И.Т.Стадник, Н.А.Цветкова

Место и роль стран Латинской Америки в системе международной и региональной кибербезопасности

В статье раскрываются особенности политики латиноамериканских государств в области кибербезопасности. Авторы оценивают влияние стран Латинской Америки и Карибского бассейна, в особенности Аргентины, Мексики и Колумбии, в двух важнейших органах ООН — Группе правительственных экспертов и Рабочей группе открытого состава. Раскрывается роль Организации американских государств в процессе создания единой региональной системы кибербезопасности. Авторы приходят к выводу, что подходы стран ЛАКБ в разной степени созвучны весьма разнообразным подходам ведущих государств мира. Таким образом, нельзя говорить о единой позиции государств региона относительно международной кибербезопасности. В заключительном разделе статьи представлены соображения о том, как политика латиноамериканских государств может способствовать продвижению международной стратегии России в области киберпространства и информационной безопасности.

Ключевые слова: кибербезопасность, Латинская Америка, ООН, Организация американских государств, ГПЭ, РГОС.

DOI: 10.31857/S0044748X0014088-5

Статья поступила в редакцию 20.01.2021.

Составными элементами процесса цифровизации сегодня являются такие аспекты, как кибербезопасность, цифровая дипломатия и дипломатия данных, глобальное управление Интернетом и цифровые избирательные технологии. Они определяют повестку дня на различных переговорах, порой осложняют взаимодействие между участниками и обуславливают повышение или понижение роли того или иного государства в системе мировой политики. В последние несколько лет развернулась широкая междуна-

Илона Тарасовна Стадник — ассистент кафедры американских исследований СПбГУ (РФ, 191060 Санкт-Петербург, ул. Смольного 1/3, i.stadnik@spbu.ru); **Наталья Александровна Цветкова — доктор исторических наук, доктор философии в социальных науках, профессор, заведующий кафедрой американских исследований СПбГУ** (РФ, 191060 Санкт-Петербург, ул. Смольного 1/3, n.tsvetkova@spbu.ru).

Статья подготовлена при финансовой поддержке РФФИ, проект №19-014-00042.

родная дискуссия о кибербезопасности, которая отражает стремление ведущих стан мира реагировать на тревожные тенденции, связанные с различными угрозами использования информационно-коммуникационных технологий (ИКТ), включая Интернет. Все чаще мы слышим призывы укреплять стабильность и безопасность киберпространства, выработать соглашения по использованию компьютерных технологий, способных подорвать информационную систему любой страны [1]. Международное сообщество сосредоточило свое внимание на таких темах, как нормы ответственного поведения государств в киберпространстве, меры укрепления доверия и наращивание потенциала.

Страны Латинской Америки и Карибского бассейна (ЛАКБ) стали заметной частью вышеупомянутой дискуссии, лидерами которой являются США, Россия, Китай, Франция, Нидерланды и Эстония. В ЛАКБ работы по обеспечению стабильности и безопасности в киберпространстве находятся, преимущественно, на ранней стадии. Основными задачами, стоящими перед регионом в области информационной безопасности, являются наращивание киберпотенциала во всех странах, оптимизация сотрудничества в борьбе с киберпреступностью и обмен информацией о передовых практиках, угрозах и уязвимости цифровых продуктов и оборудования.

Обеспечение информационной безопасности признается в регионе крайне важной задачей, поскольку посягательства на нее способны затормозить инновации и развитие интернет-экономики, подвергая риску стабильное экономическое и общественное развитие. В то время как власти почти всех стран региона понимают необходимость наличия всеобъемлющей стратегии по кибербезопасности, многие, за несколькими исключениями (например, Мексика, Бразилия, Аргентина, Чили, Коста-Рика), не продвинулись дальше стадии обсуждений и проектов [2; 3; 4; 5; 6]. Только в самых крупных и богатых государствах региона существуют специализированные организации, занимающиеся вопросами кибербезопасности, но даже там, где такие структуры есть, общая готовность к действию ограничена известным и сложно преодолимым фактором отсутствия координации между флагманами экономики и государственными ведомствами. Кроме того, в отличие от многих других мировых игроков в сфере информационной безопасности, частный сектор здесь, как правило, опережает правительство в понимании значимости вопросов ее обеспечения, в то время как осведомленность широкой общественности варьируется в зависимости от страны региона.

Согласно последнему глобальному индексу кибербезопасности (*Global Cybersecurity Index*), только Уругвай значится в списке стран, демонстрирующих высокий уровень по всем пяти его составляющим [7]. Индекс включает в себя совокупность правовых, технических и организационных мер для защиты киберпространства страны, а также меры по наращиванию потенциала и построению сотрудничества для реализации партнерства и обмена информацией. Большая часть государств ЛАКБ (к примеру, Мексика, Бразилия, Аргентина, Чили, Венесуэла, Перу и Колумбия) добились успехов только на некоторых направлениях деятельности, необходимых для обеспечения информационной безопасности. ЛАКБ пока только начи-

нает разрабатывать собственные программы и участвовать в региональных и международных инициативах. Регион имеет огромный потенциал на международной арене, а также может выступить самостоятельной силой на площадках ООН, где обсуждаются вопросы кибербезопасности, и упомянутые ведущие игроки — США, Китай или Россия — могут использовать страны ЛАКБ в качестве союзников для продвижения своей повестки и формирования новых договоренностей по вопросам обеспечения защиты информационных сетей.

