СЕМИНАР

# СОТРУДНИЧЕСТВО ЯПОНИИ С ФИЛИППИНСКОЙ РЕСПУБЛИКОЙ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ. ПОДХОДЫ И ПРОБЛЕМНОЕ ПОЛЕ

***Никипорец-Такигава Галина Юрьевна***, *д.п.н., профессор,*

*руководитель НУГ «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции» ФМЭиМП НИУ ВШЭ, Gnikiporets-takigawa@hse.ru*

***Хитева Александра Сергеевна***, *исследователь НУГ «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции» ФМЭиМП НИУ ВШЭ, akhiteva@hse.ru*


*Доклад подготовлен в рамках проекта «Национальные и региональные стратегии и институты кибербезопасности стран Восточной и Юго-Восточной Азии»*
*НУГ «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке»*

# МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ФОРМИРОВАНИЯ НОВОГО МИРОВОГО ПОРЯДКА

Кибербезопасность сохраняет перспективы взаимодействия и сотрудничества даже между непримиримыми идеологическими противниками

Актуален вопрос необходимости международного сотрудничества в сфере кибербезопасности и надстрановых форматов международного управления интернетом.

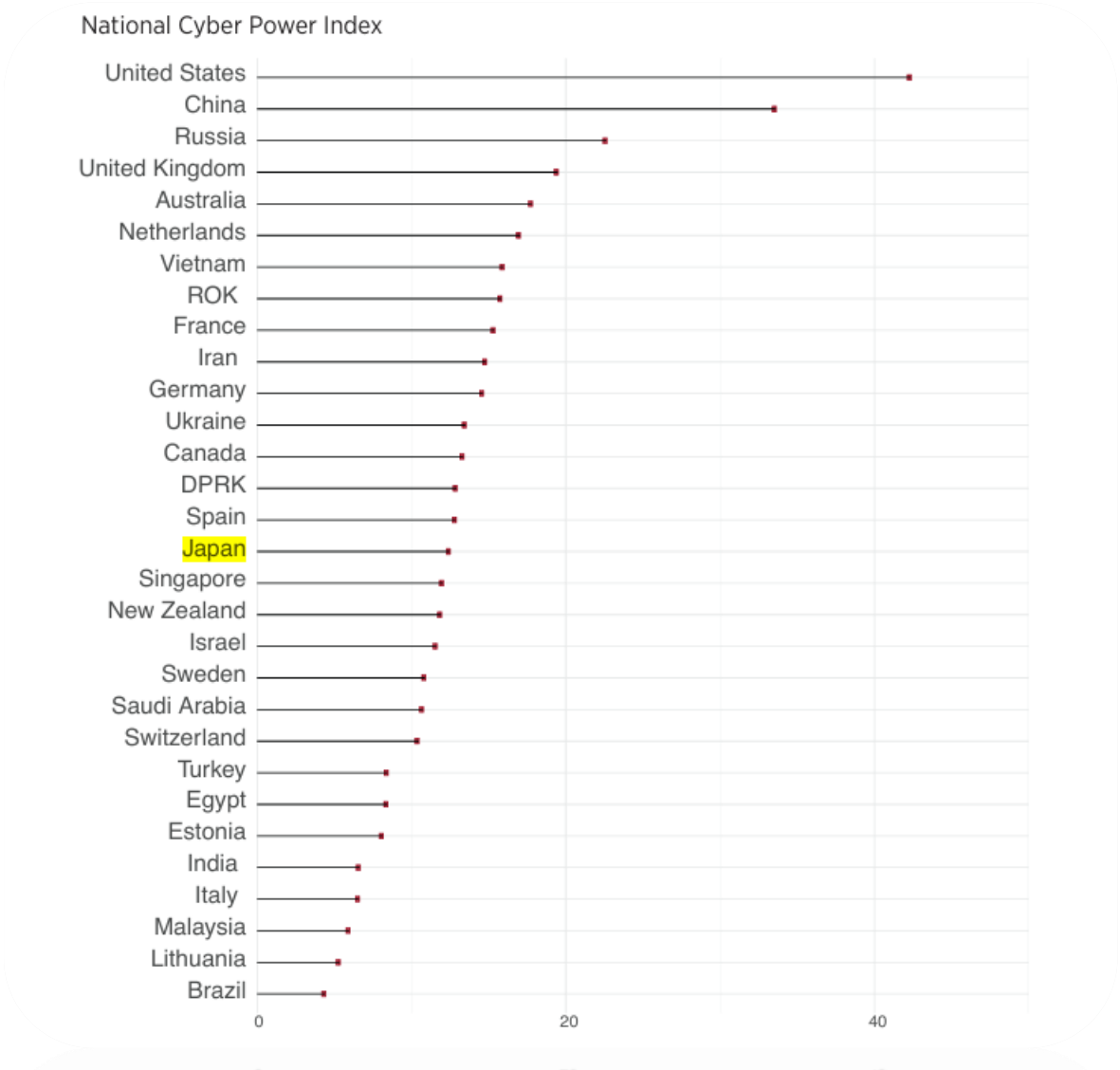
*Подходы:*

- *Американоцентричный*
- *Кибераавтономный*
- *Киберсуверенный*

# СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЯПОНИИ

- Японский опыт: роль США в глобальной кибербезопасности + роль США в безопасности Японии = квинтэссенция проблем японского подхода к национальной безопасности;
- Отсутствие намерения политических элит самостоятельно и энергично принимать необходимые законы;
- Нехватка законодательной основы для развития системы кибербезопасности Японии.

# НАЦИОНАЛЬНЫЙ ИНДЕКС КИБЕРМОЩИ 2022





Филиппины в Индекс не вошли


# Индекс Института Лоуи, с точки зрения наступательных и оборонительных кибервозможностей

2024

