РИСКИ ИНТЕРНЕТ-КОММУНИКАЦИИ В КОНТЕКСТЕ ГЛОБАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ

Светлана Викторовна Кобзева
Российская академия народного хозяйства и государственной службы

Глобализация средств массовой коммуникации и формирование единого информационно-коммуникационного пространства создают новые рамки и формы межкультурных взаимодействий: глобальное сотрудничество расширяет возможности контроля над конфликтными ситуациями, резко увеличивает возможности международной солидарности в обеспечении глобальной и региональной безопасности. Однако неравномерный характер глобальной системы международных отношений, управляемой преимущественно США, провоцирует неизбежную напряженность, столкновение государств-лидеров и блоков государств, а также идеологий будущего глобального мироустройства. Глобальная конкуренция сверхдержав за позиции на мировой арене закономерно находит отражение и в киберпространстве. Цифровой мир изобилует противоречиями: существуют идеологические конфликты, конфликты, разворачивающиеся вокруг борьбы за власть между правящими и оппозиционными силами, конфликты из-за глобальных кибератак и киберпреступлений, актов иностранного вмешательства в национальные выборы, безопасности трансграничных потоков данных – именно эти конфликты приводят к блокировкам интернет-ресурсов и даже целых IT-гигантов. Современные исследователи отмечают необходимость развития сотрудничества государств – лидеров в области сдерживания угроз безопасности, которые ставятся на повестку дня технологиями (Шваб 2016; Най 2020; Danzig 2018). Отмечается потенциал игры с положительной суммой в международных отношениях (Nye 2020). Однако ряд ученых прогнозирует нарастание конкуренции ведущих держав мира за экономическое и технологическое лидерство (Хазин 2019), которая объективно находит отражение в киберпространстве.

Системный мониторинг глобальных и региональных рисков 2021 523–542

В этом контексте для России чрезвычайно важно придерживаться позиции укрепления устойчивости системы международных отношений на основе принципов международного права и координирующей роли ООН.

Введение

Глобализация цифровых технологий, средств коммуникации и связи находится в первом эшелоне разворачивающейся Четвертой промышленной революции. Согласно Окинавской хартии глобального информационного общества, «информационно-коммуникационные технологии (ИКТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества» (Okinawa Charter of Global Information Society 2000).

Р. Аткинсон, президент Фонда информационных технологий и инноваций, в статье «Генеральная стратегия США в области глобальной цифровой экономики» пишет, что «телеграф и телефон устранили потребность в Вестфальском мире, как это делает сейчас Интернет... Когда в 1980-е и 1990-е гг. глобальная экономика вступила в новую фазу, когда появились более мощные микропроцессоры, персональные сетевые компьютеры и простое в использовании программное обеспечение, многим политикам стало ясно, что теперь она является ключевым драйвером роста и конкурентоспособности и что эффективная экономическая политика означает правильное проведение ИТ-политики» (Atkinson 2021).

Глобализация средств массовой коммуникации и формирование единого информационно-коммуникационного пространства создают новые рамки и формы межкультурных взаимодействий. Глобальное сотрудничество расширяет возможности контроля над конфликтными ситуациями, резко увеличивает возможности международного сотрудничества в обеспечении глобальной и региональной безопасности. В докладе Института менеджмента Сколково «Навыки будущего...» отмечается, что «человечество постоянно договаривается об общих протоколах маршрутизации физических

грузов (почта, авиасообщение) или информации (Интернет, телефония)» (Лошкарева и др. 2020).

Теоретик «мягкой силы» в международных отношениях Дж. Най в своей новой статье «Недооцененная опасность. Пока мир следит за конкуренцией великих держав, угрозы поджидают в других местах» справедливо указывает, что «конкуренция великих держав остается одним из важнейших аспектов внешней политики, однако мы не должны позволять ей затмевать нарастающие транснациональные угрозы безопасности, которые ставятся на повестку дня технологиями. Сдвиги в соотношении сил между государствами хорошо известны в мировой политике, однако стимулируемое технологиями смещение баланса от государств к транснациональным игрокам и глобальным силам создает новые, незнакомые сложности. Технологические изменения вводят в мировую повестку целый ряд проблем, касающихся финансовой стабильности, изменения климата, терроризма, киберпреступности и пандемий, и одновременно склонны уменьшать возможности реагирования у правительств» (Най 2021).

