DOI 10.35775/PSI.2025.114.2.027
УДК 32.327

Е.Р. ОЩЕПКОВ
стажер-исследователь научной группы «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке» Факультета мировой экономики и мировой политики НИУ ВШЭ,
Россия, г. Москва
E-mail: eroshchepkov@edu.hse.ru

АМЕРИКАНОЦЕНТРИЧНЫЕ ИНСТИТУТЫ РЕГИОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ В АТР[4]

По мере эскалации американо-китайского противостояния в АТР/ИТР, все большее значение приобретают блоковые альянсы. В то время как КНР старается полагаться преимущественно на собственные силы, США активно пользуется поддержкой союзных государств – Японии, Австралии, Новой Зеландии, Южной Кореи и не только. Помимо экономического, военного или политического противоборства на авансцену глобальной политики выходит цифровая безопасность. Над реализацией ряда кибериниициатив в Азиатско-Тихоокеанском/Индо-Тихоокеанском пространстве интенсивно работают такие проамериканские организации, как QUAD, AUKUS, ANZUS, PBP и даже NATO. В рамках данной статьи предпринимается попытка проанализировать и охарактеризовать эффективность таких альянсов на основе официальной документации, опубликованной в первую половину 2020-х годов.

Ключевые слова: *безопасность, кибербезопасность, США, КНР, Альянсы, QUAD, AUKUS, ANZUS, NATO, PBP.*

Истоки формирования американоцентричных институтов в АТР/ИТР. Основная причина существования и развития американоцентричных институтов региональной кибербезопасности в Азиатско-Тихоокеанском (Индо-Тихоокеанском) регионе заключается в нарастающих противоречиях между двумя крупнейшими экономиками мира: КНР и США. Китайское руководство активно стремится расширить цифровые возможности страны, о чем прямо говорится в официальных документах: (Источник № 1 [18]: **«Мы войдем в цифровую эру и укрепим мощь Китая в киберпространстве; будут активизированы усилия по разработке ключевых технологий для обеспечения кибербезопасности**»). Китай позиционирует себя как сторонника «здоровой киберкультуры». Чтобы расширять свое цифровое влияние, КНР интенсивно ищут новых союзников в АТР/ИТР. При этом правительство Си Циньпина не стесняется

[4] Публикация подготовлена в ходе реализации проекта № 25-00-05 («АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке») в рамках Программы «Научный фонд Национального исследовательского университета “Высшая школа экономики” (НИУ ВШЭ)».

в выражениях, когда речь заходит о цифровой конфронтации с Соединенными Штатами: (Источник № 2 [14]: **«США злоупотребляют своей технологической гегемонией, осуществляя кибератаки. США – это «империя хакеров». США используют аналоговые сигналы базовых станций для доступа к мобильным телефонам с целью кражи данных»**). Согласно позиции китайского руководства, цифровая мощь США поддерживается многочисленными союзниками Вашингтона – в первую очередь, Британией, Японией, Австралией и Новой Зеландией. В проведении цифровых атак под кодовыми названиями «Призма», «Грязный ящик», «Раздражающий рог» и «Телескопическая операция» Пекин также видит США. В свою очередь, Соединенные Штаты прилагают большие усилия для того, чтобы создать образ главного защитника демократических ценностей в информационном пространстве. Вместе с тем, правительство США отчетливо дает понять: усиление американских кибермощностей – единственный способ защитить страну от китайских хакеров: (Источник № 3 [20]: **«Обеспечение безопасности киберпространства является основополагающим фактором защиты Америки. Киберпространство является неотъемлемым компонентом всех сторон американской жизни»**). Руководство Соединенных Штатов не жалеет денег на новые сервера и подготовку кадров. Независимо от политической конъюнктуры, обе партии (и Демократическая, и Республиканская) намерены действовать решительно. Важнейшим инструментом обеспечения защиты национальных интересов в киберпространстве видится тесная кооперация с союзниками: (Источник № 4 [21]: **«Мы будем укреплять потенциал стран-партнеров в области кибербезопасности, повышая их способность к самозащите. Мы намерены содействовать снижению рисков путем наращивания потенциала партнеров в регионе по мониторингу кибердоменов»**). С приходом к власти Дональда Трампа риторика США по вопросам кибербезопасности стала еще более агрессивной. Новый лидер намерен вести диалог с позиции силы и не стесняется в выражениях: (Источник № 5 [22]: **«Мы будем отстаивать наши интересы, противостоять агрессивным и принудительным действиям Пекина. США твердо намерены противостоять неправомерным, несправедливым и незаконным действиям со стороны Китая. Мы будем работать вместе с демократическими союзниками»**). Бинарная оппозиция Соединенных Штатов и Китая – основной драйвер развития антикитайской оси. На этой логике строится повествование об американоцентричных институтах цифровой безопасности в Азиатско-Тихоокеанском (Индо-Тихоокеанском) регионе.

