Моренчук А.А. – аспірант факультету міжнародних відносин Волинського національного університету ім. Лесі Українки
Моренчук А. А. – кандидат історичних наук, доцент кафедри міжнародних відносин і регіональних студій Волинського національного університету ім. Лесі Українки

Сфера кіберпезпеки у сучасній Японії

Роботу виконано на кафедрі міжнародних відносин і регіональних студій ВНУ ім. Лесі Українки
*Науковий керівник – **Моренчук А. А.** – кандидат історичних наук, доцент кафедри міжнародних відносин і регіональних студій ВНУ ім. Лесі Українки*

Розглянуто основні нормативно-правові акти, що регулюють сферу кіберпезпеки в сучасній Японії. Визначено ключові державні органи на які покладено функцію її забезпечення. Виділено основні етапи розвитку системи кіберпезпеки Японії. Визначено стан та основні загрози кіберпезпеки Японії.
Ключові слова: національна безпека, кіберпезпека, кібератака, стратегія, кібердипломатія.

Morenchuk A.A., Morenchuk A.A. Development of cybersecurity in modern Japan

The main legal acts regulating the field of cybersecurity in modern Japan are considered. The key state bodies responsible for its provision have been identified. The main stages of development of the cybersecurity system of Japan are highlighted. The state and main threats to cybersecurity in Japan have been identified.
Key words: national security, cybersecurity, cyber attack, strategy, cyberdiplomacy.

Не дивлячись на те, що Японія є одним із лідерів в сфері інформаційно-комунікаційних технологій (information and communications technology – ICT) кібербезпеці в країні увага приділялась тривалий час недостатньо. Певним каталізатором стала перспектива проведення Олімпійських ігор в 2020 р. І адміністрація прем'єр-міністра Сіндзо Абе прийняла рішення суттєво переглянути основи політики національної безпеки країни.

При цьому, починаючи з 2000-х років Японія піддається зростаючому числу кібератак на критичну інформаційну інфраструктуру, включаючи урядові мережі. Експерти відмічають, що Японія (поряд з Австралією, Новою Зеландією, Сінгапуром та Південною Кореєю) в дев'ять разів вразливіша до кібератак, ніж інші азіатські економіки [3]. Потужних кібератак Японія зазнала в 2011 році Жертвами, серед інших, стали IHI Corporation та Kawasaki Heavy Industries, що виконували

державні військові замовлення. В результаті були викрадені надсучасні військові технології. Ще однією резонансною подією став успішний взлам Пенсійної служби Японії в травні 2015 року. В результаті хакерської атаки було викрадено особисті дані понад 1,25 мільйона осіб. Звичним явищем стають складні атаки на японські мережі, що характеризуються як передові стійкі загрози (advanced persistent threat – APT).

Зростає не лише якість, але й кількість кібератак. Так, у 2005 році було зафіксовано 310 мільйонів подібних спроб. А вже в 2014 році, за даними Національного інституту інформаційних та комунікаційних технологій (National Institute of Information and Communications Technology – NICT), Японія зазнала понад 25 мільярдів кібератак. 40 відсотків з них здійснювались з Китайської Народної Республіки, за ним йшли Республіка Корея, Російська Федерація та США [5].

В Білій книзі національної безпеки Японії також відмічається, що в кібератаках беруть участь урядові організації Китаю, Росії та Північної Кореї [1; 2].

У квітні 2005 року було створено Національний центр інформаційної безпеки (National Information Security Center – NISC). На нього покладалося завдання координувати впровадження першої стратегії інформаційної безпеки в країні та посилювати заходи безпеки. В травні 2005 року було створено Раду з питань політики інформаційної безпеки (Information Security Policy Council – ISPC). У лютому 2006 року вона запропонувала "Першу національну стратегію з питань інформаційної безпеки". Стратегія ставила за мету сформулювати "систематичний план інформаційної безпеки на основі стратегічного бачення цього питання" на наступні три роки.

NISC мала забезпечувати необхідною інформацією державні структури; налагодити партнерські стосунки з приватним сектором для обміну передовим досвідом; налагодити міжнародну взаємодію в сфері інформаційної безпеки з країнами-партнерами. При цьому кібербезпека трактувалася, насамперед, як технічне питання. Головний акцент у документі робився на підкресленні впливу IT на японське суспільство та на майбутній економічний розвиток країни. Кібербезпека не розглядалася пріоритетним політичним питанням.

