**Научная статья. Исторические науки**
**УДК** 327(592.3)
**DOI:** 10.31696/2072-8271-2024-2-2-63-208-220

# РОЛЬ СИНГАПУРА В УКРЕПЛЕНИИ КИБЕРБЕЗОПАСНОСТИ В АСЕАН

**Файзрахман Айткалиевич КАСЕНОВ** [1]

[1] МИД Республики Казахстан, ИВ РАН, Москва, Россия
faizrakhman@gmail.com, https://orcid.org/0000-0002-4759-012X

***Аннотация:*** 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.

***Ключевые слова:*** *Сингапур, АСЕАН, сотрудничество, киберугрозы, кибербезопасность*

**Для цитирования:** Касенов Ф.А. Роль Сингапура в укреплении кибербезопасности в АСЕАН // Юго-Восточная Азия: актуальные проблемы развития, 2024, Том 2, № 2 (63). С. 208–220. DOI: 10.31696/2072-8271-2024-2-2-63-208-220

**Original article. Historical science**

# THE ROLE OF SINGAPORE IN STRENGTHENING CYBERSECURITY IN ASEAN

**Faizrakhman A. KASENOV** [1]

[1] MFA of the Republic of Kazakhstan, IOS RAS, Moscow, Russia,
faizrakhman@gmail.com, https://orcid.org/0000-0002-4759-012X

***Abstract:*** Singapore plays a leading role in the field of cybersecurity in the ASEAN, demonstrating a strategic approach to protecting its digital space and actively contributing to the strengthening of cybersecurity in the entire region. Singapore occupies a key place in the formation of an ASEAN cybersecurity strategy, using its experience and resources to support neighboring countries in the development and implementation

of their own cybersecurity strategies. This cooperation contributes to the development of obstructing standards and security protocols, increases the level of awareness and readiness to counteract cyberosis at the regional level.

***Keywords:*** *Singapore, ASEAN, Cooperation, Cyberosis, Cybersecurity*

For citation: Kasenov F.A. The Role of Singapore in Strengthening Cybersecurity in ASEAN. *Yugo-Vostochnaya Aziya: aktual'nyye problemy razvitiya*, 2024, T. 2, № 2 (63). Pp. 208–220. DOI: 10.31696/2072-8271-2024-2-2-63-208-220

В последние десятилетия мир наблюдает беспрецедентный переход к цифровизации во всех сферах – от экономики и управления до образования и личных коммуникаций. Этот глобальный сдвиг активизировал использование информационных технологий, делая интернет и цифровые сервисы неотъемлемой частью повседневной жизни миллиардов людей.

С развитием цифровой экономики, электронной коммерции, облачных технологий и социальных сетей, важность надежной защиты данных, информационных систем и сетевых инфраструктур стала особенно актуальной. Эта потребность породила всемирный интерес к кибербезопасности – области, занимающейся защитой компьютерных систем и сетей от кибератак, несанкционированного доступа и других угроз цифрового пространства.

Угрозы кибербезопасности эволюционировали вместе с развитием технологий, превращаясь из относительно простых вирусов и троянов в сложные и многоуровневые кибератаки, включая фишинг, DDoS-атаки, шпионское ПО, вредоносные программы, направленные на мошенничество и кражу данных. Эти атаки могут быть направлены на крупные корпорации, малый и средний бизнес, правительственные органы и даже на инфраструктуру критической важности, такую как энергетические сети, транспорт и здравоохранение.

Воздействие киберугроз на мировую экономику огромно и продолжает расти. По оценкам Исследовательского центра кибербезопасности *Cybersecurity Ventures*, глобальный ущерб от киберпреступлений может достигнуть более 12 трлн долл. США к 2025 г., что в четыре раза превышает уровень 2015 г. Это не только прямые финансовые потери от кражи средств и нарушения работы систем, но и косвенные издержки, связанные с потерей доверия клиентов, ущербом репутации и затратами на восстановление после атак.

