Подходы Японии к международному сотрудничеству в области кибербезопасности на примере АСЕАН

 DOI: 10.31857/S013128120019300-1

Мелконян Лусине Арменовна

Ассистент кафедры теории и истории международных отношений ФГСН РУДН (адрес: 117198, Москва, ул. Миклухо-Маклая, 6). ORCID: 0000–0003–0294–8076.
E-mail: melkonyan-la@rudn.ru.

Статья поступила в редакцию 09.02.2022.

Аннотация:

В статье проанализированы основные подходы японского государства к решению проблем в области кибербезопасности путем выработки соответствующих стратегий и программ, углубления международного сотрудничества для противостояния угрозам киберпреступности и информационной безопасности. Рассмотрены эволюция национальных стратегий и международных соглашений в области кибербезопасности и динамика развития подходов к ключевым вопросам политики информационной безопасности.

В связи с ростом злонамеренного использования киберпространства международными террористами и киберпреступниками в деструктивных целях проблема объединения международных усилий в борьбе с кибератаками на критическую информационную инфраструктуру (далее — КИИ) приобретает особую актуальность. Япония и ранее подвергалась кибератакам на государственном уровне, однако за последнее десятилетие угрозы в адрес институтов государственной власти приобретают более масштабный и тревожный характер. В целях защиты персональных данных и интеллектуальной собственности Япония укрепляет свой оборонный потенциал, расширяя возможности государственных учреждений и Сил самообороны.

Международное сотрудничество Японии в области кибербезопасности рассмотрено на примере АСЕАН, в том числе в рамках соглашения о ВРЭП, с точки зрения не только географической близости со странами ассоциации и наличия тесных экономических связей с ними, но также с учетом эффективного взаимодействия и насыщенных контактов на высшем и высоком уровнях в области кибербезопасности в качестве страны-участницы ВПСТТП.

Автор сравнивает подходы ВРЭП и ВПСТТП к вопросам кибербезопасности и информационного суверенитета, выявляя основные противоречия между участниками этих многосторонних инициатив, объединяющих ключевых игроков АТР, одним из которых является Япония.

Ключевые слова:

Япония, кибербезопасность, Стратегия кибербезопасности Японии, международные отношения, АСЕАН, ВРЭП, ВПСТТП.

Для цитирования:

Мелконян Л.А. Подходы Японии к международному сотрудничеству в области кибербезопасности на примере АСЕАН. // Проблемы Дальнего Востока. 2022. № 2. С. 49–62. DOI: 10.31857/S013128120019300-1

Источники финансирования:

Данная статья подготовлена в рамках Исследовательского проекта РФФИ-ЭИСИ 21–011–31812 опн «Имитационное моделирование распространения социальных норм и ценностей: глобальные коммуникации VS информационный суверенитет РФ».

Кибербезопасность — один из основных элементов национальной безопасности государств. Угроза киберпространству той или иной страны напрямую представляет собой угрозу критической информационной инфраструктуре государства, следовательно, и ее национальной безопасности.

В рамках существующих механизмов международной безопасности проблема кибербезопасности приобретает сложный, транснациональный характер. Это подчерки-

вает необходимость объединения усилий ключевых акторов международных отношений в целях поиска новых моделей решения новых проблем, таких как киберугрозы.

Ряд авторов полагают, что в условиях сформировавшейся «новой биполярности» между США и КНР все большее значение приобретают новые мировые политические пространства, которые становятся ареной геополитического противостояния. Одним из таких «политических пространств» является киберпространство, приобретшее более критическое значение в контексте ускорения процесса цифровизации на фоне пандемии COVID-19[1].

Международное сотрудничество в области противостояния угрозам в киберпространстве прежде всего исходит из критической необходимости обмена информацией и передовым опытом между ключевыми субъектами кибербезопасности. Япония и ранее подвергалась кибератакам, но за последнее десятилетие все чаще становятся реальностью угрозы в адрес институтов государственной власти. В качестве примера можно привести, в частности, кибератаку на корпорацию Mitsubishi Heavy Industry в 2011 г., что послужило тревожным сигналом для японского государства, учитывая, что данная компания — крупнейший подрядчик Министерства обороны Японии по поставкам военной техники, обладающий сверхсекретной конфиденциальной информацией Сил самообороны[2]. Также правительственные сети страны подвергались в 2012 г. около 3000 кибератак ежедневно, что в два раза превышает число атак в 2011 г. Следовательно, проблема обеспечения кибербезопасности в Японии так же актуальна, как во всем мире.

Япония выразила интерес к кибердипломатии еще в 2006 г., когда была принята первая Национальная стратегия информационной безопасности, в которой упоминалось о намерении страны развивать международное сотрудничество в данной области. Стратегия 2006 г. предлагала «японскую модель кибердипломатии», поскольку «проблемы, с которыми сталкивается Япония как ведущая страна по широкополосному доступу к Интернету сегодня — это проблемы, с которыми другие страны будут сталкиваться в будущем»[3]. Примечательно, что 74 % зарегистрированных интернационализированных доменных имен во всем мире, согласно статистике webhosting.info, сосредоточено в трех странах: США, Корее и Японии.

В 2009 г. была принята вторая Национальная стратегия информационной безопасности, ставящей целью «международное партнерство и сотрудничество», в особенности с США и ЕС, а также «достижение лидерства страны в области установления стандартов информационной безопасности в Азии»[4].

В целях реагирования на вышеуказанные угрозы кибербезопасности в 2012 г. Кабинетом министров был учрежден Совет по политике информационной безопасности Японии для координации деятельности следующих министерств: Министерства обороны (обеспечение национальной безопасности), Министерства внутренних дел и коммуника-

1. *Дегтерев Д.А., Рамич М.С.,* Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // *Вестник международных организаций.* 2021. Т. 16. № 3. С. 7–33 (на русском и английском языках). DOI: 10.17323/1996–7845–2021–03–01
2. Подходы Японии к кибербезопасности. Как реагировать на неопределенность? // *Информационно-аналитический портал о цифровой экономике и ИКТ-политике Digital.Report*. 17.09.2015. URL: https://digital.report/podhodyi-yaponii-k-kiberbezopasnosti-2/ (дата обращения: 19.11.2021).
3. The First National Strategy on Information Security // *Information Security Policy Council Japan*. February 2, 2006. URL: https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf, p. 32 (дата обращения: 20.11.2021).
4. The Second National Strategy on Information Security // *National Information Security Policy Council*. February 3, 2009. URL: https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf, p. 71 (дата обращения: 19.11.2021).