Американский специалист по технологиям Ричард Данциг описывает технологические проблемы и пути их решения как глобальные не только в своем распространении, но и в последствиях: «…патогены, системы искусственного интеллекта, компьютерные вирусы или радиация, выброс которой может случайно произойти у других стран, способны стать в такой же мере нашей проблемой, как и их. Согласованные системы информирования, общий контроль, общие планы действий на случай чрезвычайных происшествий, нормы, договоры – ко всему этому следует стремиться как к средству смягчения наших многочисленных взаимных рисков» (Danzig 2018).

Стоит отметить, что прогноз о технологических угрозах и призыв к международному сообществу объединить свои усилия в борьбе с ними звучал еще задолго до пандемии COVID-19 в докладе Всемирного экономического форума «10 новых технологий 2016». В исследовании отмечается, что «технологии играют решающую роль в отношении к каждой из основных мировых проблем, представляя значительные экономические и социальные угрозы», «про-

гноз горизонта новых появляющихся технологий крайне важен для поступательного развития, которое может радикально преобразовать наш мир, своевременной экспертной оценки для подготовки к возможным разрушениям. Глобальное сообщество должно объединиться и договориться об общих принципах, если оно нацелено получить выгоду от технологий и застраховаться от технологических рисков» (WEF 2016).

Можно заключить, что пандемия COVID-19 актуализировала дискуссии в исследовательском сообществе по проблемам выработки согласованных норм, общих принципов контроля над технологическими угрозами и киберпреступлениями.

Вопросы глобальной кибербезопасности и риски интернет-коммуникаций: количественная динамика и экспертные оценки

В середине XX в., когда центр мировой экономической активности переместился из Европы в Северную Америку, США, начиная с периода Второй мировой войны, стали серьезно обходить европейские страны по уровню ВВП. Причины кроются не только в очевидном преимуществе в развитии, которые получили США по сравнению с охваченными мировыми войнами странами Европы, сражавшимися в антигитлеровской коалиции, и Советским Союзом; но также и в инновационном потенциале этой страны, в протяженности ее границ, экономической мощи (Atkinson 2021; Зинькина и др. 2017).

«Наиболее крупным экономическим изменением в структуре мировой экономики за последние десятилетия стало увеличение в ней доли азиатских стран», – пишет Э. Мэддисон в своем фундаментальном труде «Контуры мировой экономики». По прогнозам Мэддисона, на Азию (прежде всего, Китай и Индию) к 2030 г. будет приходиться 53 % мирового ВВП, в то время как на Западную Европу и «боковые ветви Запада» – только 33 % (Мэддисон 2015: 18; 513).

В докладе «Навыки будущего...» Московской школы управления Сколково приводятся данные: к 2030 г. «на развивающиеся экономики будет приходиться более ⅔ глобального роста и боль-

шая часть мировой торговли, флагманами мировой экономики станут страны Юго-Восточной Азии, прежде всего Китай и Индия. Ожидается, что вслед за экономической активностью в регионе будет нарастать активность и в области создания знаний и технологических инноваций. Китай уже занимает второе место по затратам на R&D среди всех стран мира, уступая только США» (Лошкарева и др. 2020).

В отчете Департамента по экономическим и социальным вопросам ООН «Исследование ООН: электронное правительство 2020. Цифровое правительство в десятилетии действий по достижению устойчивого развития» отмечается, что «Азия является самым густонаселенным – и самым разобщенным в цифровом плане – регионом в мире... Некоторые страны региона активно вовлечены в развитие и применение таких передовых технологий, как искусственный интеллект (ИИ), IoT и робототехника, и уже являются лидерами в техническом прогрессе, применении и инновациях; однако большое число стран в регионе находятся по другую сторону цифрового разрыва, и пока не появится хорошо развитая ИКТ-инфраструктура, достаточный человеческий капитал и достаточные ресурсы, чтобы мобилизовать крупномасштабные усилия по цифровизации... Приоритеты регулирования и политики в области цифровой трансформации неоднозначны в разных странах Азии... Из 47 отобранных азиатских стран 87 % приняли законы об электронных транзакциях и 79 % – законы о борьбе с киберпреступностью, но только 57 % имеют законы о конфиденциальности и менее половины приняли законы о защите прав потребителей» (ООН 2020: 66–67).

