ВОПРОСЫ НАЦИОНАЛЬНЫХ И ФЕДЕРАТИВНЫХ ОТНОШЕНИЙ

Выпуск 9(78). 2021. Том 11

Научный журнал

Журнал «Вопросы национальных и федеративных отношений» включен в перечень рецензируемых научных изданий ВАК, в которых должны быть опубликованы основные научные результаты на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по политическим и историческим наукам

МОСКВА, 2021

ВОПРОСЫ НАЦИОНАЛЬНЫХ И ФЕДЕРАТИВНЫХ ОТНОШЕНИЙ

Научный журнал

УЧРЕЖДЕН

ООО «Издательство «Наука сегодня»

ЖУРНАЛ ВКЛЮЧЕН В ПЕРЕЧЕНЬ ВАК РФ

Журнал зарегистрирован Федеральной службой по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия

Регистрационный номер ПИ № ФС77-47487 от 25 ноября 2011 г.

Журнал издается ежемесячно

Журнал включен в базу РИНЦ (Российский индекс научного цитирования)

Включен в каталог Ulrich's Periodicals Directory

Пятилетний импакт-фактор журнала: 1,006

Адрес редакции: 115598, г. Москва, ул. Загорьевская, д. 10, корп. 4, цокольный этаж, помещение I, комната 7-1, офис 4

Тел.: (910) 463-53-42

www.etnopolitolog.ru

E-mail: etnopolitolog@yandex.ru

Мнение авторов может не совпадать с мнением редакции. При перепечатке ссылка на журнал обязательна.

Научные статьи, публикуемые в журнале подлежат обязательному рецензированию.

Ответственный редактор *Перкова Д.В.*

Компьютерная верстка *Анциферова А.С.*

Подписано в печать 27.09.2021.

Формат 60×84/8. Объем 24,3. Печать офсетная. Тираж – 1000 экз. (1-й завод – 500 экз.) Заказ № 000.

Отпечатано в типографии ООО «Белый ветер»

115054, г. Москва, ул. Щипок, 28

Тел.: (495) 651-84-56

ISSN 2226-8596 (print)
12 выпусков в год и
2 выпуска в год переводной (англ.) версии
Языки: русский, английский
http://etnopolitolog
Входит в перечень рецензируемых научных изданий ВАК РФ
Включен в каталог периодических изданий Ульрих (Ulrich's Periodicals Directory: http://www.ulrichsweb.com)
Материалы журнала размещаются на платформе РИНЦ Российской научной электронной библиотеки, Electronic Journals Library Cyberleninka
Подписной индекс издания в каталоге агентства Роспечать 70114

Цели и тематика

Журнал *ВОПРОСЫ НАЦИОНАЛЬНЫХ И ФЕДЕРАТИВНЫХ ОТНОШЕНИЙ* – периодическое международное рецензируемое научное издание в области политических исследований. Журнал является международным как по составу редакционного совета и редколлегии, так и по авторам и тематике публикаций.

Научный журнал издается с 2011 года в издательстве «Наука сегодня». С 2018 года издается переводная (англ.) версия журнала. С момента своего создания, журнал ориентировался на высокие научные и этические стандарта и сегодня является одним из ведущих политологических журналов России.

Цель журнала – способствовать научному обмену и сотрудничеству между российскими и зарубежными политологами.

Журнал предназначен для публикации результатов фундаментальных и прикладных научных исследований. Тематическая направленность журнала отражается в следующих постоянных рубриках: «Отечественная история, этнология и этнография», «История международных отношений и мировой политики», «История и философия политики», «Политические институты, процессы и технологии», «Политическая культура, этнополитика и идеологии», «Политические проблемы международных отношений и глобализации».

Формат публикаций: научные статьи, обзорные научные материалы, материалы круглых столов, научные рецензии, научные сообщения, посвященные исследовательским проблемам в сфере политики и политологии.

В своей деятельности редакционный совет и редколлегия журнала руководствуется принципами, определяемыми ВАК России для научных журналов, в том числе: наличие института рецензирования для экспертной оценки качества научных статей; информационная открытость издания; наличие и соблюдение правил и этических стандартов представления рукописей авторами.