| | | США | Великобритания | Австралия | Нидерланды | Южная Корея | Франция | Япония |
|---|---|---|---|---|---|---|---|---|
| Общий Национальный индекс кибермощи [Там же: 10, Рис. 2] | | 1 | 4 | 5 | 6 | 7 | 9 | 16 |
| Национальный индекс кибермощи в зависимости от целей [Там же: 11-12. Рис. 3.a и 3.b] | | | | | | | | |
| 1 | *киберслежка* | 4 | 29 | 21 | 11 | 8 | 20 | 22 |
| 2 | *Кибероборона КВИ* | 3 | 5 | 1 | 6 | 22 | 4 | 13 |
| 3 | *информационный контроль* | 1 | 5 | 20 | 15 | 9 | 10 | 13 |
| 4 | *киберразведка* | 1 | 3 | 4 | 5 | 7 | 9 | 16 |
| 5 | *развитие ИКТ* | 2 | 4 | 8 | 7 | 5 | 11 | 6 |
| 6 | *кибератаки* | 1 | 4 | 16 | 8 | 11 | 13 | 14 |
| 7 | *кибернормы* | 1 | 2 | 8 | 5 | 7 | 6 | 11 |
| Индекс *способности* стран достичь кибермощи в зависимости от целей [Там же: 27-28. Рис. 8.a и 8.b] | | | | | | | | |
| 1 | *киберслежка* | 19 | 12 | 21 | 18 | 8 | 17 | 9 |
| 2 | *Кибероборона КВИ* | 1 | 6 | 2 | 5 | 27 | 9 | 22 |
| 3 | *информационный контроль* | 1 | 5 | 14 | 10 | 6 | 12 | 4 |
| 4 | *киберразведка* | 1 | 4 | 11 | 6 | 15 | 10 | 7 |
| 5 | *ИКТ* | 1 | 5 | 7 | 8 | 3 | 11 | 4 |
| 6 | *кибератаки* | 1 | 16 | 26 | 6 | 4 | 10 | 12 |
| 7 | *кибернормы* | 1 | 2 | 9 | 8 | 11 | 4 | 13 |
| Индекс *намерения* стран достичь кибермощи в зависимости от целей [Там же: 29-30. Рис. 9.a и 9.b] | | | | | | | | |
| 1 | *киберслежка* | 1 | 29 | 21 | 11 | 13 | 19 | 25 |
| 2 | *Кибероборона КВИ* | 3 | 9 | 1 | 12 | 16 | 4 | 6 |
| 3 | *информационный контроль* | 1 | 9 | 24 | 16 | 12 | 11 | 17 |
| 4 | *киберразведка* | 8 | 7 | 2 | 9 | 3 | 10 | 22 |
| 5 | *ИКТ* | 7 | 6 | 16 | 8 | 9 | 12 | 17 |
| 6 | *кибератаки* | 3 | 1 | 2 | 12 | 14 | 17 | 15 |
| 7 | *кибернормы* | 1 | 7 | 13 | 3 | 8 | 9 | 15 |