Борьба сверхдержав за лидирующие позиции на мировой арене нашла отражение в новой Стратегии национальной безопасности России, принятой в июле 2021 г., в которой справедливо указывается на санкционное давление на РФ со стороны недружественных государств, «стремление ослабить и изолировать нашу страну, использовать имеющиеся в России социально-экономические проблемы (экономические, демографические, социальные) для разрушения ее единства и политической стабильности. Позиция же России в реализации внешней политики неизменно опирается на ук-

репление устойчивости системы международных отношений на основе международного права, принципа всеобщей, равной и неделимой безопасности, углубления многостороннего взаимодействия без разделительных линий и блоковых подходов в целях совместного решения глобальных и региональных проблем при центральной координирующей роли Организации Объединенных Наций (ООН)» (Официальный… 2021).

В социальной сфере глобализация средств массовой коммуникации и формирование единого глобального информационно-коммуникационного пространства создают новые рамки и формы межкультурных взаимодействий, расширяют возможности контроля над конфликтными ситуациями, способствуют развитию человеческого капитала, образования, здравоохранения, социальной политики.

Интернет является стремительно развивающимся средством коммуникации и связи: по оценкам Всемирного экономического форума (ВЭФ), около 70 % человечества имеет доступ к высокоскоростному Интернету (широкополосному или 3G). В 2016 г. на 100 человек приходилось 159,95 мобильного телефона и из 100 человек 71,29 использовали мобильный доступ к сети Интернет. В России в 2016 г. пользователями Интернета являлись более 80 млн человек, что составляет около 60 % населения (WEF 2016).

Пандемия внесла свои коррективы в данные о распространении Интернета в мире: по данным ежегодного исследования глобальной аудитории Интернета We Are Social и Hootsuite, с января 2019 г. к Сети присоединилось 298 млн новых пользователей (рост составил 7 %). По состоянию на январь 2019 г. глобальное проникновение Интернета распространилось на 4,54 млрд человек, или более 67 % мирового населения. Так, аудитория Интернета в мире выросла на 316 млн чел (+7,3 % численности населения мира) и достигла 4,66 млрд человек (59,5 % численности населения мира) (We’re Social 2020).

В России, по данным РАЭК, в 2020 г. количество интернет-пользователей составило 97,4 млн человек, или 79,5 % населения (РАЭК 2020). К 2023 г., по прогнозам американской компании CISCO, пользователями Интернета в России станут около 78 %

граждан. В целом к глобальной Сети будут подключены более 66 % населения Земли и 28 млрд устройств, из которых в России – 895,5 млн, или более 6 устройств на человека (CISCO Annual Report 2020).

В то же время серьезным глобальным риском развития человечества является цифровое неравенство: по оценкам экспертов Всемирного экономического форума 2016 г., более 55 % (около 4 млрд) человек в мире не являлись активными пользователями Интернета вследствие неграмотности или бедности (включая 13 % человек, имеющих доход ниже международного прожиточного уровня) и не могли активно включиться в цифровую экономику (WEF 2016). В 2020 г., по данным компании We’re Social, лидирующие позиции по числу граждан, не включенных в интернет-коммуникации, занимали не только слаборазвитые страны Африки, Пакистан (72 %), Бангладеш (71 %), но и члены «большой двадцатки» Индия (55 %), Китай (34 %) и Бразилия (53 %) (We’re Social 2020).

Следует отметить, что цифровой разрыв (digital devide) является серьезным риском развития человечества. Интернет-коммуникации в современном цифровом мире – важное условие развития информационного общества и его отдельных индивидуумов: они позволяют улучшить качество человеческого потенциала посредством увеличения занятости, включения в активную жизнь общества социально изолированных групп населения, преодоления депривированности, бедности и различных форм дискриминации, способствует устранению территориальных, административных, цивилизационных и культурных барьеров.

Цифровой мир изобилует противоречиями: существуют идеологические конфликты, конфликты, разворачивающиеся вокруг борьбы за власть между правящими и оппозиционными силами, конфликты из-за глобальных кибератак и киберпреступлений, актов иностранного вмешательства в национальные выборы, безопасности трансграничных потоков данных – именно эти конфликты приводят к блокировкам интернет-ресурсов и даже IT-гигантов.

Р. Аткинсон отмечает, что напряженность между группами стран на международной арене разыгрывается по трем основным

группам вопросов: «1) вопросы преступной или иной вредоносной деятельности, такой как интернет-пиратство и кибератаки; 2) социальное и экономическое регулирование, включая искусственный интеллект и другие новые технологии, приватность в Интернете, Интернет и телекоммуникационные стандарты; 3) вопросы, связанные с Национальной технологической конкурентоспособностью и национальной безопасностью, включая трансграничные потоки данных, налогообложение, информационно-технологическую и цифровую конкурентоспособность, шифрование и доступ правоохранительных органов к данным, а также экспортный контроль» (Atkinson 2021).