Целевой аудиторией журнала являются российские и зарубежные специалисты-политологи, а также аспиранты и магистры, обучающиеся по направлениям политология, государственное и муниципальное управление и международные отношения.

Журнал строго придерживается международных стандартов публикационной этики, обозначенных в документе *COPE (Committee on Publication Ethics)* **http://publicationethics.org**

Полные сведения о журнале и его редакционной политике, требования о подготовке и публикации статей, архив (выпуски с 2011 года) и дополнительная информация размещена на сайте: **http://etnopolitolog.ru**

Электронный адрес: **etnopolitolog@yandex.ru**

ISSN 2226-8596 (print)
12 issues a year plus
2 issues a year of the translated (eng.) version
Languages: Russian and English
http://etnopolitolog
Included in the list of peer-reviewed scientific publications of the Higher Attestation Commission of the Russian Federation
Included in the Ulrich's Periodicals Directory
Materials of the journal are placed on the RSCI platform of the Russian scientific electronic library – Electronic Journals Library Cyberleninka
Subscription index of the journal in the Rospechat Agency catalogue is: 70114

Objectives and themes

Academic journal "*Issues of National and Federative Relations*" is an international peer-reviewed scientific periodical in the field of political studies. The journal has an international character because of the composition of its Editorial Board, its editors, its contributing authors and topics of its publications.

The scientific journal is published since 2011 at the "Publishing House "Science Today". Translated (eng.) version of the journal is published since 2018. Since its inception, the journal was guided by high scientific and ethical standards and today it is one of the leading political science journals in Russia.

The purpose of the journal is to promote scientific exchange and cooperation between Russian and foreign political scientists.

The journal is intended for the publication of the results of fundamental and applied scientific research. Thematic focus of the journal is reflected in the following permanent headings: "Domestic history, ethnology and ethnography", "History of international relations and world politics", "History and philosophy of politics", "Political institutions, processes and technologies", "Political culture, ethnopolitics and ideologies", "Political problems of international relations and globalization."

Format of publications: scientific articles, reviews, scientific materials, materials of round tables, scientific reviews, scientific reports devoted to research problems in the field of politics and political science.

The Editorial Board and the editors of the journal in their activities are guided by the principles defined by VAK of Russia for scientific journals, including: presence of the institute of peer review for the expert quality assessment of scientific articles; information openness of the publications; availability and compliance with the rules and ethical standards for the submission of manuscripts by the authors.

The target audience of the journal is Russian and foreign specialists-political scientists, as well as graduate students and masters in the fields of political science, state and municipal management and international relations.

The journal strictly adheres to the international publishing standards and publication ethics identified in the *COPE (Committee on Publication Ethics)* document. **http://publicationethics.org.**

Full details of the journal and its editorial policy, requirements to the preparation and publication of articles, archive (issues since 2011) and additional information are available on the website: **http://etnopolitolog.ru**

E-mail address: **etnopolitolog@yandex.ru**

СОДЕРЖАНИЕ

ТЕОРИЯ И ИСТОРИЯ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ВНЕШНЕЙ ПОЛИТИКИ

СТУДЕНЧЕСКАЯ НАУКА

DOI 10.35775/PSI.2021.78.9.024
УДК 94
В.И. БУЛВА
эксперт Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России, Россия, г. Москва

РОССИЯ И ЕС: «КИБЕРСОТРУДНИЧЕСТВО» ИЛИ «КИБЕРПРОТИВОБОРСТВО»?

В статье рассматриваются особенности российского и европейского подходов к проблемам международной информационной безопасности, а также глобальные инициативы России и ЕС в данной сфере. Новизна исследования заключается в попытке определить характер взаимоотношений России и Европейского Союза в киберсфере, на основе анализа таких параметров, как сопоставимость подходов к определению угроз, устранение которых могло бы стать предметом взаимодействия, совпадение базовых принципов в отношении урегулирования определенной проблемы кибербезопасности, наличие комплементарного характера у российских и европейских инициатив на международной арене.

