strategy for Cyberspace, *Orbis,* vol. 61, no. 3, pp. 381–393.

27. Fischerkeller, M. P. and Harknett, R. J. (2018), *Persistent Engagement, Agreed Competition, Cyberspace, Interaction Dynamics, and Escalation*. Institute for Defense Analyses.

28. Harknett, R. J., Callaghan, J. P. and Kauffman, R. (2010), Leaving Deterrence Behind: War-Fighting and National Cybersecurity, *Journal of Homeland Security and Emergency Management*, vol. 7, no. 1. pp. 1–24.

29. Nakasone, P. M. (2019), A Cyber Force for Persistent Operations, *Joint Force Quarterly*, vol. 92, 1st Quarter, pp. 10–14.

30. Goldman, E. O. (2020), From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy, *Texas National Security Review, Special Issue: Cyber Competition*. Fall. URL: https://tnsr.org/category/special-issue-cyber-competition/ (дата обращения: 28.11.2020).

31. Cyber Policy (2020), *The New York Times*. URL: https://www.nytimes.com/interactive/2020/us/politics/2020-democrats-cyber-policy-foreign-policy.html (дата обращения: 27.10.2022).

32. Statement of General Paul M. Nakasone Commander United States Cyber Command Before the Senate Committee on Armed Services, Senate Committee on Armed Services (2019), *Senate Committee on Armed Services*, February 14. URL: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf (дата обращения: 12.01.2023).

33. Nakashima, E. (2019), U. S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms, *The Washington Post*, February 26. URL: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6–11e9-af5b-b51b7ff322e9_story.html (дата обращения: 12.01.2023).

34. Barnes, J. E. (2019), Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections, *The New York Times*, February 26. URL: https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html (дата обращения: 12.01.2023).

35. Schneider, J. G. (2019), Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy. *Lawfare*. URL: https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy (дата обращения: 12.01.2023).

36. Martin, A. US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command (2022), *Skynews,* June 1. URL: https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (дата обращения: 27.10.2022).

37. CYBER 101 — Defend Forward and Persistent Engagement (2022), *U. S. Cyber Command,* October 25. URL: https://www.cybercom.mil/Media/News/Article/3198878/cyber101-defend-forward-and-persistent-engagement/ (дата обращения: 27.10.2022).

38. «Война хакеров»: эксперт о кибератаках между Россией и Украиной (2022), *Russia Today*, 2 мая. URL: https://russian.rt.com/ussr/video/1006738-voina-hakerov-ekspert-o-kiberatakah-mezhdu-rossiei (дата обращения: 09.01.2023).

39. Кильдюшкин, Р. (2022), Бот на бота: из-за конфликта на Украине в хакерском сообществе началась междоусобная война, *Газета.ru*, 3 марта. URL: https://www.gazeta.ru/tech/2022/03/02/14588575.shtml (дата обращения: 10.01.2023).

40. Целищев, А. (2022), Группа Killnet взломала сайт хакеров Anonymous, объявивших кибервойну России, *Газета.ru*, 1 марта. URL: https://www.gazeta.ru/tech/news/2022/03/01/17364697.shtml?updated (дата обращения: 10.01.2023).

41. Schectman, J. and Bing, C. (2022), Ukraine calls on hacker underground to defend against Russia, *Reuters*. URL: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022–02–24/ (дата обращения: 09.01.2023).

42. Об очередной антироссийской публикации в британских СМИ (2022), *Министерство иностранных дел Российской Федерации*, 23 мая. URL: https://mid.ru/ru/press_service/publikacii-i-oproverzenia/oproverzenia1/nedostovernie-publikacii/1814455/ (дата обращения: 10.01.2023).

43. Schmitt, M. N. and Vihul, L. (eds) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

44. Delerue, F. (2020), *Cyber Operations and International Law,* Cambridge: Cambridge University Press.

45. Себекин, С. А. (2021), Возможен ли режим контроля за распространением кибервооружений? Подходы России и США, *Пути к миру и безопасности*, № 2 (61), с. 139–152.

46. Ромашкина, Н. П., Марков, А. С. и Стефанович, Д. В. (2020), *Международная безопасность, стратегическая стабильность и информационные технологии*, М.: ИМЭМО РАН.

47. Nye, J. S. (2015), The World Needs an Arms-control Treaty for Cybersecurity, *Belfer Center for Science and International Affairs*. URL: https://www.belfercenter.org/publication/world-needs-arms-control-treaty-cybersecurity (дата обращения: 01.03.2023).

