Эволюция взаимодействия России и США в области международной информационной безопасности в исторической ретроспективе

Е. С. Зиновьева, И. О. Яникеева

Московский государственный институт международных отношений (университет) МИД России,
Российская Федерация, 119454, Москва, пр. Вернадского, 76

Для цитирования: *Зиновьева Е. С., Яникеева И. О.* Эволюция взаимодействия России и США в области международной информационной безопасности в исторической ретроспективе // Вестник Санкт-Петербургского университета. Международные отношения. 2022. Т. 15. Вып. 2. С. 158–173. https://doi.org/10.21638/spbu06.2022.203

В ноябре 2021 г. Россия и США внесли в Первый комитет ГА ООН проект совместной резолюции по международной информационной безопасности, что стало существенной победой российской дипломатии в деле формирования международного режима информационной безопасности. Российско-американские отношения в области международной информационной безопасности долгое время развивались исходя из конфронтационной модели, при этом именно эти два государства являются наиболее активными субъектами глобальной информационной сферы. От характера отношений между странами зависят общие тенденции формирования международного режима информационной безопасности. В статье представлен исторический анализ сотрудничества между Москвой и Вашингтоном в цифровой среде и дана оценка влияния исторического опыта взаимодействия на перспективы развития двустороннего сотрудничества в сфере международной информационной безопасности. Методологически авторы исходят из теории оборонительного реализма, согласно которой восприятие приоритетности угроз международной информационной безопасности является важным фактором двустороннего взаимодействия. Чем более значимыми воспринимаются угрозы с точки зрения национальной безопасности, тем более вероятно развитие и углубление международного сотрудничества, направленного на формирование правил поведения в данной области. В статье рассмотрена эволюция угроз международной информационной безопасности в исторической ретроспективе. Отталкиваясь от восприятия приоритетности угроз, авторы показывают эволюцию форматов двустороннего взаимодействия в сфере международной информационной безопасности. Доказано, что восприятие приоритетности угроз в области международной информационной безопасности способствует развитию и углублению двустороннего сотрудничества, что в перспективе может перерасти в полноценный режим международной информационной безопасности, основанный на правилах ответственного поведения государств в глобальном информационном пространстве.

Ключевые слова: международная информационная безопасность, отношения Россия — США, информационное противоборство, международное право.

Введение

Россия и США (наряду с КНР) являются наиболее влиятельными субъектами глобальной информационной сфере, согласно целому ряду индексов и экспертных оценок [1; 2]. В силу того, что дипломатия КНР в отношении обеспечения кибербезопасности носит выжидающий характер, именно от состояния российско-американских отношений в значительной мере зависят тенденции международного взаимодействия в области глобальной кибербезопасности.

Обе страны обладают существенным потенциалом в сфере развития информационно-коммуникационных технологий (ИКТ), а также выступают в роли важнейших участников переговорного процесса в сфере обеспечения глобальной кибербезопасности, предлагая, по сути, два конкурирующих дискурса в этой области.

Россия выступает за формирование универсального международного режима по обеспечению информационной безопасности, основанного на таких основополагающих принципах международного права, как уважение государственного суверенитета, неприменение силы или угрозы силой, мирное разрешение споров и невмешательство во внутренние дела. В долгосрочной перспективе Российская Федерация призывает к заключению обязывающего международного договора по обеспечению информационной безопасности под эгидой ООН, в котором были бы закреплены нормы и принципы ответственного поведения государств в глобальном информационном пространстве [3].

Дипломатия США, направленная на обеспечение кибербезопасности, в свою очередь делает акцент на вопросах применимости международного права к информационной сфере, предлагая разграничить нормы ответственного поведения государств в мирное время и нормы, основанные на международном гуманитарном праве, которые должны применяться в условиях вооруженных конфликтов в киберпространстве (что представляется, согласно российской позиции, затруднительным в силу специфики ИКТ, которая осложняет атрибуцию атаки, а также определение порога вооруженного конфликта). В двусторонних же отношениях в исследуемой области США выступают за подход «патчей», согласно которому спорные и конфликтные области в двусторонних отношениях, затрагивающие вопросы кибербезопасности, нуждаются в решении на основании ad hoc принципа (что вызывает вопросы в силу возможности в данном случае реализации стратегии «выбора удобных институтов» в зависимости от ситуативных интересов) [4]. Согласно мнению ведущего переговорщика по кибербезопасности со стороны США М. Маркоф, США выступают за регулирование использования технологий, в то время как Россия выступает за регулирование технологий как таковых [5]. Переговорщик со стороны России, специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, отмечает, что Россия занимает миротворческую позицию, стремится не допустить новой гонки вооружений в глобальном информационном пространстве [6]. Согласно экспертам, позиция США направлена на закрепление собственного лидерства в информационной сфере и обеспечение свободы рук в военном использовании ИКТ, в то время как Россия стремится обеспечить мирное развитие информационной сферы, в рамках которой она играла бы роль одного из центров силы [7].

Однако исторический анализ двусторонних отношений показывает, что несмотря на противоречия в официальных позициях и национальных интересах государств, существуют периоды сближения и расхождения их позиций, что находило отражение в частности в подписании официальных документов на двустороннем и/или многостороннем уровнях. Исследовательский вопрос, на который пытались ответить авторы статьи: чем обусловлено сближение и расхождение позиций России и США в области международной информационной безопасности (МИБ)?

Методологически настоящая статья исходит из теории политического реализма, прежде всего его оборонительной версии, которая увязывает динамику международного сотрудничества с восприятием приоритетности угроз безопасности — чем более значимы угрозы, тем выше вероятность развития и углубления международного взаимодействия в сфере безопасности [8]. Именно восприятие угроз как реалистичных становится стимулом к ревизии правил взаимодействия России и США в сфере безопасности и выработке новых соглашений, регламентирующих взаимодействие [9]. Как правило, трансформации восприятия предшествуют значимые кризисы в сфере кибербезопасности, демонстрирующие стратегическую уязвимость государств и подталкивающие к согласованному поиску путей ее преодоления. Примером такого кризиса может являться атака вируса Stuxnet на ядерные объекты Ирана или растущее значение и масштабы киберпреступности в условиях пандемии коронавирусной инфекции. В частности, кейс Stuxnet стал наглядным примером поражающей мощи кибероружия при его сравнительной дешевизне и доступности, что, в свою очередь, ставило под угрозу и интересы США в условиях «парадокса цифровой мощи», т. е. в ситуации, когда наиболее развития страна с точки зрения ИКТ-потенциала оказывается наиболее уязвимой.

