

Научная статья. Политические науки  
УДК 327(5)  
DOI: 10.31696/2072-8271-2025-1-1-66-214-227

## **СОТРУДНИЧЕСТВО ФИЛИППИН С ЯПОНИЕЙ И РЕСПУБЛИКОЙ КОРЕЯ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ В ФОРМАТЕ АСЕАН+3**

Денис Олегович ЗЛОБИН<sup>1</sup>, Иван Александрович МОЛДАВАНОВ<sup>2</sup>,  
Александра Сергеевна ХИТЕВА<sup>3</sup>

<sup>1,2,3</sup> НИУ ВШЭ, Москва, Россия,

<sup>1</sup> dozlobin@edu.hse.ru, <https://orcid.org/0009-0000-0898-2510>

<sup>2</sup> ivan\_moldavanov@icloud.com, <https://orcid.org/0009-0003-4494-3027>

<sup>3</sup> alexakhiteva@inbox.ru, <https://orcid.org/0009-0002-0555-9615>

**Аннотация:** Филиппины, как один из основателей АСЕАН, усиливают участие в региональных инициативах по обеспечению кибербезопасности. На фоне растущей конкуренции между США и Китаем в цифровом пространстве страна стремится сбалансировать сотрудничество с технологически развитыми партнёрами, включая Японию и Южную Корею. В условиях политической нестабильности и слабой институциональной базы Филиппины выстраивают партнёрства, способствующие повышению их цифровой устойчивости. При этом, в условиях растущей технологической зависимости и усиливающегося давления со стороны США, которые последовательно продвигают собственные интересы под прикрытием коалиционной риторики, партнёрские инициативы приобретают всё более односторонний характер. Наиболее заметными являются инициативы в рамках АСЕАН+3, а также двусторонние соглашения Филиппин с Японией и Южной Кореей, выявляя как стратегические интересы сторон, так и факторы, ограничивающие результативность этих партнёрств.

**Ключевые слова:** Кибербезопасность, Филиппины, АСЕАН, Япония, Республика Корея, АСЕАН+3, региональное сотрудничество, конкуренция США и Китая

**Благодарности:** Статья подготовлена в рамках проекта №25-00-05 («Национальные и региональные стратегии и институты кибербезопасности стран Восточной и Юго-Восточной Азии») Программы «Научный фонд Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ) <https://www.hse.ru/org/projects/1029382855>

**Для цитирования:** Злобин Д.О., Молдаванов И.А., Хитева А.С. Сотрудничество Филиппин с Японией и Республикой Корея в сфере кибербезопасности в формате АСЕАН+3 // Юго-Восточная Азия: актуальные проблемы развития, 2025, Том 1, № 1 (66). С. 214–227. DOI: 10.31696/2072-8271-2025-1-1-66-214-227

Original article. Political science

## COOPERATION OF THE PHILIPPINES WITH JAPAN AND THE REPUBLIC OF KOREA IN THE FIELD OF CYBERSECURITY IN THE ASEAN+3 FORMAT

Denis O. ZLOBIN<sup>1</sup>, Ivan A. MOLDAVANOV<sup>2</sup>, Anastasia S. KHITEVA<sup>3</sup>

<sup>1,2,3</sup> HSE University, Moscow, Russia

<sup>1</sup> dozlobin@edu.hse.ru, <https://orcid.org/0009-0000-0898-2510>

<sup>2</sup> ivan\_moldavanov@icloud.com, <https://orcid.org/0009-0003-4494-3027>

<sup>3</sup> alexakhiteva@inbox.ru, <https://orcid.org/0009-0002-0555-9615>

**Abstract:** As a founding member of ASEAN, the Philippines is increasing its participation in regional cybersecurity initiatives. The country is striving to balance cooperation with technologically advanced partners, including Japan and South Korea, in the digital space, amid growing competition between the U.S. and China. In the context of political instability and weak institutional frameworks, the Philippines has been developing partnerships that enhance its digital resilience. However, with increasing technological dependence and mounting pressure from the U.S., which has consistently promoted its own interests under the guise of coalition rhetoric, partnership initiatives have become increasingly unilateral. The most notable are the ASEAN+3 initiatives, as well as bilateral agreements with Japan and South Korea. This article examines the current formats, priorities, and limitations of cyber cooperation with Japan and South Korea, identifying both the strategic interests of the parties and the factors that limit the effectiveness of these partnerships.