Кибербезопасность становится все более важной не только для обеспечения защиты данных и инфраструктур, но и как средство поддержания экономической стабильности и безопасности на глобальном уровне. Стратегии кибербезопасности и международное сотрудничество в этой области играют ключевую роль в предотвращении киберугроз и минимизации их воздействия на мировую экономику, подчеркивая необходимость глобальных усилий для борьбы с киберпреступностью.

Цифровая экономика АСЕАН, объединяющая десять стран Юго-Восточной Азии, является одной из самых быстрорастущих в мире. По оценкам, к 2025 г. размер цифровой экономики региона может достичь 300 млрд долл. США, что свидетельствует о значительном потенциале для экономического роста и интеграции[1]. Этот рост во многом обусловлен активным внедрением цифровых технологий в бизнесе, образовании, здравоохранении и государственном управлении. Увеличение объема онлайн-торговли, развитие стартапов в сфере технологий, а также активное использование мобильного интернета и социальных сетей способствуют динамичному развитию цифровой экономики в регионе.

Однако вместе с возможностями, которые предоставляет цифровизация, возникают и новые вызовы, особенно в области кибербезопасности. С учетом того, что экономика АСЕАН становится всё более интегрированной и зависимой от цифровых технологий, уязвимость перед киберугрозами растет. Кибератаки могут привести к утечке личных данных, финансовым потерям, нарушению работы критически важных инфраструктур и подорвать доверие к цифровым услугам, что, в свою очередь, замедлит экономическое развитие и интеграцию в регионе.

В контексте этих вызовов кибербезопасность становится не просто технологической необходимостью, но и ключевым фактором устойчивого развития. Защита данных, информационных систем и сетевых инфраструктур является основой для сохранения конфиденциальности, целостности и доступности информации, что крайне важно для бизнеса, правительств и граждан. Укрепление мер кибербезопасности позволяет не только предотвращать потери от кибератак, но и поддерживать доверие населения к цифровым инновациям, что способствует дальнейшему развитию цифровой экономики.

Для обеспечения устойчивого развития цифровой экономики АСЕАН требуется комплексный подход к кибербезопасности, включающий разработку и реализацию национальных и региональных

стратегий защиты киберпространства, повышение осведомленности и квалификации в области кибербезопасности, а также сотрудничество на международном уровне для обмена опытом и лучшими практиками. Активное участие государственного сектора, бизнеса и гражданского общества в укреплении кибербезопасности будет способствовать созданию безопасного и устойчивого цифрового пространства, что является ключом к дальнейшему процветанию региона АСЕАН в эпоху глобальной цифровизации.

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. Страна признана одним из мировых лидеров в сфере информационных технологий и кибербезопасности, благодаря высокому уровню технологической развитости, квалифицированным специалистам и эффективной государственной политике.

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. Страна выступает инициатором и активным участником многочисленных международных и региональных форумов, конференций и рабочих групп, направленных на обмен знаниями, опытом и лучшими практиками в сфере кибербезопасности. Это сотрудничество способствует разработке общих стандартов и протоколов безопасности, повышает уровень осведомленности и готовности к противодействию киберугрозам на региональном уровне.

Основным шагом в укреплении национальной и региональной кибербезопасности стало создание в 2015 г. Агентства кибербезопасности Сингапура (CSA)[2]. Агентство координирует работу различных ведомств и организаций, занимающихся кибербезопасностью в стране, а также сотрудничает с частным сектором, академическими кругами и международным сообществом. Основные задачи CSA включают защиту критической информационной инфраструктуры, предотвращение и реагирование на киберинциденты, развитие навыков и компетенций в области кибербезопасности, а также повышение общественной осведомленности о киберугрозах.

*CSA* играет важную роль в разработке и реализации национальных инициатив и стратегий, таких как Национальная стратегия кибербезопасности[3] и Закона о кибербезопасности (*Cybersecurity Act*)[4], которые устанавливают правовые и организационные рамки для защиты

киберпространства Сингапура. Эти меры не только укрепляют национальную безопасность, но и служат образцом для других стран региона.