Ключевые слова: *информационная безопасность РГОС, ГПЭ, правила ответственного поведения.*

Актуальность международной информационной безопасности как в России, так и в Европейском Союзе не вызывает сомнений. Достаточно вспомнить об открытии Департамента международной информационной безопасности МИД России, о российских контактах по данной проблематике на двустороннем и региональном уровнях, а также о российских инициативах выдвигаемые в рамках ООН. Одним из достижений российской дипломатии на данном направлении стало принятие 31 декабря 2020 г. в ГА ООН российского проекта резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [10].

Другим подтверждением роста внимания со стороны российского руководства к международной информационной безопасности является инициатива В.В. Путина, которую он представил на площадке ГА ООН в октябре 2020 г. [5], а также его выступление на Всемирном экономическом форуме в Давосе в январе 2021 г. [1]. Президент РФ неоднократно подчеркивал необходимость стимулирования цифрового развития при одновременном укреплении основ технологической безопасности.

Не менее значима тема информационной безопасности и в Европейском Союзе. Так, в феврале 2020 г. была принята Цифровая стратегия ЕС [17], а в декабре 2020 г. Европейская комиссия и Верховный представитель по внешним делам и политике безопасности предложили новую Киберстратегию Союза [18]. Более того, осенью 2020 г. 40 стран, в том числе все страны ЕС, выдвинули инициативу CyberPoA [19], которая отражает стремление государств создать альтернативу российскому и американскому подходу по вопросам укрепления киберстабильности.

Особенность политики Европейского Союза состоит в том, что помимо национального уровня поддержания информационной безопасности, развивается наднациональная институциональная система. В ее основе лежит деятельность трех институтов – Агентства по сетевой и информационной безопасности ЕС (ENISA), Сети Групп реагирования на инциденты в области компьютерной безопасности (CSIRTs Network) и Компьютерной группы реагирования на чрезвычайные ситуации (CERT-EU). Помимо этого, новая Киберстратегия предусматривает формирование общих структур энергетической и военной кибербезопасности в рамках постоянного структурированного сотрудничества (PESCO) и рабочей группы киберразведки в составе Разведывательного центра ЕС.

Готовы ли Россия и ЕС укреплять сотрудничество во имя достижения общей цели – поддержания международной информационной безопасности – или же существующие разногласия свидетельствуют об углублении российско-европейского киберпротивоборства?

Сотрудничество подразумевает соблюдение нескольких императивов, основные среди которых – *сопоставимость подходов к определению угроз, устранение которых могло бы стать предметом взаимодействия; совпадение базовых принципов в отношении урегулирования определенной проблемы; взаимодополнение инициатив на международной арене.*

Изучение стратегических документов Европейского Союза и России в области цифрового развития и информационной безопасности позволяет выявить и сравнить приоритеты ЕС и РФ на данных направлениях. Одной из ключевых особенностей европейского и российского подходов является акцент на дуалистической природе технологий, т.е. возможности как мирного, так и злонамеренного их применения. В этой связи, политика в отношении использования ИКТ базируется на двух группах документов: Стратегия развития информационного общества РФ [12] (Стратегия цифрового развития ЕС [17]) и Доктрина информационной безопасности в России [4] (Стратегия по кибербезопасности в ЕС [18]).

В цифровых стратегиях России и ЕС особое внимание уделяется необходимости укрепления цифрового потенциала в интересах граждан для того, чтобы не допустить «технологического порабощения» со стороны третьего государства. И хотя мы наблюдаем явное сходство позиций РФ и европей-

ских стран в этом вопросе, сомнительно, что курс на импортозамещение технологий может стать базой для укрепления российско-европейского сотрудничества.

Важно отметить, что российское руководство и представители ЕС осознают уязвимость информационной инфраструктуры, увеличивающуюся по мере углубления технологического прогресса в этих странах. Этот феномен получил название «парадокс цифровой мощи». Именно поэтому параллельно со стимулированием научно-технологического прогресса разрабатывается комплекс мер по обеспечению международной информационной безопасности.