QUAD как американоцентричный институт кибербезопасности в АТР. Точкой отсчета четырехстороннего диалога по безопасности стал 2007 год. Формат просуществовал несколько месяцев и был повторно возрожден лишь через 10 лет по инициативе американского президента Дональда Трампа. Основная идея альянса заключается в сдерживании амбиций КНР (как военно-политически, так и научно-технически). Стороны активно вкладываются в развитие 5G и искусственного интеллекта. Лидеры QUAD не скрывают, что это должно помочь им предотвратить китайскую угрозу: (Источник № 6 [23]: **«QUAD**

решает общие проблемы безопасности в Индо-Тихоокеанском регионе, включая растущий военный потенциал КНР. Наше сотрудничество – ключевой компонент цифровой безопасности»). Продвигаемая в настоящее время концепция свободного и открытого ИТР своими корнями уходит именно сюда. Каждая из четырех стран так или иначе сталкивается с цифровой активностью китайских хакеров (или, по крайней мере, регулярно обвиняет их в этом). Кроме того, члены QUAD озабочены безопасностью подводных кабелей, от которых зависит работоспособность критической инфраструктуры в Японии, Индии, Австралии и Соединенных Штатах. Участники диалога верят, что противостоять КНР возможно лишь сообща. Впрочем, угроза хакеров-одиночек тоже не исключается: (Источник № 7 [9]: **«Страны QUAD намерены бороться с общими угрозами, исходящими от спонсируемых государством субъектов, киберпреступников и других негосударственных злоумышленников. Мы планируем координировать совместные усилия по выявлению уязвимостей и защите сетей национальной безопасности»**). Государства-члены QUAD строят свое публичное реноме на законности, честности и приверженности либерально-демократическим идеям, в том числе и на цифровом поприще. В своих нормативно-правовых актах и публичных выступлениях участники четырехстороннего диалога ссылаются на правила, установленные Организацией Объединенных Наций. Например, на принятую в 2022 году конвенцию ООН об ответственном поведении в сети (The UN Framework for Responsible State Behavior in Cyberspace) [19]. В то же время, стороны не скрывают своей проамериканской направленности. Разработанные в США инициативы не только навязываются членам QUAD, но и интенсивно распространяются среди малых государств АТР/ИТР: (Источник № 8 [10]: **«Мы высоко оцениваем прогресс, достигнутый 36 странами, поддерживающими возглавляемую США Инициативу по борьбе с вымогательством (CRI), и регулярные, ориентированные на практику консультации по борьбе с цифровой преступностью в Индо-Тихоокеанском регионе»**). Нормативно-правовая база регулярно обновляется. В числе последних инициатив четырехстороннего диалога по безопасности можно выделить «The QUAD Joint Principles for Secure Software» и «The QUAD Joint Principles for Cyber Security of Critical Infrastructure». По состоянию на начало и середину 2020-х годов, альянс нацелен на проведение взаимных консультаций. Цель таких мероприятий – укрепить обороноспособность членов союза: (Источник № 9 [28]: **«Мы повышаем осведомленность о киберпространстве и даем всему ИТР возможность защитить себя в Интернете»**). Реальные перспективы QUAD достаточно туманны. По всей видимости, альянса просуществует ровно до тех пор, пока Индия не усилится достаточно, чтобы стать третьим полюсом силы подобно КНР. Как только это случится, о киберсотрудничестве Дели и Вашингтона можно будет забыть. Следовательно, о полном доверии между участниками говорить тоже не приходится. Тем не менее, роль сдерживающего фактора QUAD выполняет.