С этой точки зрения тема цифровизации и кибербезопасности региона представляется крайне актуальной и значимой для осуществления практических шагов во внешней политики России в краткосрочной перспективе. Несмотря на важность указанных вопросов, научных работ, авторы которых изучают проблемы информационной безопасности ЛАКБ, крайне мало. В некоторых из них страны региона рассмотрены лишь в качестве объекта цифровой политики США или Китая, при этом регион не представлен в качестве субъекта международной политики [8; 9]. Вопросы политики государств в области кибербезопасности чаще изучаются с точки зрения локальной защиты информации или компьютерных сетей, но не с точки зрения роли ведущих стран региона в принятии важнейших соглашений на уровне ООН или ОАГ [10]. Современная научная литература упускает из виду данное направление международной и региональной деятельности латиноамериканских государств. Однако в историографии есть сильные работы, помогающие понять политическое и дипломатическое поведение, например, Бразилии, Колумбии или Кубы по вопросам кибербезопасности на международном уровне. Отношения между странами Латинской Америки и Россией, вопросы региональной политики, а также проблемы внутри ОАГ подробно проанализированы в ряде исследований [11; 12; 13], хотя поведение изучаемых государств в сфере информационной безопасности зачастую остается за скобками. Отметим, что данная статья, продолжая в целом сложившуюся традицию, дополняет изучение внешней политики и дипломатии стран ЛАКБ на международном и региональном уровнях. Имеющиеся документы позволяют классифицировать государства ЛАКБ по их интересам, политике, конкретным дипломатическим усилиям и позиции в международной повестке по кибербезопасности. В этом заключается новизна предлагаемого исследования.

Цель данной работы — выявить место и роль ЛАКБ в сфере международной и региональной информационной безопасности. Для решения этой задачи использованы официальные правительственные и международные статистические документы и традиционные методы анализа — системный, документальный и сравнительный. Системный анализ позволяет рассмотреть исследуемый вопрос в рамках международного контекста с учетом влияния расстановки политических сил в мире, а также переговорного процесса и дипломатии. Документальный анализ дает возможность выявить официальные позиции, включить в научный оборот заявления представителей стран ЛАКБ и результаты их голосования по вопросам кибербезопасности в международных и региональных структурах. Сравнительный анализ используется при реконструкции конкретных подходов к проблеме.

СТРАНЫ ЛАТИНСКОЙ АМЕРИКИ В ООН

Поскольку вопрос обеспечения кибербезопасности даже на национальном уровне во многом зависит от взаимоотношений глобального порядка, странам ЛАКБ, чтобы оставаться в курсе текущей повестки, приходится наращивать механизмы сотрудничества не только в рамках региона, но и выходить на международный уровень. Самые известные процессы на уровне ООН, охватывающие заявленную повестку, проходят в Первом комитете Генеральной Ассамблеи (ГА) ООН, а также в рамках Группы правительственных экспертов (ГПЭ) по вопросам использования информационных технологий в контексте международной безопасности и недавно появившейся Рабочей группы открытого состава (РГОС), ставшей катализатором вовлечения большего количества стран, в том числе и из ЛАКБ.

Как известно, в 1998 г. Россия впервые обратила внимание мирового сообщества на проблему использования информационно-коммуникационных технологий и сохранения международной безопасности. После принятия первой резолюции и включения в повестку ООН пункта о достижениях в сфере телекоммуникаций и информатизации, ГА ежегодно принимала резолюции, призывающие государства информировать генерального секретаря о своих взглядах на проблемы обеспечения международной информационной безопасности. Некоторые страны ЛАКБ, в частности, Куба, регулярно реагировали на эти призывы.

Несколько лет спустя было решено создать специальные группы правительственных экспертов, поскольку их «встречи... способствовали лучшему пониманию существа проблем международной информационной безопасности и связанных с ними понятий» [14]. Именно так были заложены основы для развития современных норм и принципов международной кибербезопасности. Этот механизм можно критиковать или защищать, однако необходимо учитывать, что группы ООН работали и работают в условиях постоянно меняющихся технологий, что создает сложности в достижении консенсуса.

В 2004 г. первая группа ГПЭ собрала представителей 15 государств, включая Россию, США, Китай, Германию, Великобританию, Францию, Бразилию, Мексику и др. В течение года она должна была рассмотреть влияние достижений в области ИКТ на национальную безопасность и военную сферу, а также представить согласованный доклад Генеральному секретарю ООН. Однако консенсуса достичь тогда не удалось, поскольку среди участников не было единого мнения о том, какие проблемы следует обсуждать: вопросы безопасности информационного контента или только информационной инфраструктуры. Группа закончила работу, так и не подготовив итоговый доклад [15].

Несмотря на неудачный опыт работы первой ГПЭ, генеральный секретарь продолжал информировать ГА об оценках состояния международной информационной безопасности на основе докладов, представляемых государствами — членами ООН [16]. В 2008 г. было решено продолжить работу в формате ГПЭ [17]. За последующие два года группа в составе представителей 15 стран, включая Бразилию, смогла представить первый доклад, в

котором были отражены договоренности, достигнутые в отношении дилеммы контент/инфраструктура [18]. В тексте документа дана нейтральная формулировка — «использование ИКТ», что позволяет трактовать ее значение в широком и узком смыслах. Помимо списка угроз и рисков, сопряженных с использованием информационных технологий государствами и негосударственными акторами, в докладе содержался ряд рекомендаций. Основной вывод состоял в том, что необходимо выработать нормы государственного использования ИКТ для сокращения рисков на международной арене, которые сегодня проявляются в виде хакерских атак. Было также предложено заняться разработкой мер по углублению доверия, включая обмен мнениями по вопросу использования ИКТ в военных конфликтах; обмениваться информацией о национальных стратегиях и законах по обеспечению информационной безопасности; содействовать укреплению потенциала развивающихся стран. Таким образом, в 2010 г. в ООН был принят первый прорывной документ в отношении международной информационной безопасности. Несмотря на то, что он носил рекомендательный характер и не являлся обязательным к исполнению, это был значительный шаг вперед в деле налаживания международного диалога по разработке норм для киберпространства. Чтобы не утратить позитивный заряд, в резолюции, где отмечались успехи работы второй ГПЭ, содержалось требование созыва следующей группы в 2012 г. [19].