Через международное сотрудничество и региональные инициативы, такие как *ASEAN Cyber Capacity Programme* (*ACCP*)[5], *ASEAN-Singapore Cybersecurity Centre of Excellence*[6], *ASEAN Regional Forum* (*ARF*) по вопросам кибербезопасности, Глобальный форум по киберэкспертизе (*GFCE*) и другие платформы Сингапур активно вносит вклад в укрепление кибербезопасности в регионе АСЕАН. Эти программы направлены на обучение и развитие квалификации специалистов в области кибербезопасности, улучшение взаимодействия при реагировании на киберинциденты и обмен важной информацией о киберугрозах между странами АСЕАН.

Сингапур демонстрирует, что эффективная кибербезопасность требует не только передовых технологий и квалифицированных специалистов, но и активного международного сотрудничества, стратегического планирования и постоянного обмена знаниями и опытом. Благодаря этому подходу Сингапур не только защищает свое киберпространство, но и способствует созданию более безопасной и устойчивой цифровой среды в регионе АСЕАН.

Сингапур активно работает над созданием законодательной и стратегической основы для обеспечения национальной и региональной кибербезопасности. Эти усилия направлены на защиту критически важной информационной инфраструктуры, повышение уровня осведомленности и подготовленности к киберугрозам, а также на развитие международного сотрудничества в области кибербезопасности.

Одним из ключевых элементов законодательной базы Сингапура в области кибербезопасности является Закон о кибербезопасности (*Cybersecurity Act*)[7], принятый в 2018 г. Этот закон создает правовую основу для управления и защиты киберпространства страны, а также устанавливает ответственность за безопасность критически важной информационной инфраструктуры в различных секторах экономики, включая энергетику, транспорт, здравоохранение и банковские услуги.

*Закон о кибербезопасности предусматривает следующие ключевые аспекты:*

- Управление киберинцидентами: Агентство кибербезопасности Сингапура (CSA) получает полномочия координировать реагирование на серьезные киберинциденты, включая сбор информации и проведение расследований.

- Защита критической инфраструктуры: Операторы критической информационной инфраструктуры обязаны соблюдать стандарты безопасности и регулярно сообщать о киберугрозах и инцидентах.
- Регулирование: Введение механизмов регулирования для поставщиков услуг в области кибербезопасности, направленных на обеспечение качества и надежности предоставляемых услуг.

В дополнение к Закону о кибербезопасности, Сингапур разработал и реализует Национальную стратегию кибербезопасности, которая охватывает широкий спектр мер, направленных на защиту национального киберпространства и поддержку устойчивого развития цифровой экономики.

*Стратегия включает в себя четыре основных направления:*

1. Защита критической инфраструктуры: Укрепление защиты секторов, имеющих ключевое значение для национальной безопасности и экономики;
2. Создание системы раннего предупреждения и быстрого реагирования на киберугрозы;
3. Развитие экосистемы кибербезопасности: Поддержка инноваций, исследований и развитие кадрового потенциала в области кибербезопасности;
4. Укрепление международного сотрудничества: Развитие партнерства и совместной работы с другими странами и международными организациями для обмена знаниями и совместного решения глобальных вызовов в области кибербезопасности.

Один из ярких примеров национальных инициатив Сингапура - запуск программы *Cybersecurity Labelling Scheme* (*CLS*),[8] цель которой – повысить уровень безопасности потребительских устройств в интернете вещей (*IoT*).

Законодательные и стратегические инициативы Сингапура в области кибербезопасности оказывают значительное влияние на регион АСЕАН, являясь образцом для разработки собственных мер и стратегий защиты киберпространства в соседних странах.