AUKUS как американоцентричный институт кибербезопасности в АТР. Трехсторонний блок официально оформился в 2021. В его состав вошли

Австралия, Британия и США. Как и в случае QUAD, лейтмотивом кооперации стало сдерживание внешнеполитических устремлений КНР в мире вообще и на территории Азии в частности. Все три участника AUKUS входят в так называемую «англосферу»: неформальное сообщество англоговорящих стран с общими культурными и политическими традициями. Схожие идеалы лишь укрепляют американо-британо-австралийский альянс изнутри. Кроме военно-политического единства (к примеру, в вопросах строительства подводных лодок) государства AUKUS не скрывают своих амбиций в цифровой сфере: (Источник № 11 [24]: **«В рамках инициативы планируется сосредоточиться на кибернетических возможностях, искусственном интеллекте и квантовых технологиях»**). Участники AUKUS намерены любой ценой обеспечивать безопасность своих подводных кабелей, способствовать формированию нового поколения специалистов в сфере цифровой безопасности, обмениваться разведданными, а также инвестировать в высокотехнологичную промышленность (например, в области производства полупроводников). Стремительно растущие возможности Китая заставляют Британию, Австралию и Соединенные Штаты с каждым годом наращивать темп: (Источник № 12 [25]: **«Альянс занимается вопросами радиоэлектронной борьбы и гиперзвука»**). Ввиду стремительной гонки вооружений все участники AUKUS заинтересованы в обмене оборонными технологиями, однако для Соединенных Штатов и Британии это – еще и возможность вести разведку в Тихом и Индийском океане (в относительной близости от границ Китая) с австралийской территории. Самым известным узлом перенесения интересов ЦРУ, MI6 и австралийских спецслужб стала база Pine Gap, расположенная на севере континенте. Именно здесь британские и американские специалисты ведут спутниковую и радиоэлектронную слежку за китайскими войсками, а также перехватывают сигналы патрульных/сторожевых судов КНР. Почти тысяча американских военных каждый день ведут работу с колоссальными массивами данных. В свою очередь, на предоставляемые с базы сведения ориентируются военно-морской флот США (160 кораблей), а также военно-морской флот Британии (свыше 60 судов). Если азиатский аналог NATO когда-нибудь и появится, то его ядром станет именно AUKUS. Принимая во внимание стратегическую значимость описанных выше объектов, участники альянса стремятся защитить их от взломов любой ценой: (Источник № 13 [11]: **«Мы направляем наши усилия на укрепление кибернетического потенциала, включая защиту критически важных систем связи и операций»**). С годами члены AUKUS неуклонно увеличивают расходы на национальную оборону, что напрямую затрагивает вопросы кибербезопасности. По традиции тренд задают Соединенные Штаты, однако Австралия старается не отставать. В недавних отчетах руководство страны с гордостью рассказывало о том, как новые инициативы в рамках AUKUS положительно скажутся на оборонно-промышленном комплексе страны и укрепят национальную безопасность: (Источник № 14 [6]: **«В течение следующих четырех лет в промышленный потенциал и рабочую силу Австралии будет инвестировано 6 миллиардов долларов, что позволит создать около**

20 000 прямых рабочих мест за следующие 30 лет. Это открывает возможности для всей страны в области науки, технологий и цифровых разработок»). Разумеется, у AUKUS имеются и слабые стороны. Самая очевидная – географическая удаленность всех трех участников друг от друга. Разные часовые пояса (когда в Лондоне 20:00, в Канберре – 7:00, а в Вашингтоне – 15:00) осложняют кооперацию спецслужб. Впрочем, совместный мониторинг цифрового пространства продолжается.