Глобальная кибербезопасность и безопасность правительственных данных – значимый вопрос в агенде мировой дипломатии в современном дискурсе о глобальном контроле спецслужб США над Интернетом и обвинениями в хакерских кибератаках и вмешательстве во внутренние дела суверенных государств, в частности обвинениями США России во вмешательстве в выборы. В повестке ООН построение конфиденциальности и безопасность использования информационно-коммуникативных технологий в целях устойчивого развития должно стать приоритетом национальных государств в контексте возрастающих угроз киберпреступлений (UN 2016).

Израильский историк, футуролог, профессор Еврейского университета в Иерусалиме Юваль Ной Харари, выступая на Всемирном экономическом форуме в 2020 г., очертил три вызова, угрожающие человечеству как виду: ядерная война, экологический кризис, разрушительная сила технологий. В своих прогнозах писатель-футуролог сконцентрировался на рисках, которые несут в себе технологии, выделив среди потенциальных проблем опасность цифровой диктатуры, неравенство между странами, растущую власть алгоритмов и риск потери человечности мировым сообществом (Харари 2020).

Согласно российскому политику А. В. Лосеву, члену Совета по внешней и оборонной политике, «цифровизация создала невероятные уязвимости для любого государства. Кибератака может обойтись государству до 1 трлн долларов, как хороший экономический

кризис. Будущее – за кибератаками на критическую инфраструктуру. Война будущего – это война 3К» (Международное обозрение 2020):

1. Когнитивная война – война за сознание, которая будет вестись в информационном пространстве.

В новой стратегии информационной безопасности России, принятой в июле 2021 г., указывается актуальность проблемы морального лидерства и борьба конкурирующих идеологий будущего мироустройства. «На фоне кризиса западной либеральной модели рядом государств предпринимаются попытки целенаправленного размывания традиционных ценностей, искажения мировой истории, пересмотра взглядов на роль и место России в ней, реабилитации фашизма, разжигания межнациональных и межконфессиональных конфликтов. Проводятся информационные кампании, направленные на формирование враждебного образа России» (Официальный… 2021).

2. Кибернетическая война – война за контроль над критической инфраструктурой и экономикой.

По данным компании Positive Technologies, количество киберинцидентов стремительно растет: в IV квартале 2020 г. выявлено на 3,1 % больше атак, чем в IV квартале 2019 г. По сравнению с аналогичным периодом 2019 г. прирост составил 41,2 %. В течение 2020 г. высокую активность проявляли группировки, атаки которых были направлены преимущественно на государственные учреждения, промышленные предприятия, финансовую отрасль и медицинские организации. Доля атак на госучреждения среди всех атак на организации резко выросла с 12 %, зафиксированных в I квартале 2021 г., до 20 % во II квартале 2021 г. (Positive Technologies 2020; 2021).

Клаус Шваб, руководитель Всемирного экономического форума, в книге «Четвертая промышленная революция» пишет, что «с 2008 г. произошло множество кибератак, направленных как на конкретные страны, так и на конкретные предприятия, но обсуждение вопроса о новой эре военных действий все еще находится в зачаточном состоянии, и все шире пропасть между теми, кто разбирается в непростых технических вопросах кибервойны, и теми, кто

работает над созданием правил для киберпространства. Остается открытым вопрос о том, будет ли создан комплекс общих норм в отношении кибервойны, наподобие тех договоренностей, которые разработаны в отношении ядерных, биологических и химических вооружений. У нас отсутствует даже классификация, позволяющая нам прийти к согласию в отношении того, что считать нападением, а что – адекватным на него реагированием, какими способами эти действия могут производиться и кем» (Шваб 2016: 69).

В аналитической статье для журнала «Международная жизнь» Андрей Крутских, спецпредставитель президента РФ по вопросам международного сотрудничества в сфере информационной безопасности, прогнозирует, что за «биопандемией» последует «киберпандемия». По мнению Крутских, некоторые страны заявляют о праве наносить превентивные удары по критической инфраструктуре потенциальных противников, что, на взгляд эксперта, может привести к втягиванию в «киберконфронтацию или даже войну», от которой будет сложно удержать человечество (Педанов 2020).

