



СТРАТЕГИЯ НАЦИОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ ЯПОНИИ: ПРОБЛЕМНОЕ ПОЛЕ И ЛОВУШКИ ПОДХОДА

Г.Ю. Никипорец-Такигава

НИКИПОРЕЦ-ТАКИГАВА Галина Юрьевна, доктор политических наук, профессор, факультет мировой экономики и мировой политики, Национальный исследовательский университет “Высшая школа экономики”, Москва, email: gnikiporets-takigawa@hse.ru

Никипорец-Такигава Г.Ю. 2025. Стратегия национальной кибербезопасности Японии: проблемное поле и ловушки подхода. *Полис. Политические исследования*. № 3. С. 162-175. <https://doi.org/10.17976/jpps/2025.03.11>. EDN: QATTIV

Статья подготовлена в рамках проекта № 25-00-05 (“АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке”) Программы “Научный фонд Национального исследовательского университета “Высшая школа экономики” (НИУ ВШЭ).

Статья поступила в редакцию: 18.07.2024. Принята к публикации: 24.02.2025

Аннотация. Цель статьи – анализ подходов, проблем и результатов в процессе разработки и реализации стратегии национальной кибербезопасности, которая в рамках неоклассического реализма операционализируется через понятие кибермощи. Необходимость укреплять кибермощь понимается как независимая переменная, которая обусловлена международной системой и является постоянным и общим для различных государств внешним вызовом. Реакция на него каждого конкретного государства зависит от вмешивающихся переменных, ряд из которых показан на кейсе Японии. Утверждается, что новейшая японская стратегия кибербезопасности, которая формулирует амбициозные задачи внедрения “активной обороны” и достижения уровня США, нереализуема. Трудности и препятствия обусловлены такими внутривнутриполитическими факторами, как отсутствие намерения политических элит самостоятельно и энергично принимать необходимые законы, а также американоцентричность японской политики национальной безопасности. Дискутируются риски делегирования непропорционально большой доли вопросов национальной безопасности на внешний контур; к его негативным последствиям относится утрата технологического суверенитета в расчете на заимствование технологий вместо развития собственных, углубление политической зависимости, угрозы для региональной безопасности, низкая практическая эффективность сотрудничества. Предложенное понимание кибермощи и кибербезопасности указывает на то, что ряд действий для развития национальной кибербезопасности требуют индивидуальных усилий каждого государства. Сделанные выводы имеют отношение к развитию дискуссии о будущем безопасности строящейся многополярности, национальных политиках безопасности, добавляют новое знание о методиках расчета кибермощи и использования данных индексов и рейтингов для аналитики.

Ключевые слова: стратегия национальной безопасности, кибербезопасность, кибермощь, киберсуверенность, американоцентричный подход, Япония, США, Великобритания, ЕС.

ВВЕДЕНИЕ

Актуальность исследования стратегии национальной кибербезопасности (СНКБ) связана с гибридным характером международных конфликтов, ростом

участия в них интернета и значимости кибербезопасности, что требует от политиков пересмотра стратегий безопасности, а от экспертов — аналитической поддержки, опирающейся на широкую базу сравнительных исследований.

В ответ на данный запрос Белферский центр Гарвардского университета, созданный для оценки “величайшей угрозы холодной войны — ядерного противостояния СССР и США”, изучает риски конфликтов в киберпространстве [Voo, Hemani, Cassidy 2022: 3]. Более десятилетия в фокусе внимания исследователей присутствуют такие термины как *кибероперации*, *кибероружие*, *кибервооружение*, *кибервойна*, *гонка кибервооружений*, *информационная война в киберпространстве* [Ито 2012; Rid, McBurney 2012; Lindsay 2013; Gartzke 2013; Liff 2017; Taddeo, Floridi 2018, Whyte, Mazanec 2019; Ямада 2019; Maschmeyer 2021], а также “информационная война” как синоним “кибервойны” [Lei 2019]. Впрочем, кибербезопасность все еще относят к “мягким” или невоенным видам безопасности, поскольку в ней задействован интернет, который в однополярном мире хотели видеть глобальным институтом, способным отменить национальные государства, сформировать глобальные нормы и мягкую силу [Nye 2017]. Акцент на государство и национальные интересы в современном научном дискурсе обесценивает данные идеи: интернет национализируется и используется государством в том числе в военных целях, кибербезопасность сближается с военной безопасностью. На примере кибербезопасности можно увидеть квинтэссенцию сложностей выхода из однополярности, так как СНКБ должна учитывать национальные интересы, а корневые серверы системы доменных имен, Корпорация по управлению доменными именами, IP-адресами и прочие базовые элементы архитектуры интернета по-прежнему находятся в США.

Некоторые страны стремятся оградить свои национальные киберпространства от внешнего влияния, добываясь максимально возможной локализации интернета. Такой подход (условно, с учетом все еще ведущей роли США) можно назвать киберсуверенным. Примером служит Китай, уже в 1998 г. запустивший проект “Золотой щит” (*Golden Shield Project*), частью которого является Великий китайский файрвол (*China Great Firewall*) [Griffiths 2019], и в 2006 г. начавший “импортозамещение”, создав *Baidu Baike* вместо Википедии и *Youku* вместо *YouTube*. Китайский опыт показал, что киберсуверенность ресурсозатратна, но усилия, вложенные в ее достижение, выводят страну на передовые позиции в мировой экономике и системе международной безопасности. К киберсуверенному пути присматривается все больше стран, среди которых присутствуют и оппоненты Китая, например, страны — члены ЕС.

Среди противников такого пути — Япония, политику кибербезопасности которой можно считать американоцентричной, поскольку в ее основе приоритет коллективных с США интересов, попытка внедрить американские стандарты в функционирование национального киберпространства и намерение строить систему национальной кибербезопасности совместно с США. Такой выбор детерминирован рядом факторов, среди которых внутривосточные являются важнейшими. Несмотря то, что этот выбор кажется естественным и весьма прагматичным для союзников США, он создает риски и негативно влияет на разработку и реализацию стратегии и всю систему национальной безопасности.