«Сингапур стремится развивать сильное и устойчивое киберпространство в АСЕАН, которое будет способствовать экономическому росту и интеграции региона», – заявил министр внутренних дел и

министр юстиции и права Сингапура К. Шанмугам. Сингапур активно содействует укреплению кибербезопасности на региональном уровне через обмен опытом, совместные учения и программы подготовки специалистов, способствуя созданию согласованной и эффективной системы кибербезопасности в АСЕАН.

Сингапур активно продвигает сотрудничество и международное партнерство в области кибербезопасности, как внутри АСЕАН, так и за его пределами. Эта стратегия основана на понимании, что киберугрозы не знают границ, и эффективное противодействие им требует координированных усилий на международном уровне. Неотъемлемой частью работы сообщества стала *ASEAN Ministerial Conference on Cybersecurity*, где обсуждаются стратегии и меры по укреплению кибербезопасности, обмен опытом и лучшими практиками между странами-участницами[9].

Выступая как катализатор регионального и международного сотрудничества в области кибербезопасности, Сингапур использует свой опыт и ресурсы для поддержки инициатив, направленных на укрепление киберустойчивости. Страна регулярно организует и участвует в международных конференциях, семинарах и учениях по кибербезопасности, таких как *Singapore International Cyber Week*, которые служат платформой для обмена знаниями и опытом между государственными органами, частным сектором и академическим сообществом.

Сингапур также активно работает над развитием двусторонних и многосторонних отношений в области кибербезопасности, заключая соглашения о сотрудничестве с другими странами и международными организациями. Это позволяет строить эффективные механизмы для быстрого обмена информацией о киберугрозах, совместного реагирования на киберинциденты и координации усилий в развитии норм и стандартов кибербезопасности.

В 2018 г. Сингапур и АСЕАН подписали Меморандум о взаимопонимании (*MoU*) по сотрудничеству в области кибербезопасности, который предусматривает обмен информацией об угрозах, совместные исследования и разработку образовательных программ.

В рамках своей стратегии кибербезопасности Сингапур уделяет особое внимание образовательным программам и инициативам по повышению осведомленности. Программа *Cybersecurity Capacity Building Programme* предлагает тренинги и семинары для стран АСЕАН, направленные на укрепление их кибербезопасных способностей. С 2018 г. по этой программе было обучено более 140 чиновников из разных стран региона. Курсы охватывают широкий спектр тем, от

управления киберинцидентами до разработки национальных стратегий кибербезопасности.

Сингапур также активизировал усилия по созданию эффективных механизмов обмена информацией о киберугрозах между странами АСЕАН. Примером такого сотрудничества является *ASEAN Cyber Threat Intelligence Sharing Platform*, платформа, позволяющая странам-участницам обмениваться данными о киберугрозах в реальном времени. Одним из заметных примеров инициатив Сингапура в области кибербезопасности является создание *ASEAN-Singapore Cybersecurity Centre of Excellence* (*ASCCE*). Центр направлен на укрепление кибербезопасности в регионе АСЕАН через обучение, разработку политики и сотрудничество в области кибербезопасности. *ASCCE* предлагает обучающие программы и мастер-классы для представителей государственного сектора АСЕАН, способствуя повышению квалификации и обмену лучшими практиками в сфере защиты киберпространства.

Кроме того, Сингапур является активным участником международных платформ и инициатив, таких как Глобальный форум по киберэкспертизе (*GFCE*) и *ASEAN Regional Forum on Cybersecurity*, где страна демонстрирует свою приверженность развитию глобального сотрудничества в области кибербезопасности[10].

Через эти и многие другие инициативы Сингапур способствует созданию координированной и эффективной системы кибербезопасности на региональном и международном уровне. Страна использует свое лидирующее положение для продвижения культуры безопасности в цифровом пространстве, что является ключевым фактором устойчивого развития в эпоху глобальной цифровизации.

Сингапур признаёт, что развитие кадров и повышение осведомленности о кибербезопасности играют важную роль в создании устойчивой и безопасной цифровой среды. Страна предпринимает значительные усилия для обучения специалистов в области кибербезопасности и информирования общественности о рисках, связанных с киберугрозами.