Як результат, координація та реалізація спільних політик інформаційної безпеки та реагування на кіберзагрози була розділена між чотирма ключовими відомствами – Національним агентством поліції (NPA), Міністерством внутрішніх справ та зв’язку (MIAC), Міністерством Економіки, торгівля та промисловість

(METI) та Міністерством оборони Японії (JMOD). Причому кожне міністерство, по суті, переслідувало власну незалежну стратегію боротьби із кіберзагрозами [16].

"Друга національна стратегія з інформаційної безпеки" 2009 року, побудована на попередньому документі, зосереджувалась на чотирьох темах – центральних та місцевих органах влади, критичній інфраструктурі, суб'єктах господарювання та приватних особах – в першу чергу прагнучи запобігти значному впливові IT-збоїв на повсякденне життя та соціально-економічну діяльність. Також робилось акцентування на цифровій економіці. При цьому дуже мало уваги, знову ж таки, приділялось наслідкам кіберзагроз для національної безпеки. Тим не менше, нова стратегія містила більш окреслений підхід до формування міжнародних партнерських відносин з інформаційної безпеки, і, орієнтуючись на кіберзлочинність і тероризм, вперше також обговорювалась загроза АТС через низку гучних кібератак у цілому світі [17].

Трирічний стратегічний план на 2009 рік посилював роль NISC. На нього у документі покладалось завдання збирати "найкращі розвідувальні дані як в країні, так і за кордоном" з питань інформаційної безпеки. Національний центр інформаційної безпеки зберігав свою роль загального координатора урядової кіберполітики.

У 2009 році японська виконавча влада також офіційно розділила свою структуру кібербезпеки на три основні наглядові органи: Центр управління кризовими ситуаціями (крім кіберзагроз орган також реагує на інші надзвичайні ситуації), Управління з питань розвідки кабінету міністрів та NISC.

У 2009 році Японія знову потрапила під низку масштабних кібератак спрямованих проти уряду, засобів масової інформації та фінансових веб-сайтів. У відповідь на це, в травні 2010 року ISPC опублікувала нову чотирирічну стратегію, направлену на забезпечення "національної безпеку та ефективного врегулювання криз". Стратегія передбачала реалізацію плану "Захищена Японія 2009". Даний план щорічно переглядається з врахуванням нових можливостей посилення кіберзахисту Японії та перетворення її в найбільш "просунуту країну інформаційної безпеки" у світі. Харакетрно, що кібератаки у документі розглядаються не як результат конкретних дій державних та недержавних зловмисних структур, а як аналог непередбачуваних стихійних лих [14].

Однак у новій стратегії можна знайти незначні зрушення у зміні політики. Вперше Японія виступала за розробку більш активних та міждержавних скоординованих заходів з реагування на широкомасштабні кібератаки. Він також

закликав до "розбудови міжнародних союзів". Щоб сприяти більш міжнародному співробітництву, Японія внесла зміни до законів про кіберзлочинність, які дозволили їй приєднатися до Будапештської конвенції про кіберзлочинність. Договір набув чинності в листопаді 2012 року. Однак документ не зміг порушити "силосний підхід" японських урядових структур при боротьбі з кібератаками та не наділив NISC новими повноваженнями.

Поступові зміни відбулися після хвилі чотирьох основних кібератак між липнем і листопадом 2011 року, спрямованих на японський парламент, ряд японських посольств за кордоном та японського оборонного підрядника Mitsubishi Heavy Industries. Ці кібератаки проявили відсутність повноважень NISC координувати узгоджену відповідь державних структур на кіберинциденти. Як результат, у новому документі IPSC від липня 2012 року під назвою "Інформаційна безпека 2012" висвітлено необхідність налагодження більш тісної співпраці приватного та державного секторів та посилення можливостей реагування у державних органах. Він також наголосив на центральній ролі Секретаріату Кабінету Міністрів та NISC як головного урядового координатора відповідей на атаки з кіберпростору. Крім того, у документі пропонується добровільне навчання для державних міністерств та відомств. Також Японія закликала зробити свій внесок у розробку "міжнародних норм поведінки в кіберпросторі" [15].