3. Конвенциональная война – давление, чтобы подчинить то, что нельзя подчинить с помощью кибератак. Российское государство и гражданское общество активно противостоят глобальной монополии транснациональных корпораций, внедряя российское ПО и разработки российских ИТ-компаний. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) при экспертной поддержке некоммерческой организации «Лига безопасного Интернета» инициирует ставшие уже многочисленными судебные дела по вопросам локализации персональных данных пользователей, борьбы с распространением в сети незаконного интернет-контента (Форбс 2021). Широкую известность получил иск телеканала «Царьград» против интернет-гиганта Google по вопросу блокировки Youtube-канала российского СМИ (Коммерсант 2021).

Таким образом, неравномерный характер глобальной системы международных отношений, управляемой преимущественно США, провоцирует неизбежную напряженность, столкновение государств-лидеров и блоков стран, а также идеологий будущего глобального мироустройства. Глобальная конкуренция сверхдержав

за позиции на мировой арене закономерно находит отражение и в киберпространстве, поскольку Интернет является ценным ресурсом, влияющим на качество человеческого потенциала и социального развития.

Вопросы кибербезопасности в законодательстве и политике США и России

Согласно американскому политику и публицисту Р. Аткинсону, Соединенные Штаты Америки демонстрируют смену курса в отношении управления Интернетом: администрация Барака Обамы в глобальной цифровой политике была привержена демократической стратегии «открытой Сети». С позиции политика разоблачения Эдварда Сноудена в 2014 г., давшие ясный сигнал всему миру о том, что американские спецслужбы используют цифровые технологии для слежки за гражданами, в том числе за первыми лицами государств, привели к подрыву доверия к правительству США в мире и спровоцировали ответную волну реакции администрации Дональда Трампа, которая в условиях растущей цифровой конкуренции нашла выражение в принципах реальной политики (real politic): была исполнена решимости поставить интересы США на первое место в сочетании с наращиванием присутствия Соединенных Штатов в цифровом мире и отстаиванием их интересов на международной арене (Atkinson 2021).

Отражением политики администрации Д. Трампа стала Концепция кибербезопасности США, принятая в 2018 г. Политика Концепции опирается на четыре столпа: 1) защита американских граждан, страны и американского образа жизни; 2) содействие процветанию Америки; 3) поддержание мира силой; 4) распространение американского влияния (National… 2018).

Первостепенное внимание в новой киберстратегии уделяется формированию образа внешней угрозы свободе и демократии, значительный акцент в стратегии сделан на действия, которые должны способствовать расширению американского влияния в мире. Одним из таких направлений является развитие возможностей стран-партнеров по противодействию киберпреступности (National… 2018).

В государственной идеологии РФ информационно-коммуникативные технологии рассматриваются в контексте защиты суверенитета и обеспечения национальных интересов страны. В Стратегии национальной безопасности Российской Федерации до 2020 года информационная угроза представляется в качестве важнейшей угрозы суверенитету страны, Интернет рассматривался как канал распространения экстремизма и терроризма, навязывания чужой идеологии и внешнеполитической пропаганды, средство ведения информационной войны (Бухарин 2016; Лопатин 2017).

В принятой 3 июля 2021 г. указом Президента РФ новой Стратегии национальной безопасности РФ, в главе «Россия в современном мире: тенденции и возможности» Стратегии указывается, что «Современный мир переживает период трансформации. Увеличение количества центров мирового экономического и политического развития, укрепление позиций новых глобальных и региональных стран-лидеров приводят к изменению структуры мирового порядка, формированию новых архитектурных правил и принципов мироустройства. Стремление стран Запада сохранить свою гегемонию, кризис современных моделей и инструментов экономического развития, усиление диспропорций в развитии государств» (Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»).

Во внешней политике в области глобальной кибербезопасности Россия в 2017 г. выдвинула проект конвенции Организации Объединенных Наций (ООН) о сотрудничестве в сфере противодействия информационной преступности, который лег в основу предложенной Россией резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях» и был принят 18 ноября 2019 г. Предложенная Россией резолюция фактически закрепляет цифровой суверенитет государств над своим информационным пространством и открывает новую страницу в истории глобального противодействия киберкриминалу. В практическом плане под эгидой Генассамблеи ООН создается переговорная площадка для разработки универсальной конвенции по борьбе с киберпреступностью. Таким международным органом станет Спецкомитет, в который войдут эксперты из всех стран ми-

ра. В свое время аналогичный путь прошли Конвенция ООН против коррупции и Конвенция ООН против транснациональной организованной преступности (МИД 2019).

С целью защиты национальной критической инфраструктуры страны Россия 26 июля 2017 г. приняла закон «О безопасности критической информационной инфраструктуры Российской Федерации» (№ 187-ФЗ), согласно которому в стране создается «государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», которая «представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (Консультант Плюс 2017).

