Научная статья. Исторические науки
УДК 327(5)
DOI: 10.31696/2072-8271-2025-2-2-67-106-119

ИНИЦИАТИВЫ РОССИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ В РАМКАХ РЕГИОНАЛЬНОГО ФОРУМА АСЕАН (АРФ): ОТ ЗАЯВЛЕНИЙ К ПРАКТИЧЕСКОМУ СОТРУДНИЧЕСТВУ (2010–2024 гг.)

Анатолий Сергеевич ДОНЦОВ [1]

[1] РУДН, Москва, Россия,
asdontsov@bk.ru, https://orcid.org/0000-0001-6062-6783

Аннотация: В статье рассматриваются подходы Российской Федерации к развитию сотрудничества в сфере кибербезопасности в рамках Регионального форума АСЕАН по безопасности (АРФ) за период 2010–2024 гг. Цель исследования — проанализировать эволюцию российских инициатив, оценить их восприятие странами Юго-Восточной Азии, а также выявить ключевые институциональные и политические барьеры на пути к практической реализации. Автор рассматривает нормативные положения, институциональные инициативы и отдельные практические действия России в рамках АРФ. Работа опирается на анализ официальных документов форума, экспертных публикаций и аналитических материалов. В результате изучения механизмов АРФ выявлены как достижения — проведение совместных семинаров и обсуждений, выдвижение инициатив по раннему реагированию, — так и ограничения, в числе которых недостаточная институционализация, слабая представленность в профильных платформах АСЕАН, а также политические разногласия. Сделан вывод о частичном успехе российской дипломатии в области информационной безопасности в регионе, а также обозначены перспективы дальнейшего углубления сотрудничества при условии учета региональной специфики и повышения координации с ключевыми механизмами АСЕАН.

Ключевые слова: *АСЕАН, АРФ, кибербезопасность, цифровой суверенитет, информационная безопасность, информационное пространство, сотрудничество Россия–АСЕАН, безопасность ИКТ, цифровое регулирование, кибердипломатия*

Для цитирования: *Донцов А.С.* Инициативы России в области кибербезопасности в рамках регионального форума АСЕАН (АРФ): от заявлений к практическому сотрудничеству (2010–2024 гг.) // Юго-Восточная Азия: актуальные проблемы развития, 2025, Том 2, № 2 (67). С. 106–119. DOI: 10.31696/2072-8271-2025-2-2-67-106-119

Original article. Historical science

RUSSIA'S CYBERSECURITY INITIATIVES IN THE ASEAN REGIONAL FORUM (ARF): FROM DECLARATIONS TO PRACTICAL COOPERATION, 2010–2024

Anatolii S. DONTSOV [1]

[1] RUDN, Russia, Moscow,
asdontsov@bk.ru, https://orcid.org/0000-0001-6062-6783

Abstract: The paper explores Russia's approach to fostering cooperation in the field of cybersecurity within the framework of the ASEAN Regional Forum (ARF) from 2010 to 2024. The aim of the study is to trace the evolution of Russian initiatives, assess their reception by Southeast Asian countries, and identify key institutional and political obstacles to practical implementation. The author examines Russia's regulatory framework, institutional initiatives, and specific practical actions undertaken within the ARF. The analysis draws on official ARF documents, expert publications, and analytical reports. The study identifies both achievements — such as joint seminars and discussions, and the proposal of early response initiatives — and limitations, including insufficient institutionalization, limited representation in key ASEAN platforms, and political disagreements. The article concludes that Russian diplomacy has achieved partial success in promoting information security in the region, while also outlining prospects for deepening cooperation, provided that regional specifics are taken into account and coordination with core ASEAN mechanisms is strengthened.

Keywords: *ASEAN, ARF, cybersecurity, digital sovereignty, ICT security, information space, Russia–ASEAN relations, information security, cyberspace, cyber diplomacy*

For citation: Dontsov A.S. Russia's Cybersecurity Initiatives in the ASEAN Regional Forum (ARF): From Declarations to Practical Cooperation, 2010–2024. *Yugo-Vostochnaya Aziya: aktual'nyye problemy razvitiya*, 2025, T. 2, № 2 (67). Pp. 106–119. DOI: 10.31696/2072-8271-2025-2-2-67-106-119