Только в 2013 г. третья ГПЭ (при участии Аргентины) представила содержательный доклад, в котором были прописаны меры по укреплению доверия и обмена информацией [20]. Но главным в документе был раздел, где содержался перечень принципов ответственного поведения государств, при полной реализации которых число нынешних угроз было бы значительно сокращено. Участники группы договорились также о том, что международное право и устав ООН должны быть применимы к киберпространству; государственный суверенитет и международные нормы, вытекающие из принципа суверенитета, должны распространяться на поведение государств в рамках использование информационных технологий; усилия по обеспечению безопасности ИКТ не должны нарушать основные права и свободы человека; государства не должны использовать посредников для совершения международных противоправных действий с использованием ИКТ и не допускать того, чтобы негосударственные субъекты использовали их территорию для применения ИКТ в незаконных целях; частный сектор и гражданское общество должны играть надлежащую роль в укреплении безопасности при создании и использовании ИКТ.

В 2015 г. был опубликован новый доклад четвертой группы ГПЭ под председательством Бразилии (при участии Мексики и Колумбии), который считают ключевым документом для разработки всеобщих кибернорм [21; 22]. Эксперты из 20 стран предложили идеи по выработке стандартов, укрепления доверия, наращивания потенциала и применения норм международного права. В список были добавлены правила по предотвращению кибератак на объекты критической инфраструктуры и помощи в устранении последствий в случае, если такая атака все же произошла. Члены группы предложили не использовать практику так называемых вредоносных

«закладок» или «бэкдоров» в производстве ИТ-оборудования и программного обеспечения. Напротив, было предписано способствовать обнародованию проблем, связанных с уязвимостью в информационных технологиях, и обмениваться информацией о методах их устранения. Наконец, появилась значимая норма о ненападении на группы экстренного реагирования на компьютерные инциденты (или в англоязычной версии названия — *CERT/CSIRT*), а также о запрете использования этих групп в осуществлении кибератак.

В отношении применимости норм международного права к использованию информационных технологий была подтверждена юрисдикция государств над ИКТ-инфраструктурой, расположенной на их территориях, что сегодня способствует развитию дискуссий в отношении цифрового суверенитета. Наконец, в процессе использования ИКТ международным акторам было предписано соблюдать принципы государственного суверенитета, суверенного равенства, разрешения споров мирными средствами и невмешательства во внутренние дела других государств. Важным дополнением являлось уточнение, что «указание на то, что та или иная деятельность в сфере ИКТ была начата или иным образом происходит с территории или объектов ИКТ-инфраструктуры государства, может быть недостаточным для присвоения этой деятельности указанному государству» [21]. Требуется обоснование обвинений в организации и совершении противоправных действий против государств. Тем не менее широкий круг вопросов, касающихся применения международного права, остался незатронутым.

Несмотря на достигнутый успех, ГПЭ пятого созыва при участии Мексики, Кубы и Бразилии завершила работу летом 2017 г., не обнародовав согласованного итогового доклада [23]. Мандат группы предусматривал подготовку документа, который должен был конкретизировать вопрос о том, как именно международное право применимо к сфере ИКТ, но участники не смогли договориться о возможности применения права государства на самооборону в ответ на вредоносное использование ИКТ, а также применения международного гуманитарного права к киберпространству, что сегодня является самым чувствительным вопросом. Согласно итоговому заявлению представителей Кубы, согласование данного вопроса узаконило бы ведение военных действий в контексте ИКТ, что противоречит заявленной ранее цели предотвращения конфликтов в киберпространстве [24]. Свою роль сыграли и напряженные отношения между Российской Федерацией и США, являющихся постоянными участниками ГПЭ. Как известно, американская сторона обвинила Россию во вмешательстве в президентские выборы 2016 г., а также в совершении кибератак и проведении информационных кампаний в социальных сетях [25]. Более того, высказывались мнения, что формат работы таких групп себя изжил, и необходимо искать новые площадки для обсуждения правил ответственного поведения государств в киберпространстве [26].

Тем не менее страны ЛАКБ и РФ продолжили диалог по кибернормам [27]. В 2018 г. Россия вместе с Боливией, Венесуэлой и Кубой, а также еще 12 странами представила проект резолюции по созданию новой рабочей группы открытого состава (РГОС) при ООН для широкого обсуждения

вопросов международной информационной безопасности. Страны предлагали расширить состав участников, приглашая все государства — члены ООН присоединиться к диалогу. США вместе с союзниками вынесли на рассмотрение свой проект резолюции, в котором предлагалось продолжить заседания ГПЭ в старом формате с ограниченным количеством экспертов, выбранных по принципу географического представительства.