Президент РФ Владимир Путин подписал закон 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”», в соответствии с которым в России будет создана национальная система маршрутизации интернет-трафика. Законом определяются правила маршрутизации трафика и организуется контроль их соблюдения, а также регулируются вопросы создания инфраструктуры, которая позволит обеспечить работоспособность российских интернет-ресурсов в случае невозможности подключения российских операторов связи к зарубежным корневым серверам. Кроме того, законом создается возможность для минимизации передачи за рубеж данных, которыми обмениваются между собой российские пользователи. Наконец, законом вводится необходимость проведения регулярных учений органов власти, операторов связи и владельцев технологических сетей по выявлению угроз и отработке мер по восстановлению работоспособности российского сегмента Сети (Федеральный закон «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации” от 01.05.2019 № 90-ФЗ).

Последние учения по устойчивости Рунета в России были проведены в июне-июле 2021 г. Была протестирована возможность ра-

боты в условиях физического отключения России от глобальной Сети. По информации СМИ, учения прошли успешно (Интерфакс 2021). О готовности России законодательно и технически к отключению от глобального Интернета в феврале 2021 г. заявил в интервью зампред Совета безопасности РФ Дмитрий Медведев. По его словам, «ключевые права на управление» Интернетом, безусловно, находятся в США, но на Сеть «завязано управление всем государством, получение огромного количества социальных функций». Он добавил, что, «как и в случае системы SWIFT, для которой в России ЦБ разработал альтернативную систему передачи финансовых сообщений, Россия не могла оставить без контроля свой сегмент Интернета и приняла закон для того, чтобы этот сегмент мог управляться автономно» (Finanz.ru 2021).

Пандемия COVID-19 фактически поставила мир на паузу, что негативно сказалось не только на экономическом и политическом развитии мировой системы и отдельных кластеров домохозяйств, обусловило всплеск популизма и политической нестабильности в мире. Произошли существенные изменения, связанные с переходом на режим удаленной работы, который коснулся как первых лиц государств, так и рядовых граждан. Правительства стали активно вводить протекционистские меры, что вызвало широкий резонанс в среде правозащитников. Human Rights Watch, Amnesty International, Access Now, Privacy International и еще 103 организации опубликовали совместное заявление, в котором призвали правительства государств проявить лидерство в борьбе с пандемией таким образом, чтобы обеспечить неукоснительное соблюдение прав и свобод при использовании цифровых технологий для отслеживания и мониторинга населения (Human Rights Watch 2020).

В апреле 2020 г. в разгар пандемии COVID-19 МИД РФ призвало взять Интернет под международный контроль для обеспечения более эффективной борьбы с такими глобальными проблемами, как эпидемии. Директор Департамента международной информационной безопасности МИД РФ Андрей Крутских заявил: «Стоит задача сделать Интернет более эффективным и менее уязвимым. Он должен реально принадлежать международному сообществу, должен реально быть интернационализирован и, соответственно,

находиться под объективным международным контролем, чтобы не повторять ошибки прошлого и чтобы максимально эффективно организовывать в будущем работу по борьбе с глобальными угрозами» (Крутских 2020).

В интервью журналу «Международная жизнь» Крутских отметил: «Предвижу, что будущее Интернета должно рассматриваться всем мировым сообществом с учетом всех игроков (это и гражданское общество, и бизнес, и научное сообщество). Работу по реальной интернационализации и неуязвимости Интернета нужно активизировать, прежде всего, в рамках ООН, и для этого созданы необходимые механизмы. Собственно, в рамках группы открытого состава эти аспекты будущего Интернета уже затрагиваются, и думаю, что в дальнейшем они будут интенсифицированы» (Педанов 2020).

Таким образом, стоит отметить, что Интернет как сеть, объединяющая объекты критической инфраструктуры, представляет собой поле конкурентной борьбы между США, стремящимися к укреплению своих идеологических позиций и влияния в мире посредством киберпространства, и Россией, которая заинтересована в сдерживании идеологического и политического давления Америки, а также в том, чтобы глобальная сеть была интернационализирована и находилась под международным контролем.

Заключение

Глобализация средств массовой коммуникации и формирование единого глобального информационно-коммуникационного пространства создают новые рамки и формы межкультурных взаимодействий, расширяют возможности контроля над конфликтными ситуациями, способствуют развитию человеческого капитала, образования, здравоохранения, социальной политики; резко увеличивают возможности международного сотрудничества в обеспечении глобальной и региональной безопасности.