Введение

История развития цифровой среды видела не мало киберинцидентов, однако в последние десятилетия все чаще происходят целевые атаки на критически важную инфраструктуру, растут риски для национальных экономик, распространяется трансграничная киберпреступность, заставляя государства выстраивать новые механизмы коллективного реагирования в киберпространстве. Для стран Ассоциации

государств Юго-Восточной Азии (АСЕАН), находящихся на перекрёстке геополитических и геоэкономических интересов, цифровая безопасность становится не только внутренним приоритетом, но и фактором региональной стабильности. Уже в начале 2010-х гг. Лаборатория Касперского фиксировала использование вредоносного кода, впервые классифицированного как кибероружие, в странах Юго-Восточной Азии в военно-политических целях (*DuQu, Stuxnet, Net Traveller*)[1].

На этом фоне Россия последовательно наращивает сотрудничество с государствами региона, участвуя в Региональном форуме по безопасности АСЕАН (АРФ) с 1994 г. В 2010 г. решением 17-й сессии АРФ за Россией, Малайзией и Австралией была закреплена ведущая роль в выработке политики в области кибербезопасности и борьбы с кибертерроризмом[2], заложив институциональную точку отсчета для продвижения российских инициатив. Москва внесла значимый вклад в подготовку обновленного профильного Рабочего плана АРФ на 9-м Межсессионном совещании АСЕАН по борьбе с терроризмом и транснациональной преступностью (МВ-ПТТП) в 2011 г.[3]. Более того, в 2012 г. в ходе 19-ой сессии АРФ по инициативе России было принято заявление министров иностранных дел АРФ по сотрудничеству и обеспечению международной кибербезопасности, которое легло в основу политики форума в этой сфере[4]. Совместная работа России, Малайзии и Австралии стала ключевым фактором разработки *ARF Work Plan on Security of and in the Use of Information and Communication Technologies (ICTs)*, представленного в декабре 2013 г. Россия продолжает играть деятельную роль в формировании политики в области кибербезопасности.

Настоящее исследование охватывает период 2010–2024 гг., в течение которого Россия продемонстрировала заинтересованность в активизации сотрудничества с АСЕАН по линии АРФ в области информационной безопасности. Особое внимание уделяется политическим инициативам, нормативным документам и экспертному диалогу, направленным на выработку общих подходов к вопросам кибербезопасности и борьбы с киберугрозами. Цель статьи — проанализировать эволюцию российских предложений в рамках АРФ, оценить их восприятие странами Юго-Восточной Азии, а также выявить институциональные и политические барьеры на пути к реализации многостороннего сотрудничества в условиях нарастающей геополитической напряженности. Методологически работа основывается на анализе официальных документов форума, экспертных публикаций, а также аналитических

материалов профильных исследовательских центров, занимающихся вопросами региональной и международной кибербезопасности.

Продвижение концепции цифрового суверенитета

Одним из ключевых направлений инициатив России в рамках АРФ стало последовательное продвижение концепции цифрового суверенитета, согласно которой государства обладают исключительным правом контролировать свою цифровую инфраструктуру, информационные ресурсы и потоки данных. Данная позиция отражает более широкий российский подход к международной информационной безопасности, который отличается от западного акцента на технические аспекты «кибербезопасности» и включает в себя политико-правовую и идеологическую составляющую[5].

Принципы цифрового суверенитета были отражены *в Совместном заявлении Российской Федерации и АСЕАН по вопросам безопасности использования информационно-коммуникационных технологий*, принятом 14 ноября 2018 г. В этом документе стороны признали, что использование ИКТ может непосредственно влиять на политическую, экономическую и социальную стабильность, и подчеркнули необходимость соблюдения основополагающих принципов международного права, в частности невмешательство во внутренние дела государств (п. 2)[6].

Особое внимание в заявлении уделено праву разрабатывать и применять национальные законодательства, регулирующие цифровую сферу, включая защиту критической информационной инфраструктуры и персональных данных. Участники заявили о необходимости выработки международно признанных правил, норм и принципов ответственного поведения в киберпространстве, при этом Россия подчёркивала приоритет государственно ориентированных подходов и ведущую роль ООН как универсального механизма регулирования в этой области (п. 4, 6)[7].