NATO как американоцентричный институт кибербезопасности в АТР. Хотя исходное название Североатлантического альянса подразумевает географическую привязку к одноименному океану, сфера присутствия стран Северной Америки и Западной Европы вовсе не ограничена данным регионом. По состоянию на середину 2020-х годов, в организацию входят 32 государства. Все они объединены верой в либерально-демократическую идеологию и ведут свою внешнюю политику в интересах Соединенных Штатов. С 1949 года вся архитектура безопасности в рамках NATO базируется на статье № 5, согласно которой агрессия против одного члена союза равноценна агрессии против всех его участников. В XXI веке центральный фокус Североатлантического альянса по-прежнему держится преимущественно на европейском направлении, но все чаще в сферу интересов NATO входят другие темы: 1) цифровая преступность; 2) сдерживание военного присутствия КНР в АТР/ИТР. Доказательством тому служат многочисленные заявления на официальном сайте альянса: (источник № 15 [15]: **«Заявленные амбиции и принудительная политика Китайской Народной Республики бросают вызов нашим интересам, безопасности и ценностям. КНР пытается подорвать основанный на правилах глобальный порядок»**. Военно-политическое присутствие NATO в Азиатско-Тихоокеанском/Индо-Тихоокеанском регионе неоспоримо: ФРГ [2] и Франция [8] уже давно проводят здесь регулярные учения своих ВМС и ВВС. Обеспечение цифровой безопасности – еще один приоритет как европейских, так и американских военных. В рамках Североатлантического альянса на постоянной основе действуют саммиты кибербезопасности, на полях которых пристальное внимание уделяется бескомпромиссной борьбе с китайскими, российскими и северокорейскими хакерами. Ближайшее совещание цифровых экспертов NATO должно состояться в Сеуле, столице Южной Кореи (2025 год) [16]. Нельзя забывать и про радиолокационные комплексы, расположенные на Тихоокеанском побережье США и Канады: протяженность береговой линии от Сан-Диего на юге до Уналашки на севере равна 5.500 километров. Специальные подразделения (так называемые «цифровые юниты») ведут круглосуточный мониторинг сети на военных базах в Калифорнии (1 – Camp Cooke, 2 – Camp Haan, 3 – Camp Roberts, 4 – Camp San Luis, 4 – Fort Hunter Liggett, 5 – Fort Irwin, 6 – Los Alamitos Joint Forces Training Base, 7 – Military Ocean Terminal Concord, 8 – Parks Reserve Forces Training Area, 9 – San Joaquin Depot, 10 – Sierra Army Depot), Орегоне (Camp Rilea) и Вашингтоне (1 – Camp Murray, 2 – Fort Lewis, 3 – Yakima Training Center). Стоит отметить, что и американские, и европейские военные учитывают растущую мощь КНР в геополитическом и цифровом

контексте: (источник № 16 [17]: **«Мы разрабатываем трехсторонний подход к Китаю: единство, устойчивость и разделение. Несмотря на то что КНР удалена от евроатлантического региона, Североатлантический союз признает ее растущее влияние**»). Впрочем, эффективность NATO как одного из американоцентричных блоков в АТР/ИТР остается дискуссионной. Во-первых, польза от европейских членов блока остается преимущественно номинальной – они слишком далеко находятся и инвестируют в инновации слишком мало денег (меньше 2% ВВП). Во-вторых, все ресурсы NATO уже сейчас уходят на украинское направление. Вести равную борьбу с китайскими хакерами едва ли получится. Высокие налоги, разветвленная бюрократия, мощное регулирование – все это мешает полноценному развитию цифровых инициатив в странах NATO (к примеру, на 1 миллион человек в КНР и США регистрируются 46 и 37 AI патентов соответственно, в то время как в Германии, Британии, Франции и Италии этот показатель существенно меньше: 12, 6, 4 и 1 [4]. Иными словами, это не Соединенные Штаты активно нуждаются в научно-технической и военной поддержке членов Североатлантического альянса, а наоборот. Страны NATO – балласт, не приносящий США реального влияния.