**Keywords:** *Cybersecurity, Philippines, ASEAN, Japan, South Korea, ASEAN+3, regional cooperation, digital resilience, U.S.-China competition, bilateral agreements*

**Acknowledgments:** *The publication was prepared within the framework of the Academic Fund Program at HSE University (grant №25-00-05 “National and Regional Strategies and Institutions of Cybersecurity in East and Southeast Asia”).*

**For citation:** Zlobin D.O., Moldavanov I.A., Khiteva A.S. Cooperation of the Philippines with Japan and the Republic of Korea in the Field of Cybersecurity in the ASEAN+3 Format. *Yugo-Vostochnaya Aziya: aktual'nyye problemy razvitiya*, 2025, T. 1, №1 (66). Pp. 214–227. DOI: 10.31696/2072-8271-2025-1-1-66-214-227

## Введение

Кибербезопасность становится неотъемлемым элементом национальной и региональной безопасности. Для Филиппин, сталкивающихся с растущими угрозами в цифровом пространстве и уязвимой внутривластной обстановкой, сотрудничество с внешними партнерами — один из ключевых инструментов модернизации. В условиях формирующейся многополярности, нестабильного международного порядка и геополитической напряженности в Южно-Китайском море основным вызовом становится не только развитие технической устойчивости, но и сохранение стратегической автономии, чтобы не превратиться в инструмент реализации внешней повестки США.

Необходимость переосмысления международных отношений подчеркивается в книге Амитава Ачарьи *The End of American World Order*<sup>1</sup>, где автор ставит под сомнение доминирующий западноцентричный взгляд на международные отношения и мировые порядки и акцентирует внимание на важности учёта альтернативных, незападных перспектив. Однако реальные процессы в АТР показывают сложность этого перехода. Исследования авторов Г.Ю. Никопорец-Такигава, Е.Р. Ощепкова, О.А. Филатова и А.С. Хитевой показывают, что, несмотря на стремление стран АСЕАН развивать собственную стратегию кибербезопасности, их усилия во многом политизируются и оказываются под влиянием геополитических амбиций ведущих держав<sup>2</sup>. Для некоторых государств региона, таких как Филиппины, ориентация на американоцентричный вектор остаётся вынужденной стратегией, отражающей стремление обеспечить национальную безопасность в условиях растущей нестабильности и ограниченных внутренних ресурсов.

## Методология исследования

Данное исследование основано на использовании методов качественного анализа нормативно-правовых актов, стратегических документов и межгосударственных соглашений, а также на сопоставлении подходов Филиппин, Южной Кореи и Японии к обеспечению кибербезопасности в контексте АСЕАН+3.

Материалом являются первоисточники и открытые данные ведущих международных организаций и государственных структур:

1. Национальные стратегии кибербезопасности Филиппин<sup>3</sup>, Японии<sup>4</sup> и Республики Корея<sup>5</sup>. Эти документы позволили определить прио-

ритеты государств в сфере кибербезопасности, институциональные подходы и меры по защите критической инфраструктуры.

2. Межгосударственные соглашения и политические заявления: Соглашение между Японией и Республикой Филиппины о содействии взаимному доступу и сотрудничеству между Силами самообороны Японии и Вооруженными силами Филиппин (*The Agreement between Japan and the Republic of the Philippines concerning the facilitation of Reciprocal Access and Cooperation between the Self-Defense Forces of Japan and the Armed Forces of the Philippines*)<sup>6</sup>, Меморандум о взаимопонимании по вопросам защиты персональных данных между Южной Кореей и Филиппинами (*MOU on data protection*)<sup>7</sup>, Совместная декларация о стратегическом партнерстве между Республикой Филиппины и Республикой Корея (*Joint Declaration on the Strategic Partnership between the Republic of the Philippines and the Republic of Korea*)<sup>8</sup>, Совместное заявление Японии и Филиппин (*Japan–Philippines Joint Statement*)<sup>9</sup>, План действий АСЕАН-Республики Корея по реализации Совместного заявления о видении мира, процветания и партнерства (2021-2025 гг.) (*ASEAN-Republic of Korea Plan of Action to Implement The Joint Vision Statement for Peace, Prosperity and Partnership (2021–2025)*)<sup>10</sup>. Анализ данных источников позволил выявить характер и направленность двустороннего сотрудничества, в том числе в области кибербезопасности, защиты персональных данных и обмена информацией.
3. Региональные инициативы и другие платформы взаимодействия в рамках АСЕАН+3: стратегия АСЕАН по сотрудничеству в области кибербезопасности (*ASEAN Cybersecurity Cooperation Strategy 2021-2025*)<sup>11</sup>, итоги 16-го совещания АСЕАН и Японии по вопросам политики кибербезопасности (*Outcomes of the 16th ASEAN-Japan Cybersecurity Policy Meeting*)<sup>12</sup>, итоги 16-го заседания АСЕАН с Республикой Корея и Японией по составлению плана действий по реализации Совместного заявления о видении мира, процветания и партнерства (2021-2025 гг.) (*ASEAN-Republic of Korea Plan of Action to Implement the Joint Vision Statement for Peace, Prosperity and Partnership (2021-2025)*)<sup>13</sup>, Соглашение о региональном всеобъемлющем экономическом партнерстве (RCEP)

(*Regional Comprehensive Economic Partnership (RCEP Agreement)*)<sup>14</sup>, Альянс сообщества кибербезопасности АСЕАН и Японии (*ASEAN-Japan Cybersecurity Community Alliance, AJCCA*)<sup>15</sup>, Фонд интеграции Японии и стран АСЕАН (*Japan-ASEAN Integration Fund*)<sup>16</sup>, Организационная структура ACICE (*ACICE Organization Structure*)<sup>17</sup> — эти источники использовались для анализа архитектуры региональной кооперации, вовлеченности Японии и Республики Корея в инициативы по построению устойчивой системы кибербезопасности в Юго-Восточной Азии, а именно, формате АСЕАН+3.