Российская концепция цифрового суверенитета также нашла выражение на глобальном уровне через инициативу по разработке *Кодекса поведения государств в информационном пространстве*. Хотя данный проект был выдвинут на площадке ООН и носил универсальный характер, он использовался Москвой и как ориентир для регионального взаимодействия, в том числе в рамках сотрудничества с АСЕАН. Документ предусматривал выработку юридически значимых обязательств для государств, направленных на предотвращение

конфликтов в киберпространстве, защиту критической инфраструктуры и соблюдение принципа ненападения с использованием ИКТ[8].

В контексте взаимодействия со странами-членами АСЕАН этот подход нашёл благоприятный отклик, учитывая обеспокоенность государств региона трансграничными киберугрозами. Более того, в заявлении 2018 г. страны ЮВА выразили готовность рассмотреть российскую инициативу по учреждению *Диалога Россия–АСЕАН по вопросам безопасности ИКТ*, что свидетельствует о стремлении обеих сторон институционализировать взаимодействие в этой области (п. 14)[9].

Москва также активно использовала платформу АРФ для продвижения принципов правовой защиты персональных данных и расширения сотрудничества в области борьбы с кибертерроризмом, апеллируя к документам регионального значения, таким как *ASEAN Cybersecurity Cooperation Strategy* (2017) и *ASEAN Framework on Personal Data Protection* (2016). Данный подход позволил России вписать собственную нормативную повестку в существующие региональные рамки, избегая прямого противоречия с принятыми нормами, но при этом способствуя их переосмыслению и развитию[10].

Создание многосторонних диалоговых платформ

Одним из ключевых направлений прикладного сотрудничества России в рамках Регионального форума АСЕАН по безопасности (АРФ) стал запуск и развитие многосторонних диалоговых платформ в сфере информационной безопасности. В августе 2021 г. Москва была избрана сопредседателем механизма межсессионных встреч АРФ по безопасности информационно-коммуникационных технологий (ИКТ) на 2022–2024 гг. Совместно с Индонезией, Австралией и Республикой Корея российская сторона получила возможность координировать и формировать повестку работы соответствующей экспертной группы. По словам тогдашнего заместителя министра иностранных дел РФ И.В. Моргулова, российская делегация акцентировала внимание на необходимости развития практического взаимодействия и мер доверия в регионе в условиях нарастающих киберугроз[11].

Значимой инициативой в рамках данного формата стал *третий семинар АРФ по противодействию использованию ИКТ в преступных целях*, прошедший в Москве 23–24 мая 2024 г. Мероприятие, организованное при совместном председательстве России, Китая и Таиланда, собрало свыше 100 участников, включая представителей правоохранительных и дипломатических ведомств стран АСЕАН, Восточного

Тимора, Индии, Монголии и КНДР, а также экспертов Управления ООН по борьбе с наркотрафиком и международной преступностью[12].

Тематика семинара охватывала широкий спектр вызовов: от онлайн-экстремизма и терроризма до распространения наркотиков, мошенничества и злоупотребления персональными данными с использованием цифровых технологий. Особое внимание было уделено международно-правовым аспектам борьбы с киберпреступностью и вопросам трансграничного правового сотрудничества. Россия последовательно продвигает идею разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях под эгидой ООН, подчеркивая необходимость регулирования цифрового пространства в рамках универсальных международных механизмов[13].

Москва отметила значимость практического обмена опытом по расследованию киберинцидентов и взаимодействию правоохранительных органов, что особенно актуально для государств Азиатско-Тихоокеанского региона, где наблюдается рост трансграничной киберпреступности. По итогам мероприятия было заявлено о намерении продолжить регулярные встречи и наладить сотрудничество в этой сфере, укрепляя диалоговые механизмы АРФ как платформу коллективного реагирования на киберугрозы[14].

Реформа терминологии и подходов

Одной из малоизученных, но принципиально важных составляющих российских инициатив в рамках АРФ и ООН стало предложение пересмотра терминологического аппарата, применяемого в международных обсуждениях по кибербезопасности. Россия последовательно отстаивает необходимость замены понятий *«киберпространство»* и *«кибербезопасность»* на *«информационное пространство»* и *«безопасность в использовании ИКТ»* соответственно. Такой подход отражает более широкий политико-правовой взгляд Москвы на проблематику, отличающийся от преобладающего в западных странах технократического фокуса на сугубо технических угрозах (вирусы, уязвимости, защита сетей)[15].