PBP как американоцентричный институт кибербезопасности в АТР. Partners in the Blue Pacific – формат сравнительно недавний (основан в 2022 году). В отличии от перечисленных выше государств, PBP неформален, то есть не имеет никакой институциональной базы. Встречи представителей Австралии, Британии, Японии, Новой Зеландии и Соединенных Штатов (5 основных членов), а также Канады, ФРГ и Южной Кореи (3 дополнительных членов) носят преимущественно номинальный характер. По своей сущности Partners in the Blue Pacific аналогичен G7. По состоянию на 2025 год, члены альянса имеют общую стратегию кибербезопасности и планируют развитие совместных цифровых центров: (Источник № 17 [12]: **«Стратегия 2050 признает расширенную концепцию безопасности, включающую кибербезопасность в качестве регионального приоритета, и призывает к коллективным действиям по борьбе с киберпреступностью. Partners in the Blue Pacific совместно с тихоокеанскими партнерами учредила конференцию по развитию и координации цифрового потенциала**»). С организационной точки зрения PBP полностью повторяет структуру «втулки и спиц», где ключевым звеном были и остаются Соединенные Штаты. Примечательно, что встречи неформального клуба тоже проходят в США: (Источник № 18 [3]: **«22 сентября в Нью-Йорке (США) в течение примерно 75 минут проходило министерское совещание PBP**»). Все идеи альянса сводятся к слогану «за все хорошее и против всего плохого». Чтобы утвердить верховенство либерально-демократических ценностей западного образца в глобальной сети, члены альянса намерены создать еще один центр кибербезопасности. Основная фишка PBP заключается в тесной кооперации с малыми островными государствами Тихого океана. В планах Partners in the Blue Pacific – осуществлять мониторинг цифрового пространства Меланезии, Микронезии и Полинезии (Вануату, Кирибати, Науру, Ниуэ, Фиджи, Маршалловы острова, Соломоновы

острова, а также ФШМ). Стороны диалога РВР намерены проводить ежегодные конференции по цифровой безопасности с участием представителей этих стран. Примечательно, что киберсаммит Partners in the Blue pacific 2023 года посетили 80 специалистов [7]. Дальше – больше. По крайней мере, так сказано в официальных документах: (источник № 19 [13]: **«Участники обсудили такие перспективные инициативы, как ежегодная конференция по кибернетическому потенциалу Тихоокеанского региона»**). По всей видимости, в ближайшие годы список членов РВР будет расширяться. Чтобы перетянуть малые островные государства Микронезии, Полинезии и Меланезии на свою стороны, сторонники США будут вкладываться в развитие инфраструктурных проектов на их территории. Велика вероятность, что до конца 2020-х годов от имени Partners in the Blue Pacific будут построены совместные тренинговые центры в непосредственной близости от Тайваня и Китая: например, где-то в районе Палау или Марианских островов. Нечто подобное в истории этого региона уже было: с 1944 по 1947 год американские военные прослушивали радиоволны в базе «Paleliu». Схожие инициативы уже в XXI веке Вашингтон намерен претворить в жизнь под эгидой либерально-демократических идей. Реальное будущее Partners in the Blue Pacific туманно. Формат достаточно сырой и не имеет радикальных отличий от уже устоявшихся альянсов вроде AUKUS, QUAD, ANZUS, FIVE EYES и так далее. Весь смысл существования Partners in the Blue Pacific – продвигать американскую гегемонию по принципу «мир может быть многополярным, но под эгидой одного, самого сильного на планете государства, которым точно не должен стать Китай» [1]. Удастся ли РВР как минимум сохраниться, а как максимум заручиться поддержкой новых союзников в, покажет время.

ANZUS как американоцентричный институт кибербезопасности в АТР. Формат АНЗЮС существует с 1951 года. Центральная задача альянса – сдерживание противников США в Тихом океане. Как и в случае NATO, все стороны – Соединенные Штаты, Новая Зеландия и Австралия – несут военные обязанности: (источник № 20 [5. P. 2]: **«Австралия и Новая Зеландия как члены Британского Содружества наций имеют военные обязательства как за пределами, так и в Тихоокеанском регионе»**). Этот касается не только военного, но также научно-технического и информационного сотрудничества: (источник № 21: **«Учитывая тесное сотрудничество в области разведки (АНЗЮС и «ПЯТЬ ГЛАЗ»), кибербезопасности и торговли, существует значительный потенциал для развития комплексной системы сдерживания»** [26. P. 98]. В 2001 и 2003 году страны ANZUS сражались в Афганистане и Ираке на стороне американских военных [27. P. 45]. Спустя четверть века, они борются с противниками США уже в цифровой плоскости: пресекая атаки КНР и параллельно осуществляя собственные.