Российский подход к противодействию информационным и киберугрозам отражен в Доктрине информационной безопасности от 05.12.2016 г. Одной из задач, выполнение которой позволит повысить уровень кибербезопасности страны, является защита критической информационной инфраструктуры. Как отметили в Совете безопасности РФ, за 2020 г. возросло количество компьютерных атак на инфраструктуру органов власти, финансовых учреждений и предприятий. Подобная тенденция препятствует укреплению киберстабильности государства [7].

Кроме этого, обострилась проблема использования ИКТ в террористических и криминальных целях. В подтверждение этому Совет безопасности ссылается на российские правоохранительные органы, которые зафиксировали в 3 раза больше киберпреступлений за январь-ноябрь 2020 г. по сравнению с 2018 г. [11]. Что касается случаев «сетевого экстремизма», то по сравнению с 2019 г. их количество увеличилось практически на 30% [11].

В дополнение к мерам по противодействию киберпреступности, принимаемым на национальном уровне, Россия проводит активную международную политику в этой сфере. Ее практическим воплощением стало принятие в декабре 2019 г. российского проекта резолюции по киберпреступности в рамках ГА ООН, который инициировал работу специального комитета по разработке юридически обязательного документа в этой области.

Среди других угроз в цифровой среде, на борьбу с которыми направлена политика РФ, следует выделить дестабилизацию внутриполитической ситуации с помощью ИКТ, информационно-психологическое воздействие и размывание духовно-нравственных идеалов, а также рост в СМИ материалов, в которых содержится предвзятая оценка государственной политики России. И хотя наличие данного типа угроз признается Европейским Союзом, они служат скорее поводом для взаимных обвинений, нежели потенциальным предметом сотрудничества.

В Европейском Союзе на первый план выходят такие вызовы и угрозы, как уязвимость критической инфраструктуры, слабая защищенность персональных данных, применение ИКТ в военно-политических целях.

На фоне роста числа кибератак на объекты критически важной информационной инфраструктуры во время пандемии COVID-19, Европейская

Комиссия совместно с Верховным представителем по внешним делам и политике безопасности Жозепом Боррелем предложила расширить действие Директивы NIS 2016 г. (1) на сферу государственного управления, пищевой сектор и фармацевтическое производство.

Поводом для включения подобного положения стал взлом сети Европейского агентства лекарственных препаратов накануне предложения новой Киберстратегии. В целом, по заявлению Жозепа Борреля, за 2019 г. количество киберинцедентов достигло 450, в частности, участились кибератаки на финансовый и энергетический секторы, а также на объекты здравоохранения.

Более того, выведение из строя объектов критически важной инфраструктуры впервые завершилось человеческой смертью. В немецком городе Дюссельдорф в результате кибератаки на госпиталь вышла из строя реанимация, из-за чего врачи не смогли оказать должную медицинскую помощь пациентке. В итоге, женщина скончалась по дороге в другую больницу [2].

По-прежнему в ЕС пристальное внимание уделяется вопросу безопасности данных Интернет-пользователей. Деятельность Союза на данном направлении регулируется Регламентом о защите персональных данных (GDPR) [16]. Данный Регламент направлен на построение региональной (европейской) системы по обеспечению безопасности личных данных. Несмотря на то, что GDPR частично применяется на территории РФ (2), российское руководство приоритет отдает разработке договоренностей на глобальном уровне.

Как и в России, в ЕС в качестве одной из киберугроз выделяется киберспретупность. Однако, в отличие от России, Европейский Союз в качестве нормативного ориентира использует Будапештскую конвенцию по борьбе с киберпреступлениями 2001 г. [6]. Для России подобный подход недопустим ввиду того, что в Конвенции не криминализируются киберпреступления, которые появились после 2001 г., а ведь по мере развития технологий мы наблюдаем экспоненциальный рост не только числа, но и типа компьютерных атак.