Был разработан ряд программ по подготовке и переподготовке специалистов в области кибербезопасности, чтобы удовлетворить растущий спрос на квалифицированные кадры. Например, программа *Cyber Security Associates and Technologists* (*CSAT*) предназначена для поддержки профессионального развития и предоставляет обучение и стажировки для тех, кто стремится построить карьеру в сфере кибербезопасности. Такие программы помогают укреплять кадровый по-

тенциал страны и региона, подготавливая специалистов, способных эффективно противостоять киберугрозам.

Для повышения осведомленности о кибербезопасности среди населения и предприятий Сингапур реализует образовательные кампании и инициативы, такие как программа *Go Safe Online*. Эта национальная кампания направлена на информирование общественности о киберугрозах и способах защиты в интернете. *Go Safe Online* охватывает широкий спектр тем, от защиты персональных данных до мер предосторожности при онлайн-покупках и использовании социальных сетей. Кампания использует различные медиаформаты и платформы, включая вебсайты, социальные сети и публичные мероприятия, чтобы достичь максимально широкой аудитории[11].

Кроме программы *Go Safe Online*, Сингапур реализует другие образовательные проекты и инициативы. Например, проводятся регулярные семинары и воркшопы для школьников, студентов и педагогов, нацеленные на развитие понимания основ кибербезопасности и навыков безопасного поведения в сети. Агентство кибербезопасности Сингапура (*CSA*) также сотрудничает с университетами и политехническими институтами для внедрения курсов и программ, специализированных на кибербезопасности, что способствует подготовке высококвалифицированных специалистов в этой области.

Через эти и многие другие инициативы Сингапур вносит значительный вклад в развитие кадров и повышение уровня осведомленности о кибербезопасности, как на национальном, так и на региональном уровне. Эти усилия помогают формировать культуру кибербезопасности среди граждан и организаций, что является ключевым элементом в защите цифрового пространства от киберугроз.

Сингапур активно внедряет инновации и технологические решения для укрепления кибербезопасности, используя передовые технологии, включая искусственный интеллект (ИИ), машинное обучение и блокчейн, чтобы обеспечить более эффективную защиту от киберугроз.

Искусственный интеллект и машинное обучение играют ключевую роль в современных системах кибербезопасности, обеспечивая возможность обнаружения и анализа сложных угроз в реальном времени. Эти технологии способны анализировать большие объемы данных, выявляя аномалии и потенциальные угрозы, что позволяет предотвратить кибератаки до того, как они нанесут ущерб. Кроме того, ИИ может обучаться на основе новых данных о киберугрозах, постоянно улучшая свою эффективность.

Блокчейн используется для обеспечения целостности и безопасности данных благодаря своей децентрализованной и неподдельной структуре. Эта технология находит применение в защите цифровых идентификаторов, создании безопасных систем обмена данными и повышении прозрачности операций в киберпространстве.

Примеры успешных технологических решений и инициатив: *SG-Cyber Safe* — это инициатива Агентства кибербезопасности Сингапура, направленная на повышение уровня киберустойчивости среди малого и среднего бизнеса, а также среди общественности. В рамках этой программы предприниматели и граждане могут получить доступ к ресурсам и инструментам для защиты своих цифровых активов, включая рекомендации по кибергигиене, инструменты оценки кибербезопасности и обучающие материалы[12].

Сингапур разработал системы, которые используют ИИ для мониторинга и анализа сетевого трафика в реальном времени, чтобы обнаруживать и предупреждать о потенциальных киберугрозах. Это позволяет оперативно реагировать на инциденты и предотвращать их распространение.

Сингапур внедряет образовательные программы, использующие интерактивные технологии и игровые механики для обучения детей и взрослых основам кибербезопасности. Эти платформы повышают осведомленность о киберугрозах и учат пользователей безопасному поведению в интернете.