Заключение.

• Проамериканские альянсы в АТР/ИТР объединяют самые разные страны, но связующим элементом всегда остаются Соединенные Штаты. Главная задача таких блоков – сдерживание цифрового потенциала КНР.

• Представители проамериканских организаций – AUKUS, QUAD, ANZUS, PBP и NATO – регулярно встречаются, чтобы публично заявить о своей обеспокоенности и объявить Китай в качестве киберугрозы.

• Подавляющее большинство официальной документации не содержит конкретных шагов, необходимых для достижения цифрового паритета с Китаем. Если такая информация и имеется, то она зачастую засекречена.

• Риторика членов проамериканских блоков достаточно резкая. Страны QUAD, AUKUS, ANZUD, PBP и NATO открыто упрекают Китай в цифровых амбициях; противостоят КНР они не делами, а словами

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Пале С.Е.** QUAD, AUKUS, PBP: векторы антикитайской политики США и их союзников в Южной части Тихого океана в 2020-е годы // Юго-Восточная Азия: актуальные проблемы развития. 2023 (2) // https://sea.ivran.ru/f/sea2023n259p11-22.pdf.
2. Bundeswehr. Germany Navy Begins Indo-Pacific Deployment. 2024 // https://www.bundeswehr.de/en/organization/navy/news/german-navy-begins-indo-pacific-deployment-2024-5782518.
3. Ministry of Foreign Affairs of Japan. The Partners in the Blue Pacific Ministerial Meeting on Cooperation with Pacific Island Countries. 2022 // https://www.mofa.go.jp/a_o/ocn/shin4e_000049.html.
4. Our World in Data. Annual patent applications related to AI per million people. 2020 // https://ourworldindata.org/grapher/artificial-intelligence-patents-submitted-per-million.
5. Security Treaty between Australia, New Zealand and the United States of America (ANZUS). 1951 // https://www.aph.gov.au/~/media/wopapub/house/committee/jfadt/usrelations/report/appendixb_pdf.ashx.
6. The AUKUS Forum. A new world where innovation and technology rule. 2025 // https://aukusforum.com/opportunities-1.
7. The Cybil Portal. The Partners in the Blue Pacific P4C Outcomes Report. 2024 // https://cybilportal.org/publications/the-partners-in-the-blue-pacific-p4c-outcomes-report/.
8. The Diplomat. La Pérouse 25: France Bolsters Its Strategic Commitments in the Indo-Pacific. 2025 // https://thediplomat.com/2025/01/la-perouse-25-france-bolsters-its-strategic-commitments-in-the-indo-pacific/.
9. The Government of Australia. Joint statement from the leaders of Australia, India, Japan, and the United States. 2024 // https://www.pm.gov.au/media/joint-statement-leaders-australia-india-japan-and-united-states.
10. The Government of Australia. QUAD Foreign Ministers Statement on Ransomware. 2022 // https://www.dfat.gov.au/international-relations/quad-foreign-ministers-statement-ransomware.