Более того, Будапештская конвенция не является универсальным документом. Россия считает необходимым заключение Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях под эгидой ООН, которая позволила бы разработать механизм глобальной защиты от подобного рода преступлений. Разработка подобной Конвенции ведется в специальном межправительственном комитете экспертов, созданном на основании Резолюции ГА ООН 2019 г. [9].

Для России наиболее неприемлемым положением новой Стратегии ЕС является сохранение механизма киберсанкций. Впервые киберсанкции ЕС были введены против России, Китая и Северной Кореи в июле 2020 г. Новшеством является то, что документ предусматривает возможность приме-

нения режима санкций в ответ на киберинциденты на основе голосования квалифицированным большинством. Отказ от консенсуса подчеркивает стремление ЕС облегчить процедуру введения в действие киберсанкций.

Таким образом, сравнительная характеристика подходов России и ЕС в отношении определения и классификации информационных и киберугроз позволяет констатировать невыполнение первого императива эффективного сотрудничества. Несмотря на то, что в Российской Федерации и в Европейском Союзе в целом выделяются одни и те же угрозы, отличается набор инструментов, предназначенных для противодействия им. Так, возможность введения киберсанкий ЕС свидетельствует о конфронтационном подходе Союза, в то время как в России предпочтение отдается мерам сотрудничества, направленным на укрепление международной нормативной и институциональной базы.

Еще большее сомнение вызывает следующий императив – совпадение базовых принципов в области обеспечения международной информационной безопасности. Камнем преткновения в данном случае становится принцип невмешательства во внутренние дела государств.

ЕС проводит политику, основанную на ценностях (value based policy), которая направлена на укрепление «нормативной силы» ЕС за счет продвижения демократических ценностей. Подчеркнем, что их трактовка дается самим Европейским Союзам, а не остается на усмотрение суверенных демократических государств. Такой подход демонстрирует предвзятое отношение европейских стран к любому политическому режиму, который не вписывается в идеалы «европейской модели».

Для Европейского Союза «информационное поле» служит площадкой для воздействия на массовое сознание граждан. Де-факто нарушается принцип суверенитета государства: происходит ограничение его полного контроля над своими гражданами, и, как следствие, над территорией.

Россия признает демократические ценности. Согласно Конституции, РФ – это демократическое государство. В то же время, в основе российского подхода лежит понимание невозможности единообразного толкования демократии без учета национальных особенностей. Из этого следует, что ни одно государство мира не уполномочено констатировать наличие угрозы мира и стабильности в результате нарушения демократических принципов другим государством.

Единственная инстанция, уполномоченная давать заключение о наличии угрозы мировой безопасности, а также правам и свободам человека – это Совет Безопасности ООН. Поэтому любая деятельность извне без санкции Совета Безопасности ООН, направленная на дискредитацию действующего режима, в том числе посредством распространения соответствующей информации, нарушает основополагающий принцип международного права – гарантию невмешательства во внутренние дела.

Итак, основной концептуальной преградой на пути выстраивания сотрудничества между Россией и ЕС служит различное понимание понятие «демократии» и «угрозы демократии». Помимо этого, укреплению российско-европейского диалога по кибербезопасности препятствует открытое пренебрежение принципу невмешательства во внутренние дела государств со стороны ряда государств ЕС.

Наконец, вопросы вызывает выполнение третьего императива – взаимодополняемость международных инициатив России и ЕС, ориентированных на укрепление информационной безопасности. Российская позиция заключается в том, что центральную роль в поддержании безопасности информационно-коммуникационной среды должна играть Организация Объединенных Наций. Запад, в том числе и ряд стран ЕС, пытаются отодвинуть на второй план ООН, делегируя ряд полномочий региональным организациям, либо же создавая псевдоуниверсальные площадки.