Также в статье применялся сравнительный метод, позволяющий сопоставить национальные стратегии и практики Японии, Филиппин и Южной Кореи в контексте их вклада в архитектуру кибербезопасности региона. Сравнительный анализ позволил проследить как общие черты (ориентация на международное сотрудничество, развитие кадрового потенциала, повышение защищенности критической инфраструктуры), так и различия, обусловленные национальными приоритетами и геополитическими обстоятельствами.

### **Инициативы АСЕАН в сфере коллективной кибербезопасности**

Формат АСЕАН+3 (включая Японию, Южную Корею и Китай) является важным региональным механизмом в сфере цифровой безопасности в Юго-Восточной Азии. В рамках Стратегии сотрудничества АСЕАН в сфере кибербезопасности (*Cybersecurity Cooperation Strategy, CCS*) на 2021–2025 гг., принятой в 2017 г., разработаны ключевые инициативы для укрепления региональной безопасности в киберпространстве<sup>18</sup>.

Одной из ключевых инициатив является создание Региональной группы реагирования на компьютерные чрезвычайные ситуации (*ASEAN CERT*)<sup>19</sup>. С января 2025 г. Малайзия стала первым региональным координатором *ASEAN CERT*, базирующейся в Сингапуре и отвечающей за реакцию на киберугрозы в регионе<sup>20</sup>.

Важными элементами в региональной архитектуре кибербезопасности также являются такие инициативы, как *ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)*, финансируемый Фондом интеграции Япония-АСЕАН (*JAIF*), *ASEAN-Japan*

*Cybersecurity Policy Meeting*, а также *ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)*, *ASEAN-China Cyber Dialogue*, *ASEAN-Republic of Korea (ROK) Digital Work Plan (2021–2025 годы)* и *ASEAN Ministerial Conference on Cybersecurity (AMCC)*, *ASEAN Cybersecurity Coordination Centre (ACCC)* и *ASEAN Digital Ministers' Meeting (ADGMIN)*<sup>21</sup>. Кроме того, Япония всесторонне развивает сотрудничество в области технологий кибербезопасности, продвигая проект *JASPER (Japan-ASEAN Security Partnership)*<sup>22</sup>.

Филиппины активно участвуют в региональных инициативах, поскольку страна крайне заинтересована в выработке коллективных решений в области кибербезопасности, что отражено в действующем Национальном плане кибербезопасности на 2023–2028 гг.<sup>23</sup>. В то же время для достижения этих целей важную роль играет и развитие двустороннего сотрудничества, которое позволяет более оперативно и эффективно реагировать на возникающие киберугрозы.

### **Двустороннее сотрудничество Филиппин с Южной Кореей в сфере кибербезопасности**

Республика Корея занимает лидирующие позиции в сфере кибербезопасности, что подтверждается её высоким рейтингом в глобальном индексе кибербезопасности 2024 г.<sup>24</sup>. Страна демонстрирует успешные результаты по пяти ключевым параметрам: законодательной базе, техническим возможностям, организации национальной стратегии, образовательной политике и международной кооперации. Эти достижения, однако, частично обусловлены геополитической ситуацией в регионе, в частности угрозами со стороны Северной Кореи, что оказывает влияние на приоритеты национальной безопасности Республики Корея<sup>25</sup>.

Сотрудничество в области кибербезопасности с Филиппинами основано на ряде важных проектов, которые демонстрируют рост двусторонних связей и общих интересов. В 2024 г. правительство Филиппин выразило намерение обратиться к Республике Корея с просьбой о предоставлении финансовой помощи в размере 20 млн долларов, предполагая использование этих средств для модернизации национальной инфраструктуры в сфере кибербезопасности<sup>26</sup>. Планируется, в частности, развитие центров обработки данных, а также усиление механизмов киберзащиты. На момент подготовки данного материала официальных данных о фактическом предоставлении финансирования выявлено не было, что позволяет предположить — обсуждение проекта продолжается и окончательных договорённостей стороны пока не

достигли. Тем не менее сам факт проведения переговоров указывает на растущее значение киберсотрудничества в двусторонней повестке.