**Источник:**
**составлено**
**Г.Ю. Никипорец-Такигава на основе данных Национального Индекса Кибермощи 2022**

# ЛОВУШКИ АМЕРИКАНОЦЕНТРИЧНОСТИ СНКБ

- Отсутствие собственного прогресса развития ИКТ или даже его регресс. Развитие ИКТ является одним из действий для наращивания кибермощи;
- Не все проблемы национальной безопасности подлежат коллективным решениям. ИКТ - это очень конкурентная область, в которой страны не сотрудничают друг с другом в ущерб своему лидерству;
- «Возрастающая асимметрия» во взаимоотношениях с США;
- Сомнительный реальный эффект американской помощи Японии в области кибербезопасности.

# ЭВОЛЮЦИЯ СНКБ ЯПОНИИ

- *2000* г. - «План действий по созданию системы защиты информационных систем», «Специальный план действий по борьбе с кибертерроризмом», «Инаугурационная национальная стратегия по информационной безопасности»;
- *2014* г. - «Базовый Акт по Кибербезопасности», Стратегический штаб и Совет по кибербезопасности;
- *2015* г. - Национальный центр готовности к инцидентам и стратегии кибербезопасности, который вместе с Силами самообороны Японии (ССЯ) и полицией должен был координировать политику и командовать созданной в составе ССЯ Кибергруппой. Национальная стратегия кибербезопасности (НСКБ);
- *2017-2020* г. - Отчеты о неудовлетворительном состоянии системы кибербезопасности и необходимости создания рабочей стратегии;
- *2022* г. - Обновленные стратегические документы в связи с усложнившейся международной обстановкой в 2022 году. В частности СНБ с разделом по кибербезопасности с тремя задачами;
- *2024* г. - неудовлетворительные результаты и темп решения задач и возрастающее отставание Японии.

# УГЛУБЛЕНИЕ ИНТЕГРИРОВАННОСТИ ЯПОНИИ В АМЕРИКАНОЦЕНТРИЧНУЮ СИСТЕМУ СОТРУДНИЧЕСТВА В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

- *2020* г. - подписана Индивидуальная программа партнерства в области кибербезопасности с НАТО
- *2021* г. - заявлено намерение укреплять сотрудничество в сфере кибербезопасности с AUKUS
- в *2022* г. Декларации о будущем интернета – американского проекта, закрепляющего деление киберпространства на «своих» и «чужих»
- *2023* г. - создана Рабочая группа МИД Республики Корея, США и Японии по сотрудничеству в связи с киберугрозами КНДР

