УДК 004.56
DOI: 10.31673/2409-7292.2025.016955

Гайдук О. В., Звєрєв В. П.

ІГРОВІ ІНДЕКСИ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНИХ КОМУНІКАЦІЙ: КІБЕРСТІЙКІСТЬ, КІБЕРПОТУЖНІСТЬ ТА КІБЕРБЕЗПЕКА

Запропоновано підхід до оцінювання ефективності міжнародних стратегій кібербезпеки, що базується на синтезі теорії ігор та кількісному аналізі показників співпраці між державами у кіберпросторі. Автори аналізують стратегічні рішення країн як раціональних гравців, що вибирають між оборонними та наступальними стратегіями в кіберпросторі, враховуючи можливості співпраці та конфлікту. Проведений аналіз основних існуючих індексів кібербезпеки, таких як Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI) та інших, які оцінюють кіберздатність держав на різних рівнях. Представлено розроблення трьох умовних ігрових індексів: кібербезпеки, кіберстійкості та кіберпотужності, які дозволяють оцінювати рівень захищеності, відновлюваності та наступального потенціалу держав відповідно. Також акцентується на важливості розроблення більш гнучких та точних методів для оцінки кіберможливостей, які враховували б міжнародні взаємодії та політичний контекст. За основу оцінювання взято матрицю рівня співпраці в кіберпросторі, що відображає рівень взаємної довіри та готовності обмінюватися даними й технологіями. Методика продемонстрована на прикладі симульованих даних п’яти країн, для яких обчислювалися згадані індекси на основі модельних матриць взаємодії. Результати свідчать, що більш інтенсивна та рівномірно розподілена співпраця підвищує як загальний рівень безпеки, так і стійкість держави до атак, а висока кіберпотужність корелює з лідерством у глобальному кіберпросторі. Запропонований підхід може застосовуватися для оперативного моніторингу, аналізу слабких ланок у міжнародній кооперації та сценарного моделювання в умовах динамічно змінних загроз. Стаття прагне внести вклад у покращення методологічних підходів до кібердипломатії, оцінки кіберпотенціалів держав, використовуючи інструментарій теорії ігор для розуміння складних міждержавних взаємодій в галузі кібербезпеки та розвитку більш ефективних стратегій міжнародного співробітництва. Результати дослідження становлять інтерес для кібердипломатів, фахівців із кібербезпеки, державних органів, аналітичних центрів та міжнародних організацій.

Ключові слова: кібербезпека, теорія ігор, кіберзагрози, кіберстійкість, кіберпотужність, моделювання, кібератаки, міжнародні комунікації, ігрові індекси, кібердипломатія.

Вступ та постановка проблеми в загальному вигляді

У зв'язку зі зростанням загроз кібербезпеці, особливо для критичної інфраструктури держави, виникає необхідність у розробці та впровадженні ефективних методів оцінювання рівня кіберзахисту. Критична інфраструктура держави (енергетика, транспорт, медичні установи тощо) все більше стає залежною від інформаційних технологій. Порушення безпеки цих технологій може призвести до серйозних наслідків для життя та здоров'я громадян, а також економічних втрат. Багато країн встановлюють різні регулятивні вимоги стосовно кіберзахисту, наприклад, GDPR в Європейському Союзі або NIST у Сполучених Штатах. Це змушує організації, що управляють критичною інфраструктурою, активно шукати та впроваджувати ефективні методи оцінювання рівня кіберзахисту [1].

Впродовж останніх років кіберзагрози перетворилися на один із ключових викликів безпеці держав та міжнародних організацій. Це особливо яскраво проявляється у випадку України, де триваюча гібридна війна з російською федерацією зумовила системні кібератаки та інформаційні операції, спрямовані на підрив критичної інфраструктури, викрадення чутливих даних, інформаційний вплив на населення та дискредитацію органів державної влади. Останні тенденції свідчать, що російські спецслужби та пов’язані з ними хакерські угруповання головним чином націлені на отримання доступу до систем ситуаційної обізнаності та каналів зв’язку Сил оборони України, державних реєстрів та національних інформаційних систем. У такій ситуації особливого значення набуває пошук нових підходів до оцінювання взаємодії між державами та визначення рівня їхньої готовності до спільної протидії кіберзагрозам [2]. У цій роботі робиться акцент на поєднанні теорії ігор та інструментів кількісного аналізу (розрахунку індексів кіберстійкості, кібербезпеки та кіберпотужності) для побудови сценарно-алгоритмічної моделі міжнародних комунікацій у складних умовах гібридних кібератак та кібервійни.