11. The Government of Australia. Implementation of the Australia – United Kingdom – United States Partnership (AUKUS). 2022 // https://pmtranscripts.pmc.gov.au/sites/default/files/AUKUS-factsheet.pdf.
12. The Government of Australia. Joint Statement on Partners in the Blue Pacific Foreign Ministers Meeting. 2023 // https://www.dfat.gov.au/news/media-release/joint-statement-partners-blue-pacific-foreign-ministers-meeting-0.
13. The Government of the United Kingdom. Partners in the Blue Pacific (PBP): joint statement. 2022 // https://www.gov.uk/government/news/partners-in-the-blue-pacific-pbp-joint-statement-september-2022.
14. The Ministry of Foreign Affairs of the People's Republic of China. US Hegemony and its perils. 2023 // https://www.fmprc.gov.cn/eng/gjhdq_665435/3376_665447/3432_664920/3434_664924/202302/t20230220_11027664.html.
15. The North Atlantic Treaty Organization (NATO). NATO Strategic Concept. 2022 // https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf.
16. The North Atlantic Treaty Organization (NATO). NATO Allies and Indo-Pacific Partners discuss cybersecurity cooperation. 2024 // https://www.nato.int/cps/po/natohq/news_228454.htm?selectedLocale=en.
17. The North Atlantic Treaty Organization (NATO). NATO 2030: Embrace the change, guard the values. 2021 // https://www.nato.int/nato_static_fl2014/assets/pdf/2021/2/pdf/210204-NATO2030-YoungLeadersReport.pdf.
18. The People's Government of Fujian Province. Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China. 2021 // https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm.
19. The United Nations (UN). The UN norms of responsible state behavior in cyberspace. 2022 // https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.
20. The US Department of Defense. Cyber Issues. 2025 // https://www.state.gov/policy-issues/cyber-issues/.
21. The US Department of Defense. Joint Regional Strategy – East Asia and the Pacific. 2023 // https://www.state.gov/wp-content/uploads/2023/01/JRS_EAP-Asia_06JAN2023_Public.pdf.
22. The US Department of Defense. US relations with China – bilateral relations fact sheet. 2025 // https://www.state.gov/u-s-relations-with-china/.
23. The US Department of Defense. The Quadrilateral Security Dialogue's Path to Institutionalization. 2024 // https://media.defense.gov/2024/May/07/2003458343/-1/-1/1/VIEW%20-%20KUMAR%20AND%20KHAN%20-%20JIPA.PDF.
24. The US Department of Defense. AUKUS: The Trilateral Security Partnership Between Australia, UK and US. 2025 // https://www.defense.gov/Spotlights/AUKUS/.

25. The US Department of Defense. AUKUS Collaboration Advancing Capabilities in Indo-Pacific Region. 2024 // https://www.defense.gov/News/News-Stories/Article/Article/3918579/aukus-collaboration-advancing-capabilities-in-indo-pacific-region-austin-says/.
26. The US Department of Defense. The Role of Deterrence in Australian Strategic Thought: Implications for ANZUS. 2024 // https://media.defense.gov/2024/Sep/10/2003540652/-1/-1/1/JIPA%20-%20FEATURE_RAHMAN_&_GOPAL.PDF.
27. The US Department of Defense. Constructing Like-Mindedness: Australian Contribution to the ANZUS Alliance. 2024 // https://media.defense.gov/2024/Sep/10/2003540649/-1/-1/1/JIPA%20-%20FEATURE_DELL'ERA_&_MARTIN.PDF.
28. The US Embassy in Australia. QUAD leaders' joint statement. 2023 // https://au.usembassy.gov/quad-leaders-joint-statement/.

E.R. OSHCHEPKOV
Research Assistant of the Research and Study Group «ASEAN+, BRICS+, NATO+: Prospects for Asian Integration in the New World Order», Faculty of World Economy & International Affairs, HSE University, Moscow, Russia

US-CENTRIC REGIONAL CYBERSECURITY INSTITUTIONS IN ASIA

As the US-China confrontation in the Asia-Pacific/Indo-Pacific region escalates, bloc alliances are becoming increasingly important. While the PRC tries to rely mainly on its own forces, the US actively utilizes the support of allied states – Japan, Australia, New Zealand, South Korea, and beyond. In addition to economic, military or political confrontation, digital security is coming to the forefront of global politics. Pro-American organizations such as QUAD, AUKUS, ANZUS, PBP and even NATO are working intensively on the implementation of a number of cyber initiatives. This article attempts to analyze and characterize the effectiveness of such alliances based on official documentation published in the first half of the 2020s.

Key words: *Security, Cybersecurity, USA, China, Alliances, QUAD, AUKUS, ANZUS, NATO, PBP.*