Подтверждением этому является предложенный осенью 2020 г. 40 странами, в том числе всеми странами Европейского Союза, Программа действий по продвижению ответственного поведения государств в киберпространстве (CyberPoA) [19]. По заявлению авторов программы, будет создан новая площадка для переговоров, которая будет учитывать опыт Группы правительственных экспертов (ГПЭ) и Рабочей группы открытого состава (РГОС). При этом, дискуссии будут проходить на базе специально сформированных тематических групп, что позволит отойти от увязки различных вопросов. Подобная мера должна облегчить процесс согласования и принятия решений и одновременно сохранить инклюзивный характер диалога.

Россия не поддерживает разделение мандата РГОС на отдельные аспекты, а саму РГОС на несколько групп, поскольку это противоречит принципу комплексного рассмотрения вопроса построения международной системы информационной безопасности. Неурегулированность по крайней мере одной из проблем, связанных с поддержанием международной информационной безопасности, в результате следования сепаратному подходу сохраняет риск эскалации конфликта в киберпространстве.

Помимо этого, Программа дублирует достижения прошедших лет, а именно – то, чего удалось добиться в ходе деятельности ГПЭ на текущий момент. Так, авторы данного документа заявляют, что содержательная база их плана действия будет основана на принятых ранее консенсусом докладов ГПЭ 2010, 2013 и 2015 гг., а также резолюций ГА ООН, которые сохраняют действие.

Более того, среди одного из положений CyberPoA фигурирует задача привлечения частного сектора к диалогу по кибербезопасности. Напомним, что созданная на основе российского проекта резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 5 декабря 2018 г. [8]. Рабочая группа открытого состава открыта не только для правительственных экспертов, но и для представите-

лей бизнеса, НПО и академического сообщества. При этом, особенностью РГОС является то, что работа группы позволяет пользоваться преимуществами мультистейкхолдерного подхода и одновременно сохранять за ООН центральную роль в принятии решений.

Выводы, сделанные на основании изучения инициативы CyberPoA, отнюдь не означают, что данная Программа лишена перспективных идей. К примеру, актуальной представляется предложение по разработке механизма имплементации договоренностей и системы мониторинга выполнения ранее выработанных рекомендаций в области международной информационной безопасности. Однако для реализации данного положения создавать новые форматы диалога нецелесообразно.

Таким образом, российско-европейское взаимодействие по вопросам международной информационной безопасности невозможно охарактеризовать как эффективное полномасштабное сотрудничество. На практике это отражается в противоречивом характере инициатив ЕС и России на международной арене, равно как и в различии инструментов по защите цифровой среды.

Мы являемся свидетелями углубления российско-европейского **киберпротивоборства**, которое можно охарактеризовать как соперничество субъектов с целью укрепления собственного влияния и получения преимущества над противоборствующей стороной, а также оказания на нее деструктивного воздействия.

Прямым доказательством данного тезиса служит комплекс инструментов кибердипломатии (The Cyber diplomacy toolbox), набирающий популярность в ЕС [13. С. 43]. Одним из таких инструментов являются киберсанкции, которые ЕС, согласно внутренним документам Союза, может вводить против другого государства (его граждан и/или юридических лиц) в случае обнаружения с их стороны злонамеренной активности в информационном пространстве, наносящей ущерб интересам европейских государств.

Проблема усугубляется тем, что фактически, следуя примеру США, некоторые европейские страны занимаются публичной аттрибуцией кибератак. Выдвигая беспочвенные обвинения в адрес России, государства ЕС, пытаются создать в лице России образ агрессора и легитимизировать введение ограничительных мер против российских физических и юридических лиц. Достаточно вспомнить официальный повод введения Европейским Союзом киберсанкций против граждан и структур РФ, Китая и КНДР в июле 2020 г. Россия была якобы «причастна к киберинцедентам, имевшим место в прошлом» [3], причем еще до существования в ЕС механизма по введению санкций за киберпреступления. Российским гражданам А.В. Минину, А.С. Моренецу, Е.М. Серебрякову и О.М. Сотникову вменялась в вину кибератака на Организацию по запрещению химического оружия (ОЗХО). Главный центр специальных технологий Главного управления Генерального штаба ВС РФ обвинялся в осуществлении кибератак, извест-

ные как «NotPetya» или «EternalPetya» в июне 2017 г. против европейских компаний, а также кибератак против украинских сил [14].