Неравномерный характер глобальной системы международных отношений, управляемой преимущественно США, и борьба государств-лидеров за позиции на мировой арене провоцирует неизбежную напряженность, столкновение государств-лидеров и бло-

ков государств, а также идеологий будущего глобального мироустройства. Нобелевский лауреат по экономике Дж. Стиглиц характеризует современную мировую систему как «глобальное правление без глобального правительства», справедливо указывая на отсутствие в ней системы сдержек и противовесов, изоляцию институтов и единоличное принятие решений без учета мнения развивающихся стран (Stiglitz 2002).

В отношении управления Интернетом американский исследователь Дж. Най отмечает, что «не существует единого режима управления киберпространством, есть набор двойных норм и институтов, которые ранжируются между иерархически интегрированными институтами и фрагментированными практиками» (Nye 2014).

В своих последних работах Дж. Най пишет о будущем глобальном мироустройстве с той точки зрения, что «в этом новом мире сети и связанность становятся важными источниками силы и безопасности». В книге «Важна ли мораль?» Дж. Най рассуждает о международной политике как игре с положительной суммой: «в этом новом мире некоторые аспекты силы представляют собой игру с положительной суммой. Недостаточно думать исключительно с позиций американской силы и власти над остальными. Мы обязаны думать и о силе, необходимой для достижения совместных целей, а это предполагает использование силы вместе с другими» (*Idem* 2020).

В отчете Всемирного экономического форума 2016 года указывается, что, «переживая четвертую промышленную революцию, жизненно важно, чтобы мы развивали отдельные нормы и протоколы, которые будут гарантировать, что технологии будут служить человечеству и способствовать процветанию и стабильному будущему» (WEF 2016).

Однако в свете последних событий новейшей мировой истории и политики потенциала «мягкой силы» данный сценарий выглядит чрезмерно оптимистично. Известный российский экономист и политолог Михаил Хазин в своей книге «Воспоминания о будущем» пишет о перспективах мирового развития следующее: «Если новой модели экономического развития, альтернативной НТП (научно-

техническому прогрессу. – *С. К.*), не будет, то нас ждет повторение истории XX века, то есть конкурентная борьба новых технологических зон друг с другом за рынки сбыта, то есть за возможность дальнейшего развития» (Хазин 2019: 440).

Таким образом, можно констатировать, что современные исследования архитектуры международных отношений характеризуются дуализмом концепций конфликта и сотрудничества между странами – лидерами мирового развития. Конфликтный потенциал современной глобальной медиасистемы детально описан в данной работе концептуально с позиции концепция войны 3К А. В. Лосева.

Особой геостратегической реальностью является перспектива интеграции акторов мировой политики и дипломатии с целью выработки консенсуса по управлению технологическим развитием, интернационализация глобальной политики по управлению Интернетом. Однако в отношении потенциала выстраивания в системе международных отношений сотрудничества и кооперации между ведущими акторами, выработки ими общих норм и протоколов с целью контроля над технологическим рисками и угрозами в экспертном сообществе преобладают оценки рекомендательного характера, а в политическом пространстве наличествует явный вакуум.

Библиография

Бухарин В. В. 2016. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности. *Вестник МГИМО-Университета* 6(51): 76–91. URL: https://doi.org/10.24833/2071-8160-2016-6-51-76-91.

Зинькина Ю. В., Гринин Л. Е., Ильин И. В., Андреев А. И., Алешковский И. А., Шульгин С. Г., Коротаев А. В. 2017. *Историческая глобалистика*. Т. 2. М.: Моск. ред. изд-ва «Учитель», Изд-во Моск. ун-та.

Интерфакс 2021. Учения по устойчивости Рунета прошли успешно. *Интерфакс* 23 декабря. URL: https://www.interfax.ru/russia/689098.

Коммерсант. 2021. Нашел Google на «Царьград» Почему затянулся спор между американской корпорацией и российским телеканалом. *Коммерсант* 16 августа. URL: https://www.kommersant.ru/doc/4946507.

Консультант Плюс. 2017. Федеральный закон 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры

Российской Федерации» от 26.07.2017 № 187-ФЗ. *Консультант Плюс.* URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

Лопатин В. Н. 2017. Проблемы информационной безопасности и риски интеллектуальной собственности в цифровой экономике. *Информационное право* 2(52).

Лошкарева Е., Лукша П, Ниненко И., Судаков Д. 2020. Доклад «*Навыки будущего: что нужно знать и уметь в современном мире*». URL: https://futuref.org/futureskills_ru.

Международное обозрение. 2020. Эфир от 25 декабря. *Россия 24*. URL: https://www.youtube.com/watch?v=WIPMmA51OQQ.

МИД РФ. 2019. *Комментарий Департамента информации и печати МИД России об итогах голосования в Третьем комитете ГА ООН по российскому проекту резолюции по противодействию киберпреступности*. URL: https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3909516.

Мэддисон Э. 2015. *Контуры мировой экономики. 1–2030 гг. Очерки по макроэкономической истории*. М.: Изд-во Ин-та Гайдара.

Най Дж. 2020. Недооцененная опасность. Пока мир следит за конкуренцией великих держав, угрозы поджидают в других местах. *IPG – Международная политика и обществе* 11 августа. URL: https://www.ipg-journal.io/regiony/mir/nedoocenennaja-opasnost-1120/.

Официальный интернет-портал правовой информации. 2021. Указ Президента РФ от 02.07.2021. № 400 «О Стратегии национальной безопасности Российской Федерации». *Официальный интернет-портал правовой информации*. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001.

ООН. 2020. *Цифровое правительство в десятилетии действий по достижению устойчивого развития*. Исследование ООН: электронное правительство 2020. URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020.

Педанов Е. 2020. А. Крутских: за «биопандемией» последует «киберпандемия». *Международная жизнь* 8 апреля. URL: https://interaffairs.ru/news/show/25925.

РАЭК. 2020. *Экономика Рунета*. URL: https://raec.ru/upload/files/runet-economy-20-21.pdf.

Форбс. 2021. Разведка боем: как Роскомнадзор меняет модель управления Рунетом. *Форбс* 11 марта. URL: https://www.forbes.ru/tehnologii/423155-razvedka-boem-kak-roskomnadzor-menyaet-model-upravleniya-runetom.

Хазин М. 2019. *Воспоминания о будущем*. М.; СПб.: Сфера.

Харари Ю. Н. 2018. Большинство людей вообще не осознают, что происходит и что на кону. *Капитал* 27 января. URL: https://www.capital.ua/ru/publication/106820-bolshinstvo-lyudey-voobsche-ne-osoznayut-chto-proiskhodit-i-chto-na-konu#ixzz6wBVI4rsv.

Шваб К. 2016. *Четвертая промышленная революция*. М.: Эксмо.

Atkinson R. D. 2021. A U.S. Grand Strategy for the Global Digital Economy. *Policy Report, Information Technology and Innovation Foundation* (ITIF). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773652.

CISCO Annual Report. 2020. URL: https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html.

Danzig R. 2018. Technology Roulette. Managing Loss of Control as Many Militaries Pursue Technological Superiority. URL: https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-Technology-Roulette-DoSproof2v2.pdf?mtime=20180628072101&focal=none.

Finanz.ru. 2021. Медведев заявил о готовности России к отключению от мирового интернета. *Finanz.ru* 1 февраля. URL: https://www.finanz.ru/novosti/aktsii/medvedev-zayavil-o-gotovnosti-rossii-k-otklyucheniyu-ot-mirovogo-interneta-1030026498.

Human Rights Watch. 2020. *Governments Should Respect Rights in COVID-19 Surveillance*. Groups Urge Leadership in Digital Measures on Pandemic. URL: https://www.hrw.org/ru/news/2020/04/09/340281.

National Cyberstrategy of the United States of America. 2018. September. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Nye J. S., Jr. 2014. The Regime Complex for Managing Global Cyber Activities. URL: http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/The%20Regime%20Complex%20for%20Managing%20Global%20Cyber%20Activities.pdf.

Nye J. S. 2020. Do Moral Matter? Presidents and Foreign Policy from FDR to Trump. Oxford: Oxford University Press.

Okinawa Charter of Global Information Society. 2000. URL: http://www.iis.ru/library/okinawa/charter.ru.html.

Positive Technologies 2020. Актуальные киберугрозы: IV квартал 2020 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/.

Positive Technologies 2021. Актуальные киберугрозы: II квартал 2021 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/.

Stiglitz J. E. 2002. *Globalization and its Discontents.* New York: W.W. Norton.

We're Social. 2020. *Digital 2020*. URL: https://wearesocial.com/digital-2020.

WEF. 2016. Top 10 Emerging Technologies of 2016. *World Economic Forum*. URL: https://www.weforum.org/agenda/2016/06/top-10-emerging-technologies-2016/.

UN. 2016. United Nations E-governance Survey. *United Nations.* URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016.