Мета і завдання дослідження

Метою є дослідити та апробувати підхід, у якому країни розглядаються як раціональні гравці, що роблять вибір стратегій у кіберпросторі (наприклад, зміцнювати оборонні спроможності чи розвивати наступальний потенціал), а рівень співпраці між ними відображається у формі спеціальних матриць. На цій основі пропонуються три умовні ігрові індекси (кібербезпеки, кіберстійкості та кіберпотужності) як агреговані показники "виграшу" в багатоакторній грі.

Виклад основного матеріалу

Теорія ігор (англ. *Game Theory*) є одним із фундаментальних інструментів математичної економіки та прикладної математики, який дає змогу формалізувати процес прийняття рішень у середовищах із багатьма учасниками (гравцями) [3], [4], [5], [6].

Наступні чотири базові концепції, на яких часто базується дослідження безпеки та оборони:

Рівновага Неша (Nash equilibrium)

Розв'язком гри в сенсі Неша вважається такий набір стратегій $\{s_i^*\}$, за якого жоден гравець не може поліпшити свій виграш (payoff), переходячи до іншої стратегії, якщо стратегії решти гравців лишаються незмінними. Формально, для гравця ii існує функція корисності $U_i(\dots)$, і точка $\{s_1^*, s_2^*, \dots, s_n^*\}$ є рівновагою Неша [7], якщо:

$$U_i(s_i^*, s_{-i}^*) \geq U_i(s_i, s_{-i}^*) \text{ для будь-якого } s_i \in S_i,$$

де s_{-i}^* – це стратегії решти гравців, а S_i – множина стратегій гравця i.

Інтерпретація в кіберпросторі: Якщо дві держави ведуть "кіберперегони озброєнь" (розвивають наступальні або оборонні засоби), то стан, коли жодна зі сторін не бачить вигоди змінювати свою стратегію, можна вважати *рівновагою кіберарсеналу*. У контексті рівнів співпраці це може проявлятися в тому, що країна не зацікавлена знижувати чи підвищувати взаємодію з партнером, якщо він уже дотримується певної лінії.

Парето-оптимальність (Pareto optimality)

Набір стратегій (або ситуація) вважається Парето-оптимальним, якщо *не існує* такого переходу до іншої комбінації стратегій, за якого принаймні один гравець виграє більше, а решта не виграють менше [8].

Інтерпретація в кіберпросторі: У сценарії кооперативних кібератак або кіберзахисту Парето-оптимальна угода означає, що неможливо покращити безпеку або вигоду однієї держави, не погіршуючи становище іншої. Простіше кажучи, усі "швидкі покращення" без шкоди для третіх сторін уже вичерпано, й будь-який перерозподіл ресурсів або зміна політики призводить до чийогось погіршення.

Мінімакс (Maximin) і антагоністичні ігри

Концепція мінімаксу (або максиміну) звично виникає в антагоністичних або нульовосумних іграх, коли гравець припускає найгіршу поведінку противника. Гравець i обирає $y_i \in A_i$, яка максимізує його гарантований результат [9], [10]:

$$\max_{y_i} \min_{y_{-i}} U_i(y_i, y_{-i}).$$

Інтерпретація в кіберпросторі: Сценарій жорсткого протистояння між державами, особливо в контексті воєнних дій та серйозних кібератак, можна моделювати через мінімакс-стратегію, коли кожна сторона очікує найгірші дії від опонента і намагається мінімізувати власні втрати (або максимізувати "мінімальний гарантований виграш").

Типова постанова гри складається з:

1. Набору гравців, що діють у спільному середовищі (в нашому випадку — держави або блоки держав).

2. Набору стратегій кожного гравця — передбачуваних або можливих планів дій, які той може обрати для досягнення своїх цілей.

3. Виграшів (пейофів), що залежать від вибору стратегій усіх гравців одночасно. У класичній теорії ігор виграш зазвичай виражають у кількісних показниках (валюта, бали корисності тощо).