48. Шариков, П. А. (2020), Информационные угрозы и контроль над вооружениями: возможен ли диалог между Россией и США? *Валдай. Международный дискуссионный клуб*, 20 ноября. URL: https://ru.valdaiclub.com/a/highlights/informatsionnye-ugrozy-i-kontrol-nad-vooruzheniyami/ (дата обращения 05.03.2023).

49. Giles, M. (2018), We need a cyber arms control treaty to keep hospitals and power grids safe from hackers, *MIT Technology Review*. URL: https://www.technologyreview.com/2018/10/01/139955/we-need-a-cyber-arms-control-treaty-to-keep-hospitals-and-power-grids-safe-from-hackers/ (дата обращения: 01.03.2023).

Статья поступила в редакцию 5 февраля 2023 г.;
рекомендована к печати 13 марта 2023 г.

Контактная информация:

*Себекин Сергей Александрович* — канд. ист. наук; sebserg37gmail.com

## How will the conflict in Ukraine affect the system of international information security?

*S. A. Sebekin*

Irkutsk State University,
1, ul. Karla Marksa, Irkutsk, 664003, Russian Federation

**For citation:** Sebekin S. A. How will the conflict in Ukraine affect the system of international information security? *Vestnik of Saint Petersburg University. International Relations*, 2023, vol. 16, issue 2, pp. 170–190. https://doi.org/10.21638/spbu06.2023.205 (In Russian)

The article is devoted to the consideration of the main changes taking place in the system of ensuring international information security after the start of a special military operation in Ukraine. An attempt is made to predict the challenges and risks that the IIS system will face in the future. The priority transformations are connected with the negotiation process within the UN, which, in the context of increasing political antagonism between the key subjects of the dialogue, is becoming increasingly politicized and is beginning to experience some difficulties. It is assumed that in the conditions of the new political reality, the issue of "comprehensive" counteraction to international cybercrime will remain unresolved. There is some fragmentation of the international information security system itself, which is experiencing centrifugal tendencies in terms of promoting alternative approaches to solving key issues in this sphere. Finally, it can be expected that the United States, in interaction with Russia, will more actively engage in a proactive strategy of so-called defend forward, which should be implemented

through the concept of persistent engagement. The preliminary conclusions demonstrated by the actions in Ukraine regarding the role and place of cyber attacks directly within the framework of the armed conflict are also considered. It is assumed that in the near future cyber attacks will not be considered as a means of achieving real strategic effects on the battlefield, where conventional weapons play a dominant role. An attempt is made to give some recommendations on maintaining a certain dynamic of the development of the IIS system.

*Keywords*: international information security, open-ended working group, *Programme of Action*, cybercrime, defend forward.

## References

1. Fundamentals of the State Policy of the Russian Federation in the field of international information security: Approved by Decree of the President of the Russian Federation No. 213 of April 12, 2021 (2021), *Security Council of the Russian Federation*. Available at: http://www.scrf.gov.ru/security/information/document114/ (accessed: 25.02.2023). (In Russian)

2. Sebekin, S. A. (2016), Russian Cyberdiplomacy in International Institutions: Providing international Information Security, *Russia — XXI century: IX Intern. sci.-pract. conf., Vladivostok, 28–31 Oct., 2016: materials*, ed. by Sonin, V. V., Smirnov, V. P., Panov, V. V. et al., Vladivostok: Far Eastern Federal University.

3. Boyko, S. (2018), UN Panel of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security: A Look from the Past into the Future, *Mezhdunarodnaia zhizn'*, no. 8, pp. 54–71. (In Russian)

4. Zinchenko, A. V. and Tolstukhina, A. Yu. (2018), Peace or war in cyberspace? *Mezhdunarodnaia zhizn'*, no. 9, pp. 82–90. (In Russian)

5. Russia Proposed to Establish a Working Group on Cyber Security at the UN (2018), *TASS*, October 27. Available at: https://tass.ru/politika/5727314 (accessed: 09.01.2023). (In Russian)

6. Chernenko, E. V. (2018), Russia and the United States are pulling the World Wide Web, *Kommersant*, November 12. Available at: https://www.kommersant.ru/doc/3797617 (accessed: 09.01.2023). (In Russian)

7. Chernenko, E. V. (2021), The UN General Assembly Committee approved the Russian-American resolution on cybersecurity, *Kommersant*, November 3. Available at: https://www.kommersant.ru/doc/5062751 (accessed: 09.01.2023). (In Russian)

8. Approving 15 Texts, First Committee Spotlights Impact of Illicit Weapons Trade on Women, Value of Gender Perspective in Reducing Armed Conflict (2022), *United Nations*, November 3. Available at: https://press.un.org/en/2022/gadis3705.doc.htm (accessed: 08.01.2023).

9. *Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security: Draft resolution A/C. 1/77/L. 73, General Assembly: Seventy-seventh session. First Committee. Agenda item 94. Developments in the field of information and telecommunications in the context of international security*, October 13, 2022. Available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N22/632/19/PDF/N2263219.pdf?OpenElement (accessed: 29.10.2022). (In Russian)

10. *Developments in the field of information and telecommunications in the context of international security: Revised draft resolution A/C. 1/77/L. 23/Rev.1, General Assembly: Seventy-seventh session. First Committee. Agenda item 94. Developments in the field of information and telecommunications in the context of international security*, October 20, 2022. Available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N22/655/80/PDF/N2265580.pdf?OpenElement (accessed: 29.10.2022). (In Russian)

11. Chernenko, E. and Isakova, T. (2022), Mines in the information field, *Kommersant*, July 25. Available at: https://www.kommersant.ru/doc/5480485 (accessed: 23.10.2022). (In Russian)

12. Shields, T. (2022), Kaspersky Named First Russian Company on Security Risk List, *Bloomberg*. 6 March. Available at: https://www.bloomberg.com/news/articles/2022–03–25/fcc-calls-kaspersky-china-telecom-china-mobile-security-risks (accessed 22.10.2022).

13. KA-SAT Network cyber attack overview (2022), *Viasat*, March 30. Available at: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview (accessed: 08.01.2023).

14. Arsentiev, A. Putin refused to sign the Convention on Cybercriminals (2008), *CNews*, March 27. Available at: http://safe.cnews.ru/news/top/putin_otkazalsya_podpisat_konventsiyu (accessed: 23.10.2022). (In Russian)

15. *United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes: Draft (2021), Kommersant*, June 29. Available at: https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf (accessed: 23.10.2022). (In Russian)

16. *Convention on Cybercrime*, Budapest, November 23, 2001. Available at: https://base.garant.ru/4089723/d78e49c48a908b41f776c768d5f3dc38/ (accessed: 23.10.2022). (In Russian)

17. Egorov, I. (2022), Security Council of the Russian Federation: The White House closed the only official channel of communication with the Kremlin, *RG.ru*, April 7. Available at: https://rg.ru/2022/04/07/sovbez-rf-belyj-dom-zakryl-edinstvennyj-oficialnyj-kanal-sviazi-s-kremlem.html (accessed: 10.23.2022). (In Russian)

18. Nakasone, P.M. and Sulmeyer, M. (2020), How to Compete in Cyberspace, *Foreign Affairs,* August 25. Available at: https://www.foreignaffairs.com/articles/united-states/2020–08–25/cybersecurity (accessed: 27.02.2023).

19. Goldsmith, J. (2022), *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*, Oxford: Oxford University Press.

20. *The United States of America Cyberspace Solarium Commission: Legislative Proposals, Cyberspace Solarium Commission*. Available at: https://www.solarium.gov/report (accessed: 28.02.2023).

21. Fischerkeller, M.P., Goldman, E.O. and Harknett, R.J. (2022), *Cyber Persistence Theory: Redefining National Security in Cyberspace,* Oxford: Oxford University Press.

22. Sebekin, S.A. (2020), Choosing between Persistent engagement and deterrence in the American Cybersecurity strategy, *Mezhdunarodnye protsessy*, vol. 18, no. 3 (62), pp. 96–125. (In Russian)

23. Jasper, S. (2017), *Strategic Cyber Deterrence: The Active Cyber Defense Option,* New York: Rowman & Littlefield.

24. Sulmeyer, M. (2018), How the U.S. Can Play Cyber-Offense: Deterrence Isn't Enough, *Foreign Affairs*. Available at: https://www.foreignaffairs.com/articles/world/2018–03–22/how-us-can-play-cyber-offense (accessed: 27.02.2023).

25. The Department of Defense Cyber Strategy 2018: Summary (2018), *U.S. Department of Defense*. Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.pdf (accessed: 28.02.2023).

26. Fischerkeller, M.P. and Harknett, R.J. (2017), Deterrence is Not a Credible Strategy for Cyberspace, *Orbis,* vol. 61, no. 3, pp. 381–393.

27. Fischerkeller, M.P. and Harknett, R.J. (2018), *Persistent Engagement, Agreed Competition, Cyberspace, Interaction Dynamics, and Escalation*. Institute for Defense Analyses.

28. Harknett, R.J., Callaghan, J.P. and Kauffman, R. (2010), Leaving Deterrence Behind: War-Fighting and National Cybersecurity, *Journal of Homeland Security and Emergency Management*, vol. 7, no. 1. pp. 1–24.

29. Nakasone, P.M. (2019), A Cyber Force for Persistent Operations, *Joint Force Quarterly*, vol. 92, 1st Quarter, pp. 10–14.

30. Goldman, E.O. (2020), From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy, *Texas National Security Review*, *Special Issue: Cyber Competition*, Fall. Available at: https://tnsr.org/category/special-issue-cyber-competition/ (accessed: 28.11.2020).

31. Cyber Policy (2020), *The New York Times*. Available at: https://www.nytimes.com/interactive/2020/us/politics/2020-democrats-cyber-policy-foreign-policy.html (accessed: 27.10.2022).

32. Statement of General Paul M. Nakasone Commander United States Cyber Command Before the Senate Committee on Armed Services (2019), *Senate Committee on Armed Services*, February 14. Available at: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf (accessed: 12.01.2023).

33. Nakashima, E. (2019), U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms, *The Washington Post*, February 26. Available at: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6–11e9-af5b-b51b7ff322e9_story.html (accessed: 12.01.2023).

34. Barnes, J.E. (2019), Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections, *The New York Times*, February 26. Available at: https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html (accessed: 12.01.2023).

35. Schneider, J.G. (2019), Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy, *Lawfare*. Available at: https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy (accessed: 12.01.2023).

36. Martin, A. (2022), US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command, *Skynews,* June 1. Available at: https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (accessed: 27.10.2022).

37. CYBER 101 — Defend Forward and Persistent Engagement (2022), *U.S. Cyber Command,* October 25. Available at: https://www.cybercom.mil/Media/News/Article/3198878/cyber101-defend-forward-and-persistent-engagement/ (accessed: 27.10.2022).

38. "Hacker War": An expert on cyber attacks between Russia and Ukraine (2022), *Russia Today*, May 2. Available at: https://russian.rt.com/ussr/video/1006738-voina-hackerov-ekspert-o-kiberatakah-mezhdu-rossiei (accessed: 09.01.2023). (In Russian)

39. Kildyushkin, R. (2022), Bot for Bot: Civil War Started in the Hacker Community Because of the Conflict in Ukraine, *Gazeta.ru*, March 3. Available at: https://www.gazeta.ru/tech/2022/03/02/14588575.shtml (accessed: 10.01.2023). (In Russian)

40. Tselishchev, A. (2022), The Killnet group hacked the site of Anonymous hackers who declared cyber war on Russia, *Gazeta.ru*, March 1. Available at: https://www.gazeta.ru/tech/news/2022/03/01/17364697.shtml?updated (accessed: 10.01.2023). (In Russian)

41. Schectman, J. and Bing, C. (2022), Ukraine calls on hacker underground to defend against Russia, *Reuters*. Available at: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022–02–24/ (accessed: 09.01.2023).

42. On another anti-Russian publication in the British media (2022), *Ministry of Foreign Affairs of the Russian Federation*, May 23. Available at: https://mid.ru/ru/press_service/publikacii-i-oproverzenia/oproverzenia1/nedostovernie-publikacii/1814455/ (accessed: 10.01.2023). (In Russian)

43. Schmitt, M. N. and Vihul, L. (eds) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

44. Delerue, F. (2020), *Cyber Operations and International Law,* Cambridge: Cambridge University Press.

45. Sebekin, S. A. (2021), Is the regime of control over proliferation of cyber weapons feasible? The Russian and U. S. approaches, *Puti k miru i bezopasnosti*, no. 2 (61), pp. 139–152. (In Russian)

46. Romashkina, N. P., Markov, A. S. and Stefanovich, D. V. (2020), *International Security, Strategic Stability and Information Technologies*, Moscow: IMEMO of RAS Press. (In Russian)

47. Nye, J. S. (2015), The World Needs an Arms-control Treaty for Cybersecurity, *Belfer Center for Science and International Affairs.* Available at: https://www.belfercenter.org/publication/world-needs-arms-control-treaty-cybersecurity (accessed: 01.03.2023).

48. Sharikov, P. A. (2020), Information Threats and Arms Control: Is Russian-US Dialogue Possible? *Valdai Discussion Club,* November 20. Available at: https://ru.valdaiclub.com/a/highlights/informatsionnye-ugrozy-i-kontrol-nad-vooruzheniyami/ (accessed: 05.03.2023). (In Russian)

49. Giles, M. (2018), We need a cyber arms control treaty to keep hospitals and power grids safe from hackers, *MIT Technology Review*. Available at: https://www.technologyreview.com/2018/10/01/139955/we-need-a-cyber-arms-control-treaty-to-keep-hospitals-and-power-grids-safe-from-hackers/ (accessed: 01.03.2023).

Received: February 5, 2023
Accepted: March 13, 2023

Author's information:

*Sergey A. Sebekin* — PhD in History; sebserg37gmail.com