ТЕОРЕТИЗИРУЯ КИБЕРБЕЗОПАСНОСТЬ В НОВЫХ ПОЛИТИЧЕСКИХ РЕАЛИЯХ

Отнесение кибербезопасности к “мягким” или невоенным видам безопасности является следствием применения либеральных линз к осмыслению роли интернета в политике. В рамках более актуального для современных политических

реалий неоклассического реализма необходимость для государства наращивать кибермощь можно понимать как постоянный внешний вызов международной системы, выступающий независимой переменной. Ответы государства на данный вызов индивидуальны и обусловлены внутривнутриполитическими факторами, которые выступают как вмешивающиеся переменные. Эта теоретическая база при помощи соответствующего ей метода кейс-стади, а также сравнительного анализа, контент и дискурс-анализа первичных данных (рейтингов, индексов, результатов экспертного интервьюирования, статистических данных, нормативно-правовых документов и других примеров официального дискурса) позволяет прояснить специфику подхода Японии к СНКБ, причинно-следственные связи, а также операционализировать центральное для СНКБ понятие кибермощи.

Под СНКБ мы предлагаем понимать план действий по достижению, поддержанию и наращиванию кибермощи. К наблюдаемым и измеримым характеристикам кибермощи относим активность государства в следующих областях: 1) *киберслежка* за деятельностью своих граждан в киберпространстве; 2) *кибероборона* критически важной инфраструктуры (КВИ); 3) *информационный контроль*; 4) *киберразведка*; 5) *развитие ИКТ*; 6) *кибератаки* на противника; 7) продвижение своих *кибернорм* и технических стандартов на региональный и глобальный уровень.

В данном контексте очевидна безосновательность типичных для западного дискурса утверждений, что киберслежку, киберразведку или кибершпионаж, кибератаки на другие государства, а также продвижение своих ИКТ и стандартов в другие страны осуществляет Китай, подвергая угрозе западные демократии, которые ничем подобным не занимаются [Gordon 2020: 50; Spade 2011: 77; Mochinaga 2020: 43]. В действительности, обвиняя Китай в государственной узурпации интернета, а также в том, что он внедряет *TikTok* в США, чтобы получить доступ к данным местных пользователей¹, американское государство узурпировало интернет с момента его появления, а также пользуется доступом к данным пользователей большинства стран мира [Никипорец-Такигава, Филатов 2024: 195-196]. Критикуя Китай за то, что он закрыл собственное киберпространство “Золотым щитом”², среди прочего запретив использование на своей территории *Google*, США закрыли свое киберпространство от Китая “Чистой сетью”³, в частности, блокируя *TikTok*. Эта симметрия подтверждает, что необходимость разрабатывать и реализовывать СНКБ не зависит от внутривнутриполитических факторов, но является условием выживания любого государства в международной системе. Успех же данной разработки и реализации подтвержден воздействию внутренних факторов.

ЯПОНСКАЯ СНКБ: ЭТАПЫ И ПРОБЛЕМЫ РАЗВИТИЯ

Япония проявила озабоченность вопросами кибербезопасности в 2000 г., сначала в более широком контексте, приняв “План действий по созданию

¹ Annual Threat Assessment of the US Intelligence Community. *Office of the Director of National Intelligence*, 09.04.2021. P. 8, 10-11, 14, 15-16. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/3532-2021-annual-threat-assessment-of-the-u-s-intelligence-community> (accessed 21.02.2025).

² Cyber Capabilities and National Power: A Net Assessment. *The International Institute for Strategic Studies*, 28.06.2021. P. 89. <https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/> (accessed 21.02.2025).

³ The Clean Network. <https://2017-2021.state.gov/the-clean-network/> (accessed 21.02.2025).

системы защиты информационных систем”, в скором времени дополненный “Специальным планом действий по борьбе с кибертерроризмом” и “Инаугурационной национальной стратегией по информационной безопасности”. В 2014 г. был принят “Базовый акт по кибербезопасности”, образованы Стратегический штаб и Совет по кибербезопасности; в 2015 г. — Национальный центр готовности к инцидентам и стратегии кибербезопасности (*NISC*), который вместе с Силами самообороны Японии (ССЯ) и полицией должен был координировать политику и командовать созданной в составе ССЯ Кибергруппой. В 2015 г. утвердили Стратегию национальной кибербезопасности (СНКБ 2015)⁴, обновленную в 2021 (СНКБ 2021). В 2021 г. была открыта еще одна организация, отвечающая за цифровизацию — Цифровое агентство⁵, и назначен профильный министр⁶. В 2022 г. “самая суровая и сложная ситуация в области безопасности в послевоенное время”, как объясняется в решениях Совета национальной безопасности и Кабинета министров⁷, потребовала пересмотра основных стратегических документов — “Стратегии национальной безопасности” (СНБ 2022), “Национальной стратегии в области обороны” и “Программы наращивания обороноспособности”, содержащих разделы по кибербезопасности.

Несмотря на все эти шаги, они не приводят к осязаемым результатам. Структуры ограничены в функциях и не отвечают за антикризисное управление страной в киберпространстве [Мацумура 2020: 5], не укомплектованы кадрами⁸ и настолько малоэффективны, что их регулярно (в 2018 г. [Группа проектов... 2018], в 2019⁹, в 2022¹⁰ и в 2024 гг.¹¹) предлагали распустить, реорганизовать, усилить созданием какой-нибудь новой.

Что касается стратегических документов, в них до сих пор содержатся лишь “расплывчатые политические ориентиры”, т.е. они по сути “не являются стратегией” [Мацумура 2021: 4]. Если в области военной безопасности заявляется “приобретение ракет Томагавк в США, разработка собственных крылатых ракет большой дальности, инвестиции в запасы боеприпасов и запасных частей

⁴ サイバーセキュリティ戦略、平成 27 年 9 月 4 日。[Стратегия кибербезопасности. *NISC*, 04.09.2015]. <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf> (accessed 21.02.2025).

⁵ デジタル庁設置法。令和三年法律第三十六号。[Закон о создании цифрового агентства. Закон № 36 от 2021 г.]. <https://laws.e-gov.go.jp/law/503AC0000000036> (accessed 21.02.2025).

⁶ デジタル大臣 [Министр по цифровизации]. <https://www.digital.go.jp/about/member> (accessed 21.02.2025).