У червні 2013 року ISPC випустив свою першу "Стратегію кібербезпеки", використовуючи саме слово "кібер", а не "інформація", як це було в попередніх стратегічних документах. Це ілюструвало більш широкий і всеохоплюючий підхід до вирішення загроз у кіберпросторі. Нова урядова політика, викладена в документі, полягала у створенні стійкої "нації з питань кібербезпеки", оскільки кібератаки стали питаннями "національної безпеки" та "врегулювання криз". Це свідчило про важливий зрушення у сприйнятті кіберзагроз. Таким чином, уперше у великому розділі висвітлено роль Міністерства оборони в захисті кіберпростору – особливо, коли мова йде про "кібератаки на національному рівні, в яких підозрюється участь іноземних урядів". У стратегії – на яку, ймовірно, повпливали американські підходи, – кіберпростір трактується як нове поле ведення війни. Документ закликав до систематичного посилення можливостей кіберзахисту Сил самооборони Японії (JSDF), частково шляхом створення нового підрозділу кіберзахисту. У документі також обговорювалася необхідність чіткого розмежування відповідальності між JMOD та цивільними міністерствами, коли мова заходила про захист критичної інфраструктури та інших, пов'язаних з

обороною систем. Таким чином простежується перехід до мілітаризації японської кіберзахисту. Стратегія також закликала до зміцнення приватно-державного партнерства, створення "системи обміну інформацією, що базується на угоді про конфіденційність", та посилення Координаційної групи урядових операційних служб безпеки, Групи реагування на випадки загроз комп'ютерної безпеки та Координаційного центру з питань комп’ютерного реагування на надзвичайні ситуації [11].

Нова кіберстратегія запропонувала найбільш вичерпні на сьогодні підходи Японії до кібердипломатії. Поряд з підкресленням необхідності міжнародних союзів та постійного діалогу з країнами-однодумцями, документ детально розробив зусилля Японії щодо формування міжнародних норм поведінки в кіберпросторі. Він також підкреслив важливість американо-японського союзу у формулюванні цих норм та висловив підтримку Токіо багатостороннім підходам до управління Інтернетом.

У грудні 2013 року було прийнято Закон про захист спеціально призначеної таємниці, який визначає державною таємницею певну сс-інформацію (Social Security Information), зокрема технології ІКТ, що стосуються національної оборони. А в листопаді 2014 року – Основний закону про кібербезпеку, що зобов'язує уряд встановити єдині стандарти кібербезпеки. Відповідно з цими документами державні органи контролюють систему урядової інформаційної мережі, виявляють та аналізують несанкціоновані вторгнення та кібератаки. Також у 2014 р. була опублікована друга ітерація японської "Стратегії кібербезпеки", що окреслювала підхід країни до кібербезпеки на найближчі три роки.

Хоча новий документ висвітлював економічний потенціал інформаційних технологій, головним чином він наголошував на важливості більш всеохоплюючої національної стратегії кібербезпеки напередодні підготовки до Олімпійських і Паралімпійських ігор у Токіо 2020 року. У документі чітко видно, що кібербезпека була визначена однією з основних проблем національної безпеки Японії. Відображаючи принцип "активного сприяння миру", пропагований адміністрацією Сіндзо Абе, документ зазначав, що для забезпечення "вільного, справедливого та безпечного кіберпростору" Японія повинна проводити більш активну політику в кіберпросторі. У документі також висвітлено дедалі більшу роль, яку JMOD відіграє в захисті Японії від широкомасштабних та складних кібератак, а також важливість співпраці між JSDF та американськими військовими згідно з новими Керівними принципами японсько-американського оборонного співробітництва [12].