Структурно статья состоит из трех частей — в первой части рассмотрена эволюция угроз международной информационной безопасности в исторической ретроспективе, во второй части представлен анализ эволюции взаимодействия России и США в области МИБ, а в третьей — дается оценка перспективам выработки правил ответственного поведения государств в глобальном информационном пространстве в контексте развития отношений России и США в области информационной безопасности.

Угрозы между народной информационной безопасности в исторической ретроспективе

Международно-политическая значимость угроз МИБ возрастала по мере поступательной эволюции (ИКТ и их проникновения в различные сферы жизни личности, общества и государства). Вслед за классификацией, принятой в ООН, в настоящей статьей выделяется триада угроз международной информационной безопасности: военно-политические, террористические и преступные.

Российская Федерация стала пионером в обсуждении угроз МИБ в рамках ООН. Именно по инициативе России в 1999 г. в резолюции ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» была впервые сформулирована вышеуказанная триада угроз. При этом, несмотря на опасность всех проявлений злонамеренного использования ИКТ, наиболее значимой угрозой международной стабильности рассматривалось использо-

вание ИКТ в военных целях. С подобной позицией и сегодня выступают официальные лица Российской Федерации. «С учетом того, что международная обстановка обостряется, и информационное пространство все больше используется именно для оказания влияния на социально-экономическую обстановку в других странах, в сфере военного применения, это представляет наибольшую угрозу», — отмечает первый заместитель председателя комитета Госдумы по безопасности и противодействию коррупции Э. Валеев [10].

В конце XX — начале XXI в. быстрое развитие ИКТ способствовало росту значимости угроз МИБ для всего международного сообщества, а их транснациональный характер диктовал необходимость международного сотрудничества. Однако в конце 1990-х — начале 2000-х годов США, будучи уверенными в своем лидерстве в сфере развития ИКТ, не признавали наличия военно-политической составляющей угроз МИБ, не желая связывать себе руки международными обязательствами. Подобный подход нашел отражение в таких документах, подписанных США, как Окинавская Хартия группы восьми от 2000 г. [11] и ряде резолюций ГА ООН [12], принятых по инициативе США, где признавалась лишь опасность преступного и террористического использования ИКТ, однако вопросы военного их использования никак не рассматривались. Россия же всегда выступала за недопущение новой гонки вооружений, уже в информационном пространстве.

Однако позднее, после атак вируса Stuxnet в 2010 г., который остановил работу более 1300 центрифуг по обогащению урана в иранском Нетензе, международное сообщество и США признали значимость угроз информационной безопасности, что нашло отражение в докладах Группы правительственных экспертов ООН по международной информационной безопасности 2010, 2013 и 2015 гг., куда, по настоянию российской стороны, включили угрозы военно-политического использования ИКТ. Это стало важным сигналом о сближении позиций международного сообщества, в том числе США и России, по вопросу о сотрудничестве в сфере МИБ. Показательно, что в 2013 г. в рамках саммита G8 в Шотландии, в Лох-Эрне, было заключено двустороннее соглашение между Россией и США о новой области доверия, которое включало в себя и вопросы сотрудничества в области обеспечения кибербезопасности.

Позднее, в конце 2010-х — начале 2020-х годов, в условиях новой технологической реальности повестка дня в области МИБ дополнилась угрозами злонамеренного использования таких технологий, как анализ «больших данных», возможности искусственного интеллекта, вредоносное воздействие на «интернет вещей», которые все более плотно проникают в повседневную жизнь.

Как отмечает авторитетный российский автор С. М. Бойко, сегодня наибольшую угрозу представляют компьютерные атаки на объекты атомной энергетики [13]. Кроме того, все чаще серьезной опасности стали подвергаться объекты промышленности. По данным российской компании «Positive Technologies», только за первые десять месяцев 2020 г. количество таких атак достигло 170, тогда как за весь 2019 г. их было 125 [13]. Особенно заметными стали атаки киберпреступников, которые использовали вирусы-вымогатели, на объекты пищевой и энергетической промышленности США в 2021 г.

Нельзя не отметить того влияния, которое эпидемия коронавирусной инфекции и обусловленная ею изоляция оказали на значимость угроз международной

информационной безопасности. Так, по оценкам МВД Российской Федерации, только за 2020 г. количество киберпреступлений увеличилось на 75 % [14]. При этом в условиях пандемии выросло число пользователей социальных сетей, а также время, проводимое в сети (так, например, согласно отчету Digital 2020 [15], в среднем люди проводят в социальных сетях порядка 6 часов), что привело к росту преступлений в онлайн-среде, в том числе посредством социальных сетей и социального инжиниринга, что отмечают эксперты таких международных организаций, как ВОЗ и ООН [16].

Однако военно-политическое измерение проблематики сохраняет свою значимость в силу особого влияния проблем информационной безопасности на стратегическую стабильность в современном мире. Как отмечают авторы доклада Валдайского клуба от 2021 г., «цифровые технологии постепенно заполняют ту нишу, которую традиционно в эпоху биполярности занимало ядерное оружие — как ключевой стратегический инструмент, одинаково важный для военного лидерства, экономического развития и глобального престижа» [17]. Возрастает количество стран, разрабатывающих военные программы в сфере ИКТ. Кибератаки являются одной из форм и инструментом ведения войн в настоящее время [18]. При этом ключевые параметры кибератак не поддаются проверке, и в настоящее время атрибуция кибератак затруднена, что осложняет (но не делает невозможным) определение ответственных за злонамеренные действия в киберпространстве.