⁷ 国家安全保障戦略について 国家安全保障会議決定、閣議決定 [О стратегии национальной безопасности. Решения Совета национальной безопасности, Кабинета министров] 16.12.2022. <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf> (accessed 21.02.2025).

⁸ 小谷 賢『【日本国家の弱点】いまこそサイバー・セキュリティ改革が外交、安全保障、技術開発に不可欠』 [Кен Котани. Слабые стороны японского государства: реформа кибербезопасности в настоящее время необходима для дипломатии, безопасности и технологического развития. *Wedge Online*, 2024]. <https://wedge.ismedia.jp/articles/-/33583?page=2> (accessed 21.02.2025).

⁹ サイバーセキュリティ庁創設を首相に提言自民。NHK 政治マガジン。2019 年 5 月 14 日。[ЛДП предлагает премьер-министру создать агентство по кибербезопасности. *NHK Politics Magazine*, 14.05.2019]. <https://www.nhk.or.jp/politics/articles/statement/17565.html> (accessed 21.02.2025).

¹⁰ 日本政府「国家安全保障戦略」令和4年12月[Стратегия национальной безопасности. *Правительство Японии*, декабрь 2022. С. 30]. <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf> (accessed 21.02.2025).

¹¹ Japan’s ‘Active Cyber Defence’ System: Now Set to Become Reality? *NSBT Japan*, 08.10.2024. <https://www.asianmilitaryreview.com/2024/10/japans-active-cyber-defense-system-now-set-to-become-reality/> (accessed 21.02.2025).

и расширение баз пассивной обороны” [Watanabe 2022: 120], то для кибербезопасности ставится задача “превзойти крупные европейские страны и США в реагировании в области кибербезопасности”, а также перейти к “активной обороне” (能動的サイバー防御, *noudou teki saiba bougyo*)¹². Эти, верно названные “удивительно высокими”¹³ цели, являются примерами “расплывчатых политических ориентиров” и заведомо не реализуемы — прежде всего потому, что между США (исключительно на которые ориентируется Япония, упоминая “крупные европейские страны” в официальном дискурсе лишь в виде фигуры речи) и Японией в сфере развития кибербезопасности огромная разница.

В Национальном индексе кибермощи 30 стран, созданном Белферским центром киберпроектов Гарвардского университета, Япония на 16-м месте [Voo, Nemani, Cassidy 2022: 9], тогда как США — на первом. Если в 2022 г. общий японский рынок кибербезопасности оценивался в 7,35 млрд долл. и прогнозировалось, что данный показатель будет ежегодно расти на 13.6%, достигнув к 2032 г. 26,8 млрд долл.¹⁴, то рынок кибербезопасности США уже в том же 2022 г. оценивался в 53,45 млрд долл. По данным индекса сиднейского Института Лоуи, с точки зрения наступательных и оборонительных кибервозможностей среди развитых азиатско-тихоокеанских стран, США занимают первое место (Китай второе, Сингапур пятое, Южная Корея шестое, Тайвань восьмое), а Япония — предпоследнее девятое¹⁵.

Связанный с кибербезопасностью потенциал и готовность японской экономики к внедрению и изучению цифровых технологий для экономических и социальных преобразований в 2024 г. оценен как очень слабый: в мировом рейтинге цифровой конкурентоспособности, который регулярно издает Международный институт развития менеджмента, Япония заняла 31-е место среди 67 стран, тогда как США — четвертое (Сингапур находится на первом месте, Южная Корея на шестом, Тайвань на девятом, Китай на 14-м)¹⁶. В Японии до сих пор не решена обозначенная еще в СНКБ 2021 г. как приоритетная задача “обеспечить цифровую трансформацию, без которой невозможно развитие кибербезопасности”¹⁷.

Поэтому внедрять “активную кибероборону” в Японии, как удачно выразился исполнительный директор НИИ киберобороны Т. Нава в интервью еженедельному журналу “Никкей Бизнес”, “это все равно как сесть за руль ‘Феррари’, не пройдя подготовку для получения водительских прав”¹⁸.

¹² СНБ 2022. С. 30.

¹³ Osawa J. How Japan is modernizing its cybersecurity policy: views from the next generation. *Stimson*, 02.02.2023. <https://www.stimson.org/2023/japan-cybersecurity-policy/> (accessed 21.02.2025).

¹⁴ Spherical Insights (SI). Japan Cybersecurity Market Insights Forecasts to 2032. 2023. <https://www.sphericalinsights.com/reports/japan-cybersecurity-market#:~:text=The%20Japan%20Cybersecurity%20Market%20Size,USD%2026.8%20Billion%20by%202032> (accessed 21.02.2025).

¹⁵ Asia Power Index. 2024 Edition. Cyber Capabilities. Expert survey: Defensive and offensive cyber capabilities, two-year rolling average, 0–100 (2022–24). 2024. *Lowy Institute*. <https://power.lowyinstitute.org/data/military-capability/signature-capabilities/cyber-capabilities/> (accessed 21.02.2025).

¹⁶ IMD World Digital Competitive Ranking. 2024. <https://imd.widen.net/s/xvhldkrrkw/20241111-wcc-digital-report-2024-wip> (accessed 21.02.2025).

¹⁷ 「サイバーセキュリティ戦略の概要」、令和3年9月28日。[Обзор стратегии кибербезопасности Японии. *NISC*, 28.09.2021]. <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf> (accessed 21.02.2025).

¹⁸ 狙われる重要インフラ、サイバー攻撃は国家ぐるみ。日経ビジネス。2023.07.18. [В атаки на критически важную инфраструктуру вовлечены государства. *Никкей Бизнес*, 18.07.2023]. <https://www.nikkei.com/article/DGXZQOUC1347Q0T10C23A700000/> (accessed 21.02.2025).

Невысокий уровень готовности СНКБ к вызовам международной системы Японии может объясняться внутриэкономическими и социально-культурными причинами: нехваткой высококвалифицированных профессионалов в области ИИ, обработки данных и разработки программного обеспечения¹⁹, особенностями японской традиционной корпоративной культуры²⁰ и “консервативной” тактикой и “оборонительным стилем” японских компаний по отношению ко всему комплексу ИКТ и кибербезопасности²¹. Справедливы указания на “непобедимость” японской бюрократии, которая мешает “успешному внедрению информационного хайтека в систему государственного управления” [Чугров 2023: 129, 139], из-за которой “государственный сектор Японии застрял в аналоговом веке с его бесконечным бумажным оборотом, скрепленным ручными печатями”²². Внутриполитические факторы, тем не менее, оказывают решающее влияние.

