УДК 338.242(477)

КІБЕРСТІЙКІСТЬ ЯК ОСНОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Онищенко Світлана Володимирівна,
д.е.н., професор
Глушко Аліна Дмитрівна,
Маслій Олександра Анатоліївна,
к.е.н., доценти
Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна

Анотація. В умовах кібервійни, розгорнутою російською федерацією поряд з військовою агресією, питання захисту інформаційного простору, в тому числі кіберпростору, від деструктивних дій, які створюють реальну загрозу національній безпеці є безперечно актуальним. У ході проведення дослідження здійснено ідентифікацію ризиків кібербезпеці України та проведено оцінюванню рівня кіберстійкості на основі даних міжнародних рейтингів. Визначено перспективні напрями посилення кіберстійкості національної інформаційної інфраструктури.

Ключові слова: кіберстійкість, національна безпека, кібербезпека, кібервійна, інформаційна інфраструктура.

З початку 2022 року російська федерація розгорнула повномасштабну кібервійну проти України. Це підтверджується зростанням кібератак на державні структури та об’єкти критичної інфраструктури, порушення функціонування яких є загрозою національним інтересам. Кібервійна стала реальною загрозою національній безпеці і передумовою порушення державного суверенітету та територіальної цілісності України країною-агресором 24 лютого 2022 року.

Згідно з офіційними даними Служби безпеки України у січні 2022 року було ідентифіковано 6,8 млн підозрілих подій інформаційної безпеки, 25,5 тис. потенційних кіберінцидентів та зупинено 121 кібератаку. В цілому, за січень-

лютий 2022 року було здійснено 436 кібератак на ресурси органів державної влади та військового управління України, а також ІТ-систем об'єктів критичної інфраструктури, ресурси операторів зв'язку та ЗМІ. Для порівняння за аналогічний період 2021 року було здійснено 64 кібератаки [1]. Враховуючи вищезазначене правомірно стверджувати, що кібербезпека є складовою національної безпеки країни, а кіберстійкість – основою її гарантування.

На сьогоднішній день відсутній єдиний підхід до трактування поняття «кіберстійкість». Згідно з Порядком проведення огляду стану кіберзахисту критичної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом кіберстійкість критичної інформаційної інфраструктури – це стан критичної інформаційної інфраструктури, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз [2]. Отже, кіберстійкість країни доцільно визначити як спроможність національної системи протидіяти кіберзагрозам, зокрема кібертероризму, кібердиверсіям, кібератакам стосовно національної інформаційної інфраструктури.

Для оцінювання рівня кіберстійкості країни розроблено ряд глобальних індексів: Національний індекс кіберезпеки (National Cyber Security Index), Глобальний індекс кібербезпеки (Global Cybersecurity Index) та Національний індекс кіберпотужності (NCPI).

NCSI – це глобальний індекс кібербезпеки, який розроблений Фондом академії електронного врядування Естонії та вимірює здатність країн запобігати кіберзагрозам і управляти кіберінцидентами. В його основі закладено розрахунок 12 індикаторів, які засвідчують досягнення країни за такими напрямами: розробленість політики з кібербезпеки, моніторинг та аналіз кіберзагроз, освіта та підвищення кваліфікації у сфері кіберзахисту, внесок у глобальну кібербезпеку, захист цифрових сервісів, захист основних послуг у кіберпросторі, послуги електронної ідентифікації, захист персональних даних, реагування на кіберінциденти, кіберкризове управління, боротьба з кіберзлочинністю та військові кібероперації. У 2021 році у рейтингу NCSI

Україна посіла 24 місце серед 160 країн та поліпшила свою позицію на 1 пункт у порівнянні з 2020 роком [3]. За рівнем кіберстійкості національного інформаційного простору Україна наблизилася до Швейцарії (23 місце) та Великобританії (22 місце). Детальний аналіз кіберстійкості України в розрізі зазначених індикаторів представлено на рисунку 1.