Дополнительным свидетельством активизации взаимодействия в данной сфере стал Меморандум о взаимопонимании по вопросам защиты персональных данных, подписанный в ноябре 2024 г. между Комиссией по защите персональной информации Республики Корея и Национальной комиссией по защите персональных данных Филиппин<sup>27</sup>. Этот документ можно рассматривать как шаг к углублению сотрудничества и выработке согласованных подходов к регулированию цифровой сферы.

Кроме того, в 2024 г. была подписана Совместная декларация о стратегическом партнерстве, в которой отражено намерение расширить взаимодействие в области обороны, безопасности, экономики и технологий, включая кибербезопасность<sup>28</sup>.

Еще одним документом, затрагивающим вопросы кибербезопасности и защиты данных, стал Меморандум о взаимопонимании о морском сотрудничестве, который, наряду с укреплением взаимодействия в области морской безопасности, предусматривает обмен данными для повышения оперативного реагирования на инциденты, включая возможные киберугрозы<sup>29</sup>.

Однако, несмотря на заключение ряда соглашений, сотрудничество в области кибербезопасности между Республикой Корея и Филиппинами остается ограниченным. Большинство инициатив реализуется через многосторонние форматы, прежде всего в рамках АСЕАН, тогда как прямые двусторонние механизмы пока развиты недостаточно.

Республика Корея активно работает в рамках региональных платформ, таких как *ADMM-Plus*, в которых обсуждаются вопросы кибербезопасности<sup>30</sup>. Это сотрудничество даёт возможность обеим странам делиться опытом, но не всегда приводит к формализации двусторонних соглашений.

Тем не менее, определённые положительные результаты сотрудничества подтверждаются такими инициативами, как киберучения *CYTREX*, организованные Южной Кореей в 2023 г.<sup>31</sup>. Учения включали исследование кибератак и работу с вредоносным ПО, что способствовало повышению уровня взаимодействия в сфере киберугроз. Также стоит отметить проект *ASEAN Cyber Shield*, в котором Республика Корея активно участвует, предоставляя образовательные и тренинговые ресурсы для стран-членов АСЕАН, включая Филиппины<sup>32</sup>.

Среди факторов, замедляющих развитие более глубокого двустороннего сотрудничества, можно выделить различия в приоритетах Филиппин и Республики Корея, а также постоянно обновляющуюся стратегию развития кибербезопасности на Филиппинах, что ограничивает возможности для создания устоявшихся механизмов взаимодействия.

Это связано, во-первых, с тем, что Республика Корея активно сотрудничает в области кибербезопасности через механизмы АСЕАН: большая часть взаимодействия происходит именно в многостороннем формате, а не через прямые двусторонние соглашения. Во-вторых, у Филиппин и Республики Корея различаются национальные приоритеты: Филиппины акцентируют внимание прежде всего на обороне, инфраструктурных проектах, торговле и экономическом партнёрстве, в то время как кибербезопасность занимает менее значимое место в их двусторонней повестке. В-третьих, Филиппины продолжают процесс укрепления собственной национальной инфраструктуры кибербезопасности, а их стратегические подходы пока не полностью совпадают с южнокорейскими, что также тормозит выстраивание формализованных соглашений. В результате, вместо заключения юридически обязывающих документов, сотрудничество между странами в сфере кибербезопасности реализуется преимущественно через программы обучения, обмена опытом и наращивания потенциала.

Таким образом, несмотря на формальные шаги и высокие намерения, сотрудничество Филиппин и Южной Кореи в области кибербезопасности остаётся на стадии развития и во многом зависит от внешнеполитических факторов и региональных инициатив.

### **Двустороннее сотрудничество Филиппин с Японией**

Япония оказывает значительное влияние на формирование политики кибербезопасности Филиппин, опираясь как на двусторонние соглашения, так и на участие в региональных инициативах. Однако это влияние всё чаще реализуется в логике общей стратегии США по усилению контроля над цифровыми пространствами своих союзников.

Япония выделила кибербезопасность в отдельное направление ещё в 2000 г., приняв в 2015 г. «Стратегию кибербезопасности», обновлённую в 2021 г.<sup>33</sup>. Основное внимание уделялось защите критически важной инфраструктуры, включая коммуникационные сети Сил самообороны и государственные интернет-ресурсы. Однако значительная часть запланированных мер не была реализована из-за хронической нехватки финансирования и кадрового дефицита<sup>34</sup>. Нацио-

нальная стратегия безопасности 2022 г.<sup>35</sup> зафиксировала стремление Японии увеличить инвестиции в киберсферу, однако фактические затраты по-прежнему остаются значительно ниже потребностей<sup>36</sup>.

В условиях ограниченных внутренних возможностей<sup>37</sup> Япония активизировала сотрудничество с Филиппинами, рассматривая его как способ укрепления своего влияния в Юго-Восточной Азии. Одним из ключевых шагов стало подписание Соглашения о взаимном доступе (RAA) 8 июля 2024 г., которое, помимо оборонного компонента, заложило основу для развития совместных инициатив в сфере кибербезопасности. В частности, положения о защите данных военнослужащих (Статья 15 Соглашения) подразумевают углубление взаимодействия в вопросах цифровой защиты, что особенно актуально на фоне возросших угроз со стороны Китая<sup>38</sup>.