Эти и многие другие инициативы и технологические решения демонстрируют приверженность Сингапура использованию инноваций для создания более безопасного киберпространства. Путем интеграции передовых технологий в стратегии кибербезопасности и развития сотрудничества на всех уровнях, Сингапур укрепляет свои позиции как лидера в области кибербезопасности в АСЕАН и за его пределами.

В регионе АСЕАН, как и во всем мире, кибербезопасность сталкивается с рядом вызовов, которые обусловлены как технологическими изменениями, так и социально-экономическими факторами.

*Текущие вызовы:*

- Рост киберпреступности: Увеличение количества и сложности кибератак, направленных на кражу данных, финансовые мошенничества и нарушение работы критической инфраструктуры.

- Недостаточное осведомленность и подготовка: Низкий уровень осведомленности о киберугрозах среди населения и предприятий, а также недостаток квалифицированных специалистов в области кибербезопасности.
- Отсутствие согласованной политики и стандартов: Различия в национальных подходах к кибербезопасности и отсутствие единых стандартов и регулирования в регионе.

*Будущие вызовы:*

- Развитие технологий: Внедрение новых технологий, таких как Интернет вещей (IoT), искусственный интеллект (ИИ) и квантовые вычисления, создает новые угрозы и вызовы для кибербезопасности.
- Международная кибершпионаж: Усиление геополитических напряженностей и рост международного кибершпионажа могут привести к увеличению целенаправленных атак на государственные и военные объекты.
- Защита персональных данных: Увеличение объемов генерируемых данных и их ценность делают защиту персональных данных одним из ключевых вызовов кибербезопасности.

Сингапур, будучи одним из лидеров в области кибербезопасности в регионе АСЕАН, играет ключевую роль в формировании будущего кибербезопасности в регионе.

*Развитие международного сотрудничества:* Сингапур активно продвигает развитие регионального и международного сотрудничества в области кибербезопасности, что включает обмен знаниями, опытом и лучшими практиками, а также координацию усилий по противодействию киберугрозам.

*Инвестиции в образование и подготовку специалистов:* Сингапур продолжит вкладывать ресурсы в образовательные программы и тренинги по кибербезопасности, чтобы удовлетворить спрос на квалифицированных специалистов и повысить уровень осведомленности среди населения и бизнеса.

*Инновации и технологические решения:* Продолжение разработки и внедрения передовых технологических решений для обеспечения безопасности в цифровом пространстве, включая использование ИИ для обнаружения и предотвращения кибератак, будет иметь ключевое значение.

*Укрепление законодательной базы:* Сингапур будет продолжать совершенствовать свою законодательную базу в области кибербезопасности, стимулируя другие страны АСЕАН к разработке и реализации согласованных правовых и регуляторных рамок.

Подводя итог, можно сказать, что будущее кибербезопасности в АСЕАН будет зависеть от способности региона адаптироваться к новым угрозам, инвестировать в развитие человеческого капитала и технологий, а также развивать сотрудничество как внутри региона, так и на международном уровне. Сингапур, безусловно, будет играть ведущую роль в этом процессе, демонстрируя пример эффективной политики и практики в области кибербезопасности.

Сингапур занимает лидирующую позицию в области кибербезопасности в регионе АСЕАН, активно внося вклад в развитие безопасного цифрового будущего для всех стран-членов. Благодаря стратегическому видению и комплексному подходу к кибербезопасности, Сингапур стал образцом для подражания в регионе, демонстрируя, как эффективно противостоять киберугрозам, развивать кадровый потенциал и повышать общественную осведомленность о важности кибербезопасности.

Сингапур разработал и реализовал ряд законодательных и стратегических инициатив, включая принятие Закона о кибербезопасности и разработку Национальной стратегии кибербезопасности. Эти меры направлены на защиту критической инфраструктуры, обеспечение координации усилий по противодействию киберугрозам и развитие способностей реагирования на киберинциденты[13]. Кроме того, Сингапур активно вкладывает ресурсы в развитие образовательных программ и инициатив по повышению осведомленности о кибербезопасности, что способствует формированию культуры безопасности среди населения и бизнеса.