Как полагает сотрудник Массачусетского технологического института Бен Бьюкенен, в силу специфики информационно-коммуникационных технологий дилемма безопасности в данной сфере носит более острый характер, чем в других областях мировой политики, т. е. обеспечение международной безопасности и формирование устойчивого режима безопасности более сложная задача, но это не делает сотрудничество менее востребованным [19, с. 187].

В этих условиях угрозы международной информационной безопасности воспринимаются как приоритетные всеми государствами международного сообщества. Страны Запада, в том числе США, заинтересованы в сохранении технологического превосходства и пытаются активно использовать ИКТ, чтобы диктовать свою волю, оказывать влияние на внутреннюю политику других государств, а также для технической разведки. Обострение угроз информационной безопасности и формирование многополярности делает такую стратегию внешней политики неэффективной, что признает и политическая элита США.

Показательно, что в ноябре 2021 г. председатель Объединенного комитета начальников штабов США М. Милли заявил, что США вступают в конфигурацию триполярной войны, в которой им придется противостоять России и Китаю, при этом современный мир стратегически нестабилен, а новые технологии, такие как роботизация и технологии искусственного интеллекта, принципиально меняют характер войны [20]. Можно сделать вывод о том, что США уже не воспринимают себя единоличным лидером в глобальном информационном пространстве и с озабоченностью относятся к уязвимостям в данной области, что обусловливает их заинтересованность в углублении международного сотрудничества, как на глобальном, так и на двустороннем уровнях.

В свою очередь, Российская Федерация выступает за мирное развитие глобального информационного пространства, за его использование, основанное на осно-

вополагающих принципах международного права, которые предполагают уважение государственного суверенитета, невмешательство во внутренние дела, а также мирное разрешение конфликтов и споров, неприменимость силы или угрозы силой. Подобный подход, однако, не означает отказа от развития собственного информационного потенциала и укрепления оборонительных возможностей в данной области.

Эволюция отношений России и США в области международной информационной безопасности

Еще в 1998 г. Россия предложила США подписать на уровне президентов двух государств заявление по вопросам обеспечения информационной безопасности, которое предусматривало бы совместное определение вызовов и угроз в цифровой среде, выработку понятийного аппарата, обсуждение темы обеспечения МИБ на уровне ООН, а также работу над заключением международного многостороннего договора о борьбе с информационным терроризмом и преступностью [7, с. 728–742]. Однако обсуждение проекта заявления не привело к сближению Москвы и Вашингтона на этом направлении, в основном в силу слабой заинтересованности со стороны США.

Долгое время двустороннее взаимодействие велось на площадке Группы правительственных экспертов ООН по международной информационной безопасности. При этом актуализация угроз информационной безопасности стала важным стимулом для развития международного сотрудничества. В 2010 г. был принят итоговый доклад ГПЭ ООН, в котором отмечалась растущая значимость угроз МИБ, в том числе в военно-политической плоскости, а также необходимость международного сотрудничества и выработки правил ответственного поведения государств, мер доверия. Группа также согласовала доклады в 2013 и 2015 гг., в рамках которых по инициативе российской дипломатии был сделан акцент на выработке норм, правил и принципов ответственного поведения государств в глобальном информационном пространстве [13].

В 2017 г. президенты России и США «на полях» Группы восьми в Лох-Эрне договорились создать механизм обмена информацией о киберугрозах для защиты критически важных национальных информационных систем, о создании прямого канала связи между высокими должностными лицами в России и США для обмена информацией, была также создана российско-американская рабочая группа в рамках института президентских комиссий по вопросам угроз в сфере использования ИКТ в контексте международной безопасности, были заключены соглашения между двумя государствами о новой области доверия, которые в настоящее время еще продолжают свое действие [21]. При этом в 2014 г. работа российско-американской рабочей группы была приостановлена по инициативе США и в целом российско-американские отношения в киберпространстве существенно деградировали. Долгое время после 2014 г. российско-американские отношения в сфере международной информационной безопасности были заложниками контрпродуктивного курса на сдерживание России, взятого администрацией Б. Обамы под предлогом внутриукраинского кризиса. Вашингтон информационно и психологически воздействовал на международное общественное мнение, формируя образ Российской

Федерации как главного виновника всех проблем внутренней и внешней политики не только Соединенных Штатов, но и всего Запада в целом, при этом акцент делался на якобы имевших место агрессивных действиях в киберпространстве. Например, Вашингтон обвинил Москву в том, что она повлияла на результаты президентских выборов в США и европейских стран в 2016 г. (вводя в этой связи киберсанкции в отношении российских компаний и россиян) [22]; получила доступ к секретным данным в информационных системах правительства США [23]; распространяет «фальшивую» информацию и осуществляет антиамериканскую, антизападную пропаганду [24]; создала вредоносную программу Drovorub, которая якобы может использоваться для кибершпионажа [25]; что «русские хакеры» якобы пытались украсть информацию и интеллектуальную собственность, которая имела отношение к разработке и тестированию вакцин от COVID-19 [26], что Россия причастна к кибератакам в отношении американских правительственных учреждений, которые пользуются услугами ИТ-компании SolarWinds [27]. На официальном уровне Россия отрицает все вышеуказанные обвинения. В то же самое время Соединенные Штаты размещали «кибербомбы» в объектах критической информационной инфраструктуры России, которые могут быть использованы для подрыва экономической и социальной стабильности российского общества [28]. Кроме того, ЦРУ разработало программное обеспечение для осуществления компьютерных атак, в том числе под «чужим флагом» [29]. Президент США Д. Трамп санкционировал кибератаку на Агентство интернет-исследований [30]. США осуществили кибероперации в отношении российских структур, «нацеленные на компьютерную инфраструктуру, связанную с правительственными хакерами в России» [31]. Более того, согласно информации российского МИДа, Большинство кибернападений на Россию в 2020 г. осуществлялось с адресов, зарегистрированных в США, Германии и Нидерландах, мишенями хакеров были объекты, связанные с госуправлением, финансовым сектором, ВПК, здравоохранением и разработкой вакцин [32].