Отдельное значение имеет развитие трехстороннего формата Япония–США–Филиппины. В октябре 2024 г. состоялся первый кибердиалог, на котором стороны обменялись мнениями по широкому кругу вопросов в области кибер- и цифровой безопасности. В частности, обсуждались меры по защите подводных интернет-кабелей, укрепление взаимодействия между национальными центрами реагирования на инциденты (*CERT*), развитие технологий *Open RAN*, а также вопросы наращивания потенциала в области кибербезопасности<sup>39</sup>. Эта работа стала частью американской инициативы *Hunt Forward*, направленной на укрепление киберустойчивости союзников США<sup>40</sup>. Япония активно поддерживает эти усилия, выступая одновременно в роли самостоятельного участника и проводника стратегических интересов Вашингтона.

Помимо двусторонних и трёхсторонних форматов, Япония сохраняет активность в рамках региональных платформ АСЕАН, таких как *AJCPM* и *AJCSA*<sup>41</sup>. Однако повестка встреч всё чаще определяется внешними приоритетами — усилением информационного обмена, развитием глобальных систем мониторинга угроз и созданием единого пространства безопасности в интересах крупнейших держав<sup>42</sup>. Особое внимание заслуживает договор о Всестороннем региональном экономическом партнёрстве (ВРЭП), в котором кибербезопасность рассматривается как элемент цифровой инфраструктуры торговли. Статья 12.13 ВРЭП подчёркивает необходимость развития совместных «соответствующих компетентных органов, отвечающих за реагирование на инциденты, связанные с компьютерной безопасностью»<sup>43</sup>. Похожие положения зафиксированы в соглашении *DEFA (Digital Economy*

*Framework Agreement*), разрабатываемом странами АСЕАН, в котором особый акцент сделан на необходимости развития кибербезопасности и мер цифровой аутентификации. В качестве основного критерия по отслеживанию прогресса в области кибербезопасности предлагается ориентироваться на *GCI (Global Cybersecurity Index)*, рассчитывающий возможности стран в данной сфере при помощи оценки риска, которому подвергается корпоративная, промышленная и правительственная информационная инфраструктура в результате воздействия целого спектра угроз кибербезопасности<sup>44</sup>. Помимо оценки состояния, планируется создание единого центра реагирования по противодействию кибератакам и соответствующая доработка правовой базы. Это позволяет ожидать, что с развитием электронной торговли в рамках ВРЭП опыт *DEFA* станет основой для укрепления системы кибербезопасности, направленной на защиту электронной торговли от угроз.

Таким образом, сотрудничество Японии и Филиппин в сфере кибербезопасности развивается в двух направлениях: как средство укрепления позиций Токио в регионе и как элемент более широкой стратегии США по созданию сети союзников в цифровом пространстве. При этом самостоятельность филиппинской киберполитики постепенно снижается под влиянием внешних факторов.

### Геополитический контекст сотрудничества

Геополитическое соперничество между США и Китаем оказывает прямое влияние на формирование стратегий кибербезопасности стран Азиатско-Тихоокеанского региона. Формат АСЕАН+3, включающий Японию, Южную Корею и Китай, становится не только площадкой для технического сотрудничества, но и ареной конкуренции за цифровое влияние. В этом контексте США всё чаще действуют через своих союзников, что ограничивает автономию стран региона, таких как Филиппины, в выборе внешнеполитических и оборонных стратегий.

Китай активно продвигает свою цифровую повестку, предлагая АСЕАН совместные проекты по развитию инфраструктуры, облачных вычислений и ИИ<sup>45</sup>. Однако его вовлечённость воспринимается неоднозначно. Для Южной Кореи и Японии главной угрозой остаётся КНДР<sup>46</sup>, тогда как Филиппины всё чаще рассматривают Китай как источник киберугроз. В Японии это отражено в стратегии безопасности<sup>47</sup>, а на Филиппинах — в риторике и практике взаимодействия, особенно в контексте ситуации в Южно-Китайском море<sup>48</sup>. Это разли-

чие в восприятии источников угроз подталкивает страны региона к выбору стратегических партнёров.

Однако усиливая сотрудничество с Японией и Южной Кореей, Филиппины фактически втягиваются в орбиту американской политики, где платформы вроде *DEFA* и *RCEP* всё больше становятся инструментами не только продвижения цифровой инфраструктуры, но и усиления внешнего контроля над внутренними цифровыми процессами. Программные инициативы, такие как *Hunt Forward*, делают партнёров США не только активными участниками, но и проводниками американских стратегических интересов в регионе.