В конце декабря 2018 г. прошли голосования по обоим документам. Резолюцию о создании РГОС под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» поддержали практически все страны ЛАКБ. Лишь Чили и Бразилия воздержались от голосования [28]. Американская резолюция под названием «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» также получила одобрение с большим перевесом голосов, но Куба, Боливия, Никарагуа и Венесуэла проголосовали против. Здесь, конечно, свою роль сыграли факторы не только непривлекательности закрытого формата ГПЭ, но и усилия российской дипломатии по созданию коалиции из стран-единомышленников для голосования в ГА ООН [29]. Как правило, надежные партнеры России в ЛАКБ всегда голосовали за резолюции по кибербезопасности, предлагаемые Москвой. А та группа стран, которая выступала против, как, например, Бразилия, руководствовалась тезисом о том, что нет необходимости дублировать работу ГПЭ, в которой она занимала прочные позиции.

Новая структура действительно оказалась более открытой, что привлекало страны региона с точки зрения возможности четко заявить о своей позиции. Примечательно, что многие их них — Аргентина, Мексика, Барбадос, Колумбия, Коста-Рика, Эквадор, Гватемала, Гондурас, Ямайка, Парагвай, Перу и Уругвай — голосовали за оба формата. Это свидетельствует о возросшем интересе региона к проблемам международной кибербезопасности и готовности Латинской Америки участвовать в дискуссии.

В итоге для обсуждения и выработки решений по международной повестке, касающейся вопросов информационной безопасности, при ООН были созданы два значимых института — Группа правительственных экспертов и Рабочая группа открытого состава, что повлекло за собой вероятность принятия взаимоисключающих документов. Несомненно, это привело и к невозможности выработать общепринятые нормы поведения и начать политику сдерживания потенциальных конфликтов в киберпространстве.

До сентября 2021 г. действует шестой созыв ГПЭ опять под председательством Бразилии. В группу из стран ЛАКБ также входят Мексика и Уругвай. Примечательно, что в рамках работы этой группы достижение консенсуса для разработки итогового доклада предусмотрено не было. Напротив, страны должны представить документы, отражающие их собственные взгляды на вопрос применения международного гуманитарного права к киберпространству. Именно этот вопрос является ключевым и вызывает наибольшее количество разногласий.

Рабочая группа открытого состава под председательством Швейцарии работает до весны 2021 г., и у нее есть больше шансов принять согласован-

ные документы. Открытый состав группы позволяет участвовать в ее работе всем заинтересованным странам, в отличие от ограниченного числа членов предыдущих ГПЭ, а условие достижения консенсуса обеспечит отражение общих интересов всех участников в итоговом документе. Но есть и существенные минусы: обязательность выработки согласованной позиции может сыграть блокирующую роль, как это произошло в 2017 г., либо заметно повлиять на итоговые формулировки доклада, сделав их более общими. Наконец, привлечение представителей из числа представителей бизнеса и гражданского общества к обмену мнениями по вопросам международной кибербезопасности формирует так называемый мультистейкхолдерный подход, что подразумевает участие всех заинтересованных сторон к решению проблемы. Взаимодействие между правительством и частными компаниями оказалось сегодня еще одним значимым вопросом в контексте проблем контроля за социальными сетями и распространяемой информацией, что впервые стало широко обсуждаться после исторических слушаний в конгрессе США в октябре 2017 г. [30]. Вопрос о том, кто должен контролировать киберпространство — технологические компании или правительство, является самым «горячим» в повестке цифровизации системы международных отношений.

Первое заседание РГОС в сентябре 2019 г. позволило, в силу открытого во всех смыслах формата работы, проанализировать отношение большинства стран ООН, в том числе и ЛАКБ, к проблеме информационной безопасности и в целом готовности полноценно участвовать в дискуссиях. Анализ заявлений участников группы показал, что латиноамериканские страны по-разному относятся не только к форматам ГПЭ и РГОС, но и к ключевым вопросам, стоящим перед группами. По мере развития информационных технологий и проявления цифрового неравенства среди государств региона позиции стран стали меняться. В частности, Мексика заявила о необходимости сосредоточиться на имплементации мер доверия в киберпространстве как простом и понятном практическом шаге. Она представила конкретные предложения по ведению хранилищ данных (репозиториев) в соответствии с лучшими практиками государств в отношении выполнения имеющихся кибернорм. Аргентина, Бразилия и Куба настаивали на продолжении работы над нормами ответственного поведения государств в части их уточнения и интерпретации. Было и заявление от Карибского сообщества (*Caribbean Community, CARICOM*) о необходимости работы над международным договором по киберпространству. Чили, Бразилия и Колумбия тоже рассматривали такую возможность. По вопросу, касающемуся применимости международного гуманитарного права к киберпространству, также появились разногласия.

В то время как Куба вместе с Россией продолжает заявлять о милитаризации киберпространства в случае формулирования конкретных норм использования ИКТ во время военных конфликтов, Чили и Бразилия допускают применение международного гуманитарного права с оговорками, а Коста-Рика и Мексика однозначно выступают за интерпретацию существующего международного гуманитарного права для киберпространства. Из этой же темы вытекает другой важный вопрос — право государств на самооборону в киберпространстве, где распреде-

ление позиций примерно совпадает с расстановкой сил по предыдущему вопросу. Еще одним индикатором интересов стран региона является обсуждение включения темы киберпреступности в сферу РГОС. Для Карибского сообщества данная тема является наиболее чувствительной и важной [31]. Для многих стран открылась возможность повысить свою осведомленность о наиболее актуальных проблемах в этой сфере.

В декабре 2020 г. в ГА ООН состоялось голосование по продлению РГОС еще на пять лет, что позволило превратить формат в регулярный институциональный диалог. Хотя резолюция и прошла с некоторыми затруднениями (92 стран поддержали, 50 выступили против, 21 воздержалась и 30 не голосовали), страны региона также продемонстрировали свои приоритеты. Бразилия воздержалась от голосования наряду с Гватемалой и Уругваем; Чили и Колумбия проголосовали против, но большая часть, включая Мексику, Кубу, Венесуэлу, Аргентину, Боливию, поддержали продление РГОС, считая этот формат эффективным [32].