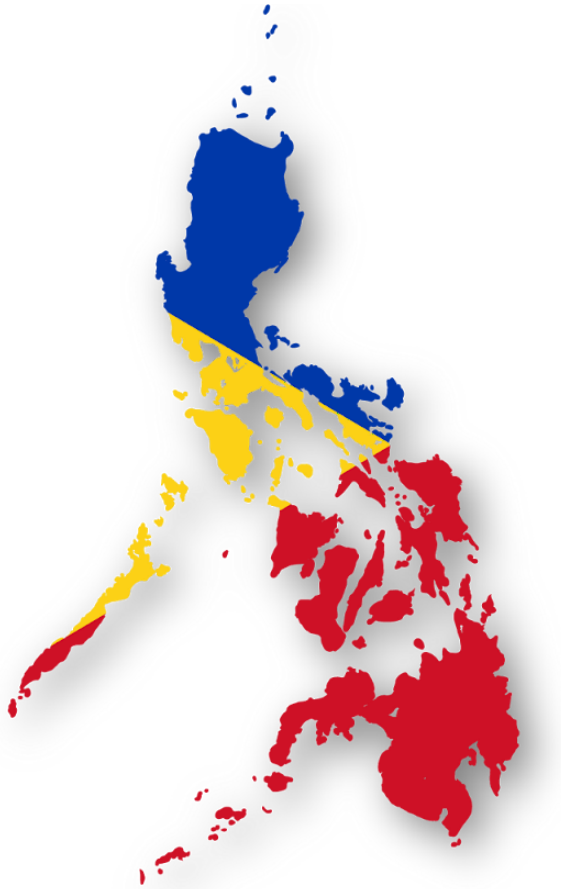
# ПЛАТФОРМЫ ВЗАИМОДЕЙСТВИЯ ЧЕРЕЗ ФОРМАТ АСЕАН+3

- ASEAN-Japan Cybersecurity Policy Meeting (AJCPM);
- ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC);
- ASEAN-Japan Cybersecurity Community Alliance (AJCCA) ;
- RCEP

# ПОДХОД ФИЛИППИН

**АМЕРИКАНОЦЕНТРИЧНЫЙ**

- **Совместные учения и тренировки;**
- **Билатеральные и многосторонние соглашения;**
- **Программы обмена и тренингов;**
- **Создание совместных киберцентров**



# НАЦИОНАЛЬНЫЙ ПЛАН КИБЕРБЕЗОПАСНОСТИ ФИЛИППИН (NCSP) 2023–2028

- NCSP 2023-2028 — это вторая итерация NCSP. Он улучшает основу предыдущего плана и является продуктом содержательных консультаций между различными заинтересованными сторонами как из государственного, так и из частного секторов.
- Программа NCSP соответствует Плану развития Филиппин на 2023–2028 годы, Стратегии национальной безопасности, Национальной стратегии борьбы с киберпреступностью и другим стратегиям, разработанным другими национальными правительственными учреждениями, которые занимаются вопросами кибербезопасности.

# ЭВОЛЮЦИЯ СТРАТЕГИИ ФИЛИППИН

— 2024

Department Circular No. 001 s. 2024: Guidelines for The Submission of the Information Systems Strategic Plan for the Technical Review, Evaluation, and Endorsement of the Department of Information and Communications Technology

Department Circular No. 002 s. 2024: Declaration of the Theme and Guide for the National ICT Month 2024 Celebration

Department Circular No. 003 s. 2024: Prescribing Policies and Guidelines on the Cybersecurity Protection of Government Digital Assets Stipulated in the National Cybersecurity Plan 2023-2028

Department Circular No. 004 s. 2024: Prescribing the Adoption of a Layered Security and Defense Approach to Digital Information Security Measures Relevant to Cybersecurity for Government Agencies

Department Circular No. 005 s. 2024: Reporting Mechanisms and Mandatory Disclosure of Cybersecurity Incidents for the Government

Department Circular No. 006 s. 2024: Guidelines for the Vulnerability Disclosure Initiative

— 2023

DICT Technical Advisory on Medusa Ransomware

Department Circular No. 001 s. 2023: Startup Grant Fund Guidelines

Department Circular No. 002 s. 2023: Implementation of the Courses for Literacy in the Internet and Computer Knowledge Project (Project CLICK) and Providing Amendments to the Terms of Engagement

— 2022

Department Circular No. 01 – Rationalizing the Registration, Accreditation and Monitoring of Independent Tower Companies, Satellite Service Providers and Operators, and Private Express and/or Messengerial Delivery Service Operators

Department Circular No. 02 – Election Offenses Under the Omnibus Election Code For Telecommunications Service Providers, Holders Of Certificate Of Public Convenience, Franchises, And Other Forms Of Authorization Issued By The Department Of Information And Communications Technology And The National Telecommunications Commission

Department Circular No. 03 – Consolidation of The Digital Learners and Teachers, Cybersafe Learning, and Information and Communications Technology (ICT) Skilling/ Upskilling Projects into the Digital Learners Project (DLP) As COVID-19 Response, Resiliency, And Recovery Measures

**Источник: https://dict.gov.ph/department-circulars**

# НАЦИОНАЛЬНЫЙ ПЛАН КИБЕРБЕЗОПАСНОСТИ ФИЛИППИН (NCSP) 2023–2028

**3 основные цели:**

- Проактивная защита и обеспечение безопасности в киберпространстве;
- Повышение уровня компетенций в области кибербезопасности;
- Укрепление нормативно-правовой базы кибербезопасности.


