Обзорная статья. Исторические науки
УДК 94+327(5)
DOI: 10.31696/2072-8271-2024-2-2-63-381-396

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ РЕШЕНИЕ В СТРАНАХ БОЛЬШОЙ АЗИИ – 2024

Екатерина Михайловна АСТАФЬЕВА [1]

[1] Институт востоковедения РАН, Москва, Россия
katy-ast@yandex.ru, https://orcid.org/0000-0001-8091-407X

Аннотация: В статье представлен обзор докладов международной научной конференции «Проблемы информационной безопасности и их решение в странах Большой Азии», которая состоялась 18 апреля 2024 г. в Институте востоковедения РАН в Москве.

Ключевые слова: *информационная безопасность, кибербезопасность, киберугрозы, глобальные проблемы безопасности, страны Большой Азии*

Для цитирования: *Астафьева Е.М.* Проблемы информационной безопасности и их решение в странах Большой Азии – 2024 // Юго-Восточная Азия: актуальные проблемы развития, 2024, Том 2, № 2 (63). С. 381–396. DOI: 10.31696/2072-8271-2024-2-2-63-381-396

Overview article. Historical science

INFORMATION SECURITY PROBLEMS AND THEIR SOLUTIONS IN THE COUNTRIES OF GREATER ASIA – 2024

Ekaterina M. ASTAFIEVA [1]

[1] Institute of Oriental Studies RAS, Moscow, Russia
katy-ast@yandex.ru, https://orcid.org/0000-0001-8091-407X

Abstract: The article provides an overview of the reports of the international scientific conference “Problems of Information Security and Their Solutions in the Countries of Greater Asia,” which took place on April 18, 2024 at the Institute of Oriental Studies of the Russian Academy of Sciences in Moscow.

Keywords: *information security, cybersecurity, cyber threats, global security issues, countries of Greater Asia*

For citation: Astafieva E.M. Information Security Problems and Their Solutions in the Countries of Greater Asia – 2024. *Yugo-Vostochnaya Aziya: aktual'nyye problemy razvitiya*, 2024, T. 2, № 2 (63). Pp. 381–396. DOI: 10.31696/2072-8271-2024-2-2-63-381-396

18 апреля 2024 г. в Институте востоковедения РАН в смешанном формате состоялась Международная конференция «Проблемы информационной безопасности и их решение в странах Большой Азии».

Организаторами конференции выступили Центр Юго-Восточной Азии, Австралии и Океании ИВ РАН, Лаборатория цифровых исследований современного Востока ИВ РАН, Информационное агентство «Караван Инфо».

В работе конференции приняли участие более 30 человек. Было представлено более 20 докладов, посвященных актуальным проблемам информационной безопасности и путям их решения в странах Большой Азии.

С докладами выступили ученые и молодые специалисты из Института востоковедения РАН, Института Китая и современной Азии РАН, Института стран Азии и Африки МГУ имени М.В. Ломоносова, Института мировой экономики и международных отношений им. Е.М. Примакова РАН, Российского университета дружбы народов им. Патриса Лумумбы, Национального исследовательского университета «Высшая школа экономики». ФГБОУ ВО «Комсомольский-на-Амуре государственный университет», Финансового университета при Правительстве РФ, Института истории и международных отношений Саратовского национального исследовательского государственного университета им. Н.Г. Чернышевского, Санкт-Петербургского государственного университета, МИД Республики Казахстан, Делийского университета, Белорусского государственного университета, Болонского университета.

Работа конференции проходила в рамках трех панелей. Первые две панели: рабочий язык – русский, модератор – к.и.н. Е.М. Астафьева, третья панель: рабочий язык – английский, модератор – к.и.н. А.А. Гарин.

С приветственным словом к участникам и гостям конференции обратился заместитель директора ИВ РАН, доктор исторических наук Валентин Цуньлиевич Головачев, он отметил актуальность темы и своевременность проведения конференции, высоко оценил ее практическую значимость.

С первым докладом 1-й панели на тему «*E-Governance в национальных стратегиях обеспечения кибербезопасности в странах АТР*» выступил **О.А. Филатов** (НИУ ВШЭ). Доклад был подготовлен совместно с **Г.Ю. Никипорец-Такигава** (НИУ ВШЭ). В выступлении были рассмотрены подходы ряда стран региона АТР к вопросам раз-

вития
e-governance как части национальной стратегии кибербезопасности, а также проанализирована вариативность понимания киберпространства как глобального/национального, вытекающие из данного выбора: определение границ киберпространства, подпадающего под национальную юрисдикцию; содержание программ по управлению киберпространством на национальном уровне; идентификация акторов, вызовов и угроз, влияющих на гармоничное развитие национального киберпространства.