ВНУТРИПОЛИТИЧЕСКИЕ ФАКТОРЫ РАЗВИТИЯ ЯПОНСКОЙ СНКБ

Разработка СНКБ должна сопровождаться принятием законов, которые пока отсутствуют в Японии. Например, необходимо законодательно закрепить обязательство объектов КВИ сообщать о том, что они подверглись кибератакам, а также право государства иметь доступ к коммуникационным сетям [Группа проектов... 2018: 29, 31], чтобы “осуществлять перехват нежелательного контента”²³. Необходимо легитимировать право государства на активную кибероборону: пакет законов 2015 г. разрешил применять силу в рамках коллективной самообороны, но это не касается киберобороны [Мацумура 2021: 14]. При этом данные законы не только не приняты, но находятся в самом начале процесса обсуждения. Целесообразность принятия закона о доступе к коммуникации граждан в интернете начали обсуждать только в 2023 г.²⁴, к разговору о законе о киберобороне приступили лишь в ноябре 2024 г.²⁵, а 7 февраля 2025 г. вынесли на обсуждение проект киберобороны КВИ²⁶. Это несколько запоздалые попытки относительно уже принятых

¹⁹ Yokoi T. Japan poised for digital transformation? *Forbes*, 11.05.2023. <https://www.forbes.com/sites/tomokoyokoi/2023/05/11/japan-poised-for-digital-transformation/> (accessed 21.02.2025).

²⁰ 日本がデジタル化で遅れる決定的な構造要因. 田中 道昭 [Митиаки Танака. Решающие структурные факторы задержки перехода Японии к цифровизации, 10.03.2020]. <https://toyokeizai.net/articles-/378961?page=4> (accessed 21.02.2025).

²¹ 日本はなぜデジタル分野で世界に大きく遅れたか 岩本 晃一 [Коити Ивамото. Почему Япония сильно отстала от мира в области цифровизации?]. https://www.rieti.go.jp/jp/columns/s20_0012.html (accessed 21.02.2025).

²² Yokoi T. Japan poised for digital transformation? *Forbes*, 11.05.2023. <https://www.forbes.com/sites/tomokoyokoi/2023/05/11/japan-poised-for-digital-transformation/> (accessed 21.02.2025).

²³ 小谷 賢『【日本国家の弱点】いまこそサイバー・セキュリティ改革が外交、安全保障、技術開発に不可欠』[Кен Котани. Слабые стороны японского государства: реформа кибербезопасности в настоящее время необходима для дипломатии, безопасности и технологического развития. *Wedge Online*, 2024]. <https://wedge.ismedia.jp/articles/-/33583?page=2> (accessed 21.02.2025).

²⁴ Japan’s New National Security Strategy and Contribution to a Networked Regional Security Architecture. 2023. <https://www.csis.org/analysis/japans-new-national-security-strategy-and-contribution-networked-regional-security> (accessed 21.02.2025).

²⁵ 日本は脆弱なサイバーセキュリティを強化すべき一党首が警告08 Nov 2024 アラブニュース [Япония должна усилить уязвимую кибербезопасность – лидер партии предупреждает. *Arab News*, 08.11.2024]. https://www.arabnews.jp/article/japan/article_133405/ (accessed 21.02.2025).

²⁶ サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）[Инициативы в области кибербезопасности (исследование возможностей реализации активной киберзащиты и т.д.), 07.02.2025]. https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html (accessed 21.02.2025).

в Японии стратегических документов с декларацией “активной киберобороны”. Более того, нет и признаков скорейшего завершения обсуждений желаемым результатом в виде принятых законов. Поэтому на сегодняшний день и обозримую перспективу, если даже японское государство располагает техническими возможностями осуществлять киберслежку, кибероборону КВИ, контроль киберпространства, кибератаки для наращивания кибермощи, оно не может использовать свои возможности, так как они до сих пор незаконны.

Данные Национального индекса кибермощи, который вычисляет ее уровень по формуле соотношения показателей возможностей государства достичь кибермощи (по 29 индикаторам [Voo, Hemani, Cassidy 2022: 44-49]), и намерений государства ее достичь (по 47 индикаторам) [ibid.: 30-43], помогают иллюстрировать данный вывод и продвинуться глубже в понимании японской политики безопасности. Сравнив показатели США и их союзников из первой десятки Индекса с японскими (см. табл.), можно увидеть, что низкое итоговое место Японии свидетельствует не столько о невозможности, сколько об отсутствии намерения японского государства укреплять и развивать кибермощь.

Согласно Индексу, возможности японского государства весьма широки. Так, по возможностям заниматься киберслежкой, японское государство (девятое место в Индексе) даже опережает США, Великобританию, Австралию, Нидерланды, Францию и лишь на один пункт уступает Южной Корее. По возможностям контролировать информацию и манипулировать ею Япония лишь незначительно уступает США, находясь на четвертом месте и опережая все названные выше страны. Здесь уместно, вслед за американским исследователем М. Факлером, вспомнить, как Япония умеет добиваться полной “зачистки” информационного пространства при помощи традиционных СМИ, которые “захвачены” государством и являются “придатками” власти в большей степени, чем в других демократических странах [Fackler 2021: 4-6], “обеспечивая единообразное монолитное освещение событий, более близкое к тому, что наблюдается в недемократических обществах” [ibid.: 5]. Но данная деятельность японского государства не распространяется на интернет, к коммуникации в котором у него нет легального доступа.

Это создает риски для национальной безопасности, особенно с учетом того, что такой доступ имеют как минимум три других государства: США, Южная Корея и Китай, поскольку их поисковыми системами и соцсетями пользуются в Японии. По состоянию на декабрь 2024 г. 79,1% японцев пользовались с ПК *Google*, 11,9% – *Microsoft Bing*, и только 3% японской *Yahoo*. Со смартфонов 86,3% пользовались *Google*, 11,0% – *Yahoo* (0,8% пользовались *Bing*)²⁷. Также 83,7% японцев пользовались южнокорейской соцсетью *Line*²⁸, 42,3% – *Twitter*, 39,9% – *Instagram*^{*29}, 24,7% – *Facebook*^{*} и 10,5% китайским *TikTok*.