У контексті кібербезпеки та кіберконфліктів виникає потреба адаптувати канонічні підходи, адже гравці можуть мати складні та довготривалі мотивації — зокрема, політичні, економічні, технологічні; інформація часто розподілена асиметрично: не всі учасники однаково розуміють та оцінюють силу або слабкість свого опонента/партнера; взаємодія має характер як конфліктної, так і кооперативної гри одночасно: припустимо, що країни можуть бути суперниками у військовому чи в торгівельному плані, але водночас співпрацювати в питанні глобальної стабільності чи боротьбі з кіберзлочинністю.

Репутація і повторювані ігри

У реальних конфліктах кіберсторони зазвичай взаємодіють неодноразово, а отже, дотримання чи порушення домовленостей впливає на "репутацію" гравця та готовність партнерів співпрацювати у майбутньому. У повторюваних іграх (repeated games) можуть з'являтися стратегії покарання (grim trigger), спонукання до кооперації (tit-for-tat) тощо. У контексті повторюваних ігор, кожна індивідуальна гра, що грається більше одного разу, називається стадією гри. Припустимо, що гра G грається нескінченно багато разів, а загальний виграш кожного гравця є сумою виграшів, отриманих на кожній стадії гри, причому виграші дисконтуються з часом. Таке дисконтування враховує преференції гравців щодо часу (преференція теперішнього перед майбутнім) [27], [28].

Нехай $u_i(s)$означає виграш гравця i в одній стадії гри, де s - вектор стратегій усіх гравців. Якщо гра грається нескінченно багато разів, загальний виграш гравця i, який дисконтується з дисконтним фактором δ, можна визначити як:

$$U_i = \sum_{t=0}^{\infty} \delta^t \, u_i(s_t)$$

де δ- це дисконтний фактор між 0 і 1, а s_t- стратегія на кожному кроці t.

У повторюваних іграх гравці можуть вибирати стратегії, які базуються на історії попередніх ходів. Одним з класичних прикладів є стратегія тит-за-тат (tit-for-tat) у "дилемі в'язня", коли гравець спочатку співпрацює, а потім повторює попередній хід опонента. Ця стратегія ефективна для підтримання співпраці та запобігання зраді. У довгостроковій перспективі репутація стає вирішальним чинником. Гравці, які постійно зраджують або відмовляються від співпраці, можуть зіткнутися з відплатою у майбутньому, оскільки інші гравці адаптують свої стратегії, виходячи з попередньої поведінки. Важливим аспектом є визначення, чи можуть гравці досягнути рівноваги Неша, враховуючи довгострокову перспективу. Існують умови, при яких рівновага в повторюваних іграх включає можливість покарання за зраду, що змушує гравців підтримувати співпрацю.

Інтерпретація в кіберпросторі: Якщо держава таємно проводить шкідливі кібератаки проти "союзника" й це викривається, рівень співпраці у наступних періодах різко падає, що шкодить обом сторонам. Таким чином, навіть за відсутності "офіційних" санкцій, у довгостроковій перспективі раціональні країни схильні уникати зради партнерів, аби не втратити репутаційні та коаліційні вигоди.

Ці концепції і стратегії важливі для розуміння складних міжнародних взаємодій в кібербезпеці, де держави повинні враховувати як короткострокові так і довгострокові наслідки своїх дій в кіберпросторі.

Значення цих понять для нашої моделі:

– Рівновага Неша може слугувати теоретичним "граничним" станом, коли жодна країна не прагне міняти свою стратегію співпраці чи конфронтації, знаючи стратегії решти.

– Парето-оптимальність здатна вказати, чи можна одночасно покращити “кібервиграш” усім учасникам (наприклад, встановити глибшу взаємодію за допомогою відкритого обміну шкідливими IP-адресами).

– Мінімакс ілюструє екстремальну поведінку країни, коли вона очікує від суперника найгіршого (особливо якщо йдеться про військово-політичний конфлікт із високим ступенем ризику).

– Повторювані ігри та репутація відображають реальний геополітичний аспект, коли ситуація розвивається в часі, а виявлена “зрада” сьогодні матиме негативні наслідки для співпраці завтра.

Усе це вимагає введення комплексних моделей, які поєднували б ідеї класичних ігор у нормальній (або матричній) формі з поняттями кооперації, мережевої взаємодії, а також урахуванням параметрів довіри та репутації [11], [12]. У межах даного дослідження пропонується розглянути адаптований підхід, де “виграші” кожної держави відображаються через низку агрегованих індексів.