Несмотря на активность Китая в рамках АСЕАН+3 и наличие множества инициатив по кибербезопасности, скрытая доминанта США через Японию и Южную Корею ограничивает пространство манёвра для стран, таких как Филиппины. Это делает их участие в региональных инициативах менее самостоятельным, подверженным влиянию изменений в политике Вашингтона.

### Заключение

Развитие сотрудничества Филиппин с Японией и Республикой Корея в области кибербезопасности подчеркивает растущую роль цифровой сферы в региональной повестке и внешнеполитических стратегиях стран Восточной Азии. Тем не менее за внешне прагматичными инициативами прослеживается сложный геополитический фон: даже наиболее структурированные и амбициозные партнёрства оказываются ограничены рамками влияния ведущих внешних акторов.

Япония и Республика Корея, при всей риторике стратегической автономии, продолжают действовать в рамках интересов США. Их участие в программах, таких как *Hunt Forward*, и в двусторонних форматах взаимодействия с Вашингтоном указывает на подчиненность логике союзнических обязательств. В этом контексте Филиппины сталкиваются с риском: даже те инициативы в области кибербезопасности, которые позиционируются как нейтральные, могут быть адаптированы в зависимости от изменений внешнеполитического курса США.

Следовательно, несмотря на наличие практической отдачи от текущих форм киберсотрудничества, они вряд ли могут служить фундаментом для устойчивого и независимого развития в цифровой сфере. Без стратегической переориентации и постепенного формирования собственной институциональной базы в области кибербезопасности страна рискует сохранить зависимое положение, где внешняя помощь

всё чаще выступает не как катализатор модернизации, а как канал для внешнего влияния.

В условиях роста киберугроз и обострения глобальной конкуренции центральным вызовом для Филиппин становится не только техническое укрепление цифрового сектора, но и политико-стратегический выбор в пользу цифрового суверенитета — как основы долгосрочной устойчивости и самостоятельности.

#### ИНФОРМАЦИЯ ОБ АВТОРАХ

**ЗЛОБИН Денис Олегович**, стажер-исследователь научно-учебной группы «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке», НИУ ВШЭ, Москва, Россия

**МОЛДАВАНОВ Иван Александрович**, стажер-исследователь научно-учебной группы «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке», НИУ ВШЭ, Москва, Россия

**ХИТЕВА Александра Сергеевна**, менеджер и руководитель медиа-направления Научно-учебной лаборатории исследований современного Ирана, стажер-исследователь научно-учебной группы «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке», руководитель проекта «Поворот на Восток: Филиппины», НИУ ВШЭ, Москва, Россия

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 10.05.2025; одобрена после рецензирования 26.05.2025; принята к публикации 30.05.2025.

#### INFORMATION ABOUT THE AUTHORS

**Denis O. ZLOBIN**, research intern, scientific and educational group “ASEAN+, BRICS+, NATO+: Prospects for Asian Integration in the New World Order”, HSE University, Moscow, Russia

**Ivan A. MOLDAVANOV**, research intern, scientific and educational group “ASEAN+, BRICS+, NATO+: Prospects for Asian Integration in the New World Order”, HSE University, Moscow, Russia

**Alexandra S. KHITEVA**, manager and head of the media department of the Scientific and Educational Laboratory for Contemporary Iranian Studies, research intern of the scientific and educational group “ASEAN+, BRICS+, NATO+: Prospects for Asian Integration in the New World Order”, head of the project “Turn to the East: Philippines”, HSE University, Moscow, Russia

Contributions of the authors: the authors contributed equality to this article. The authors declare no conflicts of interests.

The article was submitted 10.05.2025; approved 26.05.2025; accepted to publication 30.05.2025.

<sup>1</sup> Acharya A. The end of American world order. – 2018.

<sup>2</sup> Никипорец-Такигава Г. Ю., Ощепков Е. Р., Филатов О. А., Хитева А.С. Национальные и региональные стратегии и институты кибербезопасности стран АСЕАН в контексте архитектуры кибербезопасности ЮВА / В кн.: Проблемы информационной безопасности и их решение в странах Юго-Восточной Азии и Южно-Тихоокеанского региона. М. : Институт востоковедения РАН, 2024. Гл. 3. С. 69-100.