²⁷ 【2024年12月調査】検索エンジンシェア率のランキングと推移（日本・世界）[Опрос 2024/12. Рейтинг и изменение доли поисковых систем (Япония и весь мир)]. Ohdo.at21. <https://ohdo.at21.jp/web/search-engine-share/> (accessed 21.02.2025).

²⁸ SNS利用率調査 SNS [Обзор использования социальных сетей. *Hottolink*, 06.01.2025]. https://www.hottolink.co.jp/column/20250106_114872/ (accessed 21.02.2025).

²⁹ Компания *Meta* и соцсети, которыми она владеет (*Instagram* и *Facebook*), признаны в России экстремистскими и запрещены.

Таблица (Table)

Кибермощь Японии согласно данным Национального индекса кибермощи
Japan's cyber power according to the data of the National Cyber Power Index

		США	Велико- британия	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.а и 3.б]								
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.а и 8.б]								
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.а и 9.б]								
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 автором на основе данных Национального индекса кибермощи 2022.

Японские политики осознают, что использование зарубежных платформ, которые японское государство не может контролировать в целях безопасности, создает киберриски как для КВИ, так и для населения. Именно политикам, а не японским разработчикам, надо адресовать вопрос о том, почему Япония не создает “новые бизнес-модели подобные *Google, Amazon, Facebook**,

*Apple*³⁰ и “отстает в цифровой трансформации”³¹. Население Японии, судя по соцопросам, достаточно обеспокоено ростом кибератак, чтобы поддержать разумную политику стимулирования перехода на отечественную *Yahoo* и подобные, пропаганду цифровой гигиены и грамотности и любые другие государственные меры обеспечения безопасности интернета. Но власть не проводит данной политики и не предлагает таких мер.

Важен и фактор политического лидерства. Кибербезопасность выделили в особую зону ответственности государства при администрации С. Абэ. Безусловно, этот шаг свидетельствовал не только об осознании Токио возрастающего влияния интернета на оборону и безопасность, но и соответствовал амбициозному плану политика превратить страну в мощную кибердержаву [Hughes, Kallender 2016: 118]. Сформулированная в 2022 г. в японской СНБ задача довести японскую кибербезопасность до уровня США не менее амбициозна. Но она продиктована давлением международной системы, которое требует от каждого государства наращивать кибермощь, и не подкреплена личной заинтересованностью японского премьер-министра.

Еще один политический фактор связан с американоцентричностью японского подхода к стратегии национальной безопасности. На альянсе с США Япония традиционно основывает всю политику в области обороны и безопасности [Dosch 2011: 34; Easley 2016: 80; Стрельцов 2023: 187], сотрудничая в этих вопросах с “близкими по духу” странами “при обязательном лидерстве США” [Стрельцов 2023: 189]. Те же надежды на США как единственного гаранта своей безопасности перенесены и на киберпространство.

Японская СНКБ согласовывается с США³² на совещаниях с американскими советниками³³ в разных форматах. США в японских стратегических документах указываются в качестве главного и практически единственного партнера³⁴, а содержание СКНБ непременно включает “упрочение японо-американского Альянса”³⁵. Сравнительный контент-анализ показывает, что в японских документах США упоминаются значительно чаще в контексте безопасности, чем

³⁰ 日本はなぜデジタル分野で世界に大きく遅れたか 岩本 晃一 [Коити Ивamoto. Почему Япония сильно отстала от мира в области цифровизации?]. https://www.rieti.go.jp/jp/columns/s20_0012.html (accessed 21.02.2025).

³¹ Yokoi T. Japan poised for digital transformation? *Forbes*, 11.05.2023. <https://www.forbes.com/sites/tomokoyokoi/2023/05/11/japan-poised-for-digital-transformation/> (accessed 21.02.2025).

³² Basu P. From reactive to proactive: Japan’s advances in cybersecurity and cyber defense strategies. *Digital Frontiers*, 2024. <https://www.orfonline.org/expert-speak/from-reactive-to-proactive-japan-s-advances-in-cybersecurity-and-cyber-defence-strategies> (accessed 21.02.2025).

³³ 内閣サイバーセキュリティセンター、「重要インフラのサイバーセキュリティに係る行動計画」、2024年3月8日。[План действий по обеспечению кибербезопасности критической инфраструктуры. *Национальный центр готовности к инцидентам и стратегии кибербезопасности*, 08.03.2024]. https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf (accessed 21.02.2025).

³⁴ 内閣官房内閣サイバーセキュリティセンター、「人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する・国際ガイドランスへの共同署名について」、令和6年5月15日。[Совместное подписание международного руководства по снижению киберугроз для организаций и частных лиц, участвующих в защите прав человека и продвижении демократии. *Национальный центр готовности к инцидентам и стратегии кибербезопасности*, 15.05.2024]. https://www.nisc.go.jp/pdf/press/press_Mitigating_Threats.pdf (accessed 21.02.2025).

³⁵ 内閣サイバーセキュリティセンター、「サイバーセキュリティ戦略の概要」、令和3年9月28日 [Краткое содержание стратегии кибербезопасности. *Национальный центр готовности к инцидентам и стратегии кибербезопасности*, 28.09.2021]. <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf> (accessed 21.02.2025).

в аналогичных документах союзников. Ближайший союзник США, Британия, либо не упоминает США³⁶, либо включает их в список других стран в контексте сходства киберугроз³⁷ и способов на них реагировать³⁸. В стратегических документах по кибербезопасности стран-членов ЕС не только нет отсылок к США, но артикулируется киберсуверенный подход, провозглашенный Европейским парламентом уже в 2020 г. в программе “Киберсуверенитет для Европы”³⁹. На европейском фоне приверженность Японии американоцентричному подходу к национальной безопасности особенно очевидна. Она же заводит Японию в ряд ловушек, сказывающихся на безопасности нации.