Следует отметить, что страны ЛАКБ занимают сегодня довольно четкие позиции по отношению к двум вышеуказанным международным процессам, связанным с обсуждением вопросов кибербезопасности и принятием основополагающих документов в этой сфере. Именно в ходе работы ГПЭ и РГОС будут сформулированы конкретные шаги и планы действий, которые повлияют на международную обстановку в ближайшие пять-десять лет. От позиции стран ЛАКБ во многом зависят результаты деятельности РГОС. В силу этого Москве необходимо наращивать взаимодействия с ключевыми игроками региона в области цифровизации для выработки приемлемых решений и укрепления своих позиций при вынесении их на голосование в ООН.

РЕГИОНАЛЬНЫЕ УСИЛИЯ

Региональный уровень является ключевым для развития киберпотенциала стран и укрепления доверия между ними в информационном пространстве. Такие региональные организации, как, например, ОАГ, вносят неоценимый вклад в развитие входящих в них стран не только с точки зрения технической помощи по созданию собственных ресурсов для отражения возможных кибератак, но и предоставляют рекомендации по написанию стратегий национальной кибербезопасности [33; 34; 35].

Для понимания общего развития системы информационной безопасности в той или иной стране создан рейтинг так называемой «зрелости» стран региона в данной области — *Cybersecurity Capability Maturity Model*. Рейтинг составлен экспертами ОАГ и Межамериканского банка развития [36]. Модель, по которой оцениваются страны, состоит из пяти критериев: национальная политика и стратегия в области кибербезопасности; киберкультура и общество, образование и профессиональная подготовка в области кибербезопасности; правовая и нормативная база; стандарты и технологии. «Зрелость» также варьируется в рамках пяти стадий: от начальной, когда страна только начинает осознавать важность обеспечения информационной безопасности, до динамической, когда она способна быстро адаптироваться к внутренним и внешним киберугро-

зам и рискам. Ситуацию осложняет низкий уровень распространения Интернета в отдаленных частях ЛАКБ и недостаточное понимание важности вопросов, связанных с кибербезопасностью, среди населения. При этом правительства стран региона осознают важность принятия комплексных мер по наращиванию технического и политического потенциала для обеспечения безопасности.

Однако одним ключевых элементов, который упущен из виду разработчиками вышеупомянутого рейтинга, является готовность и способность стран участвовать в дипломатических переговорах по вопросам, связанным с киберпространством. Например, Гватемала, будучи председателем Межамериканского комитета ОАГ по борьбе с терроризмом (*Inter-American Committee against Terrorism, CICTE*), в ведении которого после соответствующей резолюции 2004 г. также находятся вопросы кибербезопасности в 2012 г. приложила немало усилий к тому, чтобы члены ОАГ приняли декларацию об укреплении информационной безопасности в Северной и Южной Америке [37; 38]. В декларации подтверждена их приверженность к осуществлению Всеобъемлющей межамериканской стратегии ОАГ по борьбе с угрозами кибербезопасности. В числе прочего страны — участницы ОАГ признали необходимость создания национальных групп реагирования на инциденты, связанные с компьютерной безопасностью, а также важность повышения безопасности и устойчивости критической информационной инфраструктуры к киберугрозам, включая энергетические, финансовые, транспортные и телекоммуникационные системы.

Общая межамериканская стратегия кибербезопасности 2004 г. является основополагающим региональным документом по формированию позиции стран и направлена на создание культуры информационной безопасности для предотвращения злоупотребления технологиями [39]. Стратегия предполагает развитие региональной сети для информирования о компьютерных инцидентах, создание общей защищенной инфраструктуры для управления конфиденциальными коммуникациями групп реагирования с частным сектором и другими заинтересованными сторонами, разработку технических стандартов безопасности и расширение правового потенциала для борьбы с киберпреступностью.

В 2012 г. *CICTE* принял декларацию об укреплении кибербезопасности, а в 2016 г. — декларацию об укреплении сотрудничества и развития в области кибербезопасности и борьбы с терроризмом в Северной и Южной Америке, в которой государствам-членам предлагалось уважать права человека при использовании киберпространства, укреплять сотрудничество между национальными группами реагирования, а также между правоохранительными органами; разрабатывать протоколы для связи между членами ОАГ в случае инцидентов, последствия которых выходят за пределы национальных границ, а также процедуры взаимной помощи при реагировании на них [40; 41]. Нельзя не отметить, что странам ЛАКБ на формальном и декларативном уровне удалось достичь некоторого взаимопонимания по вопросу о необходимости обмена информацией о возможных конфликтах в киберпространстве.

Однако ОАГ не только приняла декларации. Организация ведет еще и обширную практическую работу. Ее работа по наращиванию киберпотен-

циала часто ставится в пример подобным структурам, созданным в других регионах мира. ОАГ организовала обширную серию семинаров и учебных мероприятий по национальным киберстратегиям, мерам укрепления доверия и развитию потенциала. Наиболее результативной оказалась инициатива, выдвинутая в 2017 г. Чили, Колумбией, Перу, Коста-Рикой, Канадой, Гватемалой и Мексикой, по созданию рабочей группы по сотрудничеству и укреплению доверия в киберпространстве [42]. Результатом работы группы стал новый список мер по укреплению доверия в киберпространстве 2018 г. Составители списка частично базировались на положениях доклада ГПЭ ООН 2015 г., а также выделили следующие приоритетные меры: предоставление информации о политике информационной безопасности (стратегии, правовые инструменты и т.д.) и назначение национальных контактных лиц на политическом уровне, способных обсуждать последствия киберугроз в масштабах полушария [43].