Смысл этой реформы терминов заключается в том, чтобы подчеркнуть двойственную — техническую и идеолого-политическую — природу информационных угроз. В частности, российская позиция исходит из признания использования ИКТ не только с целью шпионажа или нарушения закона, но и в рамках информационных операций, направленных на вмешательство во внутренние дела государства,

дестабилизацию общества, подрыв суверенитета и распространение политически мотивированной дезинформации[16].

Доклад Центра международной информационной безопасности МГИМО подчёркивает, что термин *«международная информационная безопасность»* охватывает гораздо более широкий спектр рисков, включая информационно-психологическое воздействие и информационные войны. Пока в западном дискурсе термин *«кибербезопасность»* используется преимущественно для обозначения вопросов цифровой инфраструктуры, российская дипломатия обращает внимание на юридическую и политическую составляющую таких угроз[17].

В рамках Рабочей группы открытого состава ООН (*Open-ended Working Group, OEWG*) представители России неоднократно выступали за переосмысление используемой терминологии[18]. Так, в экспертных обсуждениях, инициированных в формате CSCAP (*Council for Security Cooperation in the Asia Pacific*), российская сторона предлагала заменить ряд англоязычных терминов, используемых в международном дискурсе. В частности, предлагалось использовать термин *«information space»* вместо *«cyberspace»*, *«security in the use of ICTs»* вместо *«cybersecurity»*, а также отказаться от политически нагруженного выражения *«rules-based cyberspace»* в пользу более нейтральной формулировки — *«open, secure and stable ICT environment»*. Эти предложения, направленные на повышение юридической определенности и отражение политических реалий, были официально зафиксированы в итоговом меморандуме группы CSCAP по международному праву и киберпространству[19].

Предлагаемая концептуализация служит не только политическим сигналом, но и инструментом правовой универсализации подходов. Россия, таким образом, добивается включения в повестку не только сугубо технических аспектов, но и вопросов контроля над информационными потоками, суверенного управления цифровой инфраструктурой и защиты информационного пространства от политически мотивированного вмешательства. Данные инициативы формируют основу для пересмотра международных норм, подчеркивая политическую ответственность государств за действия в цифровой среде и способствуя признанию принципа информационного суверенитета наравне с территориальным и экономическим.

Укрепление регионального сотрудничества

Вопросы налаживания взаимодействия между Россией и АСЕАН в сфере кибербезопасности приобрели особое значение в условиях

обострения глобальной напряженности и нарастания трансграничных киберугроз. Значимый шаг в этом направлении был сделан в ходе 4-й Консультации высоких представителей по вопросам безопасности России и АСЕАН, состоявшейся 24 апреля 2024 г. на полях Международного совещания высокого уровня в Санкт-Петербурге. В рамках встречи стороны подтвердили намерение расширить стратегическое партнёрство и запустить совместные инициативы, включая программы подготовки кадров в области информационной безопасности, а также развивать системы раннего предупреждения о кибератаках, способных нарушить стабильность критически важной инфраструктуры региона[20].

Особое внимание в рамках консультаций было уделено необходимости наращивания потенциала государств АСЕАН в обеспечении устойчивости информационных систем, задействованных в сфере энергетики, транспорта и телекоммуникаций. В качестве одного из приоритетных направлений было выделено создание механизмов коллективного реагирования на инциденты в киберсреде на основе платформ Регионального форума АСЕАН по безопасности (АРФ), в частности — через развитие совместных систем обмена информацией и координации[21].

Данные усилия органично вписываются в более широкий контекст региональной стратегии, обозначенной в рекомендациях рабочей группы CSCAP по международному праву и киберпространству. Согласно докладу группы, строительство эффективного механизма обеспечения кибербезопасности в Азиатско-Тихоокеанском регионе невозможно без выработки согласованных норм защиты критической инфраструктуры, такой как оптоволоконные линии связи, энергосети и транспортные узлы. При этом предлагается рассматривать эти объекты в трёх категориях — национальной, региональной и общей (коллективной), что позволяет гибко распределять ответственность и меры защиты между странами региона[22].

Рабочий план АРФ по безопасности в сфере ИКТ (2015) также включает положение о необходимости разработки национального законодательства по вопросам защиты критической инфраструктуры и усиления правового режима предупреждения киберинцидентов. Участники подчёркивают, что подобные меры должны сопровождаться институционализацией диалога и регулярными межведомственными консультациями, как в двустороннем, так и в многостороннем формате[23].