Порівняльний аналіз індексів кіберздатності держав: оцінка впливу та ефективності

У сучасному динамічному цифровому середовищі, оцінка кібербезпеки на національному рівні виступає як фундаментальний елемент стратегій національної безпеки будь-якої держави. З появою широкого спектру кіберзагроз, які постійно еволюціонують, країни, міжнародні організації та наукова спільнота взяли на себе ініціативу розробляти різноманітні індекси та інструменти для комплексної оцінки кіберздатностей. Такі інструменти, як NCSI, GCI, ENISA Evaluation Tool, CRI, CMM, NCPI та CCNP, стають важливими у зміцненні кіберстійкості, визначенні слабких сторін національних стратегій кібербезпеки, та формулюванні напрямків для їх покращення. Використання цих індексів сприяє не тільки підвищенню транспарентності та порівняльної оцінки кіберготовності на міжнародному рівні, але й забезпечує можливість систематизації підходів до управління кіберресурсами. Це дозволяє країнам ефективніше ідентифікувати прогалини у своїх національних стратегіях та адаптувати передові міжнародні практики, сприяючи таким чином зміцненню міжнародної співпраці у сфері кібербезпеки. В руслі цих зусиль, розгляд ключових індексів кібербезпеки в контексті академічних досліджень є невід'ємним для глибшого розуміння поточних та майбутніх викликів у сфері кіберзахисту та розробки більш резилієнтних стратегій національної та міжнародної кібербезпеки.

Розглянемо більш детально основні механізми та підходи, які використовуються в цих індексах для оцінки кібербезпекової здатності країн, а також підкреслимо аспекти, на які вони зосереджують увагу, включаючи законодавчі рамки, технологічні можливості, управління ризиками, культуру безпеки та міжнародну співпрацю тощо.

Враховуючи, що це дослідження концентрується на вивченні індексів, розроблених для оцінювання кіберздатностей на національному та міжнародному рівнях, індекси, спеціалізовані на аналізі кібербезпеки корпоративного та інших секторів, зокрема Cybersecurity Exposure Index (CEI) [13], Bitsight Cyber Security Rating (BCSR) [14] та інші не були включені до цього аналізу."

National Cyber Security Index (NCSI) розроблений e-Governance Academy в Естонії. Цей індекс оцінює здатність країни захищатися від кіберзагроз та ефективно реагувати на кіберінциденти. NCSI враховує різні аспекти кібербезпеки, включаючи законодавчу базу, технічні можливості, організаційну структуру та міжнародну співпрацю. Методика оцінки ґрунтується на аналізі публічно доступної інформації та відповідей на запитання зі спеціальної анкети, при цьому кожен показник має певну вагу в загальному оцінюванні. Результати індексу публікуються онлайн, де можна переглянути оцінки та рейтинги країн, і ці дані можуть

використовуватися як основа для політичних рішень і стратегій в області кібербезпеки на національному рівні [15], [16].

Global Cybersecurity Index (GCI) створений Міжнародним союзом електрозв'язку (ITU). Цей індекс оцінює кібербезпеку країн з урахуванням юридичних, технічних, організаційних аспектів, розвитку потенціалу та міжнародної співпраці. Методика GCI базується на зборі даних через опитування, яке розсилається країнам-членам ITU. Кожен аспект кібербезпеки оцінюється на основі серії індикаторів, які мають визначену вагу в загальному рейтингу. Результати аналізуються експертами для визначення сильних та слабких сторін кожної країни у відповідних областях. Кінцевий звіт GCI включає детальні профілі країн та рекомендації щодо поліпшення їхньої кібербезпеки, що визначає їхні національні здібності та зобов'язання в сфері кібербезпеки на глобальному рівні [17].

Інструмент ENISA National Cyber Security Strategies Evaluation Tool розроблений Агентством Європейського Союзу з кібербезпеки (ENISA). Цей інструмент дозволяє країнам самостійно оцінювати виконання своїх національних стратегій кібербезпеки, визначати прогалини та розробляти рекомендації для підвищення ефективності заходів у сфері кібербезпеки. Методика оцінки базується на використанні кваліативних та кількісних даних, які збираються через анкетування та інтерв'ю з ключовими зацікавленими сторонами. Інструмент враховує такі аспекти, як розвиток кадрового потенціалу, співпраця з приватним сектором, міжнародні відносини у сфері кібербезпеки, а також правові та регулятивні рамки. Результати, отримані за допомогою цього інструменту, допомагають країнам планувати та впроваджувати належні коректівні заходи для зміцнення національної безпеки у кіберпросторі [18].