Докладчик сделал выводы, что: 1) национальные стратегии кибербезопасности обнаруживают пересечения в сходном понимании беспрецедентного темпа роста киберугроз, сопровождающих развитие текущего политического момента; 2) в связи с данным пониманием общим является и осознание странами региона необходимости защиты национального кибепространства; 3) в зависимости от степени политической самостоятельности той или иной страны в национальных стратегиях различным образом трактуется роль государства в решении данной задачи, а также желательности и/или необходимости киберсуверенитета, то есть независимости государственного контроля над национальным интернетом, запрета вмешательства других государств во внутренние дела, связанные с цифровой безопасностью и внутренней цифровой политикой.

В заключение Олег Александрович указал, что делегирование управления киберпространством на надстрановый уровень становится все менее популярной идеей. По пути КНР, впервые разработавшей разветвленную стратегию и идеологию управления национальным сегментом мирового киберпространства, готовы двигаться другие представители региона. Данная готовность реализуется в конкретных мерах защиты от киберугроз и кибератак, разработке и уточнении, исходя из национальных интересов, определения киберугроз, национальных границ киберпространства и других базовых элементов политики кибербезопасности и управления киберпространством.

Е.С. Коренев (СГУ) выступил с докладом *«Взаимодействие НАТО с государствами Юго-Восточной Азии и Южно-Тихоокеанского региона в сфере информационной безопасности»*. В своем выступлении докладчик указал, что в настоящее время Североатлантический альянс уделяет повышенное внимание вопросам реагирования на угрозы и вызовы в киберпространстве. НАТО в рамках своих многочисленных партнёрств по всему миру налаживает взаимодействие с теми партнерами, которые обладают высококвалифициро-

ванными специалистами и прорывными технологиями в информационной сфере. Особую роль в этом контексте играют отношения НАТО с государствами ЮВА и ЮТР. Уровень взаимодействия Альянса с партнерами может в данном случае довольно сильно отличаться.

Докладчик проанализировал состояние сотрудничества Организации Североатлантического договора с государствами АСЕАН в информационной сфере, которое находится на начальной стадии. Особое внимание было уделено оценке взаимодействия Альянса в киберпространстве с Австралией и Новой Зеландией в контексте попыток создать информационную инфраструктуру для возможного сдерживания Китая в будущем.

Евгений Сергеевич отметил, что помимо развития отношений в многостороннем формате, отдельные государства-члены НАТО также стремятся к тому, чтобы установить долгосрочное партнёрство с государствами ЮВА и ЮТР в сфере информационной безопасности. Докладчик проанализировал активность США и других лидеров Альянса (Великобритания, Германия, Франция) на данном направлении и сделал вывод о том, что это не просто позволит усилить позиции Альянса в киберпространстве, но и в той или иной мере в среднесрочной перспективе будет способствовать осуществлению сдерживания Китая и отчасти России.

В заключение Е.С. Коренев указал, что можно прогнозировать наращивание активности Организации Североатлантического договора в ближайшем будущем на данном направлении.

Д.С. Тасмагамбетова («Караван Инфо», Финуниверситет) представила доклад *«Формирование медиапространства в Центральной Азии: роль политических акторов, их влияние на политические процессы региона; построение информационного суверенитета»*. Дамиля Сулейменовна отметила, что формирование медиапространства в Центральной Азии (ЦА) является сложным процессом и связано с развитием технологий, культурными особенностями и политической ситуацией в регионе. Также она указала, что интернет изменил само понятие «медиапространство», рассказала о медиапредпочтениях населения стран ЦА, о роли политических акторов в этом процессе, о силах, которые способны оказать влияние на политические процессы региона, о проблемах переформатирования информационного поля, о том, как достигнуть информационного суверенитета в странах ЦА и о роли России в выстраивании совместного благоприятного информационного климата со странами ЦА и предпринятых действиях.