ЛОВУШКИ АМЕРИКАНОЦЕНТРИЧНОСТИ СНКБ

Первая ловушка, в которую попадают страны, предпочитающие решать задачи национальной кибербезопасности за счет более сильного партнера — отсутствие собственного прогресса развития ИКТ или даже его регресс (японский случай, судя по лонгитюдным рейтингам, в которых показатели страны неуклонно снижаются). Развитие ИКТ — одна из ключевых составляющих наращивания кибермощи. Если киберсуверенный подход выступает существенным источником мотивации для технологического развития, то американоцентричный — напротив. Полагающаяся на США в сфере кибербезопасности Япония обречена на следование в американском фарватере, ставя на паузу технологический прогресс в расчете на более легкий путь заимствования.

Вторая ловушка связана с тем, что не все проблемы национальной безопасности подлежат коллективным решениям. Даже страны НАТО испытывают серьезные проблемы в выстраивании координации и сотрудничества в области кибербезопасности. Для внешних же для НАТО партнеров, подобных Японии, это тем более затруднительно. США не могут вместо Японии заниматься киберслежкой за ее гражданами, не заинтересованы оборонять японскую КВИ. Вряд ли Вашингтон готов делиться технологиями кибершпионажа и тем более передавать секретные сведения, опасаясь их утечки из незащищенных японских сетей⁴⁰. Осуществлять кибератаки на Китай Вашингтон готов лишь в своих интересах, и в меньшей, чем Токио, степени обеспокоен кибервойной с Северной Кореей. Наконец, США крайне заинтересованы в глобальном распространении американских стандартов и не терпят конкуренции. ЕС уже сталкивается с противодействием США в этом вопросе и не находит в Вашингтоне одобрения своего желания “обрести ки-

³⁶ Online Safety Act. 2023. <https://www.legislation.gov.uk/ukpga/2023/50> (accessed 21.02.2025).

³⁷ Government Cyber Security Strategy: Building a cyber-resilient public sector. 2022. P. 17. <https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf> (accessed 21.02.2025).

³⁸ Cybersecurity in the UK. 2024. P. 42, 54, 58. <https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf>; National Cyber Strategy. 2022. P. 127. <https://assets.publishing.service.gov.uk/media/620131fdd3bf7f78e469ce00/national-cyber-strategy-amend.pdf>; National Cyber Strategy 2022 – Annual Progress Report 2022-2023. 2023. P. 30, 36, 38. https://assets.publishing.service.gov.uk/media/64e60e4b1ff6f3000d70ae7c/14.283_CO_National_Cyber_Strategy_Progress_Report_Web_v3.pdf (accessed 21.02.2025).

³⁹ Digital sovereignty for Europe. 2020. P. 3. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf) (accessed 21.02.2025).

⁴⁰ 手塚 悟. わが国の国家安全保障におけるサイバーセキュリティとデジタル化戦略 慶應義塾大学 特任教授 [Сагору Тедзука. Стратегии кибербезопасности и цифровизации в национальной безопасности Японии]. https://www.defense-tech.or.jp/dcms_media/other/202405_free.pdf (accessed 21.02.2025).

берсуверенитет” [Burwell, Propp 2022: 22-23], “устанавливать стандарты, а не следовать чужим”⁴¹, так как “зависимость ЕС от технологических компаний, расположенных за пределами ЕС, ограничивает его лидерство и стратегическую автономию в цифровом мире”⁴².

“Возрастающая асимметрия” [Европа... 2022: 349] во взаимоотношениях США с партнерами относится и к Японии. В случае кибербезопасности американоцентричный подход усиливает ее, так как интернет все еще во многом находится под управлением США. Чем больше Япония полагается на США в вопросах национальной безопасности, тем больше зависимость и асимметрия. В этом заключается третья ловушка, и она имеет отношение ко всей японской системе безопасности. Поэтому нельзя не согласиться, что выбор японской политики в области кибербезопасности (суть которой в отсутствии собственных возможностей как с точки зрения политической воли, так и с точки зрения технических возможностей) “качественно” (質的, *shitsuteki ni*) полагаться на США в политическом плане ставит под сомнение независимость Японии [Мацумура 2021: 6].

Четвертая ловушка связана с крайне сомнительным реальным эффектом американской помощи Японии в области кибербезопасности. Слабая интегрированность японских сетей исключает применение к ним американских протоколов кибербезопасности [Katagiri 2022: 83]. Из-за ограничений, налагаемых конституцией, “Япония не может разделить американское понимание киберугроз и технику реагирования на данные угрозы” [ibidem]. Но японские политики продолжают заставлять государственные предприятия, представителей бизнеса переходить именно на американские стандарты, показывая американской стороне свою приверженность сотрудничеству.

С этой же целью Япония системно поддерживает США на уровне официальной риторики⁴³. Например, в каждом программном документе, заявляя о росте киберугроз из Китая⁴⁴ или подписав в 2022 г. Декларацию о будущем интернета⁴⁵ – американский проект с выраженной антикитайской направленностью, который фактически на официальном уровне провозглашает условное разделение киберпространства на блоки, отделяя сторонников американоцентричности интернета от остальных государств [Никипорец-Такигава, Филатов 2024: 198]. Чем активнее Япония поддерживает антикитайскую риторику США, тем сильнее осложняет взаимоотношения с Китаем.

⁴¹ European Commission. A Europe fit for the digital age: Empowering people with a new generation of technologies. 2019. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en (accessed 21.02.2025).

⁴² European Economic and Social Committee. Digital Sovereignty: a crucial pillar for EU’s digitalisation and growth. 2022. <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-sovereignty-crucial-pillar-eus-digitalisation-and-growth> (accessed 21.02.2025).

⁴³ Japan Ministry of Defence, Joint Statement of the Security Consultative Committee (2+2). 11.01.2023. P. 2. <https://www.mod.go.jp/en/article/2022/01/8158c6e96630df45b4b7baf10072dd3206b93f86.html> (accessed 21.02.2025).

⁴⁴ 外務省「国際情勢認識と日本外交の展望」2023年 [Восприятие международной ситуации и перспективы японской дипломатии. Министерство иностранных дел Японии, 2023]. https://www.mofa.go.jp/mofaj/gaiko/bluebook/2023/pdf/pdfs/1_2_1.pdf (accessed 21.02.2025).

⁴⁵ Declaration for the Future of the Internet. https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (accessed 21.02.2025).