Cyber Readiness Index (CRI), розроблений Potomac Institute for Policy Studies, вимірює готовність країн до кібервикликів, аналізуючи їхню здатність захищати національні інтереси в кіберпросторі. Цей індекс оцінює кіберготовність за допомогою аналізу ключових даних та індикаторів у п’яти основних сферах: національна стратегія, інцидентне реагування, е-урядування, дипломатія та торгівля, та захист критичної інфраструктури. Кожна сфера розглядається через призму відповідних законодавчих актів, політик, організаційних структур, і інших факторів, що формують національну політику в галузі кібербезпеки. Результати, отримані з цих аналізів, допомагають країнам визначити не тільки поточний стан, але й області, що потребують покращення, дозволяючи планувати та впроваджувати відповідні коректівні заходи для зміцнення кібербезпеки [19].

Cybersecurity Capacity Maturity Model for Nations (CMM) розроблена Global Cyber Security Capacity Centre (GCSCC) Оксфордського університету. Ця модель є методичною рамкою для оцінки кібербезпекової здатності країни та складається з п'яти вимірів, які включають розробку національної стратегії кібербезпеки, управління ризиками, інцидентами та кризами, захист критичної інфраструктури, кібербезпеку в обороні та національній безпеці, сприяння відповідальній кібербезпековій культурі в суспільстві, а також міжнародну взаємодію.

Це зображення (Рис. 1) ілюструє п'ять основних вимірів *CMM*, які взаємопов'язані між собою, підкреслюючи їх взаємодію:

1. Політика та стратегія кібербезпеки (Dimension 1) - представлена іконкою з гайковим ключем і викруткою, символізує розробку та виконання стратегічних підходів і політик у галузі кібербезпеки.
2. Культура та суспільство кібербезпеки (Dimension 2) - зображена у вигляді руки, що потискає іншу руку, акцентує на важливості культурного та соціального контексту у зміцненні кібербезпеки.
3. Розвиток знань та можливостей у галузі кібербезпеки (Dimension 3) - представлений зубчастим колесом, що підкреслює технічну складову і необхідність підвищення компетенції у цій сфері.

© Гайдук О. В., Звєрєв В. П. (2025). Ігрові індекси в інформаційних технологіях забезпечення міжнародних комунікацій: кіберстійкість, кіберпотужність та кібербезпека. Сучасний захист інформації, 1(61), 44–59. https://doi.org/10.31673/2409-7292.2025.016955.

4. Правові та регуляторні рамки (Dimension 4) - іконка терезів, що символізує роль законодавства та регулятивних стандартів у захисті кіберпростору.

5. Стандарти та технології (Dimension 5) - показано бінарним кодом, що наголошує на технічному аспекті впровадження стандартів і новітніх технологій у кібербезпеці.

Рис. 1 п'ять основних вимірів *CMM*

Згадана модель CMM демонструє, як різні аспекти кібербезпеки взаємопов'язані та як вони спільно формують комплексний підхід до захисту інформації та інфраструктури. Вона також включає п'ять рівнів зрілості: початковий, формуючий, встановлений, стратегічний та динамічний. Оцінка за допомогою CMM дозволяє країнам визначити свої сильні та слабкі сторони у сфері кібербезпеки та розробити стратегії для покращення своєї кіберготовності [20].

National Cyber Power Index, Індекс Національної Кіберпотужності (NCPI) розроблений Блефер центром (Belfer Center) Гарвардської школи Кеннеді (Harvard Kennedy School) у 2020 році [21], та в другій редакції з порівняннями в 2022 році [22], має на меті оцінити і порівняти кіберпотужності 30 країн світу. Цей індекс включає оцінку як намірів, так і можливостей країн у сфері кібербезпеки, враховуючи їхні національні цілі. NCPI надає глибше розуміння кіберпотужності, аналізуючи не лише кіберзахист, але й офензивні кіберможливості, розподіл ресурсів, приватний сектор, інновації та робочу силу.