Докладчик отметила, что с развитием информационных технологий (ИТ) в ЦА появляются новые возможности для свободного обмена информацией, а в последние годы наблюдается увеличение числа независимых онлайн-медиа и блогеров, которые играют важную роль в информационном пространстве региона, что делает задачу контроля медиапространства более сложной для политических акторов. Доминирование государственных телеканалов серьезно нарушено распространением альтернативных источников новостей. Резкий рост использования смартфонов и повышение уровня проникновения интернета способствуют этому процессу, поскольку молодые поколения почти полностью полагаются для получения информации на социальные сети.

Сейчас проводятся исследования, мониторинг, контент-анализы СМИ, выявляются основные информационные поводы, характеризующие проблематику в медиапространстве ЦА. Результаты исследования показывают, что публикуемые сообщения в интересующем сегменте медиапространства в большей степени связаны с вопросами политического характера. Публикации, касающиеся историко-культурного наследия народов ЦА, его сохранения и популяризации, единства культурного пространства, единства народов России и стран ЦА занимают незначительное место.

Роль политических акторов в этом процессе, несомненно, велика. Они могут использовать медиа для достижения своих политических целей, в формировании общественного мнения, контролируя информационное пространство. Но существуют силы, которые способны оказать влияние на политические процессы региона.

Дамиля Сулейменовна сообщила, что Госдепартамент США запускает программы через федеральное Агентство по международному развитию — *USAID*, которое играет значительную роль в формировании информационной, внутренней и внешней политики в странах ЦА. В частности, в рамках визита в ЦА администратора *USAID* Саманты Пауэр, была объявлена новая региональная программа, направленная на поддержку независимых средств массовой информации и борьбу с дезинформацией. Но эта работа организации сводилась к вмешательству во внутренние дела государства и влиянию на политические процессы.

Роль политических акторов в формировании медиапространства в ЦА остается значительной, но с развитием технологий и активизацией гражданского общества их контроль становится менее эффективным. Важно давать приоритет информационному обмену между

региональными СМИ и Россией, чтобы обеспечить разнообразие мнений граждан региона. Помощь РФ странам ЦА развивать медиа и информационные технологии, обучать журналистов и специалистов в этой области, поддерживать независимые СМИ – все это будет способствовать повышению уровня информированности населения, свободному доступу к информации, роли и важности информационного суверенитета региона, – подчеркнула докладчик. Необходимо реализовать мероприятия для достижения информационного суверенитета в странах Центральной Азии: создание законодательной базы и национальной политики по информационной безопасности; развитие и модернизация информационно-коммуникационных технологий (ИКТ); обучение и повышение квалификации специалистов в области ИТ; укрепление международного сотрудничества в области информационной безопасности, борьба с киберугрозами; повышение информационной грамотности населения, качественная оценка в контексте геополитики – все это основа для политической стабильности стран ЦА, – сказала в заключение своего выступления Д.С. Тасмагамбетова.

А.А. Гарин (ИВ РАН) выступил на тему *«Информационное давление как аспект соперничества США и Австралии с Китаем в Южной Пацифике (2017–2023)»*. Артём Алексеевич сообщил, что США и Австралия проводят психологические операции и кампании, чтобы противодействовать расширению влияния Китая в Южной Пацифике. Вашингтон и Канберра пытаются привлечь внимание к потенциальным рискам и негативным последствиям сотрудничества Китая с государствами региона, используя для этого средства массовой информации и социальные сети (в т.ч. для конструирования и распространения образа «угрозы» со стороны Пекина).

Докладчик представил количественные доказательства координации информационных операций со стороны СМИ Австралии и США, проанализировал их конкретные антикитайские психологические операции, а также обозначил риски и последствия подобных действий.

С докладом *«Подходы КНР к глобальному управлению в информационном пространстве: перспектива стран Юго-Восточной Азии»* выступил **М.С. Рамич** (РУДН). Мирзет Сафетович указал, что глобализация и цифровизация определили общий курс на консолидацию ресурсов в технологической сфере и сместили фокус международной конкуренции в информационное и киберпространство. КНР, выступая одним из локомотивов мирового технологического развития, поддерживает идею цифрового (кибер) суверенитета предлагая реформиро-

вание системы глобального управления в киберпространстве и новый подход к формированию техноэкономических блоков в контексте «декаплинга» и «транзита власти».