<sup>3</sup> Government of the Philippines. National Cybersecurity Plan 2023-2028. URL: <https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf?ref=cybersecurity.ph>

<sup>4</sup> The Government of Japan. Cybersecurity Strategy. URL: <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en.pdf>

- <sup>5</sup> Government of the Republic of Korea. National Cybersecurity Strategy. URL: <https://www.president.go.kr/download/6698bbbf46cda>
- <sup>6</sup> Ministry of Foreign Affairs. The Agreement between Japan and the Republic of the Philippines concerning the facilitation of Reciprocal Access and Cooperation between the Self-Defense Forces of Japan and the Armed Forces of the Philippines. 2024. URL: <https://www.mofa.go.jp/files/100694772.pdf>
- <sup>7</sup> National Privacy Commission. South Korea and Philippines Ink MOU to Enhance Data Protection Collaboration. URL: <https://privacy.gov.ph/south-korea-and-philippines-ink-mou-to-enhance-data-protection-collaboration/>
- <sup>8</sup> National Government Portal. Joint Declaration on the Strategic Partnership between the Republic of the Philippines and the Republic of Korea. URL: [https://pco.gov.ph/news\\_releases/joint-declaration-on-the-strategic-partnership-between-the-republic-of-the-philippines-and-the-republic-of-korea/](https://pco.gov.ph/news_releases/joint-declaration-on-the-strategic-partnership-between-the-republic-of-the-philippines-and-the-republic-of-korea/)
- <sup>9</sup> Japan–Philippines Joint Statement. URL: [100457513.pdf](https://www.mofa.go.jp/files/100457513.pdf)
- <sup>10</sup> ASEAN-Republic of Korea Plan of Action to Implement the Joint Vision Statement for Peace, Prosperity and Partnership (2021–2025). URL: <https://asean.org/wp-content/uploads/2021/03/16.-ASEAN-ROK-POA-2021-2025-Final.pdf>
- <sup>11</sup> ASEAN Cybersecurity Cooperation Strategy 2021-2025. URL: [https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025\\_final-23-0122.pdf](https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf)
- <sup>12</sup> Outcomes of the 16th ASEAN-Japan Cybersecurity Policy Meeting. Ministry of Economy, Trade and Industry. URL: [https://www.meti.go.jp/english/press/2023/1006\\_003.html](https://www.meti.go.jp/english/press/2023/1006_003.html)
- <sup>13</sup> ASEAN-Republic of Korea Plan of Action to Implement the Joint Vision Statement for Peace, Prosperity and Partnership (2021-2025).
- <sup>14</sup> Regional Comprehensive Economic Partnership (RCEP) Agreement. 2020. Chapter 12. Article 12.3. URL: [http://fta.mofcom.gov.cn/rcep/rceppdf/d12z\\_en.pdf](http://fta.mofcom.gov.cn/rcep/rceppdf/d12z_en.pdf)
- <sup>15</sup> ASEAN-Japan Cybersecurity Community Alliance (AJCCA). URL: <https://ajcca.net/>
- <sup>16</sup> Japan-ASEAN Integration Fund. URL: <https://jaif.asean.org/>
- <sup>17</sup> ACICE Organisation Structure. URL: <https://www.acice-asean.org/orgstructure/>
- <sup>18</sup> ASEAN Cybersecurity Cooperation Strategy 2021-2025. URL: [https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025\\_final-23-0122.pdf](https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf)
- <sup>19</sup> International: Singapore establishes ASEAN Regional CERT. One Trust Data Guidance. February 7, 2024. URL: <https://www.dataguidance.com/news/international-singapore-establishes-asean-regional-cert>
- <sup>20</sup> Малайзия приступает к председательству в АСЕАН. NEO. 1 февраля, 2025. URL: <https://journal-neo.su/ru/2025/02/01/malajziya-pristupaet-k-predsdatelstvu-v-asean/>
- <sup>21</sup> ASEAN's Cyber Initiatives: A Select List. CSIS. July 16, 2024. URL: <https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list>
- <sup>22</sup> The National Center of Incident Readiness and Strategy for Cybersecurity. International Strategy on Cybersecurity Cooperation. 2013. P. 12. URL: [https://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation\\_e.pdf](https://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf)
- <sup>23</sup> Government of the Philippines. National Cybersecurity Plan 2023-2028. URL: <https://dict.gov.ph/wp-content/uploads/2024/02/NCSP-2023-2028-FINAL.pdf>
- <sup>24</sup> International Telecommunication Union. Global cybersecurity index 2024. URL: [https://www.itu.int/dms\\_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf](https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf)
- <sup>25</sup> Government of the Republic of Korea. National Cybersecurity Strategy. URL: <https://www.president.go.kr/download/6698bbbf46cda>
- <sup>26</sup> DICT eyes World Bank, South Korea financial aid for cybersecurity. Philstar Global. March 18, 2024. URL: <https://www.philstar.com/headlines/2024/03/18/2341368/dict-eyes-world-bank-south-korea-financial-aid-cybersecurity>
- <sup>27</sup> National Privacy Commission. South Korea and Philippines Ink MOU to Enhance Data Protection Collaboration. URL: <https://privacy.gov.ph/south-korea-and-philippines-ink-mou-to-enhance-data-protection-collaboration/>
- <sup>28</sup> National Government Portal. Joint Declaration on the Strategic Partnership between the Republic of the Philippines and the Republic of Korea. URL: [https://pco.gov.ph/news\\_releases/joint-declaration-on-the-strategic-partnership-between-the-republic-of-the-philippines-and-the-republic-of-korea/](https://pco.gov.ph/news_releases/joint-declaration-on-the-strategic-partnership-between-the-republic-of-the-philippines-and-the-republic-of-korea/)