Для оцінки кіберпотужності країни NCPI використовують індикатори можливостей і індикатори намірів, базуючись на публічно доступних даних. Основною новизною NCPI є вимірювання комплексності кібердій країни, яка визначається здатністю використовувати кіберзасоби для досягнення множини національних цілей. Методика визначення NCPI включає декілька ключових компонентів, які дозволяють оцінити кіберпотужність країн з урахуванням їхніх стратегічних цілей і здатностей. Ось основні етапи та аспекти цієї методики. На першому етапі визначаються національні цілі, які країни намагаються досягнути за допомогою кіберзасобів. До таких цілей можуть входити, наприклад, захист національної інфраструктури, збір розвідувальної інформації, вплив на інформаційне середовище, забезпечення національної безпеки, розвиток технологічних можливостей, і так далі.

Далі NCPI використовує два основних вектори аналізу для кожної країни: наміри та здібності. Причому **Наміри (Intent) о**цінюються на основі офіційних документів країни, таких як національні стратегії кібербезпеки, політичні заяви та інші публічні документи. Аналізується, наскільки активно країна декларує свої наміри розвивати кіберможливості для досягнення визначених цілей. **Можливості (Capabilities) в**изначаються на основі різних індикаторів, таких як технічні здібності, розвиток кіберінфраструктури, кількість фахівців у

галузі кібербезпеки, інноваційність у технологічній сфері, та інше. Ці індикатори допомагають оцінити реальну здатність країни впроваджувати свої наміри у життя.

Для кожної країни підраховується згорнутий індекс, який є добутком оцінок намірів та можливостей по кожній цілі. Цей підхід дозволяє забезпечити баланс між бажаннями країни та її реальними можливостями. Ключовою особливістю NCPI є оцінка комплексності кібердій країни. Вона визначається тим, наскільки країна здатна використовувати кіберзасоби для досягнення широкого спектру національних цілей. Такий підхід відрізняє NCPI від інших індексів, які можуть зосереджуватися лише на одному аспекті, такому як кібербезпека.

Rank	2020	2022
1	US	US
2	China	China
3	UK	Russia
4	Russia	UK
5	Netherlands	Australia
6	France	Netherlands
7	Germany	ROK
8	Canada	Vietnam
9	Japan	France
10	Australia	Iran

Рис. 2 Рівень NCPI країн у 2020 та 2022 роках

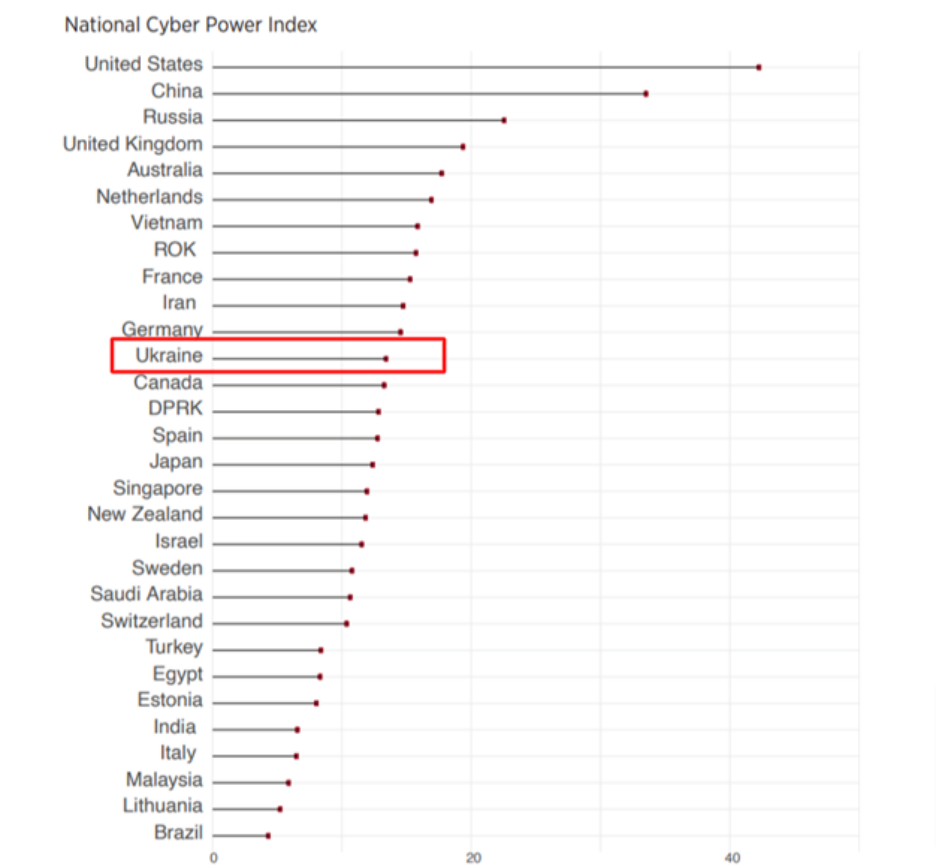

Рис. 3 Графічне представлення рівня NCPI 2022 для країн, Україна виділена червоним прямокутником