Кроме этого в ОАГ действует программа по кибербезопасности, тесно связанная с известным и принимаемым в дипломатических кругах многих стран Глобальным форумом по киберэкспертизе (*Global Forum on Cyber Expertise, GFCE*). В него входят страны, межправительственные и международные организации, а также частные компании, имеющие ресурсы для содействия наращиванию кибернетического потенциала в более слабых странах. В рамках программы ОАГ по кибербезопасности под эгидой *GFCE* осуществляется сотрудничество внутри региона и с остальным миром по ключевым вопросам. Программа состоит из семи пунктов, в которые входят: разработка национальной стратегии информационной безопасности по готовой методологии; развитие групп реагирования на инциденты, связанные с компьютерной безопасностью; обучение антикризисному управлению; повышение осведомленности; техническая помощь и доступ к экспертным знаниям. Такой подход ОАГ оценивается как наиболее эффективный с точки зрения развития региональной кибербезопасности.

Для понимания общей картины места и роли ЛАКБ в международной и региональной кибербезопасности представляем наш анализ в виде таблицы.

УЧАСТИЕ СТРАН ЛАКБ В МЕЖДУНАРОДНЫХ И РЕГИОНАЛЬНЫХ СТРУКТУРАХ ПО КИБЕРБЕЗОПАСНОСТИ

Страна	Национальная стратегия кибербезопасности	Участие в Группе правительственных экспертов ООН	Участие в Рабочей группе открытого состава ООН	Участие в Глобальном форуме по киберэкспертизе	Участие в программе кибербезопасности ОАГ
Антигуа и Барбуда	проект				
Аргентина	+	+	+	+	+
Багамские Острова	проект				
Барбадос					

Белиз	+				
Боливия	проект		+		
Бразилия	+	+	+		
Венесуэла			+	+	+
Гаити	проект				
Гайана	проект				
Гватемала	+			+	+
Гондурас	проект				
Гренада					
Доминика	проект			+	+
Доминик. Республика	+			+	+
Колумбия	+	+	+		+
Коста-Рика	+				
Куба		+	+		
Мексика	+	+	+	+	+
Никарагуа			+		
Панама	+				
Парагвай	+				+
Перу	проект		+	+	
Сальвадор					
Сент-Винсент и Гренадины	+				
Сент-Китс и Невис					
Сент-Люсия	+				
Суринам	проект			+	
Тринидад и Тобаго	+				
Уругвай	+	+	+		
Чили	+		+	+	+
Эквадор			+		
Ямайка	+				+

Из таблицы следует, что Аргентина, Колумбия и Мексика являются наиболее активными странами региона, принимающими участие в формировании повестки обсуждаемых вопросов в международных и региональных организациях по кибербезопасности. Это означает, что содержание принимаемых итоговых документов может зависеть от позиции данных государств.

На сегодняшний день существуют разные подходы к решению проблем информационной безопасности. США и страны Европы, например, рассматривают ее как систему мер, которые должны соответствовать имеющимся вызовам. Поэтому в правительственных стратегиях в данной сфере чаще всего перечислены угрозы и способы их преодоления. Россия, Китай и другие страны большее внимание уделяют такому аспекту кибербезопасности, как цифровой суверенитет. Страны ЛАКБ используют разные подходы; при обсуждении различных аспектов безопасности на международных площадках регион не выступает единым фронтом.

Если еще в 2010-е годы голос латиноамериканских государств не был слышен среди держав, активно обсуждавших чувствительные проблемы в области кибербезопасности, то сегодня многие страны региона обладают необходимым потенциалом для того, чтобы донести свое в*и*дение ситуации на международных форумах. Поскольку позиции ведущих государств по вопросам кибербезопасности значительно разнятся, России целесообразно расширять сотрудничество с ЛАКБ для выработки консенсуса и продвижения общей точки зрения. Это особенно важно, поскольку ряд крупных стран региона — Аргентина, Бразилия, Мексика и др. — склонны занимать лояльную позицию в отношении подходов США к проблемам информационной безопасности, что также оказывает влияние на решения, принимаемые в этой сфере. Увеличение числа стран — участниц глобальных диалогов по кибербезопасности является самым эффективным способом продвижения российской позиции по этому вопросу.

ИСТОЧНИКИ И ЛИТЕРАТУРА / REFERENCES

1. Эффективное обеспечение киберстабильности. Глобальная комиссия по стабильности киберпространства. Итоговый доклад. Ноябрь 2019. [Effektivnoe obespechenie kiberstabil'nosti. Global'naya komissiya po stabil'nosti kiberprostranstva. Itogovyj doklad [The effective provision of cybertablet. Global Commission on the Stability of Cyberspace. Final report]. Available at: https://cyberstability.org/wp-content/uploads/2020/08/GCSC-Advancing-Cyberstability_RU.pdf (accessed: 15.12.2020).

2. National Cybersecurity Strategy, Mexico. Available at: https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf (accessed: 16.12.2020).

3. National Cyber Security Strategy, Brazil. Available at: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Decreto/D10222.htm (accessed: 16.12.2020).

4. Jefatura De Gabinete De Ministros Secretaría De Gobierno De Modernización, Resolución 829/2019, Argentina. Available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528 (accessed: 17.12.2020).