На международном уровне Сингапур выступает за укрепление сотрудничества в области кибербезопасности, регулярно организуя и участвуя в мероприятиях, направленных на обмен знаниями и лучшими практиками. Инициативы, такие как *ASEAN-Singapore Cybersecurity Centre of Excellence*, способствуют развитию региональных способностей в области кибербезопасности и укреплению защиты киберпространства в АСЕАН.

Опыт Сингапура подчеркивает важность совместных усилий и международного сотрудничества для создания безопасного цифрового будущего. В условиях постоянно эволюционирующих киберугроз ни одна страна не может обеспечить кибербезопасность в одиночку.

Совместная работа, обмен информацией о киберугрозах, согласование правовых и нормативных рамок, а также развитие международного партнерства являются ключевыми факторами успешного противодействия киберугрозам на глобальном уровне.

Сингапур продемонстрировал, что через инновации, образование и сотрудничество можно не только повысить уровень кибербезопасности внутри страны, но и сделать значительный вклад в обеспечение безопасности цифрового пространства в обеспечение безопасности цифрового пространства в регионе АСЕАН и за его пределами. Таким образом, Сингапур продолжит играть ведущую роль в развитии кибербезопасности, стимулируя совместные усилия на пути к созданию безопасного и устойчивого цифрового будущего для всех.

**ИНФОРМАЦИЯ ОБ АВТОРЕ**

КАСЕНОВ Файзрахман Айткалиевич, заместитель директора Департамента евразийской интеграции МИД Республики Казахстан, аспирант ИВ РАН, Москва, Россия

**INFORMATION ABOUT THE AUTHOR**

Faizrakhman A. KASENOV, Deputy Director of the Eurasian Integration Department, MFA of the Republic of Kazakhstan, PhD Student, IOS RAS, Moscow, Russia

Статья поступила в редакцию 10.04.2024;
одобрена после рецензирования 24.04.2024;
принята к публикации 30.04.2024.

The article was submitted 10.04.2024;
approved 24.04.2024;
accepted to publication 30.04.2024.

[1] Florian Hoppe, Aadarsh Baijal, Willy Chang, Sapna Chadna, and Fock Wai Hoong// e-Conomy SEA 2023, https://www.bain.com/insights/e-conomy-sea-2023/, 01.04.2024
[2] Cyber Security Agency of Singapore (CSA). URL: https://www.csa.gov.sg/Explore/who-we-are
[3] National Cyber Security Masterplan 2018, July 2013, https://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf
[4] Cybersecurity Act / CSA. URL: https://www.csa.gov.sg/legislation/Cybersecurity-Act
[5] ASEAN Cybersecurity Cooperation Paper 2021-2025 / ASEAN. URL: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
[6] CSA. URL: https://www.csa.gov.sg/News-Events/Press-Releases/asean-singapore-cybersecurity-centre-of-excellence
[7] CSA. URL: https://www.csa.gov.sg/legislation/Cybersecurity-Act
[8] CSA. URL: https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme
[9] CSA. URL: https://www.csa.gov.sg/News-Events/speeches/2023/opening-address-by-mrs-josephine-teo-mci-at-the-8th-amcc-on-18-october-2023
[10] ARF. URL: https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-3_Report-of-the-Working-Group-on-ARF-Initiatives-on-Promoting-Cyber-Security-12th-ARF-EEPs.pdf
[11] CSA. URL: https://www.csa.gov.sg/docs/default-source/gso/file/resources/csa_how_to_go_safe_online_2019.pdf?sfvrsn=e0916eff_0
[12] https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme
[13] Bobro D. Methodological aspects of critical infrastructure protection // Research Gate. URL: https://www.researchgate.net/publication/322715607_The_National_Institute_for_Strategic_Studies_methodological_aspects_of_critical_infrastructure_protection