Стратегію кібербезпеки 2015 року від попередньої відрізняли юридичні та структурні зміни в ландшафті кібербезпеки Японії, що відбулися в 2014 році. Відповідно до Основного закону про кібербезпеку, IPSC був перетворений на Штаб-квартиру Стратегії кібербезпеки (Cyber Security Strategy Headquarters – CSSH), а нещодавно призначений Національний центр готовності до інцидентів та стратегії кібербезпеки (NISC) виконував обов'язки секретаріату. Ролі CSSH та NISC були офіційно оформлені. Їм було надано всебічні повноваження щодо координації та реалізації національної стратегії кібербезпеки. Згідно з новим законом, CSSH є "командно-контрольним органом національної кібербезпеки", наділеним сильним авторитетом. наприклад, надання рекомендацій національним адміністративним органам. Основним завданням NISC є "сприяння політиці кібербезпеки", викладеній у Стратегії кібербезпеки 2015 року, і це завдання підтримується Координаційною групою з питань урядової безпеки. CSSH співпрацює з Радою національної безпеки (NSC), створеною в 2013 році, але вони не мають механізму спільних нарад та інших регулярних офіційних засідань для скликання. NSC займається питаннями кібербезпеки лише в тому випадку, якщо це буде визнано надзвичайною ситуацією. CSSH зберігає функцію встановлення напрямів щодо політики кібербезпеки Японії за звичайних умов, а також відповідає за підготовку щорічного звіту з переглядом прогресу у реалізації політики.

У стратегічному документі на 2015 рік докладно викладено нові обов'язки NISC: мережева пильність та моніторинг шкідливої діяльності щодо інформаційних систем адміністративних органів; встановлення фактів про причини інцидентів та аудит відповідних державних органів; інформація збір та аналіз вітчизняної та зарубіжної кібербезпеки; сприяння міжнародному співробітництву та розвиток людських ресурсів з питань кібербезпеки для державних органів та за їх допомогою. Крім того, NISC тепер також має повноваження контролювати бюджети кібербезпеки в рамках державних установ. Після прийняття Основного закону про кібербезпеку NISC може розслідувати кібератаки на пов'язані з урядом адміністративні організації, такі як Японська пенсійна служба. Враховуючи обсяг нових обов'язків NISC, поправка до Основного закону про кібербезпеку від квітня 2016 року дозволила делегувати частину своєї діяльності Агентству сприяння інформаційним технологіям, яке консультує приватний сектор Японії з питань кібербезпеки та управляє інформацією про кібербезпеку. Спільне партнерство, сприяння обміну інформацією між урядом та приватним сектором [13].

Загалом, Японія досі є другою державою в галузі інформаційно-комунікаційних технологій після США. Проте, незважаючи на заявлену мету уряду Японії стати до 2020 року провідною державою у галузі інформаційних технологій (information technology – IT), Японія посідає десяте місце в Індексі розвитку інформаційних та комунікаційних технологій (United Nations International Telecommunication Union – ITU) [9], перебуває на п’ятнадцятій позиції за Індексом мережевої готовності Всесвітнього економічного форуму (Network Readiness Index – NRI) [4] і на чотирнадцятому місці за глобальним індексом кібербезпеки (Global Cybersecurity Index – GCI) [6, p. 58]. В регіоні за цим показником Японія поступається Сінгапуру, Малайзії та Австралії. Для порівняння: Україна займає 54 місце у світі за глобальним індексом кібербезпеки й 32 в регіоні [6, p. 61].

За Індексом кіберготовності 2.0 (Cyber Readiness Index – CRI), розробленим Потомакським інститутом політичних досліджень на основі оцінки семи параметрів зусиль та ресурсів, пов'язаних з забезпеченням кібербезпеки держави – національна стратегія; реагування на інциденти; злочинність та правоохоронна діяльність; обмін інформацією; інвестиції у науково-дослідні та дослідно-конструкторські роботи (НДДКР), дипломатію, торгівлю; оборона та реагування на кризи, Японія представляє "недостатньо доказів" у двох категоріях, а у чотирьох позначена як "частково діюча". Жодна категорія не отримала найвищої оцінки "повністю функціонуючої" [8]. Японія не має компанії з кібербезпеки глобального рівня.

Отже, до 2013 року Японія не приділяла належної уваги створенню інституцій з питань кібербезпеки. А до реалізації системних кроків щодо налагодження ефективної системи кіберзахисту приступила з 2015 р. Протягом останніх років закладено структурні та правові основи для того, щоб стати серйозним гравцем у кіберпросторі. Зі створенням Штаб-квартири Стратегії кібербезпеки (CSSH), Національного центру інформаційної безпеки (NISC) та прийняттям Основного закону про кібербезпеку у поєднанні з новою стратегією кібербезпеки Японія створила належні рамки для збільшення загальних національних можливостей кібербезпеки. Однак чи вдасться їй стати провідною кіберсилою, значною мірою залежатиме від належного фінансування та політичної волі.