Докладчик отметил, что на глобальном уровне прослеживается конкуренция между многосторонним подходом, который поддерживается КНР, РФ и развивающимися странами и мультистейкхолдеризмом, который поддерживается США, ЕС и развитыми странами. Основным полем для реализации китайской внешней политики в данной сфере становятся международные институты, формирующие правила поведения и международно-правовые режимы.

На уровне отдельных регионов особенностью китайской внешней политики является продвижение национальных поставщиков телекоммуникационных услуг и цифровых продуктов в соответствии с Национальной стратегией информатизации, принятой в 2016 г. В данной плоскости прослеживается конкуренция техноэкономических блоков, которые формируются в контексте «декаплинга», санкционного давления и иных торговых ограничений.

В заключение М.С. Рамич подчеркнул, что в информационном пространстве Китай придерживается подхода цифрового суверенитета, выступая против всех видов вмешательства во внутренние дела государства, в т.ч. через сеть Интернет. В данной сфере предпринимаются попытки повысить эффективность работы в информационном пространстве для создания позитивного образа государства и противодействия дезинформации, направленной против КНР и ее международных проектов.

С докладом на тему *«Вопросы информационной безопасности в работе Совещания министров обороны АСЕАН-плюс»* выступила **К.Г. Муратшина** (ИВ РАН). В своем выступлении Ксения Геннадьевна проанализировала, как вопросы кибербезопасности представлены в работе важной структуры взаимодействия АСЕАН с внешними партнерами – Совещания министров обороны АСЕАН-плюс. Докладчик проанализировала деятельность созданной в 2016 г. специализированной экспертной рабочей группы СМОА-плюс и реализацию на практике заложенных АСЕАН принципов сотрудничества в этой структуре, а также отражение кибер-тематики в позициях сторон.

С.А. Верхоломов (КнАГУ) представил доклад *«Информационная война против Китая в странах Юго-Восточной Азии и Тихого океана»*. Сергей Александрович указал, что во многих странах АСЕАН и Тихого океана правящие элиты используют антикитайскую риторику для формирования собственной парадигмы в регионе. Нема-

ловажную роль в ведении информационной войны против Китая играют страны Запада во главе с США, а в условиях цифровой революции информационная война приобретает новый характер, перемещаясь в киберпространство.

С докладом *«Потенциал сотрудничества Россия-АСЕАН в деле обеспечения цифрового суверенитета»* выступил **П.С. Шатерников** (ИКСА РАН). Докладчик отметил, что страны Юго-Восточной Азии пользуются в основном китайским и американским софтом в рамках цифровизации и информатизации. Несмотря на удобство и многолетний опыт использования таких программ, возникает угроза утраты цифрового суверенитета или, как минимум, цифрового шантажа со стороны производителей таких программ. Защитой от подобных действий может служить диверсификация поставщиков антивирусных, поисковых и других продуктов и здесь свои цифровые решения может предложить Россия. Продукты Лаборатории Касперского и Яндекса по праву считаются одними из лучших в мире, а сама Россия не заинтересована в покушениях на цифровой суверенитет стран АСЕАН, – подчеркнул Павел Сергеевич.

А.Р. Гараева (НИУ ВШЭ) выступила с докладом *«Партнерство РК — АСЕАН для региональной цифровой трансформации»*. Айсылу Рафаеловна подчеркнула, что на современном этапе форматы и инициативы многостороннего сотрудничества, координатором которых выступает Ассоциация стран Юго-Восточной Азии (АСЕАН), проходят процесс глубокой трансформации. Несмотря на усиление элементов конфронтации в отношениях между наиболее влиятельными азиатско-тихоокеанскими акторами, асеаноцентричные площадки и проекты остаются институциональным каркасом многостороннего регионального сотрудничества, и снижение их эффективности самым пагубным образом скажется на состоянии экономических обменов и поддержании угроз безопасности в контролируемых рамках. В связи с этим всё большее количество игроков стремится увеличить своё влияние на них.

Одним из традиционных партнеров Ассоциации является Республика Корея, в отношениях с которой многостороннее сотрудничество традиционно занимало особое место. В начале 1990-х годов нацеленность АСЕАН на создание АТССБ и АРФ было в значительной степени обусловлено необходимостью формирования многостороннего сотрудничества для снижении остроты ядерной проблемы на Корейском полуострове (сейчас Форум остается единственной азиатско-тихоокеанской площадкой многостороннего диалога, в котором

Пхеньян принимает участие), а у истоков политики АСЕАН по формированию Восточноазиатского саммита стоял Ким Дэ Чжун, в 1998 г. выдвинувший предложение об активизации сотрудничества между странами АСЕАН+3. В настоящие дни, являясь технологическим хабом региона, РК стремиться лоббировать свои проекты в области ИКТ. Примером, может служить проект «Кибер щит АСЕАН (ACS)», который направлен на укрепление кибербезпасности Ассоциации. В своем докладе А.Р. Гараева предприняла попытку оценить заинтересованность южнокорейского правительства в решение вопросов цифровой безопасности АСЕАН.