5. Bases Para una Política Nacional de Ciberseguridad, Chile. Available at: https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf (accessed: 17.12.2020).

6. Estrategia Nacional de Ciberseguridad de Costa Rica. Available at: https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf (accessed: 18.12.2020).

7. Global Cybersecurity Index. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (accessed: 18.12.2020).

8. Tsvetkova N., Kheifets V., Sytnik A., Tsvetkov I. Venezuela in U.S. Public Diplomacy, 1950s–2000s: the Cold War, Democratization, and the Digitalization of Politics. *Cogent Social Sciences*, 2019, vol, 5, N 1, pp. 1–15.

9. Цветкова Н.А., Кузнецов Н.М. Феномен дипломатии больших данных в мировой политике. *Вестник РГГУ. Серия: Политология. История. Международные отношения*. М., 2020, № 4, сс. 27–44 [Tsvetkova, N.A., Kuznetsov, N.M. [Fenomen diplomatii bolshikh dannyh v mirovoj politike [Phenomenon of Big Data Diplomacy in World Politics]. *Vestnik RGGU. Seriya: Politologiya. Istoriya. Mezhdunarodnye otnosheniya*, Moscow, 2020, vol. 4, pp. 27–44 (in Russ.).

10. Kobek L., Caldera E. Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection. *OASIS–Observatorio de Análisis de Los Sistemas Internacionales*, 2016, N 24, pp. 109–128.

11. Rouvinski V. Understanding Russian Priorities in Latin America. *Kennan Cable.* Washington, D.C. 2017. N 20. Available at: https://www.wilsoncenter.org/publication/kennan-cable-no20-understanding-russian-priorities-latin-america (accessed: 15.01.2021).

12. Еремин А.А. Организация американских государств и региональная безопасность. М., Аспект-пресс, 2020. [Eremin A.A. Organizatsia amerikanskikh gosudarstv i regionalnaya bezopasnost' [Organization of American States and Regional Security]. Moscow, Aspekt-press, 2020.

13. Хейфец В.Л., Хадорич Л.В. Латинская Америка Между ОАГ и СЕЛАК. *Мировая экономика и международные отношения*. М., 2015, № 4, сс. 90–100 [Khejfets V.L., Khadorich L.V. Latinskaya Amerika mezhdu OAG i SELAK [Latin America between the OAS and CELAC]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya.* Moscow, 2015, N 4, pp. 90–100 (in Russ.).

14. U.N. Resolution, A/RES/56/19, 2001. Available at: https://undocs.org/ru/A/RES/56/19 (accessed: 15.12.2020).

15. The Report of the General Secretary, A/60/202, 2005. Available at: https://undocs.org/ru/A/60/202 (accessed: 15.12.2020).

16. U.N. General Assembly. Documents. A/54/213, A/55/140 и Corr.1 и Add.1, A/56/164 и Add.1, A/57/166 и Add.1, A/58/373, A/59/116 и Add.1, A/60/95 и Add.1, A/61/161 и Add.1 и A/62/98 и Add.1. Available at: https://www.un.org/ (accessed: 20.12.2020).

17. U.N. Resolution, A/RES/63/37, 2008. Available at: https://undocs.org/ru/A/RES/63/37 (accessed: 19.12.2020).

18. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: https://undocs.org/ru/A/65/201 (accessed: 15.12.2020).

19. U.N. Resolution, A/RES/65/41, 2010. Available at: https://undocs.org/ru/A/RES/65/41 (accessed: 14.12.2020).

20. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: https://undocs.org/ru/A/68/98 (accessed: 14.12.2020).

21. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: https://undocs.org/ru/A/70/174 (accessed: 16.12.2020).

22. Государствам загрузили мирную программу: 20 стран заложили основу для глобального пакта об электронном ненападении. *Коммерсант*, 18 августа 2015 [Gosudarstvam zagruzili mirnuyu programmu: 20 stran zalozhili osnovu dlya globalnogo pakta ob elektronnom nenapadenii [The States were Uploaded by a Peace Program: 20 Countries Formed the Foundation for a Global Pact on Electronic Non-Aggression]. *Kommersant*, August 18, 2015. Available at: https://www.kommersant.ru/doc/2790215 (accessed: 25.12.2020).

23. The Report of the General Secretary, A/72/327, 2017. Available at: https://undocs.org/ru/A/72/327 (accessed: 19.12.2020).

24. 71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security, 23 June, 2017. Available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information (accessed: 15.12.2020).

25. Tsvetkova N.A. Dealing with a Resurgent Russia: Engagement and Deterrence in U.S. International Broadcasting, 2013–2019. *Vestnik of Saint Petersburg University. International Relations*, 2019, vol. 12, N 4, pp. 435–449.

26. Segal A. The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What? *Council on Foreign Relations*, June 29, 2017. Available at: https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what (accessed: 25.12.2020).

27. «Инфофорум-2018»: российские инициативы в формировании системы международной информационной безопасности. *Международная жизнь*. М., 15 февраля, 2018 [«Infoforum-2018»: rossijskie iniciativy v formirovanii sistemy mezhdunarodnoj informacionnoj bezopasnosti [Infoforum-2018: Russian Initiatives in the Field of Interna-

tional Information Security System]. *Mezhdunarodnaya zhizn*, Moscow, February 15, 2018. Available at: https://interaffairs.ru/news/show/19338 (accessed: 15.12.2020).

28. U.N. Resolution, A/RES/73/27 2018. Available at: http://www.un.org/en/ga /search/view_doc.asp?symbol=A/RES/73/27 (accessed: 14.12.2020).