Порівнюючи застосування індексу до держав світу, можемо побачити, що протягом як мінімум двох років США утримують перше місце, Китай займає друге, а рф піднялася на третє місце, обігнавши Велику Британію. Зміни в рейтингу включають підйом Австралії з 10-го місця в 2020 році на 5-е місце в 2022 році, тоді як Франція впала з 6-го на 9-е місце, а Німеччина, Канада та Японія вийшли з топ-10. Новими учасниками топ-10 стали Республіка Корея, яка піднялася з 16-го на 7-е місце, В'єтнам з 18-го на 9-е, а Іран з 22-го на 10-е місце. Війна в Україні сприяла підвищенню позицій як росії, так і України, причому росія обігнала Велику Британію в рейтингу, а Україна піднялася з 29-го на 12-е місце [21], [22], [23], [24].

Індекс кібер можливостей та національної потужності – Cyber Capabilities and National Power (CCNP), розроблений Міжнародним інститутом стратегічних досліджень (IISS), призначений для оцінки кіберздатностей країн та їхнього впливу на національну потужність. CCNP аналізує кіберекосистему кожної держави та її взаємозв'язок з міжнародною безпекою, економічною конкуренцією та військовими справами. Індекс оцінює країни за такими категоріями, як **стратегія та доктрина, управління, командування та контроль, кіберрозвідувальні можливості держави, кібербезпека та стійкість, лідерство у кіберпросторі та наступальні кіберможливості країни.** За цим індексом IISS пропонує розділити країни на три основні рівні CCNP, перший з яких включає країни з провідними світовими можливостями у всіх категоріях, другий в деяких і третій держави з сильними або потенційно сильними можливостями в деяких категоріях, але значними слабкостями в інших [25].

Приведені індекси, такі як NCSI, GCI, ENISA Evaluation Tool, CRI, CMM, NCPI, і CCNP, мають ряд вад, які можуть впливати на їхню точність та корисність у реальному світі. Часто вони залежать від самооцінок держав, які можуть бути суб'єктивними та упередженими через політичні мотиви країн або небажання розкривати свої слабкості. Обмеження в обсязі даних, на які опираються ці індекси, не дозволяють отримати повну картину кібербезпеки, оскільки зосереджуються лише на декількох параметрах, ігноруючи інші важливі аспекти, такі як внутрішні політики або технологічні нововведення. Також, швидка зміна кіберзагроз вимагає від індексів постійного оновлення, що не завжди відбувається своєчасно, роблячи деякі дані застарілими майже одразу після публікації. Індекси зазвичай не диференціюють кібероборону та кібернапад, об'єднуючи ці категорії під однією категорією, що може призвести до помилкових висновків про реальний рівень кібер можливостей. Відсутність контекстуального аналізу, який враховує політичний і культурний ландшафти країн, додатково обмежує здатність індексів точно оцінювати кібербезпеку. Надмірна залежність від кількісних показників призводить до недооцінки якісних аспектів кіберзахисту, що також знижує загальну цінність таких оцінок. Все це підкреслює необхідність розвитку більш точних і гнучких методів оцінки, які могли б адекватно відображати динаміку та складність глобального кіберпростору. Більшості подібних рейтингів бракує ідеї багатосторонньої взаємодії: вони переважно зосереджуються на внутрішніх заходах, рівні законодавства, освіті, присутності CERT/CSIRT-команд [16], [17].