Джерела та література

1. Defense of Japan 2019 // Japan Ministry of Defense. – [Electronic resource]. – Access mode : https://www.mod.go.jp/e/publ/w_paper/wp2019/pdf/DOJ2019_Full.pdf.

2. Defense of Japan 2020 // Japan Ministry of Defense. – [Electronic resource]. – Access mode : https://www.mod.go.jp/e/publ/w_paper/wp2020/DOJ2020_EN_Full.pdf.

3. Deloitte. Asia-Pacific Defence. Outlook 2016. Defence in Four Domains. -15 p. – [Electronic resource]. – Access mode : https://www2.deloitte.com/nz/en/pages/public-sector/articles/gx-asia-pacific-defense-outlook.html.

4. Dutta S. The Network Readiness Index 2020. Accelerating Digital Transformation in a post-COVID Global Economy. – Portulans Institute, 2020. – 318 p. / Soumitra Dutta and Bruno Lanvin. – [Electronic resource]. – Access mode : https://networkreadinessindex.org/wp-content/uploads/2020/10/NRI-2020-Final-Report-October2020.pdf.

5. Gady F.-S. Japan: The Reluctant Cyberpower / Franz-Stefan Gady // IFRI. Institut francais des relations internationales. – [Electronic resource]. – Access mode : https://www.ifri.org/sites/default/files/atoms/files/gady_japan_reluctant_cyberpower_2017.pdf.

6. Global Cybersecurity Index 2018. – ITU, 2019. – 92 p. – [Electronic resource]. – Access mode : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

7. Hathaway M. Japan Cyber Readiness at a Glance. September 2016. / Melissa Hathway, Chris Demchak, Jason Kerben et al. // Cyber Readiness Index (CRI) // Potomac Institute for Policy Studies. – [Electronic resource]. – Access mode : https://www.potomacinstitute.org/academic-centers/cyber-readiness-index#inline5207.

8. Japan Cyber Readiness at a glance // Cyber Readiness Index (CRI) // Potomac Institute for Policy Studies. – [Electronic resource]. – Access mode : https://www.potomacinstitute.org/academic-centers/cyber-readiness-index#inline5207

9. Statistics // ITU. Committed to connecting the world. – [Electronic resource]. – Access mode : https://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx.

10. The Basic Act on Cybersecurity. Act No. 104 of November 12, 2014 // Japanese Law Translation. – [Electronic resource]. – Access mode : http://www.japaneselawtranslation.go.jp/law/detail/?id=3591&vm=04&re=01.

11. サイバーセキュリティ２０１３ // NISC. National center of Incident readiness and Strategy for Cybersecurity. – [Electronic resource]. – Access mode : https://www.nisc.go.jp/active/kihon/pdf/cs2013.pdf.

12. サイバーセキュリティ２０１４ // NISC. National center of Incident readiness and Strategy for Cybersecurity. – [Electronic resource]. – Access mode : https://www.nisc.go.jp/active/kihon/pdf/cs2014.pdf.

13. サイバーセキュリティ２０１５ // NISC. National center of Incident readiness and Strategy for Cybersecurity. – [Electronic resource]. – Access mode : https://www.nisc.go.jp/active/kihon/pdf/cs2015.pdf.

14. セキュア・ジャパン２００９～すべての主体に事故前提の自覚を～ // NISC. National center of Incident readiness and Strategy for Cybersecurity. – [Electronic resource]. – Access mode : https://www.nisc.go.jp/active/kihon/pdf/sjf_2009.pdf.

15. 情報セキュリティ２０１２ // NISC. National center of Incident readiness and Strategy for Cybersecurity. – [Electronic resource]. – Access mode : https://www.nisc.go.jp/active/kihon/pdf/is2012.pdf.

16. 第１次情報セキュリティ基本計画 ～「セキュア・ジャパン」の実現に向けて～ // NISC. National center of Incident readiness and Strategy for Cybersecurity. – [Electronic resource]. – Access mode : https://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf.

17. 第２次情報セキュリティ基本計画 ～IT時代の力強い「個」と「社会」の確立に向けて～ // NISC. National center of Incident readiness and Strategy for Cybersecurity. – [Electronic resource]. – Access mode : https://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf.