Андрій Моренчук,
Євгенія Вознюк
Волинський національний університет
імені Лесі Українки, Україна

КІБЕРПРОТИСТОЯННЯ ЯПОНІЇ (ДОСВІД УКРАЇНИ)

Японія позиціонувала себе однією з найрозвиненіших інформаційних країн світу і для того, щоб зберегти свою репутацію в сучасних умовах, вона повинна забезпечити гідний рівень кібербезпеки, з огляду на постійне протистояння України та значні гібридні загрози з боку Російської Федерації.

Діапазон груп, які уже постраждали від кібератак (від фізичних осіб та окремих сімей до складних підприємств соціальної інфраструктури) швидко розширюється. Незважаючи на всі зусилля японського уряду, ризик інформаційних атак збільшується із-за постійної та значної підтримки Києва у російсько-українській війні. Він впливає на такі сфери, як національна безпека, управління ризиками та конкурентоспроможність їхньої економіки.

Японська промисловість відстає від своїх американських та європейських аналогів щодо оцінки кіберзагроз, а також за словами прем'єр-міністра Японії Фуміо Кішіди, на сьогоднішній день вона значно позаду і від українських кібервоїнів, що на практиці показують прогресивність та гнучкість до вимог протистояння.

РФ все ще намагається якимось чином впливати на геополітику, використовуючи засоби гібридної війни, а особливо кібертероризму. Кібертероризм – використання комп'ютерних і телекомунікаційних технологій (особливо Інтернету) для терористичних цілей.

Законодавство України визначає «Кібертероризм – це терористична діяльність, що здійснюється в кіберпросторі або з її використанням». Це вбивча атака, спрямована на залякування для досягнення політичних результатів або пошкодження комп'ютерних мереж, особливо персональних комп'ютерів, підключених до Інтернету, з використанням таких засобів, як комп'ютерні віруси [3, 169].

Проте всі експерти впевненні в одному: інформаційний тероризм – це передусім негативний вплив на людину, суспільство і стан всіх наявних видів.

До кібертероризму відносять також деструктивні дії щодо інформаційних систем, які створюють умови для проведення актів тероризму (хакерських / кібератак). Згідно з державною статистикою лише 55% японських компаній проводять оцінки ризиків кібербезпеки, порівняно з приблизно 80% в США і 65% у Європі.

10 червня 2013 року Рада з політики інформаційної безпеки Японії прийняла Стратегію кібербезпеки. Японський уряд раніше використовував формулювання «інформаційна безпека» для своєї 54 політики і основоположних планів.

Однак у зв'язку зі зростаючим числом кіберзагроз, які виходять за рамки інформаційної безпеки, таких, наприклад, як диверсія щодо об'єктів

життєзабезпечення населення, в Токіо було прийнято рішення використовувати термін «кібербезпека» для того, щоб вперше розглянути всі ці проблеми.

Стратегія спрямована на розвиток «провідного в світі», «сталого» і «динамічного» кіберпростору і перетворення Японії у світового лідера в області кібербезпеки.

Для реалізації цих цілей в документі передбачені чотири основні принципи: забезпечення вільного обміну інформацією; забезпечення нових заходів у відповідь на те, що ризики стають більш серйозними; прийняття адекватних заходів щодо кіберзагроз на підставі оцінки ризиків; вжиття заходів і взаємодія з іншими державами на підставі їх власної соціальної відповідальності.

Державним органом, що регулює взаємовідносини в галузі кібербезпеки є Національний центр інформаційної безпеки (NISC), який розробляє проекти урядових стандартів щодо заходів з інформаційної безпеки, формулює рекомендації на основі результатів оцінки стану кібербезпеки та сприяє впровадженню заходів щодо покращення стану кібербезпеки [1].

У кінці 2021 року компанія Microsoft опублікувала загальний звіт щодо хакерських атак протягом 2020-2021 років, згідно усіх даних роботи їхніх систем безпеки, де прослідковується тенденція швидкого зростання кількості кібератак, які здійснює Росія (58% від загальної кількості). З діаграми (рис. 1) видно, що переважна більшість кібератак (за досліджуваний період) була спрямована проти США, України, Великобританії, хоча не оминули увагою і Бельгію, Японію, Німеччину та інші країни.

Рис. 1 Кібератаки РФ (2020-2021). Складено автором за: [4].

Microsoft також виділила перелік найактивніших та «ефективних» хакерських груп і серед них лідирує російська група Nobelium, яка, зокрема, й здійснювала атаки на галузі державного управління, дипломатичні установи, оборонні об’єкти.

У другій половині 2021 року стало відомо, що у 129 японських урядових установах та компаніях відбувся витік усіх даних після того, як невідомі хакери отримали повноцінний доступ до програми обміну інформацією компанії Fujitsu. Вона оновила дані щодо несанкціонованого доступу до її програми ProjectWEB, яка досить широко використовувалася багатьма урядовими установами.

Кібератаки РФ (2020-2021) Сполучені Штати Америки Україна Велика Британія Бельгія Японія Німеччина інші країни світу, частка не переважає 1% 55 установами та бізнесом, а саме секретаріатом Кабінету міністрів, Міністерством закордонних справ і Міністерством національних земель, інфраструктури, транспорту та туризму [5].

З цього випливала нагальність прийняття нової стратегії кібербезпеки Японії, як і свого часу в Україні. Над її розробкою та удосконаленням працювали тривалий період і в проекті вперше наголосили на важливості погроз з боку Російської Федерації, Китаю та Північної Кореї. Визначено, що

за останній час Москва досить активно використовує усі хакерські атаки у своїх військових та політичних цілях.

Японія задля зміцнення кібербезпеки держави готова проводити активні та регулярні навчання зі спеціалістами з Сполучених Штатів Америки, створювати новітні стандарти безпеки для ІТ-обладнання та значно нарощувати японський потенціал широкого захисту від хакерів, вести тісну співпрацю з учасниками діалогу з безпеки, в який входять Австралія, Індія та США та членами Асоціації держав Південно-Східної Азії, для того, щоб зміцнити свій кібернетичний потенціал [6].

Нова стратегія кібербезпеки схвалена 27 вересня 2021 року на засіданні штабу кібернетичної безпеки Японії терміном на три роки та оприлюднена того ж дня на сайті японського відомства. Токіо вперше прописав конкретну країну як реальну загрозу в стратегії кібербезпеки, беручи до уваги негативний досвід України. Запропонований проект стратегії кібербезпеки Японії передбачає значне посилення обороноздатності країни в кіберпросторі, боротьбу з хакерами, зокрема за допомогою кримінального переслідування або дипломатичних каналів.

У подальшому для захисту у сфері кібербезпеки держава планує використовувати повністю штучний інтелект, сприяти поглибленню дослідженням та розробкам для вирішення питань дешифрування на основі квантових обчислень [2].

За прикладом України, а саме створення великої кількості громадських організацій, що стоять на захисті інформаційного та кіберпростору, а також задля регулювання галузей у Японії ініціювали недержавні, неприбуткові організації за підтримки комерційних компаній: Форум мобільного контенту (MCF); Асоціація оцінки та моніторингу вмісту; Японська асоціація сприяння безпеці в Інтернеті (JISPA); Японська асоціація соціальних ігор (JASGA) та інші подібні організації. Найчастіше вони відповідають за визначення неприйнятність контенту та блокування забороненого контенту, наприклад, такого як дитяча порнографія.

У технічному плані основні організаційні особливості системи інформаційної безпеки Японії: це високий рівень інформаційних загроз; широкий і об’ємний ринок; загальний аутсорсинг інформаційної безпеки; сервісний підхід; висока вартість репутаційних ризиків; низька участь державних регуляторних структур в управлінні Інтернетом; велика частка внутрішнього трафіку, його переважна величина над зовнішнім; висока залученість кримінальних структур до інформаційної безпеки країни.

На сьогоднішній день Японія, як і Україна, посідає високі місця за кількістю кібератак і на даний момент знаходиться на 11 місці в списку країн світу серед джерел кібератак і 16 серед одержувачів кібератак. Загальною характерною рисою інтернет-індустрії в Токіо є добровільне саморегулювання учасників.

На відміну від нашої держави, у Японії досі не існує незалежної комісії чи державного органу, безпосередньо відповідального за регулювання Інтернету.

Отже, Японія у сучасних реаліях по своєму протистоїть впливу Росії, яка намагається змінити систему міжнародних відносин. Відчуваючи вплив також і в інформаційній сфері, відбиваючи зростаючу кількість кібератак та намагаючись не лише допомогти Україні, а й 56 забрати свої території Курильських островів, Японія набирає політичного іміджу Великобританії тільки на Сході.

Література:

1. Аналіз стану кібербезпеки в провідних країнах світу URL: https://cutt.ly/fJLvpVg

2. В Японії схвалили стратегію кібербезпеки, в якій згадані РФ і КНР URL: https://cutt.ly/wJLvxXr

3. Глосарій: навч. енцикл. слов.-довід. із питань інформ. безпеки / за заг. ред. д-ра політ. наук, проф. А. М. Шуляк. – Київ : МПБП «Гордон», 2019. 580 с.

4. Країни-жертви та країни-агресори у хакерських війнах URL: https://cutt.ly/gJLvUSL

5. У Японії понад 100 урядових установ і компаній зазнали атаки хакерів – стався витік даних URL: https://cutt.ly/dJLvHxJ

6. Японія вперше згадала про погрози з боку Росії в проекті Стратегії Кібербезпеки URL: http://opk.com.ua.