Вследствие совокупности внутривнутриполитических причин кибербезопасность Японии практически не разрабатывается и остается на уровне объявления недостижимых целей. Япония продолжает ориентироваться в вопросах безопасности на помощь США во многом в ущерб своим национальным интересам. Между тем, в строящемся мировом порядке идет активная апробация киберсуверенности, которая доказывает свою эффективность. Возможно, Япония обратит внимание на участие в этой апробации других союзников США и последует их примеру.

Трансформация внешнеполитических приоритетов новой американской администрации может вынудить Японию искать партнеров в коллективной безопасности и новые ориентиры для разработки национальной. Но это внешние факторы. Внутренним же остается отсутствие готовности политической элиты взять на себя смелость предложить национально ориентированную стратегию национальной безопасности. И если здесь не произойдет никаких перемен, то Япония не разработает конструктивного и результативного способа обеспечения национальной безопасности. Выводы также могут быть экстраполированы и на другие виды безопасности, а также касаются не только Японии, но и других союзников США, которым стратегический выбор Японии представляется достойным подражания.

DOI: [10.17976/jpps/2025.03.11](https://doi.org/10.17976/jpps/2025.03.11)

JAPAN'S NATIONAL CYBER SECURITY STRATEGY: PROBLEM FIELD AND APPROACH'S TRAPS

G. Yu. Nikiporets-Takigawa¹

¹ HSE University, Moscow, Russia

NIKIPORETS-TAKIGAWA, Galina Yur'evna, Dr. Sci. (Polit. Sci.), Professor, Faculty of World Economy & International Affairs, HSE University, email: gnikiporets-takigawa@hse.ru

Nikiporets-Takigawa, G. Yu. (2025). Japan's national cyber security strategy: problem field and approach's traps. *Polis. Political Studies*, 3, 162-175. (In Russ.) <https://doi.org/10.17976/jpps/2025.03.11>

Acknowledgements. The paper is prepared within the Project No. 25-00-05 ("ASEAN+, BRICS+, NATO+: Prospects for Asian Integration in the New World Order") of the Scientific Foundation of the National Research University Higher School of Economics (HSE) Program.

Received: 18.07.2024. Accepted: 24.02.2025

Abstract. This article analyzes the approaches, challenges, and outcomes in developing and implementing national cybersecurity strategies, framing them through the concept of cyber power within neoclassical realism. Strengthening cyber power emerges as an independent variable, driven by the dynamics of the international system and presenting a persistent, shared external challenge across states. Each state crafts its response to this challenge based on intervening variables, with Japan serving as a critical case study to illustrate several key factors. The article asserts that Japan's latest cybersecurity strategy, which ambitiously targets "active defense" and seeks parity with the United States, is unfeasible. Domestic political constraints fuel this impracticality. Political elites hesitate to independently and decisively enact essential legislation, while an entrenched reliance on the United States-termed Americanism further complicates progress. Beyond Japan's case, the analysis probes the risks of outsourcing a disproportionate share of national security responsibilities to external partners. Such delegation presents severe drawbacks: states forfeit technological sovereignty by favoring borrowed technologies over homegrown innovation, deepen their political dependence, expose regional security to threats, and gain little practical benefit from cooperative efforts. This conceptualization of cyber power and cybersecurity highlights a core principle: bolstering national cybersecurity demands each state's independent initiative. The findings enrich debates about security in an emerging multipolar world and inform national security policies.

Moreover, they contribute fresh methodological insights into calculating cyber power and leveraging indices and ratings for rigorous analysis.

Keywords: national security strategy, cybersecurity, cyber power, cyber sovereignty, U.S.-centric approach, Japan, U.S., UK, EU.

References

Burwell, F., & Propp, K. (2022). Digital Sovereignty in Practice: the EU's push to shape the new global economy. Washington: Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2022/11/Digital-sovereignty-in-practice-The-EUs-push-to-shape-the-new-global-economy_.pdf

Dosch, J. (2011). The United States in the Asia-Pacific: still the hegemon? In M.K. Connors, R. Davison, & J. Dosch (Eds.), *The New Global Politics of the Asia Pacific* (pp. 22-36). London: Palgrave Macmillan.

Easley, L. (2016). How proactive? How pacifist? Charting Japan's evolving defense posture. *Australian Journal of International Affairs*, 71(1), 63-87. <https://doi.org/10.1080/10357718.2016.1181148>

Fackler, M. (2021). Media coverage of Fukushima. Ten years later. *The Asia-Pacific Journal: Japan Focus*, 19(17), Art. 5622. <https://apjif.org/2021/17/fackler>

Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to Earth. *International Security*, 38(2), 41-73. https://doi.org/10.1162/ISEC_a_00136

Gordon, D. (2020). Targeted systems and democracy: Russia, Iran, and China's Cyber threats and disinformation campaigns to weaken and undermine Western democracies. Utica: Utica College Dissertations Publ.

Griffiths, J. (2019). The Great firewall of China: how to build and control an alternative version of the Internet. London: Zed Books Ltd. <https://doi.org/10.5040/9781350225497>

Hughes, C., & Kallender, P. (2016). Japan's emerging trajectory as a 'cyber power': from securitization to militarization of cyberspace. *Journal of Strategic Studies*, 40(1-2), 118-145. <https://doi.org/10.1080/01402390.2016.1233493>

Katagiri, N. (2022). Three conditions for cyber countermeasures: opportunities and challenges of active-defense operations. *The Cyber Defense Review*, 7(3), 79-90.

Lei, H. (2019). Modern information warfare: analysis and policy recommendations. *Foresight*, 21(4), 508-522. <https://doi.org/10.1108/FS-06-2018-0064>

Liff, A.P. (2017). Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, 35(3), 401-428. <https://doi.org/10.1080/01402390.2012.663252>

Lindsay, J.R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365-404. <https://doi.org/10.1080/09636412.2013.816122>

Maschmeyer, L. (2021). The subversive trilemma: why cyber operations fall short of expectations. *International Security*, 46(2), 51-90. https://doi.org/10.1162/isec_a_00418

Mochinaga, D. (2020). The expansion of China's Digital Silk Road and Japan's response. *Asia Policy*, 15(1), 41-60. <https://doi.org/10.1353/asp.2020.0005>

Nye, J.S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44-71. https://doi.org/10.1162/ISEC_a_00266

Rid, T., & McBurney, P. (2012). Cyber-weapons. *The RUSI Journal*, 157(1), 6-13. <https://doi.org/10.1080/03071847.2012.664354>

Spade, C.J.M. (2011). China's cyber power and America's national security. U.S. Army War College, Carlisle Barracks, PA. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf>

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, 556(7702), 296-298. <https://doi.org/10.1038/d41586-018-04602-6>

Voo, J., Hemani, I., & Cassidy, D. (2022). National Cyber Power Index (NSPI). Harvard Kennedy School Belfer Center for Science and International Affairs.