29. Стадник И. Россия и США: два разных взгляда на кибербезопасность. *Российский совет по международным делам*, 13 ноября, 2018 [Rossiya i SShA: dva raznyh vzglyada na kiberbezopasnost [Russia and the United States: Two Different Views on Cybersecurity] *Rossijskij sovet po mezhdunarodnym delam*, Moscow, November 13, 2018. Available at: http://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-dva-raznykh-vzglyada-na-kiberbezopasnost/ (accessed: 15.12.2020).

30. Tsvetkova N. Russian Digital Diplomacy: A Rising Cyber Soft Power. *Russia's Public Diplomacy: Evolution and Practice*. Velikaya, A. and Simons G. (Eds.). London - New York, Palgrave Macmillan, 2020, pp. 103–117.

31. Countering the Use of Information and Communication Technologies for Criminal purposes, Belarus, Venezuela, Nicaragua, Russian Federation and others: Draft Resolution, 2019. Available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N19/313/33/PDF/N1931333.pdf?OpenElement (accessed: 19.12.2020).

32. Developments in the Field of Information and Telecommunications in the Context of International Security Resolution adopted by the UN General Assembly, 2020. Available at: https://digitallibrary.un.org/record/3896180?ln=en (accessed: 27.12.2020).

33. Towards a Secure Cyberspace via Regional Co-operation. *DiploFoundation*, 2017. Available at: https://www.diplomacy.edu/sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf (accessed: 27.12.2020).

34. Нелина О.В. ОАГ в противодействии террористической угрозе: латиноамериканские альтернативы. *Латинская Америка*, М., 2009, № 9, сс. 38–44 [Nelina O.V. OAG v protivodejstvii terroristicheskoj ugroze latinoamerikanskie alternativy [The OAS and the Deterrence of the Terrorist Threat: Latin American alternatives]. *Latinskaya Amerika.* Moscow, 2009, N 9, cc. 38–44 (in Russ.).

35. Horwitz B. *The Transformation of the Organization of American States: A Multilateral Framework for Regional Governance*. L., N.Y., Anthem Press, 2010.

36. Cybersecurity: Are We Ready in Latin America and the Caribbean? Inter-American *Development Bank Publications*, 2016. Available at: https://publications.iadb.org/publica-tions/english/docu-ment/Cybersecurity-Are-We-Ready -in-Latin-America-and-the-Caribbean.pdf (accessed: 30.12.2020).

37. Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity. Organization of American States. Available at: http://www.oas.org/en/citel/infocitel/julio-04/ultciberseguridad_i.asp (accessed: 30.12.2020).

38. Declaration on Strengthening Cyber-Security in the Americas. Approved at the Fourth Plenary Session held on March 7, 2012. Organization of American States. Available at: http://www.cicte.oas.org/rev/en/Documents/Declarations/DEC%201%20rev%201%20DECLARATION%20CICTE00749E04.pdf (accessed: 31.12.2020).

39. Comprehensive Inter-American Cybersecurity Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity. Organization of American States. Available at: http://www.oas.org/XXXIVGA/english/ (accessed: 31.12.2020); docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm (accessed: 31.12.2020).

40. Strengthening Cyber-Security in the Americas. Declaration. Inter-American Committee Against Terrorism. Available at http://www.state.gov/p/wha/ rls/221498.htm (accessed: 31.12.2020).

41. Strengthening Hemispheric Cooperation and Development in Cybersecurity and Fighting Terrorism in the Americas. Inter-American Committee Against Terrorism. Available at http://www.state.gov/p/wha/rls/259346.htm (accessed: 01.01.2021).

42. Working Group on Cooperation and CBMs in Cyberspace was established by CICTE through Resolution, CICTE/RES.1/17 on April 7, 2017. Organization of American States. Available at: https://www.oas.org/en/sms/cicte/session_2017.asp (accessed: 01.01.2021).

43. Regional Confidence-Building Measures (CBMs) to Promote Cooperation and Trust in Cyberspace, CICTE/RES. Organization of American States. Available at: https://www.oas.org/en/sms/cicte/session_2019.asp (accessed: 01.01.2021).

Ilona T.Stadnik (i.stadnik@spbu.ru)

Assistant professor at American Studies Department at St. Petersburg State University. Her research expertise covers international cyber norm-making, Russia-US relations in the cybersecurity field and global internet governance

Smolnogo Str., 1/3, 191060 St. Petersburg, Russian Federation

Natalia A.Tsvetkova (n.tsvetkova@spbu.ru)

Professor and head of American Studies Department at St. Petersburg State University, Russia. She writes about U.S. foreign policy and digital diplomacy

Smolnogo Str., 1/3, 191060 St. Petersburg, Russian Federation

The place and role of Latin American countries in the system of international and regional cybersecurity

Abstract. The article reveals the policy of Latin American states in the field of cybersecurity. The Latin American countries have contributed to the activities of different fora and the adoption of numerous resolutions at both international and regional organizations. The paper evaluates the impact of Latin American countries (in particular of Argentina, Mexico and Colombia) within the most important UN processes, namely the Group of Governmental Experts and the Open-Ended Working Group. At the regional level, the role of the Organization of American States in terms of introducing of the regional cybersecurity system is revealed. The authors conclude, the position of particular countries of Latin America is markedly different and leans toward the leading states in the field of digitalization, namely the USA, the European Union, Russia, and China. The paper concludes with considerations of how Latin American policies can enhance Russia's cybersecurity agenda.

Key words: cybersecurity, Latin America, UN, Organization of American States, UN GGE, OEWG.

DOI: 10.31857/S0044748X0014088-5

Received 20.01.2021.