С докладом *«Роль Сингапура в укреплении кибербезопасности в АСЕАН»* выступил **Ф.А. Касенов** (МИД Республики Казахстан). Докладчик отметил, что Сингапур играет лидирующую роль в области кибербезопасности в АСЕАН, демонстрируя стратегический подход к защите своего цифрового пространства и активно содействуя укреплению кибербезопасности во всем регионе. Сингапур занимает ключевое место в формировании региональной стратегии кибербезопасности АСЕАН, используя свой опыт и ресурсы для поддержки соседних стран в разработке и реализации собственных стратегий безопасности киберпространства. Это сотрудничество способствует разработке общих стандартов и протоколов безопасности, повышает уровень осведомленности и готовности к противодействию киберугрозам на региональном уровне, – особо подчеркнул Файзрахман Айткалиевич.

Доклад на тему *«Особый объект обеспечения информационной безопасности островной Юго-Восточной Азии – подводные кабели»* представил **А.А. Рогожин** (ИМЭМО РАН). Александр Александрович сообщил, что в настоящее время по подводным оптоволоконным кабелям передаётся 95% мирового интернет-трафика. По дну океанов проложено более 550 кабелей общей протяжённостью 1,3 млн км. Немалая часть их сосредоточена в акватории, охватывающей страны островной ЮВА, и обеспечивает не только региональную связанность (*connectivity*), но и информационный транзит для стран, расположенных вне ЮВА, в первую очередь, Китая, Японии и Австралии.

В связи со стремительным развитием в странах островной ЮВА систем искусственного интеллекта, больших данных, технологий мобильных сетей пятого поколения (*5G*), облачных вычислений и Интернета вещей необходимо поддержание устойчивой и надёжной связи. С учётом того, что кабельная связь дешевле и надёжнее спутниковой, Генеральный план АСЕАН в области цифровых технологий на период до 2025 г. рассматривает подводные кабели как важнейшую

инфраструктуру, жизненно важную для быстро развивающейся цифровой экономики региона.

Подводные кабели уязвимы перед природными и техногенными опасностями. Немало проблем всё чаще возникает при обеспечении эксплуатационной надёжности подводных кабелей в режиме 24/7. Однако геостратегическая конкуренция повысила и риск шпионажа и диверсий. Неразрешённые территориальные споры в Южно-Китайском море также привлекли внимание к подводным кабелям, поскольку конфронтация между Китаем и другими странами региона, становится очевидной и реальной опасностью для подводных кабелей. Ситуация осложняется и неурегулированностью в международном праве вопросов обеспечения безопасности подводных кабелей, – указал в заключение А.А. Рогожин.

А.А. Соколов (ИВ РАН) выступил на тему *«Информационная безопасность в современном Вьетнаме»*. Анатолий Алексеевич отметил, что в последние годы Вьетнам продемонстрировал успешные результаты в управлении экономикой, активно осуществляет цифровую трансформацию правительства, экономики и общества. Развитие индустрии информационных технологий и электронной промышленности является главным направлением при реализации национальной политики промышленного развития.

Однако в области сетевой и кибербезопасности Вьетнам до сих пор испытывает большие проблемы. В 2019 г. в СРВ был принят Закон о кибербезопасности, в соответствии с которым предприятия, оказывающие соответствующие услуги на территории страны, должны размещать цифровые хранилища данных интернет-пользователей на территории этой страны, а иностранные компании должны создавать представительства на территории Вьетнама.

Между Россией и Вьетнамом подписан ряд межправительственных соглашений по вопросам сотрудничества в сфере информационной безопасности, целостности и устойчивости функционирования информационной инфраструктуры, в том числе сетей связи специального назначения. Вьетнам сможет улучшить ситуацию с информационной безопасностью, а Россия – увеличить экспорт технологий и оборудования, – сделал вывод Анатолий Алексеевич.

С докладом *«Влияние киберпреступности на внешнюю и внутреннюю политику Камбоджи»* выступил **Г.Н. Кучеренко** (ИВ РАН / ИКСА РАН). Григорий Николаевич сообщил, что размах киберпреступности в Камбодже привёл к тому, что на проблему обратили внимание как камбоджийские власти, так и международное сообщество в

лице отдельных стран, включая Китай и США, а также наднациональные объединения. О масштабе данного вида преступности в стране говорит тот факт, что, по подсчётам индийской газеты *Indian Express*, в Камбодже на данный момент в рабстве содержится более 5 тыс. индийских граждан. Из них 250 было недавно спасено министерством иностранных дел Индии, однако этого явно недостаточно. Данная новость особенно примечательна тем, что в прошлом году индонезийские власти сообщили о спасении и репатриации 41 гражданина, попавшего в Камбодже в ловушку интернет-мошенников. Как сообщило правительство Индонезии, с января по июль 2023 г. в Камбодже было зарегистрировано 515 случаев, «связанных с мошенничеством в Интернете». Интерпол характеризует ситуацию в стране как «мошенничество в промышленных масштабах, основанное на торговле людьми». Очевидно, что происходящее является одним из факторов, негативно влияющих на отношения королевства со своими партнёрами.

В то же время, правительство Камбоджи хоть и старается открещиваться от статуса страны, в которой держат «цифровых рабов», оно всё же вынуждено реагировать на ситуацию. В июне 2023 г. министерство внутренних дел страны объявило об официальном начале реализации «Стратегического плана развития цифровых технологий на 2023–2027 годы», направленного на борьбу с киберпреступностью и развитие цифрового сектора в Камбодже.

В.Н. Колотов (СПбГУ) выступил на тему *«Проблемы информационной безопасности во Вьетнаме: история и современность»*. Владимир Николаевич отметил, что проблемы информационной безопасности (в широком смысле когнитивной безопасности) неоднократно становились критически важными в истории Вьетнама и продолжают оставаться одной из ключевых проблем обеспечения национальной безопасности в современности. Еще выдающийся полководец Древнего Китая Сунь-цзы в своем знаменитом трактате «Законы войны» самый высший приоритет закреплял за т.н. «замыслами» 謀. В периоды, когда политическая элита была неспособна распознать коварные замыслы противника, страна теряла независимость, а когда элита находилась в хорошей интеллектуальной форме, страна восстанавливала и успешно защищала независимость.

В востоковедении развитое в Китае искусство применения стратегем с целью получения когнитивного преимущества получила название стратегематики. В новейшее время восстановление независимости Вьетнама было теснейшим образом связано с сочетанием технологий Коминтерна с законами войны Сунь-цзы, чем занимался

лично национальный лидер Вьетнама Хо Ши Мин. В настоящее время в связи с развитием технологий добавилась новая операционная среда – киберпространство и т.н. ИИ, который однако не может существовать без естественного, что еще больше актуализирует традиционные законы войны времен Сунь-цзы и когнитивное противоборство на уровне замыслов.

При осуществлении преступлений в области т.н. информационных технологий осуществляется традиционное агентурное проникновение или использование социального инжиниринга с целью обмана жертвы. В современном Вьетнаме когнитивное противоборство идет с переменным успехом, что проявляется в усилении борьбы за власть.

В ходе своего выступления докладчик привел конкретные примеры побед и поражений на когнитивном фронте.

С докладом *«Подходы к обеспечению информационной безопасности в Малайзии»* выступила **Е.В. Кочеткова** (ИВ РАН). Екатерина Вячеславовна отметила, что в последние годы страны Азиатско-Тихоокеанского региона все больше осознают растущие угрозы в киберпространстве и принимают ответные меры. Малайзия не исключение, и, по имеющимся данным, правительство, а также различные компании сталкиваются с растущими и все более изощренными кибератаками. Главной задачей Малайзии в этой связи стало повышение безопасности информации в десяти ключевых областях, включая здравоохранение, банковское дело и финансы, водоснабжение, энергетику, информацию и коммуникации, транспорт, оборону и безопасность. Помимо реализации этих инициатив у себя дома, Малайзия также сотрудничает с другими странами. «Лаборатория Касперского» сформировала дистрибьюторскую сеть в Малайзии и Индонезии для работы с решениями на основе операционной системы *KasperskyOS*. Эксклюзивным поставщиком этих решений была выбрана местная технологическая компания *Aswant Solution*.