Coordinate national protection, prevention, and mitigation of, and recovery from cyber incidents
Disseminate domestic cyber threat and vulnerability analysis
Protect critical infrastructure
Secure government and civilian infostructure
Investigate cybercrimes under its jurisdiction
DICT
Lead for Protection (NCERT)
Investigate, attribute, disrupt and prosecute cybercrimes
Lead domestic national security operations
Conduct domestic collection, analysis and dissemination of cyber threat intelligence
Support the national protection, prevention, mitigation of, and recovery from cyber incidents
Coordinate cyber threat investigations
Prosecute Cybercrimes
DOJ-NBI/ DILG-PNP
Lead for Investigation, Enforcement and Prosecution
NCIAC
Lead for the interagency body established for policy coordination among concerned agencies
DND
Lead for National Cyber Defense (AFPCYBERCOM)
Defend the military network from cyber attacks
Gather foreign cyber threat intelligence and determine attribution
Secure national security and military systems
Support the national protection, prevention, mitigation of, and recovery from cyber incidents
Investigate cybercrimes under military jurisdiction (cyberdefense)
INTELLIGENCE COMMUNITY:
CYBER THREAT INTELLIGENCE AND ATTRIBUTION
(NSC, NICA)
NATIONAL CYBERINTELLIGENCE PLATFORM:
SHARED SITUATIONAL AWARENESS
IDENTIFY PROTECT DETECT RESPOND RECOVER
COORDINATE WITH PUBLIC, PRIVATE, AND INTERNATIONAL PARTNERS

# CYBEX 2024

# КЛЮЧЕВЫЕ РАЗЛИЧИЯ СТРАТЕГИЙ

**Филиппины**:

- Фокус на создании новой инфраструктуры, реорганизации и кадров;
- Неопределенность в отношении источников угроз;
- Зависимость от международной помощи, но нет акцента на США

**Япония**:

- Укрепление существующих систем безопасности с опорой на сотрудничество с США;
- Прямое упоминание источников киберугроз;
- Акцент на глобальной безопасности и инновациях.

# ВЗАИМОДЕЙСТВИЕ ФИЛИППИН С ЯПОНИЕЙ

## Сотрудничество

Департамент информационно-коммуникационных технологий Филиппин **(DICT)**

Министерство внутренних дел и коммуникаций Японии **(MIC)**

**Первый японо-американо-филиппинский кибердиалог**

# ПЕРСПЕКТИВЫ СОТРУДНИЧЕСТВА JICA-DICT

- Разработка учебных модулей для повышения квалификации специалистов.
- Проведение семинаров и практикумов по координации между секторами и схемам сотрудничества.
- Повышение осведомленности в области кибербезопасности через образовательные материалы и тренинги.

# В РАМКАХ АСЕАН ФИЛИППИНЫ НАРАЩИВАЮТ СВОЕ УЧАСТИЕ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

- The ASEAN Foreign Ministers' Meeting (AMM);
- The ASEAN Digital Ministers Meeting (ADGMIN);
- The ASEAN Regional Forum (ARF) which focuses on confidence-building measures among members;
- The ASEAN Defense Ministers' Meeting-Plus (ADMM-Plus) which focuses on cybersecurity issues related to defense and military sectors;
- The ASEAN Ministerial Meeting on Transnational Crime (AMMTC) which focuses on cybercrime.
- The country shall also increase its engagement in the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC). The body coordinates discussions at the various ASEAN bodies.

**Источник: National Cybersecurity Plan 2028 | DICT**

# СПАСИБО ЗА ВНИМАНИЕ!


***Никипорец-Такигава Галина Юрьевна***, *д.п.н., профессор, руководитель НУГ «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции» ФМЭиМП НИУ ВШЭ*

*Gnikiporets-takigawa@hse.ru*

***Хитева Александра Сергеевна***, *исследователь НУГ «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции» ФМЭиМП НИУ ВШЭ*

*akhiteva@hse.ru*