- <sup>29</sup> S. Korea Upgrades Ties with Philippines, Backs Manila's Maritime Rights. The Maritime Executive. October 8, 2024. URL: <https://maritime-executive.com/article/s-korea-upgrades-ties-with-philippines-backs-manila-s-maritime-rights>
- <sup>30</sup> Korea hosts ASEAN-Plus cybersecurity training. The Korea Times. November 10, 2023. URL: <https://www.koreatimes.co.kr/foreignaffairs/20231110/korea-hosts-asean-plus-cybersecurity-training>
- <sup>31</sup> Korea hosts ASEAN-Plus cybersecurity training. The Korea Times. November 10, 2023.
- <sup>32</sup> ASEAN Korea Cooperation Fund. ASEAN Cyber Shield (ACS) Project. URL: <https://www.aseanrofund.com/our-works/project-asean-cyber-shield-acs-project>
- <sup>33</sup> Никипорец-Такигава Г. Ю. Стратегия национальной кибербезопасности Японии: проблемное поле и ловушки подхода. – Полис. Политические исследования. 2025. № 3. С. 162-175. <https://doi.org/10.17976/jpps/2025.03.11>. EDN: QATTIV С. 164-165
- <sup>34</sup> Inagaki K., Lewis L. 'Who Is Going to Pay for Japan's Military Build-up'? Financial Times. 2022. URL: <https://www.ft.com/content/f3c457e5-82ee-462f-b8f3-c701a8e4840e>
- <sup>35</sup> National Security Strategy of Japan. 2022. URL: [https://www.cas.go.jp/jp/siryoku/221216anzenhoshou/national\\_security\\_strategy\\_2022\\_pamphlet-e.pdf](https://www.cas.go.jp/jp/siryoku/221216anzenhoshou/national_security_strategy_2022_pamphlet-e.pdf)
- <sup>36</sup> National Security Strategy of Japan. 2022.
- <sup>37</sup> Takahashi Kosuke. Why Japan Is Lagging Behind in Cyber Defense Capabilities. May 24, 2024. URL: <https://thediplomat.com/2024/05/why-japan-is-lagging-behind-in-cyber-defense-capabilities/>
- <sup>38</sup> Ministry of Foreign Affairs. The Agreement between Japan and the Republic of the Philippines concerning the facilitation of Reciprocal Access and Cooperation between the Self-Defense Forces of Japan and the Armed Forces of the Philippines. 2024. URL: <https://www.mofa.go.jp/files/100694772.pdf>
- <sup>39</sup> Ministry of Foreign Affairs of Japan. The 1st Japan-U.S.-Philippines Cyber-Digital Dialogue. URL: [https://www.mofa.go.jp/press/release/pressite\\_000001\\_00661.html](https://www.mofa.go.jp/press/release/pressite_000001_00661.html)
- <sup>40</sup> Atlantic Council. The 5x5—The US-Japan-South Korea trilateral cybersecurity relationship. URL: <https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-the-us-japan-south-korea-trilateral-cybersecurity-relationship>
- <sup>41</sup> AJCCA. Annual Report. 2024. URL: <https://ajcca.net/storage/preview/GBoha8TkJ8AGIYD746fk6GjBgXyzoymcspLFOui.pdf>
- <sup>42</sup> AJCCA. Annual Report. 2024.
- <sup>43</sup> Regional Comprehensive Economic Partnership (RCEP) Agreement. 2020. Chapter 12. Article 12.3. URL: [http://fta.mofcom.gov.cn/rcep/rceppdf/d12z\\_en.pdf](http://fta.mofcom.gov.cn/rcep/rceppdf/d12z_en.pdf)
- <sup>44</sup> ASEAN. Digital Economy Framework Agreement. 2024. URL: [https://asean.org/wp-content/uploads/2024/11/DEFA-Report-public-summary-expanded\\_Final\\_25112024.pdf](https://asean.org/wp-content/uploads/2024/11/DEFA-Report-public-summary-expanded_Final_25112024.pdf)
- <sup>45</sup> China, ASEAN to boost digital cooperation. China Daily. January 22, 2025. URL: <https://global.chinadaily.com.cn/a/202501/22/WS67902db8a310a2ab06ea86a0.html>
- <sup>46</sup> Government of the Republic of Korea. National Cybersecurity Strategy. URL: <https://www.president.go.kr/download/6698bbb46cda>
- <sup>47</sup> National Security Strategy of Japan. 2022.
- <sup>48</sup> No current info compromised, DICT says of alleged Chinese hacking. Philippine News Agency. January 7, 2025. URL: <https://www.pna.gov.ph/index.php/articles/1241192>