Докладчик особо отметила, что правительство Анвара Ибрагима признает критическую важность проблем кибербезопасности и киберпреступности и стремится реализовать множество инициатив, направленных на защиту своих граждан и национальную безопасность.

Д.С. Панарина (ИВ РАН) представила доклад *«Киберпреступность и кибербезопасность на Филиппинах: современные тенденции и проблемы»*. В своем выступлении Дарья Сергеевна рассмотрела проблемы киберпреступности, свойственные для Филиппин: в каких сферах жизнедеятельности они наиболее выражены, с чем связаны массовые киберпреступления, что делает их возможным, кем и в каких

масштабах осуществляются киберпреступления и какие меры требуются от правительства Филиппин на общегосударственном уровне, чтобы снизить степень киберпреступности в стране. Докладчик также отдельно коснулась насущного вопроса: как относятся к кибербезопасности в эшелонах власти и в филиппинском обществе в целом, насколько население Филиппин грамотно в вопросах киберпреступлений, и, соответственно, насколько оно защищено или нет от различного рода мошенничества, осуществляемого с помощью современных технических средств и гаджетов.

Д.С. Панарина проанализировала каким образом возможно бороться с киберпреступностью как «сверху» (на уровне властей), так и «снизу» (на уровне простых граждан страны). В частности, докладчик останавливается и на том, как 2 года карантина на Филиппинах во время пандемии коронавируса COVID-19 повлияли на распространение различных электронных услуг и как это, в свою очередь, способствовало росту киберпреступности, в том числе, на бытовом уровне.

Также в докладе была затронута «детская проблема» в рамках кибербезопасности, когда жертвами киберпреступников и мошенников становятся дети и подростки. Докладчик привела самые громкие примеры киберпреступлений широкого масштаба, произошедшие на Филиппинах за последние годы.

С докладом *«Проблемы информационной безопасности в Индонезии»* выступила **О.Л. Петрова** (ИВ РАН). Ольга Леонидовна отметила, что Индонезия имеет самую быстрорастущую цифровую экономику в Юго-Восточной Азии. Ожидается, что этот рост продолжится, поскольку правительство поддерживает развитие цифрового бизнеса и поощряет малые и средние предприятия использовать все новые информационные технологии (ИТ). Быстрый рост цифровой индустрии увеличил необходимость в более совершенных и комплексных правилах кибербезопасности и защиты данных. В отчете ООН за 2018 г. Индонезия была отнесена к странам со средним и высоким индексом развития цифровых услуг и сервисов. А по данным отчета международного союза электросвязи (за 2020 г.) Индонезия занимала 31 место по индексу кибербезопасности в мире, поднявшись на 10 пунктов по сравнению с 2018 г.

Тем не менее, из-за нехватки специалистов в сфере ИТ, в Индонезии нет адекватной защиты от кибератак. Согласно исследованиям, количество случаев взлома увеличивается с каждым годом, регулярно происходят утечки данных. В первом квартале 2022 г. в Индонезии произошло более 11 млн кибератак, что на 22% больше, чем в 2021 г.

Правительство ведет активную работу по улучшению киберустойчивости страны за счет использования проверенных мировых практик и сотрудничества с другими странами.

Е.С. Беседин (ИМЭМО РАН) выступил на тему *«Борьба с киберпреступностью в Индонезии: правовая база и правоприменительная практика»*. В своем докладе Егор Сергеевич проанализировал проблемы успешности политики Республики Индонезия по борьбе с киберпреступностью в контексте действующего законодательства. Докладчик обратился к рассмотрению основных нормативно-правовых актов и государственных программ, регулирующих деятельность полномочных органов Республики Индонезия в сфере защиты государственных и частных интересов от киберугроз, а также проанализировал конкретные действия по реализации мер защиты от киберпреступлений.

