Секция «Региональные проблемы международных отношений: Запад»

Влияние системных факторов на политику США в сфере информационной безопасности в Латинской Америке

Научный руководитель – Глазунова Елена Николаевна

Требух Александр Дмитриевич
Аспирант
Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра региональных проблем мировой политики, Москва, Россия
E-mail: alexandr.trebukh@yandex.ru

Латинская Америка является регионом, в котором угрозы информационной безопасности и риски для цифровых государственных и корпоративных инфраструктур становятся всё более явными, а последствия кибератак всё более болезненными. Сами Соединенные Штаты Америки в последние годы также подвергались изрядному количеству кибератак, часть из которых пришлась на цепочки поставок товаров и дестабилизировала национальную безопасность Вашингтона. Кроме того, в Латинской Америке присутствуют и внерегиональные акторы, стремящиеся как расширить свои позиции на рынке продуктов и услуг в сфере информационной безопасности в регионе, так и использующие хакерские группировки для достижения своих национальных интересов. По мнению США, главным таким внерегиональным актором является Китай [1].

Нами было проведено исследование о подходах Соединённых Штатов Америки в сфере информационной безопасности в Латинской Америке в контексте американо-китайского соперничества. Хронологически исследование было ограничено президентскими администрациями Д. Трампа и Дж. Байдена. Мы опирались на теорию комплексов региональной безопасности и теорию неоклассического реализма. Сочетание этих двух теорий позволило нам избежать недостатков каждой из них, позволило рассмотреть роль географического фактора, роль нематериальных факторов и степень восприятия угроз по рассматриваемой проблематике, а также оценить степень системного фактора в лице КНР, влияющего на процесс принятия внешнеполитических решений Вашингтона в этой сфере. Гипотеза проведённого исследования заключалась в том, что подход США в этой сфере в Латинской Америке преимущественно носил реактивный, а не проактивный характер.

Позиции рассмотренных нами президентских администраций характеризовались последовательностью и преемственностью. Их действия были поддержаны и соответствующими созывами Конгресса США в рассматриваемый нами период [2].

США осознали зависимость как собственной государственной, корпоративной и частной инфраструктуры от компьютерного, аппаратного и сетевого оборудования, произведённого в КНР. Эта зависимость присутствовала и в странах Латинской Америки. В связи с этим Вашингтон начал проводить политику отказа от произведённого Китаем оборудования в этой сфере и принял меры по продвижению идеи такого отказа в регионе [3]. Объяснением этому послужила уязвимость китайского оборудования к атакам и активная их эксплуатация китайскими хакерами. В то же время, на наш взгляд, таким образом Вашингтон стремился политизировать проблему с целью экономической конкуренции и продвижения товаров собственного производства в Латинской Америке.

Вашингтон стремился создать на основе Организации Американских Государств единую коалицию стран региона, и шире – полушария, которые могли бы совместно выработать единую стратегию обеспечения информационной безопасности [4]. США же при этом имели бы существенное технологическое преимущество и формировали бы принципы защиты на основе собственных протоколов и мер обеспечения безопасности.

Роль пространственного фактора заключалась в следующем: наибольшее количество кибератак приходилось на страны Южной Америки, в то время как выделяемые средства по линии Агентства США по международному развитию направлялись в страны, расположенные ближе к южной границе США. Это позволило говорить о подтверждении тезиса теории комплексов региональной безопасности, который указывает, что территориально близкие угрозы имеют для государств большее значение, чем находящиеся на существенном от них расстоянии. В рамках политики обеспечения информационной безопасности США в Латинской Америке это подтвердилось большим акцентом на сотрудничество со странами, входящими в североамериканский комплекс безопасности.

Подводя итог, можно сделать ряд следующих утверждений: подход США к обеспечению кибербезопасности имеет экстерриториальный характер. В рассматриваемый период он был наполнен в большей степени реактивным содержанием. Политика США в области кибербезопасности основана на двухпартийном консенсусе, преемственности подходов, синхронизации исполнительной и законодательной ветвей власти в её имплементации. Однако региональное измерение этой политики не развивалось с той же интенсивностью.

В краткосрочной перспективе США будут стремиться к контролю повестки в области кибербезопасности и попытке создать и легитимизировать единые правовые и организационные основы обеспечения информационной безопасности корпоративной и государственной инфраструктуры стран Латинской Америки. Это подтверждается финансовой поддержкой США на программы подготовки специалистов в области кибербезопасности по линии ОАГ. В свою очередь процесс контроля этой повестки будет сопровождаться дискредитацией продуктов программного, сетевого и аппаратного обеспечения внерегиональных акторов, в первую очередь, продукции КНР и России.

Источники и литература

1) The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence \\ CRS. 2020. URL: https://crsreports.congress.gov/product/pdf/IF/IF11469 (accessed: 13.09.2024).
2) H.R. 1493 – Cyber Deterrence and Response Act of 2019; H.R.3462 - SBA Cyber Awareness Act; H.R.7535 - Quantum Computing Cybersecurity Preparedness Act \\ U.S. Congress. URL: https://www.congress.gov/ (accessed: 13.09.2024).
3) US Lawmakers urge probe of WiFi router maker TP-Link over fears of Chinese cyber attacks. Reuters. 16.08.2024. URL: https://www.reuters.com/world/us/us-lawmakers-urge-probe-wifi-router-maker-tp-link-over-fears-chinese-cyber-2024-08-15/ (accessed: 30.12.2024).
4) Remarks: Organization of American States Cybersecurity Symposium Opening Ceremony Remarks, Acting National Cyber Director Walden. The White House. 19.10.2023. URL: https://www.whitehouse.gov/oncd/briefing-room/2023/10/19/organization-of-american-states-cybersecurity-symposium-opening-ceremony-remarks-acting-national-cyber-director-walden/ (accessed: 31.12.2024).