Таким образом, инициатива России по созданию совместных обучающих программ и раннего предупреждения — это не изолированное действие, а часть системного подхода к формированию устойчивой

архитектуры кибербезопасности в Юго-Восточной Азии. Она усиливает роль АРФ как ключевой площадки по выработке коллективных ответов на цифровые угрозы и способствует переходу от декларативных заявлений к практическому взаимодействию.

Практические итоги и ограничения сотрудничества

Несмотря на продолжительное присутствие России в диалоговых механизмах АСЕАН, включая АРФ и Совещание старших должностных лиц по цифровым вопросам АСЕАН (ADGSOM), практическое взаимодействие остается ограниченным. Несмотря на то, что Москва участвовала в ряде профильных мероприятий, таких как семинар по терминологии в сфере ИКТ и воркшоп по противодействию преступному использованию цифровых технологий, российская команда не принимала участия в киберучениях национальных команд реагирования на инциденты информационной безопасности (*Computer Emergency Response Teams, CERT*) стран АСЕАН зафиксировано не было[24]. Между тем, учения *ASEAN CERT Incident Drill* и практики под эгидой *ASEAN-Japan Cybersecurity Centre* стали регулярными и институционализированными — без участия российской стороны[25], что указывает на неполную и фрагментарную вовлечённость Москвы в региональные механизмы реагирования.

Попытки России инициировать более амбициозные проекты, в частности юридически обязывающий кодекс поведения в киберпространстве, не нашли отклика. Регион предпочел неформальные инструменты, такие как *Norms Implementation Checklist*, предложенный по инициативе Сингапура и Малайзии[26]. Несмотря на формальное обозначение России в *ARF Work Plan* как партнёра, конкретные инициативы Москвы не были реализованы. Аналитики подчеркивают, что ценностные расхождения — между приоритетами государственного суверенитета и принципами свободы информации — затрудняют принятие российских инициатив в регионе[27].

Отдельной проблемой стала слабая интеграция России в систему регионального киберобучения. Хотя Москва участвовала в отдельных семинарах Межсессионной встречи Регионального форума АСЕАН по вопросам информационно-коммуникационных технологий (*ARF ISM on ICTs*), такие важные проекты, как Центр кибербезопасности АСЕАН–Сингапур (*ASEAN–Singapore Cybersecurity Centre of Excellence, ASCCE*) и Центр развития потенциала в сфере кибербезопасности АСЕАН–Япония (*ASEAN–Japan Cybersecurity Capacity Building Centre, AJCCBC*), функционируют без участия России[28]. Лидирующие

позиции в подготовке кадров заняли Сингапур, Япония и США[29]. При этом, несмотря на зафиксированную в брифе Женевского центра по вопросам управления сектором безопасности (*DCAF – Geneva Centre for Security Sector Governance*) возможность расширения международного сотрудничества в обучающих форматах, Россия не упоминается среди задействованных стран[30], что свидетельствует о трудностях, с которыми сталкивается Москва, по включению в институциональные образовательные процессы АСЕАН.

Важным политико-правовым вызовом, ограничивающим институционализацию российских инициатив в АСЕАН, остаются фундаментальные расхождения между подходами России и западных стран к вопросам цифрового регулирования. Если Москва выступает за принятие юридически обязательных норм поведения государств в ИКТ-сфере, то США и их союзники отдают предпочтение гибким и необязательным механизмам — рекомендациям, руководствам и общим правилам. Это концептуальное несоответствие системно осложняет выработку согласованных международных стандартов и объясняет настороженность части государств региона, несмотря на их открытость к диалогу. Как подчеркивал министр иностранных дел России С.В. Лавров, отсутствие правовой определённости в цифровом пространстве чревато не только фрагментацией, но и риском эскалации конфликтов[31]. В этом контексте инициатива России о создании универсального «кодекса поведения» государств в ИКТ-сфере на площадке ООН, с усилением роли Совета Безопасности и Генеральной Ассамблеи, также служила попыткой преодолеть эту неопределенность и институционализировать принципы киберповедения в международном праве.

Барьером для реализации механизмов раннего реагирования стало сочетание внешнего недоверия и внутренней фрагментированности региона. Даже внутри АСЕАН отсутствует единство стандартов и подходов из-за различий в правовых системах и уровнях технологического развития[32]. В этих условиях предложения России, акцентирующие юридически обязательные нормы, вступают в противоречие с консенсусным подходом, лежащим в основе архитектуры реагирования АСЕАН[33]. Кроме того, Россия воспринимается скорее как сторонний наблюдатель, чем как активный участник, что дополнительно ослабляет потенциал её инициатив.

Не менее показательно и отсутствие взаимодействия между российскими и национальными CERT-структурами стран АСЕАН. Несмотря на активное развитие внутренней координации в рамках *ASEAN CERT Information Exchange Mechanism*, механизмы *CERT-to-CERT*

обмена между Россией и странами ЮВА отсутствуют. В пресс-релизах Агентства по кибербезопасности Сингапура (*CSA*) перечисляются стратегические партнёры — Япония, ЕС, США, Австралия — но не Россия[34]. Отсутствие упоминаний России в заявлениях *ADGMIN 2025* подчёркивает сохраняющийся разрыв между политическим диалогом и техническим взаимодействием в рамках региональных платформ[35].

Заключение

Настоящее исследование позволило проследить эволюцию подхода России к сотрудничеству с АСЕАН в сфере кибербезопасности за период 2010–2024 гг., от заявлений к попыткам реализации прикладных проектов. Таким образом, поставленная в начале исследования цель была реализована в полном объёме.

Участие России в АРФ характеризуется активной позицией на уровне концептуальной и дипломатической повестки, включая продвижение принципов цифрового суверенитета[36]. Тем не менее, этот курс сталкивается с бескомпромиссной позицией западных участников диалога, предпочитающих гибкие необязательные нормы, что затрудняет выработку общих подходов[37].

Одним из ключевых ограничений стало отсутствие устойчивых институциональных механизмов реализации предложенных инициатив: семинары и обучающие программы остаются разовыми, отсутствуют устойчивые форматы совместных учений и систем реагирования[38]. Это объясняется как структурной фрагментированностью механизмов АСЕАН, так и недостаточной координацией с российской стороны.

Несмотря на ограниченные практические достижения, ряд государств ЮВА проявляет интерес к российским предложениям, особенно в части защиты цифрового суверенитета и обмена опытом в области противодействия киберпреступности. Это свидетельствует о стремлении сохранить цифровой суверенитет в условиях усиливающейся нормативной конкуренции[39].

В перспективе российско-асеановские связи имеют потенциал для укрепления при условии институционализации уже начатых форматов взаимодействия — таких как сотрудничество с *ASEAN Regional CERT* и реализация совместных образовательных программ. Успех этих усилий зависит от способности России адаптировать свою стратегию под региональные реалии и акцентировать внимание на практической пользе для партнеров.

В условиях нарастающего глобального соперничества для России открывается возможность продвигать альтернативную западным подходам модель кибербезопасности, что особенно актуально для стран, стремящихся сохранить цифровой суверенитет и свободу в выборе нормативной и технологической модели развития цифрового пространства. В этом контексте АСЕАН становится не только ареной конкуренции моделей, но и потенциальным проводником альтернативного подхода к международной информационной безопасности.

ИНФОРМАЦИЯ ОБ АВТОРЕ

ДОНЦОВ Анатолий Сергеевич, аспирант, РУДН им. Патриса Лумумбы, Москва, Россия

Статья поступила в редакцию 30.04.2025;
одобрена после рецензирования 15.05.2025;
принята к публикации 30.05.2025.

INFORMATION ABOUT THE AUTHOR

Anatolii S. DONTSOV, PhD Student, RUDN, Moscow, Russia

The article was submitted 30.04.2025;
approved 15.05.2025;
accepted to publication 30.05.2025.

[1] Васильев Б., Калинин А. Н., Лукацкий А. В. [и др.] Общая повестка дня России и АСЕАН в киберпространстве: противодействие глобальным угрозам, укрепление кибербезопасности и развитие сотрудничества // Индекс безопасности. 2014. Т. 20, № 4(111). С. 77–92. EDN TICSZH.

[2] Абрамов А. Л., Курилов В. И., Меламед И. И., Терентьева Е. А. Россия и объединения стран АТР // Азиатско-Тихоокеанский регион: экономика, политика, право. 2012. № 2 (26). С. 11–21. URL: https://cyberleninka.ru/article/n/rossiya-i-obedineniya-stran-atr

[3] Региональный форум АСЕАН по безопасности (Справочные материалы) // Министерство иностранных дел Российской Федерации. 2011. 26 окт. URL: https://www.mid.ru/ru/foreign_policy/rso/1703146/

[4] Common Agenda for Russia and ASEAN in Cyberspace: Countering Global Threats, Strengthening Cybersecurity, and Fostering Cooperation. 2014. Security Index: A Russian Journal on International Security. Vol. 20, no. 2. P. 75–87.
DOI: https://doi.org/10.1080/19934270.2014.985094.

[5] Крутских А. В., Зиновьева Е. С., Булва В. И., Алборова М. Б., Юдина Ю. А. Международная информационная безопасность: подходы России / под ред. А. В. Крутских, Е. С. Зиновьевой. Москва: МГИМО, 2021. 47 с.
URL: https://mgimo.ru/upload/iblock/047/01fgupojoj7ka0tw75bw19li4bmurfse/%D0%94%D0%BE%D0%BA%D0%BB%D0%B0%D0%B4%20%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9.pdf

[6] Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. 2018. 14 ноября. URL: http://www.kremlin.ru/supplement/5361

[7] Statement of ASEAN and the Russian Federation on Cooperation in the Field of Security of and in the Use of Information and Communication Technologies. 2018. 14 Nov. URL: https://asean.org/wp-content/uploads/2018/11/FINAL-Statement-of-ASEAN-and-the-Russian-Federation-on-Cooperation-in-the-Field-of-Security-of-and-in-the-Use-of-Information-and-Communication-Technologies.pdf

[8] Korzak E. Russia's Cyber Policy Efforts in the United Nations // NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Tallinn Paper No. 11. 2021. 20 p. URL: https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf

[9] Kanaev E. A. ASEAN-Russia Cooperation: The Digital Dimension // Yugo-Vostochnaya Aziya: aktual'nyye problemy razvitiya. 2022. T. 3, № 3 (56). P. 18–29. DOI: 10.31696/2072-8271-2022-3-3-56-018-029.
[10] Estiyovionita K., Sitamala A. ASEAN's Role in Cybersecurity Maintenance and Security Strategy through an International Security Approach // Lampung Journal of International Law. 2022. Vol. 4, № 2. P. 81–90. DOI: 10.25041/lajil.v4i2.2556.
[11] Россия стала сопредседателем механизма форума АСЕАН по информационной безопасности // ТАСС. 2021. 6 авг. URL: https://tass.ru/politika/12078021
[12] О мероприятии Регионального форума АСЕАН по тематике противодействия использованию ИКТ в преступных целях // Министерство иностранных дел Российской Федерации. 2024. 24 мая. URL: https://mid.ru/ru/foreign_policy/rso/1952782/
[13] 3-й семинар Регионального форума АСЕАН (АРФ) по противодействию использованию ИКТ в преступных целях // Постоянное представительство Российской Федерации при Ассоциации государств Юго-Восточной Азии (АСЕАН). URL: https://asean.mid.ru/ru/news/3_y_seminar_regionalnogo_foruma_asean_arf_po_protivodeystviyu_ispolzovaniyu_ikt_v_prestupnykh_tselya/
[14] О мероприятии Регионального форума АСЕАН... Указ. ресурс // МИД РФ.
[15] CSCAP Study Group on International Law and Cyberspace. URL: https://www.cscap.org/uploads/Memo%20for%20CSCAP%20Study%20Group%20on%20International%20Law%20and%20Cyberspace.pdf
[16] Radu C. C. Russia's approach to cyberspace // International Scientific Conference "Strategies XXI". December 2022. P. 533–544. DOI: 10.53477/2971-8813-22-61.
[17] Khasanova L. Conceptual Discrepancies in Russian and Western Approaches to the International Regulation of Cyber [Information] Space // Baltic Yearbook of International Law Online. 2024. Vol. 22, № 1. P. 3–21. DOI: 10.1163/22115897_02201_002.
[18] Danelyan A. A., Gulyaeva E. E. International Legal Aspects of Cybersecurity // Moscow Journal of International Law. 2020. № 1. P. 44–53. DOI: 10.24833/0869-0049-2020-1-44-53. URL: https://www.researchgate.net/publication/343213061_International_Legal_Aspects_of_Cybersecurity
[19] CSCAP Study Group on International Law and Cyberspace. Указ. ресурс. С. 1.
[20] 4th ASEAN-Russia Consultation of the High Representatives for Security Issues Convenes // ASEAN. 2024. 24 Apr. URL: https://asean.org/4th-asean-russia-consultation-of-the-high-representatives-for-security-issues-convenes/
[21] Overview ASEAN-Russia dialogue relations // ASEAN. September 2024. URL: https://asean.org/wp-content/uploads/2024/09/Overview-ASEAN-Russia-Dialogue-Relations-as-of-Sep-2024.pdf
[22] Tay K. L. ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework. The International Institute for Strategic Studies, June 2023. URL: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/06/asean-cyber-security-cooperation.pdf
[23] ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs). 2015. 7 May. URL: https://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf
[24] Lee B. T. F., Kornphetcharat K., Sims J. P., Linh Dieu D., Ali B. S. ASEAN cybersecurity cooperation strategy: combating cyber terrorism and hackers through CERT coordination // International Journal of Law and Public Policy. 2025. Vol. 7, no. 1. P. 20–30. DOI: 10.36079/lamintang.ijlapp-0701.788.
[25] Sari M. N. ASEAN's regional effort on cybersecurity and its effectiveness // Keio SFC Journal. 2023. Vol. 23, № 1. С. 26–42. DOI: 10.14991/003.00230001-0026.
[26] Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region // The Cyber Security Agency of Singapore (CSA). 2024. 16 октября. URL: https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region (дата обращения: 26.05.2025).
[27] Ang B. Next Steps for Cyber Norms in ASEAN // RSIS Commentary. 2018. № 174 (22 Oct.). Singapore: S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU). Ред. Kassim Y. R.

[28] ASEAN Cybersecurity Cooperation Strategy (2021–2025) // ASEAN. 2022. 23 января. URL: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
[29] Joint Media Statement of the 5th ASEAN Digital Ministers' Meeting and Related Meetings, 16–17 January 2025 // ASEAN. URL: https://asean.org/wp-content/uploads/2025/01/15-ENDORSED-JOINT-MEDIA-STATEMENT-5th-ADGSOM-v2-Cleaned.pdf
[30] Socquet-Clerc K., Khoo Su-Yen S., Fitriani, Gomez M. A., Nguyen Viet Lam. Cybersecurity Governance in Southeast Asia. Thematic SSG Brief. Geneva: DCAF – Geneva Centre for Security Sector Governance, 2023. Сер. ред.: Schnabel A. ISBN 978-92-9222-719-7.
[31] Лавров С. В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью // Внешнеэкономические связи. 2020. 28 сент. URL: https://www.mid.ru/ru/foreign_policy/news/1442834/
[32] Sari M. N. Указ. соч. (2023). С. 39.
[33] ASEAN Cybersecurity Cooperation Strategy (2021–2025). Указ. ресурс.
[34] Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region. Указ. ресурс.
[35] Joint Media Statement of the 5th ASEAN Digital Ministers' Meeting… Указ. ресурс.
[36] Авдийский В. И., Иванов А. В., Коннова И. Г. Институционализация цифрового суверенитета государства в сфере информационной безопасности // Информатизация в цифровой экономике. 2024. Т. 5, № 3. С. 385–400. DOI: 10.18334/ide.5.3.121571.
[37] Sari M. N. Cybercrime in Association of Southeast Asian Nations: Regional Effort and Its Effectiveness // Journal of Information Policy. 2024. Vol. 14. С. 568–598. DOI: 10.5325/jinfopoli.14.2024.0016.
[38] Rahman M. F. A. Advancing Cyber and Information Security Cooperation in ASEAN. RSIS Commentary. 2023. № 001. 4 January. URL: https://www.rsis.edu.sg/wp-content/uploads/2023/01/IP23001.pdf
[39] Россия и АСЕАН в АТР: динамика взаимодействия, региональные процессы и глобальный контекст. К 25-летию диалогового партнёрства и 30-летию отношений России и АСЕАН : сборник научных статей / под ред. Е. В. Колдуновой, Н. С. Куклина, В. В. Вершининой ; Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Центр АСЕАН. — Москва : МГИМО-Университет, 2022. — 183, [1] с. : цв. ил. ISBN 978-5-9228-2612-9.