ций Японии (выработка коммуникационной и сетевой политики), Национального полицейского агентства Японии (борьба с киберпреступностью), Министерства экономики, торговли и промышленности (разработка инициатив по партнерству в целях обмена информацией в области кибербезопасности)[5].

В качестве целей Совета по политике информационной безопасности были обозначены усиление и координация мер против кибератак на учреждения и компании, обрабатывающие информацию о национальной безопасности, поддержание безопасной и надежной киберсреды для устранения возникающих рисков, связанных с распространением новых информационных и коммуникационных технологий.

Для реализации этих целей 10 июня 2013 г. Совет принял Стратегию кибербезопасности Японии[6]. Ранее при обозначении направлений государственной политики и основополагающих планов Токио использовал дефиницию «информационная безопасность», однако в связи с ростом угроз, выходящих за рамки информационной безопасности, было принято решение использовать более всеобъемлющую формулировку «кибербезопасность» для переоценки и переосмысления всех проблем в этой области.

Ключевые принципы Стратегии кибербезопасности Японии направлены на создание передового, устойчивого и динамичного киберпространства, необходимого для обеспечения национальной безопасности, социально-экономического развития и общественной безопасности[7].

Стратегия кибербезопасности в качестве основных субъектов кибербезопасности рассматривает государство, компании, связанные с критически важной инфраструктурой и киберпространством, сферы промышленности, информационную науку, малые и средние предприятия.

В настоящее время в Японии политику в области кибербезопасности определяет принятый в 2014 г. «Основной закон о кибербезопасности», основанный на принципах, определённых в «Законе о формировании современного информационно-телекоммуникационного сетевого общества»[8].

Согласно этому закону, ведущая роль в качестве координационного центра в повышении уровня кибербезопасности принадлежит Национальному центру готовности к чрезвычайным ситуациям и стратегии в области кибербезопасности (National Center of Incident Readiness and Strategy for Cybersecurity). Центр был создан в 2015 г. на основе Национального центра информационной безопасности, действующего с 2005 г. Ключевые направления деятельности Центра включают создание свободного, справедливого и безопасного киберпространства, обеспечение сотрудничества между государственным и частным секторами, академическими кругами и другими субъектами.

Помимо демонстрации основной позиции в отношении политики кибербезопасности, формулировки ее целей и их реализации, NISC также координирует политику ки-

5. Commitment to a Free, Fair and Secure Cyberspace // *National center of Incident readiness and Strategy for Cybersecurity*. September 2021. URL: https://www.nisc.go.jp/eng/index.html#sec1 (дата обращения: 20.11.2021).
6. В Японии принята стратегия кибербезопасности // *Онлайн-издание Digital Russia*. 20.06.2013. URL: https://d-russia.ru/v-yaponii-prinyata-strategiya-kiberbezopasnoti.html (дата обращения: 18.11.2021).
7. Cybersecurity Strategy — Toward a world-leading, resilient and vigorous cyberspace // *National Information Security Center*. June 10, 2013. URL: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf (дата обращения: 19.11.2021).
8. Япония: обзор законодательства в сфере кибербезопасности // *Экспертно-аналитический центр ГК InfoWatch.* 11.07.2021. URL: https://webcache.googleusercontent.com/search?q=cache:3aGjnL1YivoJ:https://cisoclub.ru/yaponiya-obzor-zakonodatelstva-v-sfere-kiberbezopasnosti/+&cd=1&hl=ru&ct=clnk&gl=ru (дата обращения: 20.11.2021).

бербезопасности для защиты критической информационной инфраструктуры, задает единый стандарт мер информационной безопасности государственных органов, разрабатывает план развития человеческих ресурсов в области кибербезопасности и др.[9]

Стратегия кибербезопасности 2013 г. выделяет 3 главные направления деятельности. Первое направление касается обеспечения устойчивости киберпространства для основных субъектов кибербезопасности путем анализа возможных киберугроз, обмена информацией и проведения совместных учений между критически важными инфраструктурами, государственными органами, группами реагирования на инциденты (например, группами полиции и Сил самообороны). Второе направление деятельности отвечает за обеспечение динамичности киберпространства путем пересмотра программ развития человеческих ресурсов в области кибербезопасности. Третье направление касается Международной стратегии Японии по кибербезопасности, предполагающей деятельность государства, направленную на развитие общего понимания процессов, участие в действиях мирового сообщества, участие в глобальном процессе расширения технологических границ. Приоритетными областями партнерства с указанными и другими странами являются создание многосторонних механизмов обмена информацией и реагирования на кибератаки и угрозы, продвижение и поддержка научных исследований и мероприятий в сфере кибербезопасности и др.

Международная стратегия предполагает развитие сотрудничества страны по противодействию угрозам в киберпространстве с государственными органами и национальными группами реагирования на киберугрозы США, Великобритании, Франции, Германии, Индии, ЕС и АСЕАН, участие в международных конференциях, внесение вклада в процесс выработки общих правил для киберпространства. Так, в 2014 г. Япония приняла очередную конференцию, посвященную вопросам защиты КИИ в рамках Meridian Process[10].

Кабинет министров пересмотрел Стратегию кибербезопасности Японии 2013 г. и с учетом растущего количества кибератак в ноябре 2015 г. пересмотрел стратегию. Если предыдущая Стратегия была сосредоточена преимущественно на сотрудничестве в области киберзащиты и наращивания киберпотенциала, то новый документ 2015 г. был принят под воздействием Стратегии национальной безопасности администрации Абэ, ставящей акцент на понятие «проактивного», а не «реактивного» мира. Япония, таким образом, концептуализировала свое стремление стать активным игроком в киберпространстве.