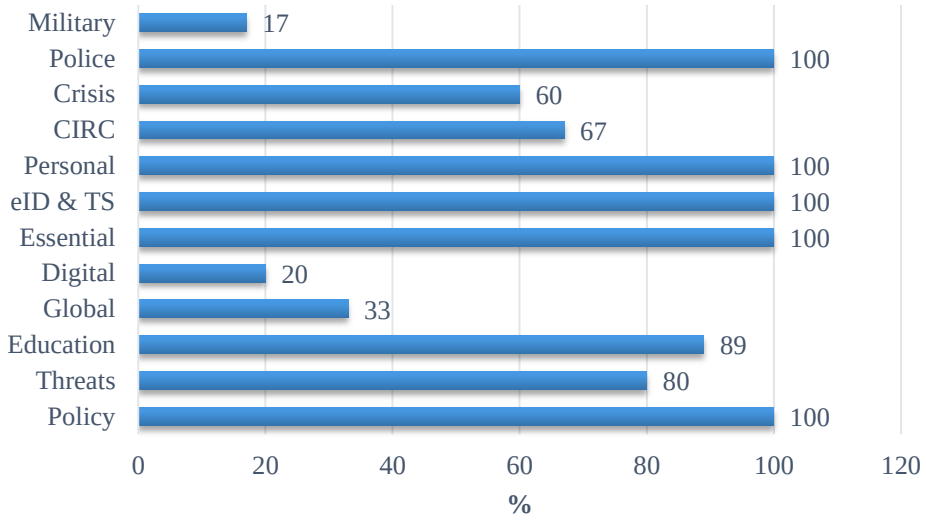

Рис. 1. Відсоток виконання індексу NCSI Україною у 2021 році в розрізі індикаторів

*Побудовано авторами за [3]

Рейтинг GCI розроблений Міжнародним союзом електрозв'язку (МСЕ) та спрямований на підвищення обізнаності щодо кібербезпеки та вимірювання прихильності країн до кібербезпеки та її широкого застосування в різних галузях і секторах. Рівень розвитку кожної країни аналізується за п'ятьма напрямами: правові заходи (рівень розробленості законодавчої бази у сфері кібербезпеки), технічні заходи (рівень реалізації технічних можливостей кіберзахисту через національні та галузеві агенції), організаційні заходи (національні стратегії кібербезпеки), розбудова потенціалу (інформаційне забезпечення, освіта та наявні стимули для розвитку потенціалу кібербезпеки) та співробітництво (рівень розвитку партнерства у сфері кібербезпеки). У 2021 році Україна посіла 78 місце – втратила 24 позиції у порівнянні з попереднім

роком [4]. Аналіз позицій України в розрізі зазначених напрямів представлено на рисунку 2.

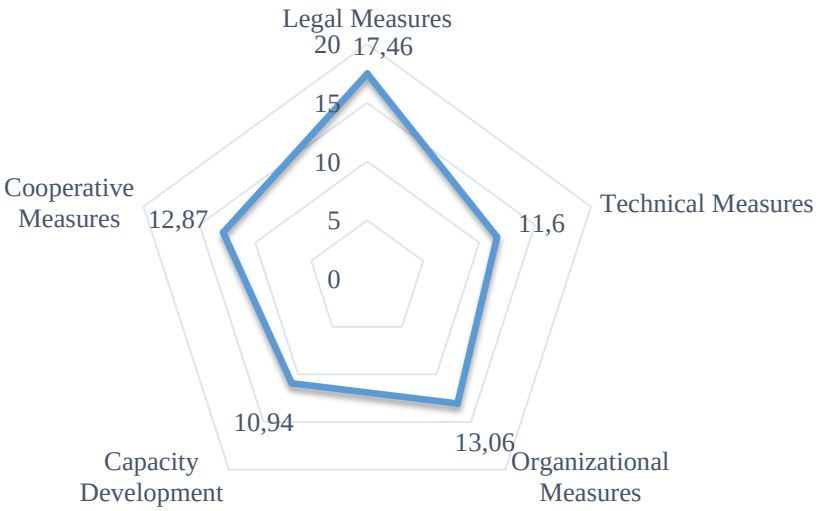

Рис. 2. Позиції України за напрямами забезпечення кібербезпеки в рейтингу GCI у 2021 році

*Побудовано авторами за [4]

NCPI впроваджено Центром науки та міжнародних відносин Роберта та Рене Бельфера. Індекс дозволяє виміряти рівень кіберпотужності країни, тобто регуляторної спроможності досягнення стратегічних цілей кібербезпеки, а саме: впровадження практик з моніторингу на загальнодержавному рівні за участю внутрішніх груп контролю, національна стратегія кібербезпеки, ефективність управління інформаційним середовищем, діяльність зовнішньої розвідки з питань національної кібербезпеки, випуск спеціалізованої продукції вітчизняного виробництва, здатність до знищення або вимкнення інформаційно-комунікаційної інфраструктури та можливостей супротивника, використання міжнародних спеціалізованих норм та технічних стандартів. У 2020 році Україна посіла 26 місце із включених до рейтингу 30 країн світу [5].

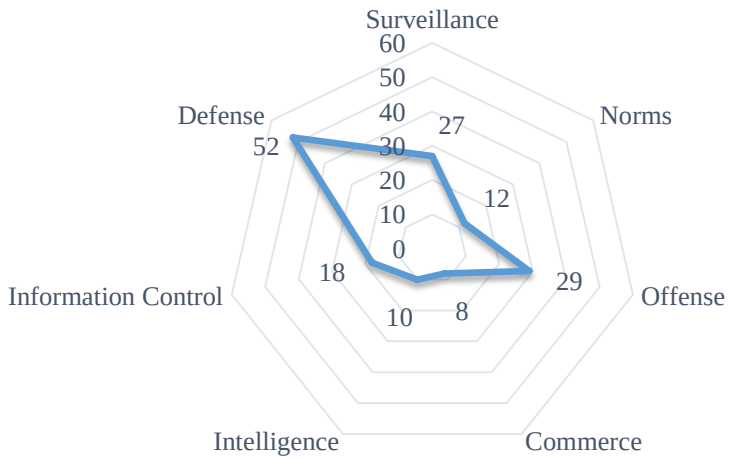

Рис. 3. Позиції України за рівнем досягнення стратегічних цілей кібербезпеки за рейтингом NCPI у 2020 році

*Побудовано авторами за [5]

Таким чином, основними напрямами, які негативно впливають на рівень кіберстійкості України, правомірно визначити низький рівень захисту цифрових послуг, недостатній рівень внеску у глобальну кібербезпеку та нерозвинений напрям військових кібероперацій. Водночас, враховуючи, що у 2022 році Україна прийнята до складу Об'єднаного центру передових технологій з кібероборони НАТО як учасник-контрибутор, відмічаючи активний процес формування кібервійська доцільно відмітити значний потенціал країни у сфері кібербезпеки та можливості його реалізації в майбутньому.

Список літератури

1. Служба безпеки України. Захист інформаційного та кіберпростору. Звіт SIEM. URL : http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (дата звернення 23.05.2022).

2. Порядок проведення огляду стану кіберзахисту критичної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, затверджений постановою Кабінету Міністрів України від 11 листопада 2020 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

3. Офіційний сайт NCSI Project Team. URL: https://ncsi.ega.ee/country/ua/ (дата звернення 12.06.2022).

4. Офіційний сайт International Telecommunication Union. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (дата звернення 12.06.2022).

5. Новий глобальний індекс кібербезпеки – Національний індекс кіберпотужності. URL : https://www.icu-ng.org/icu-ng/novyny/novyj-globalnyj-indeks-kiberbezpeky-naczionalnyj-indeks-kiberpotuzhnosti/#_ftn1 (дата звернення 12.06.2022).