Watanabe, T. (2022). Japan's security policy evolution: the interaction between think tank proposals and government implementation. *Asia Policy*, 17(3), 107-124. <https://doi.org/10.1353/asp.2022.0040>

Whyte, Ch., & Mazanec, B. (2019). Understanding cyber warfare: politics, policy and strategy. London: Routledge. <https://doi.org/10.4324/9781315636504>

Chugrov, S.V. (2023). Human capital of an academic community under digital transformation: the case of Japan. *Polis. Political Studies*, 6, 128-141. (In Russ.) <https://doi.org/10.17976/jpps/2023.06.10>

Gromyko, A.I.A. (Ed.). (2022). Evropa v krizisnom mire [Europe in a crisis world]. Moscow: Ves' Mir. (In Russ.) <https://doi.org/10.55604/9785777708953>

Nikiporets-Takigawa, G.Yu., & Filatov, O.A. (2024). E-governance in approaches to ensuring the cybersecurity in APR (cases of Taiwan and Singapore). *Yugo-Vostochnaya Aziya: aktual'nye problemy razvitiya*, 2(2), 195-207. (In Russ.) <https://doi.org/10.31696/2072-8271-2024-2-2-63-195-207>

Streltsov, D.V. (2023). Will Japan become a “normal” country”? *Russia in Global Affairs*, 21(3), 174-191. (In Russ.) <https://doi.org/10.31278/1810-6439-2023-21-3-174-191>

Security Project Group, The Sasakawa Peace Foundation. (2018). Cyber space defense enhancement project policy proposal “Establish a Cyber Security Agency in Japan!” (In Jap.) <https://www.spf.org/global-data/20181029155951896.pdf>

Ito, H. (2012). “The fifth battlefield” – the threat of cyber warfare. Shodensha Shinsho. (In Jap.)

Matsumura, M. (2021). Shortcomings and prospects for Japan’s cybersecurity strategy. *Telecommunications Development Assistance Fund Grant Report*, No. 36. (In Jap.) <https://www.taf.or.jp/files/items/1929/File/%E6%9D%BE%E6%9D%91%E6%98%8C%E5%BB%A3.pdf>

Matsumura, M. (2021). Shortcomings and prospects for Japan’s cybersecurity strategy – Ministry of Internal Affairs and Communications considers response to “peaceful state” regime fixing. *Journal of Information and Communication Policy*, 5(2). (In Jap.) https://www.soumu.go.jp/main_content/000787278.pdf

Yamada, T. (2019). Cyberwar now. Best New Book. Bestsellers. (In Jap.)

Литература на русском языке

Европа в кризисном мире. 2022. Отв. ред. Ал.А. Громыко. М.: Весь Мир. <https://doi.org/10.55604/978577708953>. EDN: PLQIBR.

Никипорец-Такигава Г.Ю., Филагов О.А. 2024. E-governance в подходах к обеспечению кибербезопасности в АТР (на примере Тайваня и Сингапура). *Юго-Восточная Азия: актуальные проблемы развития*. Т. 2. № 2. С. 195-207. <https://doi.org/10.31696/2072-8271-2024-2-2-63-195-207>. EDN: JYBCUC.

Стрельцов Д.В. 2023. Станет ли Япония “нормальной” страной? *Россия в глобальной политике*. Т. 21. № 3. С. 174-191. <https://doi.org/10.31278/1810-6439-2023-21-3-174-191>. EDN: VKETHC.

Чугров С.В. 2023. Человеческий капитал научного сообщества в условиях цифровой трансформации: опыт Японии. *Полис. Политические исследования*. № 6. С. 128-141. <https://doi.org/10.17976/jpps/2023.06.10>. EDN: XXVIIIE.

Литература на японском языке

伊東寛 『「第5の戦場」—サイバー戦の脅威』(祥伝社新書 2012年)[Хироси Ито. 2012. “Пятое поле боя” – угроза кибервойны. Shodensha Shinsho].

『サイバー空間の防衛力強化プロジェクト 政策提言 “日本にサイバーセキュリティ庁の創設を!”』2018年10月 公益財団法人 笹川平和財団 安全保障事業グループ [Группа проектов по безопасности Фонда мира Сасакава. 2018. Проект усиления обороны киберпространства. Политические рекомендации “Создать агентство кибербезопасности в Японии!”]. <https://www.spf.org/global-data/20181029155951896.pdf> (accessed 21.02.2025).

松村 昌廣『我が国のサイバーセキュリティ戦略の欠点と展望』(公益財団法人電気通信普及財団 研究調査助成報告書 第36号)[Масахиро Мацумура. 2021. Недостатки и перспективы японской стратегии кибербезопасности. Отчет о грантах Фонда содействия развитию телекоммуникаций № 36]. <https://www.taf.or.jp/files/items/1929/File/%E6%9D%BE%E6%9D%91%E6%98%8C%E5%BB%A3.pdf> (accessed 21.02.2025).

松村 昌廣『我が国のサイバーセキュリティ戦略の欠点と展望 — 「平和国家」体制の桎梏への対応を考える総務省』(情報通信政策研究 第5巻 第2号)[Масахиро Мацумура. 2020. Недостатки и перспективы стратегии кибербезопасности Японии – Министерство внутренних дел и коммуникации рассматривает меры по преодолению системы “мирного государства”. Журнал информационной и коммуникационной политики. Т. 5. № 2]. https://www.soumu.go.jp/main_content/000787278.pdf (accessed 21.02.2025).

山田敏弘『サイバー戦争の今』(第8章 ベスト新書 2020年)[Тосихиро Ямада. 2019. Кибервойна сейчас. Лучшая новая книга. Бестселлеры].