В рамках заседания по вопросам кибербезопасности 28 сентября 2021 г. Кабинет министров принял Новую стратегию кибербезопасности Японии — трехлетнюю стратегию, пришедшую заменить принятую в 2018 г. стратегию. Стоит отметить, что в последней стратегии от 2021 г. РФ, КНР и КНДР фигурируют как страны, представляющие угрозу кибератак для Японии[11], однако следует учесть, что документ был подготовлен и составлен на фоне участившихся кибератак со стороны Китая и ухудшения отношений с

9. Япония: обзор законодательства в сфере кибербезопасности // *Экспертно-аналитический центр ГК InfoWatch.* 11.07.2021. URL: https://webcache.googleusercontent.com/search?q=cache:3aGjnL1YivoJ:https://cisoclub.ru/yaponiya-obzor-zakonodatelstva-v-sfere-kiberbezopasnosti/+&cd=1&hl=ru&ct=clnk&gl=ru (дата обращения: 19.11.2021).
10. Cybersecurity Strategy // *The Government of Japan*. June 16, 2014. URL: https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf (дата обращения: 17.11.2021).
11. В новой стратегии кибербезопасности Японии упомянута Россия // *Известия*. 28.09.2021. URL: https://iz.ru/1227848/2021–09–28/v-novoi-strategii-kiberbezopasnosti-iaponii-upomianuta-rossiia (дата обращения: 21.11.2021).

этой страной из-за тайваньского вопроса[12]. В стратегии упоминается, что Китай проводит кибератаки в целях кражи информации у компаний, связанных с военными структурами и обладающими передовыми технологиями[13], а также замечается, что «Китай, Россия и Северная Корея наращивают киберпотенциал своих военных и других структур»[14].

Новизна стратегии заключается в том, что в ней особо подчеркивается элемент сдерживания за счет японо-американского альянса и путем проведения совместных учений японских Сил самообороны и ВС США.

В качестве нового элемента стратегии следует рассмотреть также поддержку наращивания киберпотенциала стран ИТР, включая АСЕАН. Преследуя цели экономической безопасности, Стратегия направлена на обеспечение безопасности КИИ для международных коммуникаций, а также создание новых стандартов безопасности и надежности информационных технологий[15].

Киберпространство в целом и социальные сети в частности — это относительно новые сферы политического влияния, в которых не все государства выработали правила игры, в связи с чем особую важность приобретает осознание необходимости законодательного регулирования государством социальных сетей и медиа. На фоне бурного роста социальных сетей и их популярности, а также опасений государств по поводу fake news и дезинформации национальные правительства многих стран вынуждены разрабатывать модели регулирования киберпространства. Говоря о национальной специфике Японии, следует отметить, что в киберпространстве Японии помимо транснациональных корпораций (Meta, Google, Twitter) представлены также местные онлайн-платформы — японский видеохостинг Niconico, японский мессенджер Line, разработанный компаниями NHN Japan, NHN Corp. и запущенный в Японии в 2011 г.[16]

Японский Консорциум электронных сетей разработал «Общие этические принципы работы онлайн-сервисов» еще в 1996 г., поставившие перед собой задачу обеспечения здорового роста и развития социальных сетей и онлайн-услуг вне зависимости от размера компании и принципов управления во избежание диффамации и проблем с общественным порядком с точки зрения морали и этики.

В 2020 г. исследовательская группа при Министерстве внутренних дел и коммуникаций Японии опубликовала отчет, в котором говорится, что добровольные меры, при-

12. Japan's New Cybersecurity Strategy. National center of Incident readiness and Strategy for Cybersecurity (NISC) // *The Government of Japan*. September 28, 2021. URL: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf (дата обращения: 18.11.2021).
13. *Glucksmann T*. How Will Japan's Cybersecurity Posture Impact its Relations with China? // *The Diplomat*. October 16, 2021. URL: https://thediplomat.com/2021/10/how-will-japans-cybersecurity-posture-impact-its-relations-with-china/ (дата обращения: 20.11.2021).
14. In first, Japan names China, Russia and North Korea as cyberattack threats // *The Japan Times*. September 27, 2021. URL: https://www.japantimes.co.jp/news/2021/09/27/national/cyber-attacks-measures/ (дата обращения: 23.11.2021).
15. *Pradhan. S.D.* Japan's new cyber security strategy: Significant dimensions // *The Times of India*. August 6, 2021. URL: https://timesofindia.indiatimes.com/blogs/ChanakyaCode/japans-new-cyber-security-strategy-significant-dimensions/ (дата обращения: 23.11.2021).
16. *Tanaka K.* Japan's Citizen Media Meet at Mikawa Medifes 2014 // *Global Voices*. May 4, 2014. URL: https://globalvoices.org/2014/05/04/japanese_citizen_media_festival/; Huffington A. Postcard from Japan: Talking Zen, Abenomics, Social Networking and the Constitution with Prime Minister Shinzo Abe // *Huffington Post*. May 9, 2013. URL: http://huff.to/1MhvStk (дата обращения: 12.12.2021).

нимаемые операторами социальных сетей, должны соблюдаться, однако они должны тщательно контролироваться государством[17].

В Японии поведение граждан в социальных сетях регламентируется на уровне этических кодексов. Так, в государственных ведомствах и крупных корпорациях существуют кодексы, регулирующие этические нормы для сотрудников. Эти нормы регулируют поведение представителей корпоративных сообществ в целом, не только в киберпространстве. В Японии редко можно встретить случаи открытой критики действующей власти или демонстрации политических взглядов госслужащими или чиновниками, что демонстрирует высокий уровень строгости этического регулирования корпоративных норм, а также поведения граждан в социальных сетях (и не только)[18].

В Японии все больше становится работодателей, которые устанавливают ограничения на использование работниками социальных сетей в рабочее время, обосновывая это требованием полностью посвятить себя своим рабочим обязанностям[19].

Несмотря на то, что значительное влияние на формирование общественного мнения оказывают СМИ и блогосфера, работники СМИ часто вынуждены ограничивать активность в соцсетях и блогосфере лишь записями о личных интересах и хобби, иначе комментарии подписчиков, содержащие критику власти, могут быть болезненно восприняты руководством компании.

Проблемы в области контроля за соцсетями в Японии часто сводятся к вопросу травли в интернете — кибербуллингу, жертвами которого чаще всего становятся японские дети и подростки. В результате учащения подобных случаев ситуация в области контроля за соцсетями в Японии в ближайшее время может измениться. Депутаты японского парламента регулярно поднимают вопрос о выработке мер по привлечению к ответственности за кибербуллинг[20].

Согласно данным FreedomHouse, некоторые соцсети в Японии иногда могут ограничивать контент по запросу правительства. В период с июля по декабрь 2019 г. Facebook закрыл доступ к трем записям после получения распоряжений суда[21]. За рассматриваемый период Twitter получил 12 496 запросов на удаление контента, что на 143 % больше, чем за предыдущие шесть месяцев[22]. Запросы на удаление контента из Японии составили 45 % подобных запросов во всем мире (рис.1).

Следует особо подчеркнуть, что в обеспечении кибербезопасности и информационной безопасности Япония, в целом, придерживается американских подходов. 23 ноября 2001 г. Япония подписала Будапештскую конвенцию о киберпреступности наряду с

17. *Fumio S., Sari K.* Social media giants juggle freedom and responsibility // *NHK (Japan Broadcasting Corporation)*. February 12, 2021. URL: https://www3.nhk.or.jp/nhkworld/en/news/backstories/1507/ (дата обращения: 15.12.2021).
18. В Японии поведение граждан в социальных сетях строго не регламентировано // *Российская газета*. Федеральный выпуск № 27(8378). 09.02.2021. URL: https://rg.ru/2021/02/09/v-iaponii-povedenie-v-socialnyh-setiah-strogo-ne-reglamentirovano.html (дата обращения: 13.12.2021).
19. Social Media and Data Privacy in Japan. Restrictions in the Workplace // *L&E Global*. October 14, 2020. URL: https://knowledge.leglobal.org/social-media-and-data-privacy-in-japan/ (дата обращения: 10.12.2021).
20. Social Media and Data Privacy in Japan. Restrictions in the Workplace // *L&E Global*. October 14, 2020. URL: https://knowledge.leglobal.org/social-media-and-data-privacy-in-japan/ (дата обращения: 10.12.2021).
21. Japan — Content Restrictions // *Facebook Transparency*. 2019. URL: https://transparency.facebook.com/content-restrictions/country/JP (дата обращения: 13.12.2021).
22. Removal Requests // *Twitter Transparency*. 2019. URL: https://transparency.twitter.com/en/reports/removal-requests.html#2019-jul-dec (дата обращения: 13.12.2021).

США, Канадой и ЮАР. Конвенция — первый международный договор о киберпреступлениях, касающихся в первую очередь нарушений авторских прав, безопасности сети и т.д. Будапештская конвенция хоть и регулирует законодательства подписавших ее государств и дает право на трансграничный сбор и использование данных без уведомления об этом ту или иную страну[23], однако в целом продвигает проамериканский подход к кибербезопасности и информационной безопасности. Ряд стран (например, Россия) считают Будапештскую конвенцию по киберпреступлениям устаревшей в связи с появлением новых, сложных проблем, которые не были предусмотрены данным документом, разработанном в 1997–2001 гг., когда преступления в сфере информационно-коммуникационных технологий были менее масштабными и часто оставались незафиксированными и не носили глобального характера. Их также не устраивает возможность зарубежных спецслужб вмешиваться без официального уведомления в деятельность компьютерных сетей государства, что несет в себе угрозы и риски для информационной безопасности[24].

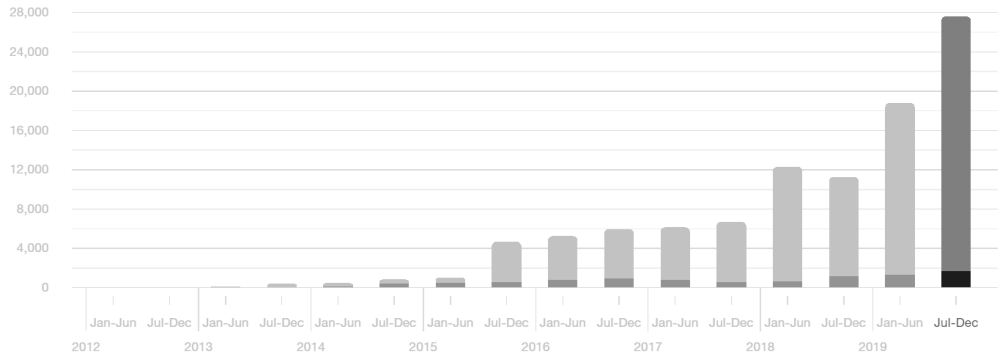

Рис. 1. Последние данные о запросах на удаление: юридические требования (рассматриваемый период: июль — декабрь 2019 г.)

Figure 1. Latest Data on Takedown Requests: Legal Requirements (July — December 2019)

Источники: Japan tells Facebook to improve data protection. Reuters. URL: https://www.reuters.com/article/us-facebook-privacy-japan-idUSKC№ 1MW0AG (дата обращения: 25.12.2021).

В Японии нет законодательных требований к локализации или местонахождению данных. Правила локализации интернет-данных существуют лишь в некоторых отраслях (здравоохранение, медицинский сектор).

В октябре 2018 г. правительство Японии обратилось к руководству Facebook с запросом улучшить защиту персональных данных своих пользователей, усилив меры безопасности и информируя регулирующие органы о любых изменениях в мерах безопасности. Запрос поступил после заявления Facebook о том, что злоумышленники украли данные 29 млн учетных записей пользователей. В апреле этого же года было разоблачено, что персональные данные почти 87 млн пользователей оказались неправомерно доступны британ-

23. *Дегтерев Д.А., Рамич М.С., Пискунов Д.А.* Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // *Вестник международных организаций*. 2021. Т. 16. № 3. С. 7–33 (на русском и английском языках). DOI: 10.17323/1996–7845–2021–03–01

24. Российский дипломат назвал Будапештскую конвенцию по киберпреступлениям устаревшей // *ТАСС*. 04.12.2017. URL: https://tass.ru/politika/4782506 (дата обращения: 25.12.2021).

ской фирме Cambridge Analytica. Примечательно, что запрос не содержит административных распоряжений или санкций и не имеет обязательной юридической силы, хотя инцидент с Cambridge Analytica мог затронуть до 100 000 японских пользователей[25].

В контексте географической близости и тесных экономических связей ключевое место в системе международного сотрудничества Японии по кибербезопасности занимают АТР и ИТР. На базе активного экономического, политического и культурно-гуманитарного диалога со странами АСЕАН развивается и укрепляется взаимодействие в сфере кибербезопасности. Регулярно проходят встречи министров стран-членов АСЕАН и Японии, основной повесткой которых становятся вопросы борьбы с киберпреступностью.

Начиная с 2009 г. Японский национальный центр информационной безопасности (до 2015 г. NISC, в настоящее время — Национальный центр готовности к инцидентам и стратегии кибербезопасности. — *Прим. автора*) ежегодно проводит семинар по сетевой безопасности между правительствами стран АСЕАН (Бруней, Камбоджа, Индонезия, Лаос, Малайзия, Мьянма, Филиппины, Сингапур, Таиланд, Вьетнам) и Японии, на котором руководители подразделений обсуждают деятельность и дальнейшие меры в области информационной безопасности[26].

В ноябре 2011 г. в рамках IV совещания по политике кибербезопасности между АСЕАН и Японией было принято решение активизировать совместные усилия по повышению осведомленности о кибербезопасности. С этой целью Япония регулярно предоставляет обучающие видео и брошюры на языках стран — членов АСЕАН, проводит тренинги по управлению кибербезопасностью для госслужащих, а начиная с 2012 г. отправляет японских экспертов на семинары и тренинги в страны АСЕАН.

Администрация Синдзо Абэ проводила внешнюю политику с акцентом на углубление диалога с АСЕАН. Уже в течение первых двух лет его правления (2012–2014 гг.) Абэ, а затем министр иностранных дел Фумио Кисида посетили все 10 стран АСЕАН с целью расширения взаимодействия в области не только кибербезопасности, но и безопасности в целом.

В сентябре 2013 г. в Токио состоялась встреча министров Японии и АСЕАН по вопросам сотрудничества в области кибербезопасности в ознаменование 40-й годовщины установления отношений между Японией и АСЕАН. В результате было подписано совместное заявление министров АСЕАН и Японии по сотрудничеству в области кибербезопасности[27], основной целью которого являлось продвижение и осуществление сотрудничества в рамках совместных проектов JASPER (расширение технического сотрудничества в области кибербезопасности), PRACTICE (принятие превентивных мер в реагировании на кибератаки посредством международного обмена), TSUBAME (обмен данными мониторинга интернет-трафика) и др.

В сентябре 2016 г. премьер-министр Синдзо Абэ выступил с важным заявлением на встрече на высшем уровне Япония—АСЕАН о том, что Япония будет продолжать оказывать содействие АСЕАН в разработке политики наращивания потенциала кибербезопасности в соответствии с «Основной политикой поддержки наращивания потенциала в об-

25. Japan tells Facebook to improve data protection // *Reuters*. October 22, 2018. URL: https://www.reuters.com/article/us-facebook-privacy-japan-idUSKC№ 1MW0AG (дата обращения: 25.12.2021).
26. Japan's Cybersecurity Capacity-Building Support for ASEAN — Shifting from What to Do to How to Do It // *Palo Alto Networks*. July 26, 2017. URL: https://www.paloaltonetworks.com/blog/2017/07/cso-japans-cybersecurity-capacity-building-support-asean-shifting/ (дата обращения: 23.11.2021).
27. Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation // *ASEAN Secretariat*. September 13, 2013. URL: https://asean.org/joint-ministerial-statement-of-the-asean-japan-ministerial-policy-meeting-on-cybersecurity-cooperation/ (дата обращения: 18.11.2021).

ласти кибербезопасности в развивающихся странах»[28], опубликованной правительством Японии в октябре 2016 г.[29] Япония заявила, что стремится снизить уязвимость кибербезопасности по всему миру, повысить безопасность повседневной жизни и деловых операций своих граждан, зависящих от КИИ в развивающихся странах, в том числе в АСЕАН, путем создания инфраструктуры для развития японской индустрии ИКТ в этих странах.

Учитывая транснациональный характер кибератак, повышение осведомленности о кибербезопасности и наращивание потенциала имеют важное значение для различных уровней кибербезопасности членов АСЕАН. В связи с этим в октябре 2016 г. АСЕАН провела первую министерскую конференцию по кибербезопасности, участники которой подчеркнули необходимость наращивания технического потенциала в области кибербезопасности для своих стран[30].

20 октября 2020 г. в дистанционном формате состоялось XIII совещание по политике в области кибербезопасности АСЕАН—Япония. Примечательным является факт, что на этой встрече страны — члены АСЕАН и Япония помимо обмена мнениями по политике кибербезопасности уделили особое внимание инициативам каждой страны в условиях распространения COVID-19. На этом совещании стороны подтвердили прогресс в совместной деятельности по вопросам выработки политики, а также договорились о новых совместных инициативах по продвижению сотрудничества между правительствами и академическими кругами в целях повышения кибербезопасности во всем регионе АСЕАН[31].

XIV совещание по политике в области кибербезопасности АСЕАН—Япония состоялось в режиме онлайн 21 октября 2021 г. В дополнение к подтверждению текущего статуса реализации 10 совместных инициатив, принятых в рамках XIII заседания, участники обсудили дальнейшее сотрудничество по таким направлениям, как совершенствование систем обмена информацией и обработки киберинцидентов, углубление сотрудничества в целях защиты КИИ, продолжение политики наращивания потенциала и повышения осведомленности, также расширение взаимодействия между правительствами, сферой промышленности и научными кругами[32].

После ухода Синдзо Абэ с поста премьер-министра партнерство Японии с АСЕАН продолжает оставаться приоритетным направлением политики обеих сторон, призванным преодолеть и минимизировать негативные последствия эскалации процесса декаплинга американо-китайских торгово-экономических отношений, а для Японии важно

28. The Japan-ASEAN Summit Meeting // Ministry of Foreign Affairs of Japan. September 7, 2016. URL: https://www.mofa.go.jp/a_o/rp/page3e_000590.html (дата обращения: 24.11.2021).
29. 国際社会の平和・安定及び我が国の安全保障に係るサイバーセキュリティ戦略の推進状況. 第10回 サイバーセキュリティ戦略本部 資料 平成28年10月 内閣官房内閣サイバーセキュリティセンター [«О мире и стабильности международного сообщества и безопасности Японии»: текущий статус продвижения стратегий кибербезопасности. Материалы 10-го заседания Секретариата кабинета министров по Стратегии кибербезопасности, октябрь, 2016 г.]. URL: https://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou09.pdf (дата обращения: 24.11.2021).
30. ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN // *Singapore Government Agency Website*. October 11, 2016. URL: https://www.csa.gov.sg/en/News/Press-Releases/ASEAN-Member-States-Call-for-Tighter-Cybersecurity-Coordination-in-ASEAN (дата обращения: 23.11.2021).
31. Outcomes of the 13th ASEAN-Japan Cybersecurity Policy Meeting // *METI Ministry of Economy, Trade and Industry*. November 6, 2021. URL: https://www.meti.go.jp/english/press/2020/1106_003.html (дата обращения: 23.11.2021).
32. Outcomes of the 14th ASEAN-Japan Cybersecurity Policy Meeting // *METI Ministry of Economy, Trade, and Industry*. October 22, 2021. URL: https://www.meti.go.jp/english/press/2021/1022_001.html (дата обращения: 23.11.2021).

также противостояние расширению влияния Китая на страны АСЕАН в период пандемии COVID-19 в виде масочной дипломатии, с одной стороны, и усиления контроля над Южно-Китайским морем — с другой.

24 февраля 2021 г. премьер-министр Японии Суга одобрил соглашение о всеобъемлющем региональном экономическом партнерстве (ВРЭП), которое считают победой многосторонности и свободной торговли, имеющей большое значение для экономической глобализации и региональной экономической интеграции. В рамках ВРЭП происходит активная цифровизация торговли, на многосторонней основе устанавливаются всеобъемлющие правила по многим ключевым вопросам, включая кибербезопасность, трансграничную передачу и хранение информации[33].

Сравнивая ВРЭП и Всеобъемлющее и прогрессивное соглашение о Транстихоокеанском партнерстве (ВПСТТП), можно отметить, что оба соглашения содержат аналогичные положения о кибербезопасности, электронной торговле (eTrading), а также личной информации и защите потребителей в Интернете. Однако ВРЭП и ВПСТТП расходятся в подходах к положениям, касающихся потоков данных и исходных кодов. В частности, ВПСТТП запрещает локализацию данных и таможенные пошлины на их электронную передачу. Эти положения приводят к утечке информации, не давая возможности размещения центров обработки данных только в пределах границ одного члена, следовательно, существует риск передачи данных стран-участниц на американские сервера. ВРЭП основывается на положениях ВПСТТП о потоках данных, но дает подписавшимся возможность исключений, ссылаясь на «законную государственную политику» и «национальную безопасность». Это означает, что страны ВРЭП могут попрежнему требовать от компаний размещения центров обработки данных в пределах своих границ, если это требование обосновано законной государственной политикой и исходит из проблем безопасности[34].

Между странами-участницами ВРЭП существует обязательство сотрудничать и обмениваться информацией о передовых методах борьбы с инцидентами кибербезопасности и наращивании потенциала властей по реагированию на эти события. Также на стадии разработки находится единый набор правил, касающихся интеллектуальной собственности в целях обеспечения большей прозрачности и сотрудничества[35].

Существует значительный разрыв в уровне экономического развития стран ВРЭП, что делает крайне сложным достижение консенсуса по ряду вопросов в рамках инициативы, в том числе по информационной и кибербезопасности, вопросам интеллектуальной собственности. Так, Япония, Австралия, Новая Зеландия и Республика Корея поддерживают инициативы глубокой либерализации по всем направлениям. Учитывая, что Япония является страной-участницей ВПСТТП, взаимные уступки могут привести к расширению свободной торговли и снижению протекционизма в других сферах по сравнению с обязательствами в действующих ЗСТ АСЕАН+1, что, в свою очередь, может повлечь значительные потери некоторых участников соглашения.

33. RCEP a good deal for globalization, regional integration // *China Daily*. May 27, 2021. URL: http://www.chinadaily.com.cn/a/202105/27/WS60af053ea31024ad0bac1cbf.html (дата обращения: 10.12.2021).
34. What's the real deal? A look inside RCEP // *Konrad Adenauer Foundation*. December 2020. URL: https://www.kas.de/documents/287213/8314289/What%27s+the+real+deal+A+look+inside+RCEP.pdf/c2e33800-a5b2–8e9e-17e5–4fd15c431745?version=1.1&t=1608109127029 (дата обращения: 10.12.2021).
35. Regional trade boost for cyber, digital and data. Denham Sadler // *InnovationAus.com*. November 16, 2020. URL: https://www.innovationaus.com/regional-trade-boost-for-cyber-digital-and-data/ (дата обращения: 11.12.2021).

* * *

Подводя итоги вышесказанному, можно подчеркнуть эффективность государственной политики и сотрудничества Токио с развивающимися странами в областях кибербезопасности, цифровизации экономик, разработки новых цифровых технологий, что служит важным индикатором потенциала и глобальных усилий Японии по превращению в ведущего актора в сфере управления данными.

В условиях декаплинга США—КНР для АСЕАН и Японии проблема выстраивания качественно новых отношений с Вашингтоном и Пекином является общим вопросом[36]. Несмотря на то, что прослеживается относительное ослабление позиций Японии в АСЕАН ввиду активизации КНР в период кризиса, вызванного пандемией, Токио воплощает в жизнь идею отношений между странами как между «равноправными партнерами», сформулированную еще в Доктрине Фукуды в 1977 г. в противовес вертикальной структуре отношений, имевших место до сих пор.

Взаимодействие Япония—АСЕАН в сфере информационной и кибербезопасности следует рассматривать как попытку продвижения Японией на страны АСЕАН проамериканских подходов. Существует также мнение, что создание и продвижение ВРЭП в качестве альтернативы ВПСТТП — инициатива Китая, целью которой является противостояние США—КНР в регионе. Тем не менее, считается, что Китай вовлекает Японию в прокитайскую экономическую инициативу посредством экономических выгод, признавая технологическое лидерство Японии и открывая для нее доступ на китайский рынок. В свою очередь, Япония получает возможность с помощью передовых технологий транслировать проамериканские подходы информационной и кибербезопасности на страны ВРЭП.

Так, Япония рассматривает кибербезопасность как важный аспект национальной безопасности. Политика Японии в области кибербезопасности заключается в усилении мер безопасности для национального правительства, поощрении исследований в сфере кибербезопасности в академической среде, исследовательских институтах и борьбе с киберпреступностью.

Важным приоритетом для Японии является защита персональных данных и интеллектуальной собственности, являющихся источниками как международной конкурентоспособности, так и важными активами, которые государство защищает. Для реализации этих целей страна укрепляет свой оборонный потенциал, расширяя возможности Сил самообороны и других государственных учреждений.

Согласно новейшей Стратегии кибербезопасности, Япония в тесном сотрудничестве со странами-партнерами планирует использовать политические, экономические, технологические, юридические, дипломатические и другие эффективные средства и возможности для поддержания стабильности в сфере кибербезопасности и расширения своей роли. Япония является активным сторонником верховенства закона в киберпространстве и поддерживает развитие и соблюдение норм международного права в управлении киберпространством.

Дальнейшее сотрудничество между Японией и АСЕАН в сфере кибербезопасности играет важную роль в контексте обеспечения стабильности киберпространства в регионе. Следовательно, правительству, сменившему администрации Синдзо Абэ и Есихидэ Суги, следует и дальше укреплять взаимодействие с АСЕАН, содействовать содержательному и эффективному диалогу как по традиционным, так и относительно новым направлениям безопасности, в том числе по линии ВРЭП.

36. Post-Abe: Japan-ASEAN partnership crucial in navigating great power rivalry // *ThinkChina*. September 9, 2020. URL: https://www.thinkchina.sg/post-abe-japan-asean-partnership-crucial-navigating-great-power-rivalry (дата обращения: 22.11.2021).

Литература

Дегтерев Д.А., *Рамич М.С.*, *Пискунов Д.А.* Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // *Вестник международных организаций*. 2021. Том 16. № 3. DOI: 10.17323/1996–7845–2021–03–01

Рогожина Н.Г. Масочная дипломатия Китая в странах Юго-Восточной Азии // *Юго-Восточная Азия: актуальные проблемы развития*. 2021. Том I. № 1 (50). DOI:10.31696/2072–8271–2021–1–1–50–073–081

ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN // *Singapore Government Agency Website*. October 11, 2016. URL: https://www.csa.gov.sg/en/News/Press-Releases/ASEAN-Member-States-Call-for-Tighter-Cybersecurity-Coordination-in-ASEAN (дата обращения: 23.11.2021).

Commitment to a Free, Fair and Secure Cyberspace // *National center of Incident readiness and Strategy for Cybersecurity*. September 2021. URL: https://www.nisc.go.jp/eng/index.html#sec1 (дата обращения: 20.11.2021).

Cybersecurity Strategy // *The Government of Japan*. June 16, 2014. URL: https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf (дата обращения: 17.11.2021).

Cybersecurity Strategy — Toward a world-leading, resilient and vigorous cyberspace // *National Information Security Center*. June 10, 2013. URL: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf (дата обращения: 19.11.2021).

Drake W. J., Cheon K. Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG) // *United Nations ICT Task Force. Paperback*. March 11, 2008. URL: https://ifap.ru/library/book271.pdf (дата обращения: 19.11.2021).

Japan's New Cybersecurity Strategy // *National center of Incident readiness and Strategy for Cybersecurity (NISC)*. September 28, 2021. URL: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf (дата обращения: 18.11.2021).

Joint Ministerial Statement of the ASEAN—Japan Ministerial Policy Meeting on Cybersecurity Cooperation // *ASEAN Secretariat*. Tokyo, September 13, 2013. URL: https://asean.org/joint-ministerial-statement-of-the-asean-japan-ministerial-policy-meeting-on-cybersecurity-cooperation/ (дата обращения: 18.11.2021).

Outcomes of the 13th ASEAN-Japan Cybersecurity Policy Meeting // *METI Ministry of Economy, Trade and Industry*. November 06, 2021. URL: https://www.meti.go.jp/english/press/2020/1106_003.html (дата обращения: 23.11.2021).

Outcomes of the 14th ASEAN-Japan Cybersecurity Policy Meeting // *METI Ministry of Economy, Trade and Industry*. October 22, 2021. URL: https://www.meti.go.jp/english/press/2021/1022_001.html (дата обращения: 23.11.2021).

Sukumar A. Resolved: Japan Could Lead Global Efforts on Data Governance // *Debating Japan.* Vol. 2 Issue 6. Center for Strategic and International Studies (CSIS). June 27, 2019. URL: https://www.csis.org/analysis/resolved-japan-could-lead-global-efforts-data-governance (дата обращения: 19.11.2021).

The First National Strategy on Information Security // *Information Security Policy Council, Japan*. February 02, 2006. URL: https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf (дата обращения: 20.11.2021).

The Japan-ASEAN Summit Meeting // *Ministry of Foreign Affairs of Japan*. September 07, 2016. URL: https://www.mofa.go.jp/a_o/rp/page3e_000590.html (дата обращения: 24.11.2021).

The Second National Strategy on Information Security // *National Information Security Policy Council*. February 03, 2009. URL: https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf (дата обращения: 19.11.2021).

Vosse W. M. Japan's Cyber Diplomacy. International Christian University (ICU), Tokyo. October 2019. URL: https://eucyberdirect.eu/research/japans-cyber-diplomacy (дата обращения: 17.11.2021).

国際社会の平和・安定及び我が国の安全保障に係るサイバーセキュリティ戦略の推進状況. 第10回 サイバーセキュリティ戦略本部 資料 平成28年10月
内閣官房内閣サイバーセキュリティセンター [«О мире и стабильности международного сообщества и безопасности Японии»: текущий статус продвижения стратегий кибербезопасности]. URL: https://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou09.pdf (дата обращения: 24.11.2021).

Japan's Approaches to International Cooperation in the Field of Cybersecurity: the Case of ASEAN

Lusine A. Melkonyan

Teaching assistant of the Department of Theory and History of International Relations, RUDN University (address: 117198, Moscow, Miklukho-Maklaya str., 6). ORCID: 0000–0003–0294–8076. E-mail: melkonyan-la@rudn.ru.

Received 09.02.2022.

Abstract:

The article studies the main approaches of the Japanese state to solving problems in the field of cybersecurity through developing appropriate strategies and programs, deepening international cooperation to counter the threats of cybercrime and information security. The evolution of national strategies and international agreements in the field of cybersecurity and the dynamics of the development of key approaches to information security policy are considered.

Regarding the growth of the malicious use of cyberspace by international terrorists and cybercriminals for destructive purposes, the problem of combining international efforts in the fight against cyber-attacks on critical information infrastructure is of relevance. Japan has been subjected to cyber-attacks at the state level in the past but over the past decade, threats to government institutions have become more widespread and alarming. In pursuance of personal data and intellectual property protection, the Japanese state is strengthening its defense potential by expanding the capabilities of government agencies and the Self-Defense Forces.

Japan's international cooperation in the field of cybersecurity is considered on the example of ASEAN, including its cooperation within the framework of the RCEP agreement, considering not only the geographical proximity with the association countries and the close economic ties with them, but also the effective interaction and extensive contacts in the field of cybersecurity as a member country of the CPTPP at the highest levels.

The author compares the RCEP and the CPTPP key approaches to the issues of cyber security and information sovereignty, identifying the main contradictions between the participants in these multilateral initiatives that unite the key players in the Asia-Pacific region, one of which is Japan.

Key words:

Japan; cybersecurity; Japan's new cybersecurity strategy; international relations; ASEAN; RCEP, CPTPP.

For citation:

Melkonyan L.A. Japan's Approaches to International Cooperation in the field of Cybersecurity: the Case of ASEAN // Far Eastern Studies. 2022. No. 2. Pp. 49–62.
DOI: 10.31857/S013128120019300-1

Funding sources:

This article was prepared with the support of RFBR-EISI within research project No. 21–011–31812 opn "Simulation of the spread of social norms and values: global communications VS information sovereignty of the Russian Federation".

References

Degterev D.A., Ramich M.S., Piskunov D.A. Podhody SSHA i KNR k global'nomu upravleniyu kiberprostranstvom: «novaya bipolyarnost'» v «setevom obshchestve» [Approaches of the United States and China to the global management of cyberspace: "new bipolarity" in the "network society"]. *Vestnik mezhdunarodnyh organizacij*. 2021. Vol. 16. No. 3. DOI: 10.17323/1996–7845–2021–03–01. (In Russ.)

Rogozhina N.G. Masochnaya diplomatiya Kitaya v stranah YUgo-Vostochnoj Azii [The Mask Diplomacy of China in Southeast Asia]. *Yugo-Vostochnaya Aziya: aktual`nyye problemy razvitiya*. 2021. T. I. No. 1 (50). DOI: 10.31696/2072–8271–2021–1–1–50–073–081. (In Russ.)

ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN // *Singapore Government Agency Website*. October 11, 2016. URL: https://www.csa.gov.sg/en/News/Press-Releases/ASEAN-Member-States-Call-for-Tighter-Cybersecurity-Coordination-in-ASEAN (accessed: 23.11.2021).

Commitment to a Free, Fair and Secure Cyberspace. *National center of Incident readiness and Strategy for Cybersecurity*. September 2021. URL: https://www.nisc.go.jp/eng/index.html#sec1 (accessed: 20.11.2021).

Cybersecurity Strategy. *The Government of Japan*. June 16, 2014.
URL: https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf (accessed: 17.11.2021).

Cybersecurity Strategy — Toward a world-leading, resilient and vigorous cyberspace. *National Information Security Center*. June 10, 2013.
URL: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf (accessed: 19.11.2021).

Drake W. J., Cheon K. Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG). *United Nations ICT Task Force. Paperback*. March 11, 2008.
URL: https://ifap.ru/library/book271.pdf (accessed: 19.11.2021).

Japan's New Cybersecurity Strategy. *National center of Incident readiness and Strategy for Cybersecurity (NISC)*. September 28, 2021. URL: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf (accessed: 18.11.2021).

Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation. *ASEAN Secretariat*. Tokyo, September 13, 2013. URL: https://asean.org/joint-ministerial-statement-of-the-asean-japan-ministerial-policy-meeting-on-cybersecurity-cooperation/ (accessed: 18.11.2021).

Outcomes of the 13th ASEAN-Japan Cybersecurity Policy Meeting. *METI Ministry of Economy, Trade and Industry*. November 06, 2021. URL: https://www.meti.go.jp/english/press/2020/1106_003.html (accessed: 23.11.2021).

Outcomes of the 14th ASEAN-Japan Cybersecurity Policy Meeting. *METI Ministry of Economy, Trade and Industry*. October 22, 2021. URL: https://www.meti.go.jp/english/press/2021/1022_001.html (accessed: 23.11.2021).

Sukumar A. Resolved: Japan Could Lead Global Efforts on Data Governance. *Debating Japan.* Vol. 2 Issue 6. Center for Strategic and International Studies (CSIS). June 27, 2019.
URL: https://www.csis.org/analysis/resolved-japan-could-lead-global-efforts-data-governance (accessed: 19.11.2021).

The First National Strategy on Information Security. *Information Security Policy Council, Japan*. February 02, 2006. URL: https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf (accessed: 20.11.2021).

The Japan-ASEAN Summit Meeting. *Ministry of Foreign Affairs of Japan*. September 07, 2016.
URL: https://www.mofa.go.jp/a_o/rp/page3e_000590.html (accessed: 24.11.2021).

The Second National Strategy on Information Security. *National Information Security Policy Council*. February 03, 2009. URL: https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf (accessed: 19.11.2021).

Vosse W. M. Japan's Cyber Diplomacy. International Christian University (ICU), Tokyo. October 2019.
URL: https://eucyberdirect.eu/research/japans-cyber-diplomacy (accessed: 17.11.2021).

国際社会の平和・安定及び我が国の安全保障に係るサイバーセキュリティ戦略の推進状況. 第10回 サイバーセキュリティ戦略本部 資料 平成28年10月
内閣官房内閣サイバーセキュリティセンター ["On peace and stability of the international community and the security of Japan": current status of cyber security strategies promotion"].
URL: https://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou09.pdf (accessed: 24.11.2021). (In Jap.)