По мнению Е.С. Беседина, представляется возможным утверждать, что в Индонезии создана обширная правовая база, регулирующая актуальные аспекты борьбы с киберпреступностью: документы затрагивают как общие вопросы обеспечения кибербезопасности, так и частные сюжеты противостояния киберпреступлениям в уязвимых областях (например, в сфере здравоохранения). Особое внимание обращено на круг институтов, обеспечивающих борьбу с киберугрозами: так, существование BSSN, как профильного компетентного органа, позволяет говорить о высоком уровне внимания правительства к рассматриваемой проблеме. Тем не менее, детальный анализ новостных сводок, заявлений официальных лиц и статистических данных даёт понять, что на фоне галопирующего роста цифровой экономики Республики Индонезия не представляется возможным обеспечить достаточный уровень защиты критической инфраструктуры и интересов частных агентов от действий киберпреступников (к примеру, в 2022 г. было зафиксировано около миллиарда аномалий, которые можно трактовать как результаты кибератаки), что поднимает вопрос о перспективах эволюции системы защиты от киберугроз, основными направлениями которой должны стать повышение осведомленности об угрозе киберпреступности и повышение уровня квалификации специалистов в данной сфере.

С докладом на тему *«Сингапур: эволюция национальной стратегии кибербезопасности»* выступила **Е.М. Астафьева** (ИВ РАН). В своем выступлении Екатерина Михайловна, в частности, обратилась анализу Закона о кибербезопасности, основных направлений деятельности Агентства кибербезопасности Сингапура (CSA), новых стандар-

тов для разработчиков приложений и руководящих принципов для телекоммуникационных компаний (TELCO), а также новых инициатив, направленных на то, чтобы сделать цифровое пространство в Сингапуре более инклюзивным и безопасным.

В рамках работы третьей панели выступили: **Шашанк С. Патель** (Делийский университет, Нью-Дели, Индия) на тему *«AI Equilibrium in Greater Asia: Remapping Politico-Digital Sphere»;* **К.И. Ярмошук** (Белорусский государственный университет, Беларусь) с докладом *«Overview of Australia's Cybersecurity Framework»*; **Акаш Саху** (руководитель программы Kubernein Initiative, Индия) на тему *«Changing Cybersecurity Landscape in Asia: Analysing India's role»*; **Л.В. Кошелева** (Болонский университет) с докладом *«China's Approach to Information Security»*. В докладах указывалось, что в большинстве стран политические процессы в основном определяются национальными интересами, а не убеждениями граждан. В области международных отношений происходят значительные изменения благодаря приложениям искусственного интеллекта, влияющим на старые практики дипломатического сотрудничества. Указывалось, что нестабильность на Ближнем Востоке является отличным примером для понимания последствий, которые оказывают технологии. По сути, в регионе Большой Азии происходит около 19 невооруженных внутринациональных конфликтов, широко распространившихся после вступления в технологическую гонку.

А.А. Гарин (ИВ РАН) выступил с заключительным докладом на тему *«Building a Media Corridor in Southeast Asia and Pacific Islands as the Key to Ensuring Information Security in the Asia-Pacific»*. Артём Алексеевич отметил, что роль СМИ, как средства укрепления взаимопонимания и сотрудничества в эпоху трансформации региональной архитектуры в АТР, важна как никогда. Это особенно актуально для Юго-Восточной Азии и Океании – динамичных субрегионов с большим потенциалом. Создание медиа-коридоров здесь представляет собой новаторскую попытку использовать возможности информационно-коммуникационных технологий (ИКТ) для укрепления региональной дружбы и взаимопонимания. Эффективный обмен информацией позволит обеспечить более полное и детальное понимание региональных проблем, а также совместно бороться с распространением ложной информации, – подчеркнул докладчик.

А.А. Гарин проанализировал перспективы создания медиа-коридоров, имеющиеся для этого условия, будущие сферы взаимодействия и потенциал участия России в соответствующих усилиях.

Видео конференции доступно на канале Центра в Rutube:
https://rutube.ru/video/c866ea0446466ce0400577b970a9246e/

ИНФОРМАЦИЯ ОБ АВТОРЕ

АСТАФЬЕВА Екатерина Михайловна, кандидат исторических наук, старший научный сотрудник Центра ЮВА, Австралии и Океании ИВ РАН, Москва, Россия

Статья поступила в редакцию 30.04.2024;
одобрена после рецензирования 15.05.2024;
принята к публикации 31.05.2024.

INFORMATION ABOUT THE AUTHOR

Ekaterina M. ASTAFIEVA, PhD (Hist.), Senior Researcher at the Center for Southeast Asia, Australia, and Oceania Studies, IOS RAS, Moscow, Russia

The article was submitted 30.04.2024;
approved 15.05.2024;
accepted to publication 31.05.2024.