Вместо того, чтобы предоставить запрашиваемые Министерством иностранных дел России доказательства причастности российских граждан и структур к данным киберинцидентам, ЕС предпочел сохранить молчания и лишь усилить жесткую риторику в СМИ. Кроме того, был проигнорирован призыв российской дипломатии преступить к разработке действенных правил предотвращения конфликтов в киберпространстве.

Каковы же перспективы российско-европейского сотрудничества в области информационной и кибербезопасности? Это зависит от ряда факторов. Во-первых, важно, чтобы у России и ЕС было общее понимание возрастающего масштаба и киберугроз и, как следствие, необходимости повышения требований к потенциалу государств для их отражения. С учетом трансграничного характера данного типа угроз, становится очевидным несостоятельность эгоистичного, узконационального подхода к разрешению проблемы. Именно поэтому на смену политике взаимных обвинений должна прийти практика обмена информацией о наличии киберугроз и полезным опытом по их устранению.

Во-вторых, не менее значимым представляется разработка стандартов деятельности государств в цифровом пространстве, причем ввиду сложности данной тематики переговоры следует проводить поэтапно (от устранения противоречий к выработке правил и норм) и на различных уровнях (от двустороннего формата, к обсуждению по линии Россия-ЕС). В случае успешного согласования подобных стандартов между Российской Федерацией и Европейским Союзом значительно возрастут шансы юридического закрепления правил ответственного поведения под эгидой ООН. Несмотря на то, что достижение данного результата маловероятно в ближайшем будущем, необходимо начать действовать сейчас, а не дожидаться переноса конфликта из киберпространства в реальную среду.

В то же время, нельзя забывать о возможных препятствиях на пути укрепления российско-европейского сотрудничества. Ключевые из них – неблагоприятный общий политический фон отношений между Россией и ЕС и даже тенденция на ухудшение общего климата двусторонних отношений. Демонстративным в этом плане является итог визита Верховного представителя ЕС по внешним делам и политике безопасности Жозепа Борреля в Москву 5 февраля 2021 г. По возвращении в Брюссель, он заявил: «Моя встреча с Сергеем Лавровым показала, что Европа и Россия отдаляются друг от друга. Кажется, что Россия постепенно теряет связь с Европой» [15]. Более того, Ж. Боррель отметил, что он обсудит с министрами иностранных дел государств-членов ЕС дальнейшие шаги в отношении России, которые могут включать санкции, в том числе за нарушение прав человека [15].

Что касается российской дипломатии, ее подход кардинально отличается от европейской тактики на конфронтацию. Подобная позиция нашла

отражение в ответе С.В. Лаврова в ходе совместной пресс-конференции по итогам переговоров с Ж. Боррелем: «Силовое давление, ультиматумы, санкции, наказание всех, кто хочет развивать нормальные отношения, путем введения экстерриториальных рестрикций – методы и инструменты из колониального прошлого» [2].

Следует предусмотреть штрафные санкции за невыполнение принятых государством обязательств. В случае добросовестной реализации этих мер, появилась бы возможность устранить правовой беспредел, «анархию», которая царит в цифровом пространстве. При этом, Россия призывает сотрудничать в рамках уже действующих форматов, прежде всего в рамках РГОС, которая получила мандат еще на 5 лет на основании российского проекта Резолюции, принятого ГА ООН 31 декабря 2020 г [10].

ПРИМЕЧАНИЯ:

(1) Директивы NIS 2016 г. – Директива ЕС, регулирующая вопросы, связанные с защитой критически важной инфраструктуры ЕС. Директива 2016 г. распространяла действие на такие отрасли, как здравоохранение, банковское дело, питьевое водоснабжение и энергетическую инфраструктуру.

(2) GDPR применяется в России, если юридическое лицо имеет доступ к персональным данным лиц, которые являются гражданами стран, которые входят в Европейский Союз или же сама компания осуществляет свою деятельность на территории такого государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Выступление В.В. Путина // Сессия онлайн-форума «Давосская повестка дня 2021» // http://www.kremlin.ru/events/president/news/64938.