При этом важно отметить, что, несмотря на прекращение в 2014 г. работы российско-американской рабочей группы по вопросам угроз в сфере использования ИКТ в контексте международной безопасности, заключенные между Россией и США соглашения о новой области доверия от 2013 г. продолжают свое действие [33]. Механизм взаимодействия на площадке ГПЭ ООН также сохранился, однако из-за расхождения позиций членов группы, в том числе России и США, по ряду ключевых вопросов, в частности касательно применимости международного права к информационной сфере, итоговый доклад не был принят.

Вашингтон вплоть до 2021 г. отказывался от инициатив Москвы по конструктивному сотрудничеству в области МИБ. Так, например, после встречи с президентом России В. Путиным на саммите G20 в Гамбурге в 2017 г. Президент США Д. Трамп объявил о начале совместной работы над созданием защищенной от воздействий извне рабочей группы по кибербезопасности, нацеленной на противодействие хакерским атакам во время выборов и избирательных кампаний. Однако политическая элита США подвергла идею жесткой критике, и американскому лидеру в итоге пришлось от нее отказаться. Другим примером стала ситуация с российско-американской встречей по кибербезопасности: она должна была состояться в Женеве в конце февраля 2018 г., но американская делегация в последний момент отказалась от нее. Продолжением сложившейся тенденции была встреча президен-

тов России и США в Хельсинки в июле 2018 г., когда Москва вновь предложила создать рабочую группу по кибербезопасности. Американская сторона в очередной раз отказалась от российской инициативы.

Показательно, что в 2018 г. Россия и США выступили с резолюциями на Генеральной Ассамблее ООН, обе из которых были приняты. По итогам резолюций были созданы две альтернативные площадки — Группа правительственных экспертов и Рабочая группа открытого состава по международной информационной безопасности. Многие эксперты увидели в этом раскол международного сообщества по вопросам обеспечения информационной безопасности [33].

25 сентября 2020 г. было опубликовано заявление президента России В. Путина, в котором сформулированы предложения к Вашингтону начать конструктивный профессиональный разговор по всему комплексу вопросов, касающихся МИБ [34]. 25 сентября 2020 г. Министр иностранных дел С. Лавров вновь обратился к США с предложением одобрить комплексную программу практических мер по перезагрузке российско-американских отношений в сфере использования ИКТ [35]. Однако 20 октября 2020 г. в ответ на российские предложения Госдепартамент США опубликовал доклад «О международной безопасности в киберпространстве: новые модели для снижения рисков» за авторством помощника государственного секретаря США по международной безопасности и нераспространению Кристофера А. Форда [36]. В докладе были сформулированы бездоказательные обвинения в «безответственном» поведении России в киберпространстве. Важно особо отметить, что в докладе был представлен тезис о том, что если кибератака приведет к последствиям, сравнимым со значительной атакой традиционными силами, то она может представлять собой значительную неядерную стратегическую атаку и в этом случае потребовать ядерного ответа. Он в очередной раз подтвердил приверженность со стороны США к односторонним действиям с позиции силы в киберпространстве.

Однако в 2021 г. во взаимоотношениях двух стран в сфере международной информационной безопасности наметился существенный прогресс. Важную роль в нем сыграла встреча на высшем уровне президента России В. Путина и президента США Дж. Байдена 16 июня 2021 г. В результате достигнутых договоренностей был институционализирован диалог между странами в области международной информационной безопасности, а также достигнуты договоренности о развитии взаимодействия в данной области.

По словам посла России в Вашингтоне Анатолия Антонова, уже прошло четыре раунда экспертных консультаций под эгидой советов безопасности двух стран. Российский посол указал на наличие результатов в сфере пресечения хакерской активности и борьбы с преступным использованием ИКТ. Борьба с киберпреступностью является одной из главных озабоченностей США на данном направлении, и в результате диалога было восстановлено взаимодействие в рамках двустороннего договора о взаимной правовой помощи по уголовным делам 1999 г., что позволяет обмениваться информацией о киберпреступниках в рамках досудебного расследования, в том числе в целях сбора улик и доказательств вины.

В международно-политической плоскости взаимодействие также дало конкретные результаты. В ноябре 2021 г. в Первом комитете 76-й сессии Генеральной Ассамблеи ООН был принят консенсусом российско-американский проект резо-

люции по проблематике международной информационной безопасности. У документа рекордное количество соавторов — 107 стран. При этом Россия и США выступают в качестве главных соавторов. Сам факт того, что Россия и США выступили с совместным проектом резолюции, стал важным достижением российской дипломатии и существенным шагом вперед в развитии двустороннего взаимодействия в области международной информационной безопасности.

Прежде всего нынешнее состояние российско-американских отношений характеризуется высоким уровнем недоверия, что затрудняет заключение любого двустороннего соглашения или принятия правил поведения, направленных на обеспечение МИБ. Однако опыт позитивного взаимодействия, в частности на уровне борьбы с киберпреступностью, способен создать первичную атмосферу доверия, необходимую для углубления взаимодействия, в том числе в отношении глубоких и сложных вопросов формирования международного режима информационной безопасности на глобальном уровне.

Как представляется, прослеживается взаимосвязь между восприятием значимости угроз международной информационной безопасности и характером двустороннего взаимодействия — значимые международные инциденты в области кибербезопасности (такие как атаки вируса Stuxnet и обострение угроз в области киберпреступности и атак на критические информационные инфраструктуры) способствуют переосмыслению внешнеполитической позиции и началу работы над выработкой новых правил в области двустороннего и многостороннего взаимодействия.

Формирование правил ответственного поведения государств и перспективы развития двустороннего взаимодействия России и США

Отсутствие единых обязательных для всех международно-правовых норм, регулирующих информационное пространство, усиливает непредсказуемость использования ИКТ в межгосударственных отношениях [37]. Непредсказуемость, в свою очередь, может спровоцировать дальнейшую деградацию российско-американских отношений, что представляет серьезную угрозу для глобального мира и безопасности [38]. Характер двусторонних отношений между США и Россией как ключевыми субъектами международного режима в области информационной безопасности оказывает существенное влияние на формирование глобального режима в данной области. В этих условиях выработка и принятие совместной резолюции является позитивным сигналом для всего международного сообщества.

Правила поведения в информационном пространстве, которые должны быть созданы, можно сравнить с правилами дорожного движения, которые были сформулированы не сразу, а только по мере развития транспортных средств и которые непрерывно модернизируются в зависимости от меняющихся условий. Как отмечает главный научный сотрудник Института проблем информационной безопасности МГУ имени М. В. Ломоносова А. Стрельцов, когда государства в рамках принципов и норм ответственного поведения возьмут на себя добровольное обязательство не допускать враждебного использования ИКТ, важно будет определить средства реализации данного обязательства в условиях отсутствия гра-

ниц цифрового суверенитета [39]. «Международные обязательства, которые государства взяли на себя, должны быть реализованы, в том числе и применительно к деятельности ИКТ-среды. Но при этом необходимо четко понимать, что должны существовать некоторые методы идентификации и авторов, и событий, которые в ИКТ-среде существуют и которые потенциально или реально могут рассматриваться как нарушение международных обязательств того или иного государства» [39]. При этом он отмечает, что необходима также разработка проекта руководства по применению принципов, норм и правил ответственного поведения государств в киберпространстве.

В совместном российско-американском проекте резолюции Генеральной Ассамблеи ООН, упомянутом ранее, содержательно представлены важные принципы и правила ответственного поведения государств в информационном пространстве, за продвижение которых российская дипломатия выступает еще с 1998 г.: поощрение использования ИКТ в мирных целях и предотвращение конфликтов, возникающих в сфере использования ИКТ, использования ИКТ в террористических и преступных целях. Особо отмечается важность недопущения кибератак на критические информационные инфраструктуры государств.

Кроме того, в проекте резолюции приветствуется принятый в рамках Рабочей группы открытого состава ООН по МИБ доклад от 2021 г., а также отмечается важность работы ее нового созыва в 2021–2025 гг. При этом из резолюции следует, что итогом работы РГОС может стать и принятие официального документа на уровне ООН в области МИБ, который будет носить обязательный характер для подписантов.

Как представляется, со стороны США и России прозвучал позитивный сигнал международному сообществу о признании угроз МИБ, а также о важности выработки правил ответственного поведения государств в информационном пространстве. Такого рода правила призваны лечь в основу международного режима информационной безопасности, цель формирования которого была поставлена в Основах государственной политики в области международной информационной безопасности Российской Федерации, принятых российским президентом 12 апреля 2021 г. Документ призван укреплять мир и международную безопасность, которая сегодня во все большей степени зависит от уровня развития информационно-коммуникационных технологий. Как отметил заместитель постоянного представителя РФ при отделении ООН в Женеве А. Белоусов, «международное сообщество на практике доказало, что способно договариваться и вырабатывать взаимоприемлемые развязки, когда речь идет о решении принципиальных вопросов национальной и международной безопасности» [40].

Эксперты призывают вовлекать в разработку принципов, норм и правил, регулирующих информационное пространство, как можно большее количество международных акторов [41]. Фирмы и НКО, как и государства или частные лица, могут формулировать и продвигать нормы поведения, в частности так действует Microsoft, продвигая глобальные нормы по обеспечению кибербезопасности [41, с. 446]. При этом существуют три способа распространения и утверждения норм: мотивация (разного рода поощрения, например, режимы наибольшего благоприятствования, и наказание, например, санкции или угроза применения силы), убеждение (убедительная аргументация о необходимости норм) и социализация (же-

лание других акторов стать частью сообщества, которое придерживается тех или иных норм поведения, а также принуждение примкнуть к сообществу, используя тактику придания гласности и позору, навешивания ярлыков) [38]. Именно на этом направлении и выстроена работа РГОС нового созыва, запланированная до 2025 г.

***

В условиях взаимного недоверия между Россией и США двустороннее сотрудничество в сфере МИБ представляется наиболее перспективным, поскольку еще с конца XX в. остро проявилась необходимость укреплять меры доверия в цифровой среде, развивать российско-американское взаимодействие на этом направлении, предотвращать конфликты в информационном пространстве, не допускать милитаризации цифровой среды, договориться использовать ИКТ исключительно в мирных целях.

Именно укрепление взаимного доверия в цифровой среде может заложить основы для дальнейшего перспективного двустороннего взаимодействия в области обеспечения МИБ. В условиях обострения угроз международной информационной безопасности, ставшего в значительной степени результатом ускоренной цифровизации, которая в условиях пандемии коронавирусной инфекции проводилась без учета соображений безопасности, а также быстрого и повсеместного проникновения ИКТ выработка правил ответственного поведения государств в информационном пространстве на глобальном уровне представляется крайне востребованной задачей.

Литература

1. ICT Development Index 2017, *ITU*. URL: https://www.itu.int/net4/ITU-D/idi/2017/index.html (дата обращения: 29.11.2021).

2. National Cyberpower Index 2020, *Belfer Center*. URL: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf (дата обращения: 29.11.2021).

3. *Основы государственной политики Российской Федерации в области международной информационной безопасности*, 12.04.2021. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 29.11.2021).

4. United States Comments on the Chair's Pre-draft of the Report of the UN Open Ended Working Group (OEWG), *UN OEWG official site*. URL: https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-usg-comments-4-6-2020.pdf (дата обращения: 29.11.2021).

5. Inside Cyber Diplomacy. A Guide to UN GGE. Interview with M. Markoff (2021), *Center for Strategic and International Studies*, July 11. URL: https://www.csis.org/podcasts/inside-cyber-diplomacy (дата обращения: 29.11.2021).

6. Спецпредставитель президента: Россия против развязывания гонки информационных вооружений (2017), *ТАСС*, 29.07. URL: https://tass.ru/politika/4374464 (дата обращения: 29.11.2021).

7. Крутских, А. В. (ред.) (2019), *Международная информационная безопасность: теория и практика, в 3 т.*, т. 2, М: Аспект-Пресс.

8. Wohlforth, W. C. (2008), Realism and foreign policy, in *Foreign policy: theories, actors, cases,* Oxford, UK, New York: Oxford University Press, pp. 35–53.

9. Фененко, А. В. (2011), Военно-техническая модернизация и циклы сближения между США и Россией, *Международные процессы*, № 2. URL: http://general-history.ucoz.ru/Fenenko-26.pdf (дата обращения: 29.11.2021).

10. Яникеева, И. (2019). Ответственное поведение большинства государств в информационном пространстве — утопия?, *Международная жизнь*, 30.05. URL: https://interaffairs.ru/news/show/22643 (дата обращения: 29.11.2021).

11. *Окинавская хартия глобального информационного общества от 22 июля 2000*. URL: https://base.garant.ru/2560931/ (дата обращения: 29.11.2021).

12. *A/RES/57/239 Создание глобальной культуры кибербезопасности, ГА ООН, 31.01.2003*. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата обращения: 29.11.2021).

13. Бойко, С. М. (2021), Угрозы международной информационной безопасности в условиях новой технологической реальности, *Международная жизнь*, № 1. URL: https://interaffairs.ru/jauthor/material/2453 (дата обращения: 29.11.2021).

14. Краткая характеристика состояния преступности в Российской Федерации за январь — октябрь 2020 года, *МВД России*. URL: https://мвд.рф/reports/item/21933965/ (дата обращения: 29.11.2021).

15. *Digital 2020: Global Digital Overview*. URL: https://datareportal.com/reports/digital-2020-global-digital-overview (дата обращения: 29.11.2021).

16. *Cybercrime and COVID19: Risks and Responses, UN Office for Drugs and Crime. Vienna, 14.04.2020*. URL: https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=nui,sc (дата обращения 29.11.2021).

17. *Realpolitik в «цифре»: суверенитет, союзы и неприсоединение XXI века. Доклад дискуссионного клуба Валдай* (2021). URL: https://ru.valdaiclub.com/files/39047/ (дата обращения: 29.11.2021).

18. Яникеева, И. (2019), Война будущего — тотальная и беспощадная, *Международная жизнь*, 29.08. URL: https://interaffairs.ru/news/show/23620 (дата обращения 29.11.2021).

19. Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*, Oxford University Press.

20. В Пентагоне заявили о необходимости поддерживать диалог с Россией и Китаем (2021), *Лента.ру,* 03.11. URL: https://lenta.ru/news/2021/11/03/uschinarus/ (дата обращения: 29.11.2021).

21. *Report of the Select Committee on intelligence United States Senate on Russian active measures campaigns and interference in the 2016 U. S election*. URL: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures (дата обращения: 29.11.2021).

22. *The White House. Office of the Press Secretary. Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment*. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (дата обращения: 29.11.2021).

23. McFadden, C., Arkin, W. & Monahan, K. (2018), Russians penetrated U.S. voter systems, top U.S. official says, *NBC News*. URL: https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721 (дата обращения: 29.11.2021).

24. *Disinformation: A primer in Russian active measures and influence campaigns. Hearing before the Select Committee on Intelligence of the United States Senate. March 30, 2017. Printed for the use of the Select Committee on Intelligence*. URL: https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm (дата обращения: 29.11.2021).

25. National Security Agency Federal Bureau of Investigation. Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware, (2020), *Cybersecurity Advisory*. URL: https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF (дата обращения: 29.11.2021).

26. Barnes, J. (2020), Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say, *The New York Times*, July, 16. URL: https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html (дата обращения 29.11.2021).

27. Vlamis, K. (2020), Here's a list of the US agencies and companies that were reportedly hacked in the suspected Russian cyberattack, *Business insider*. URL: https://www.businessinsider.com/list-of-the-agencies-companies-hacked-in-solarwinds-russian-cyberattack-2020-12 (дата обращения 29.11.2021).

28. Obama's secret struggle to punish Russia for Putin's election assault (2017), *Washington Post*, June, 23. URL: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?noredirect=on&utm_term=.98388a2652c5 (дата обращения: 29.11.2021).

29. Шитов, А. (2017), WikiLeaks: ЦРУ может устраивать кибератаки «под чужим флагом», *ТАСС*. URL: https://tass.ru/mezhdunarodnaya-panorama/4077772 (дата обращения: 29.11.2021).

30. Thiessen, M. A. (2020), Trump confirms, in an interview, a U.S. cyberattack on Russia, *Washington Post*. URL: https://www.washingtonpost.com/opinions/2020/07/10/trump-confirms-an-interview-us-cyberattack-russia/ (дата обращения: 29.11.2021).

31. СМИ сообщили о кибератаках США против России и Ирана, *Ведомости*. URL: https://www.vedomosti.ru/society/news/2020/11/04/845782-smi-soobschili-o-kiberatakah-ssha-protiv-rossii-i-irana (дата обращения: 29.11.2021).

32. В МИД назвали основные источники кибератак на Россию в 2020 году (2021), *Международная жизнь*, 12.05. URL: https://interaffairs.ru/news/show/30087 (дата обращения: 29.11.2021).

33. Крутских, А. В. (2021), *Международная информационная безопасность: теория и практика*, в 3 т., т. 3, М.: Аспект-Пресс.

34. *Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности*. URL: http://kremlin.ru/events/president/news/64086 (дата обращения: 21.12.2020).

35. *Выступление Министра иностранных дел Российской Федерации С. В. Лаврова в связи с заявлением Президента Российской Федерации В. В. Путина по международной информационной безопасности*, Москва, 25 сентября 2020 года. URL: https://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4350560 (дата обращения 29.11.2021).

36. Ford, C. (2020), *International Security in Cyberspace: New Models for Reducing Risk*. URL: https://www.state.gov/wp-content/uploads/2020/10/T-paper-series-Cybersecurity-Format-508.pdf (дата обращения: 29.11.2021).

37. Кулик, С. А. (2013), *«Электронная дипломатия». Начало. Аналитический отчет*. URL: http://www.insor-russia.ru/files/EDiplomacy_0.pdf (дата обращения: 29.11.2021).

38. Sigmar, G. (2017), *«Destroyed» US-Russia Ties May Threaten Global Peace. German Foreign Minister*. URL: https://sputniknews.com/world/201711051058829506-us-russia-destroyed-ties-threaten-peace/ (дата обращения: 29.11.2021).

39. Стрельцов, А. А. (2018), Основные проблемы применения международного права в ИКТ-среде, *XII Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Россия и глобальные вызовы в области информационной безопасности. Международная жизнь*. с. 106–109. URL: https://interaffairs.ru/virtual-read/garmish2018/publication.pdf (дата обращения: 29.11.2021).

40. *В России заявили, что совместная с США резолюция по киберсфере укрепит международный мир*, 03.11.2021. https://tass.ru/politika/12831715?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 29.11.2021).

41. Finnemore, M. and Hollis, D. B. (2016), Constructing Norms for Global Cybersecurity, *American Journal of international Law*, vol. 110, no. 3 , pp. 425–479.

Статья поступила в редакцию 10 февраля 2022 г.
Статья рекомендована к печати 22 марта 2022 г.

Контактная информация:

Зиновьева Елена Сергеевна — д-р полит. наук, проф.; elena.zinovjeva@gmail.com
Яникеева Инна Олеговна — аспирант; yanikeeva93@mail.ru

Evolution of the US — Russia relations in the area of international information security: A retrospective study

E. S. Zinovieva, I. O. Yanikeeva

Moscow State Institute of International Relations (MGIMO University),
76, pr. Vernadskogo, Moscow, 119454, Russian Federation

For citation: Zinovieva E. S., Yanikeeva I. O. Evolution of the US — Russia relations in the area of international information security: A retrospective study. *Vestnik of Saint Petersburg University. International Relations*, 2022, vol. 15, issue 2, pp. 158–173. https://doi.org/10.21638/spbu06.2022.203 (In Russian)

In November 2021, Russia and the United States submitted a draft joint resolution on international information security to the UNGA First Committee, which was a significant victory

for Russian diplomacy in the formation of an international information security regime. For a long time, Russian-American relations in the field of international information security have been developing on the basis of a confrontational model, while these two states are the most active actors in the global information sphere. The general trends in the formation of an international information security regime depend on the nature of relations between countries. The article presents a historical analysis of cooperation between Moscow and Washington in the digital environment and assesses the impact of the historical experience of interaction on the prospects for the development of bilateral cooperation in the field of international information security. Methodologically, the authors base the research from the theory of defensive realism, according to which the factor of perception of the priority of threats to international information security is an important factor in bilateral interaction. The more significant threats are perceived from the point of view of national security, the more likely is the development and deepening of international cooperation aimed at shaping the rules of conduct in this area. The article examines the evolution of threats to international information security in historical retrospect. Based on the perception of the priority of threats, the evolution of the formats of bilateral interaction in the field of international information security is shown. It has been proved that the perception of the priority of threats in the field of international information security contributes to the development and deepening of bilateral cooperation, which in the future can develop into a full-fledged regime of international information security, based on the rules of responsible behavior of states in the global information space.

Keywords: international information security, Russian-American relations, information warfare, international law.

References

1. ICT Development Index 2017, *ITU.* Available at: https://www.itu.int/net4/ITU-D/idi/2017/index.html (accessed: 29.11.2021).
2. National Cyberpower Index 2020, *Belfer Center*. Available at: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf (accessed: 29.11.2021).
3. *Fundamentals of the state policy of the Russian Federation in the field of international information security*, 12.04.2021. Available at: http://www.scrf.gov.ru/security/information/document114/ (accessed: 29.11.2021). (In Russian)
4. United States Comments on the Chair's Pre-draft of the Report of the UN Open Ended Working Group (OEWG), *UN OEWG official site*. Available at: https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-usg-comments-4-6-2020.pdf (accessed: 29.11.2021).
5. Inside Cyber Diplomacy. A Guide to UN GGE. Interview with M. Markoff (2021), *Center for Strategic and International Studies*, July 11. Available at: https://www.csis.org/podcasts/inside-cyber-diplomacy (accessed 29.11.2021).
6. Special Representative of the President: Russia is against unleashing an information arms race (2017), *TASS*, July, 29. Available at: https://tass.ru/politika/4374464 (accessed 29.11.2021). (In Russian)
7. Krutskikh, A. V. (ed.) (2019), *International Information Security: Theory and Practice, in 3 vols, vol. 2,* Moscow, Aspect-Press Publ. (In Russian)
8. Wohlforth, W. C. (2008), Realism and foreign policy, in *Foreign policy: theories, actors, cases,* Oxford, UK, New York: Oxford University Press, pp. 35–53.
9. Fenenko, A. V. (2011), Military Technical Modernization and Rapprochement Cycles between the US and Russia, *Mezhdunarodnyye protsessy,* no. 2. Available at: http://general-history.ucoz.ru/Fenenko-26.pdf (accessed: 29.11.2021). (In Russian)
10. Yanikeeva, I. (2019), Responsible behavior of most states in the information space — a utopia?, *Mezhdunarodnaia zhizn*, May, 30. Available at: https://interaffairs.ru/news/show/22643 (accessed: 29.11.2021). (In Russian)
11. *Okinawa Charter for the Global Information Society, 2000, July, 22*. Available at: https://base.garant.ru/2560931/ (accessed: 29.11.2021). (In Russian)
12. *A/RES/57/239 Создание глобальной культуры кибербезопасности, ГА ООН, 31.01.2003*. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (accessed: 29.11.2021).