2. Выступление и ответы на вопросы СМИ Министра иностранных дел Российской Федерации С.В. Лаврова в ходе совместной пресс-конференции по итогам переговоров с Высоким представителем Европейского союза по иностранным делам и политике безопасности, заместителем Председателя Европейской комиссии Ж. Боррелем. Москва, 5 февраля 2021 года // https://www.mid.ru/web/guest/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/4553286.

3. Германия предложила ЕС ввести первые «киберсанкции» за атаку на Бундестаг // Forbes // https://www.forbes.ru/newsroom/obshchestvo/404921-germaniya-predlozhila-es-vvesti-pervye-kibersankcii-za-ataku-na.

4. Доктрина информационной безопасности РФ: утверждена Указом Президента Российской Федерации, 5 декабря 2016 г. // http://www.garant.ru/products/ipo/prime/doc.

5. Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности // http://kremlin.ru/events/president/news/64086.

6. Конвенция о компьютерных преступлениях: принята государствами-членами Совета Европы, Будапешт, 23 ноября 2001 г. // Совет Европы: серия европейских договоров. № 185 // https://rm.coe.int/1680081580.

7. Межведомственная комиссия Совета Безопасности России по информационной безопасности констатировала рост киберугроз // http://scrf.gov.ru/news/allnews/2908/.

8. Резолюция A/73/PV.45 от 5 декабря 2018 г. // https://undocs.org/ru/A/RES/73/27.

9. Резолюция ГА ООН A/RES/74/247 от 27 декабря 2019 г. // https://undocs.org/ru/A/RES/74/247.

10. Резолюция ГА ООН A/RES/75/240 от 31 декабря 2020 г. // https://undocs.org/en/A/RES/75/240.

11. Совбез сообщил о стремительном нарастании киберугроз в 2020 году // Moscow Daily News // https://www.mn.ru/articles/sovbez-soobshhil-o-stremitelnom-narastanii-kiberugroz-v-2020-godu.

12. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы: утверждена Указом Президента Российской Федерации № 203, 9 мая 2017 г. // http://www.garant.ru/products/ipo/prime/doc.

13. Challenges to effective EU cybersecurity policy // Briefing Paper. March 2019 // https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

14. Council implementing regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States // https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.246.01.0004.01.ENG&toc=OJ:L:2020:246:TOC.

15. My visit to Moscow and the future of EU-Russia relations // https://eeas.europa.eu/headquarters/headquarters-homepage/92722/my-visit-moscow-and-future-eu-russia-relations_en.

16. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) // Official Journal of the European Union. L 119/1 // https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

17. Shaping Europe's digital future // Luxembourg: Publications Office of the European Union, 2020 // https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

18. The EU's Cybersecurity Strategy for the Digital Decade // Joint Proposal of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. 16.12.2020 // https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.

19. The future of discussions on ICTs and cyberspace at the UN. 10.08.2020 // https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.

20. Tödlicher Hackerangriff auf die Uniklinik Düsseldorf? // https://www.rtl.de/cms/hacker-angriff-auf-uniklinik-duesseldorf-starb-eine-patientin-wegen-einer-erpressung-4615184.html?

V.I. BULVA
Expert of the Center for International Information Security, Science and Technology Policy, MGIMO, Moscow, Russia

RUSSIA AND THE EU: CYBER COOPERATION OR CYBER CONFRONTATION?

The article examines the features of the Russian and European approaches to the problems of international information security, as well as the global initiatives of Russia and the EU in this area. The novelty of the study lies in an attempt to determine the nature of relations between Russia and the European Union in the cybersphere based on the analysis of such parameters as the comparability of approaches to defining threats, the elimination of which could become the subject of interaction, the coincidence of basic principles with respect to resolving a certain cybersecurity problem, the presence of a complementary nature among Russian and European initiatives in the international arena.

Key words: *cyber strategy, OEWG, GGE, rules of responsible behavior.*