13. Boyko, S. M. (2021), Threats to international information security in a new technological reality, *Mezhdunarodnaia zhizn*. Available at: https://interaffairs.ru/jauthor/material/2453 (accessed: 29.11.2021). (In Russian)
14. Brief description of the state of crime in the Russian Federation for January — October 2020, *Ministry of Internal Affairs of Russia*. Available at: https://мвд.рф/reports/item/21933965/ (accessed: 29.11.2021). (In Russian)
15. *Digital 2020: Global Digital Overview*. Available at: https://datareportal.com/reports/digital-2020-global-digital-overview (accessed: 29.11.2021).
16. *Cybercrime and COVID19: Risks and Responses, UN Office for Drugs and Crime. Vienna, 14.04.2020*. Available at: https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED. pdf?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=nui,sc (accessed: 29.11.2021).
17. *Digitised Realpolitik: Sovereignty, Alliances and Non-Alignment in the 21st Century. Valdai Discussion Club Report* (2021). Available at: https://ru.valdaiclub.com/files/39047/ (accessed: 29.11.2021).
18. Yanikeeva, I. (2019), The war of the future — total and merciless, *Mezhdunarodnaia zhizn*, August, 29. Available at: https://interaffairs.ru/news/show/23620 (accessed 29.11.2021). (In Russian)
19. Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*, Oxford University Press.
20. The Pentagon declared the need to maintain a dialogue with Russia and China (2021), *Lenta.ru*, November, 03. Available at: https://lenta.ru/news/2021/11/03/uschinarus/ (accessed: 29.11.2021). (In Russian)
21. *Report of the Select Committee on intelligence United States Senate on Russian active measures campaigns and interference in the 2016 U.S election*. Available at: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures (accessed: 29.11.2021).
22. *The White House. Office of the Press Secretary. Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment*. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (accessed: 29.11.2021).
23. McFadden, C., Arkin, W. and Monahan, K. (2018), Russians penetrated U.S. voter systems, top U.S. official says, *NBCNews*. Available at: https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721 (accessed: 29.11.2021).
24. *Disinformation: A primer in Russian active measures and influence campaigns. Hearing before the Select Committee on Intelligence of the United States Senate. March 30, 2017. Printed for the use of the Select Committee on Intelligence*. Available at: https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm (accessed: 29.11.2021).
25. National Security Agency Federal Bureau of Investigation. Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware, (2020), *Cybersecurity Advisory*. Available at: https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF (accessed: 29.11.2021).
26. Barnes, J. (2020), Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say, *The New York Times*, July, 16. Available at: https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html (accessed 29.11.2021).
27. Vlamis, K. (2020), Here's a list of the US agencies and companies that were reportedly hacked in the suspected Russian cyberattack, *Businessinsider*. Available at: https://www.businessinsider.com/list-of-the-agencies-companies-hacked-in-solarwinds-russian-cyberattack-2020-12 (accessed 29.11.2021).
28. Obama's secret struggle to punish Russia for Putin's election assault (2017), *Washington Post*, June, 23. Available at: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?noredirect=on&utm_term=.98388a2652c5 (accessed: 29.11.2021).
29. Shitov, A. (2017), WikiLeaks: CIA May Launch False Flag Cyberattacks, *TASS*. Available at: https://tass.ru/mezhdunarodnaya-panorama/4077772 (accessed: 29.11.2021). (In Russian)
30. Thiessen, M. A. (2020), Trump confirms, in an interview, a U.S. cyberattack on Russia, *Washington Post*. Available at: https://www.washingtonpost.com/opinions/2020/07/10/trump-confirms-an-interview-us-cyberattack-russia/ (accessed: 29.11.2021).
31. The media reported on US cyberattacks against Russia and Iran, *Vedomosti*. Available at: https://www.vedomosti.ru/society/news/2020/11/04/845782-smi-soobschili-o-kiberatakah-ssha-protiv-rossii-i-irana (accessed: 29.11.2021). (In Russian)
32. The Foreign Ministry named the main sources of cyberattacks on Russia in 2020 (2021), *Mezhdunarodnaia zhizn*, May, 12. Available at: https://interaffairs.ru/news/show/30087 (accessed: 29.11.2021). (In Russian)

33. Krutskikh, A. V. (2021), *International information security: theory and practice*, in 3 vols., vol. 3. Moscow, Aspect-Press Publ. (In Russian)
34. *Statement by Vladimir Putin on a comprehensive program of measures to restore Russian-American cooperation in the field of international information security*. Available at: http://kremlin.ru/events/president/news/64086 (accessed: 21.12.2020). (In Russian)
35. *Statement by the Minister of Foreign Affairs of the Russian Federation Sergey Lavrov in connection with the statement by the President of the Russian Federation Vladimir Putin on international information security*, Moscow, September 25, 2020. Available at: https://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4350560 (accessed 29.11.2021). (In Russian)
36. Ford, C. (2020), *International Security in Cyberspace: New Models for Reducing Risk*. Available at: https://www.state.gov/wp-content/uploads/2020/10/T-paper-series-Cybersecurity-Format-508.pdf (accessed: 29.11.2021).
37. Kulik, S. A. (2013), "*E-Diplomacy", Start, Analytical report*. Available at: http://www.insor-russia.ru/files/EDiplomacy_0.pdf (accessed: 29.11.2021). (In Russian)
38. Sigmar, G. (2017), *«Destroyed» US-Russia Ties May Threaten Global Peace. German Foreign Minister*. Available at: https://sputniknews.com/world/201711051058829506-us-russia-destroyed-ties-threaten-peace/ (accessed: 29.11.2021).
39. Streltsov, A. A. (2018), The main problems of the application of international law in the ICT environment, *XII International Forum "Partnership of the state, business and civil society in ensuring international information security." Russia and global challenges in the field of information security, Mezhdunarodnaia zhizn*, pp. 106–109. Available at: https://interaffairs.ru/virtualread/garmish2018/publication.pdf (accessed: 29.11.2021). (In Russian)
40. *Russia says joint cyber resolution with US will strengthen international peace*, 03.11.2021. Available at: https://tass.ru/politika/12831715?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (accessed: 29.11.2021). (In Russian)
41. Finnemore, M. and Hollis, D. B. (2016), Constructing Norms for Global Cybersecurity, *American Journal of international Law*, vol. 110, no. 3, pp. 425–479.

Received: February 10, 2022
Accepted: March 22, 2022

Authors' information:

Elena S. Zinovieva — Dr. Sci. in Political Sciences, Professor; elena.zinovjeva@gmail.com
Inna O. Yanikeeva — Postgraduate Student; yanikeeva93@mail.ru