В дослідженні Чіфчі Хасана (Çifci, Hasan) [25], показані концептуальні рамки, які включають 14 основних категорій і 90 індикаторів основних індексів. Це дозволяє систематично порівняти існуючі індекси та оцінити їх за охопленням та глибиною. За Чіфчі, в усьому комплексі індексів існують суттєві прогалини в охопленні деяких важливих аспектів кібербезпеки. Так, наприклад, Global Cybersecurity Index (GCI) разом з осяжною оцінкою кібербезпеки не звертає достатньо уваги на офензивні кіберможливості та не враховує економічний контекст кібердій. Йому також бракує покриття таких сфер як військові кіберздібності, залучення для аналізу розвідданих тощо. National Cyber Security Index (NCSI) фокусується на політиці безпеки та відповідях на інциденти, але не охоплює в достатньому обсязі військові кібероперації або розробку національних технічних кіберможливостей. Це створює обмеження в здатності індексу оцінювати всебічну кіберпотужність. Cyber Readiness

Index (CRI) надає глибокий аналіз національної стратегії кібербезпеки, але ігнорує такі аспекти, як міжнародне співробітництво та військові кібероперації. Також індекс не враховує економічні аспекти, що мають велике значення для кіберпотужності. Cybersecurity Capacity Maturity Model for Nations (CMM) дуже детальна в оцінці зрілості кібербезпеки, але не включає офензивні кіберздібності, які є ключовими для національної кіберпотужності.

Поняття умовних індексів "кібербезпека", "кіберстійкість" та "кіберпотужність"

В цьому дослідженні запропонована модель базується на трьох умовних ігрових індексах — кібербезпеки, кіберстійкості та кіберпотужності і включає кооперативно-конфліктний вимір, адже враховує, наскільки успішно країни взаємодіють одна з одною та як це впливає на їхню здатність захищатися, відновлюватися та впливати на інші держави. Таким чином, обчислені індекси можуть або доповнювати відомі міжнародні індекси та рейтинги, або слугувати основою для динамічного ігрового аналізу, коли відслідковують зміни матриці співпраці R у часі. Запропонований алгоритм розрахунку показників дає змогу кількісно оцінити стан кооперації/конфлікту в кіберпросторі, зокрема в умовах військових та геополітичних загроз. Приклад із п'ятьма країнами ілюструє, як різні конфігурації "рівня співпраці" можуть впливати на підсумкові значення індексів і, відповідно, сигналізувати про сильні та слабкі місця держави у міжнародному кіберландшафті.

1. **Кібербезпека (Cybersecurity)** — загальний рівень захищеності ІТ-систем, мереж та даних країни від зовнішніх втручань і зловмисних дій. Цей показник можна інтерпретувати як здатність країни **запобігати** кібератакам і **локалізувати** їхні наслідки.

2. **Кіберстійкість (Cyberstability, або Cyber Resilience)** — здатність зберегти функціональність системи та швидко **відновлюватися** після кібератаки, не втрачаючи критичних можливостей. Якщо кібербезпека більше стосується рівня поточної захищеності, то **кіберстійкість** виражає "*запас міцності*": наскільки державні чи корпоративні структури можуть продовжувати роботу, зазнаючи атак, та відновлюватися після них.

3. **Кіберпотужність (Cyberpower)** — здатність ініціювати, проводити чи підтримувати власні **активні** операції (наступальні чи розвідувальні) у кіберпросторі, а також суттєво впливати на глобальний цифровий ландшафт. Кіберпотужність асоціюється з кількістю та якістю "*кіберзброї*", професійними фахівцями, інтелектуальними ресурсами, та з тим, наскільки держава може **диктувати** (або суттєво впливати) на розвиток подій у кіберпросторі.

Поняття "кіберпотужності" тут є ширшим за **наступальний кіберпотенціал**, адже включає і здатність формувати міжнародний порядок денний, брати участь у коаліціях або створювати передові рішення в галузі кіберзахисту.

Матриця співпраці як елемент ігрової моделі

Оскільки дослідження присвячено міжнародним комунікаціям у кіберпросторі, особливу увагу зосереджено на **кооперативно-конфліктній** взаємодії між країнами. Для її кількісного опису введемо поняття **Рівня Співпраці в Кіберпросторі** (далі – РСК), яке може варіюватися від 0 до 10 і відбиває:

- Рівень *взаємної довіри* у сфері обміну чутливою інформацією,
- Активність *спільних навчань*, розробок, регулярних зустрічей,
- Наявність *угод* чи меморандумів про співпрацю в кіберсфері,
- Готовність *відповідати спільно* на кібератаки третіх сторін,
- Обсяги *регулярного обміну* аналітичною інформацією про кіберзагрози тощо.

Значення РСК між двома країнами **i** та **j** (позначимо його $\mathbf{R_{ij}}$) зберігаються у спеціальній **матриці R**. Якщо взяти **n** країн, то матриця має розмір **n×n**. На діагоналі **R** стоять нулі (оскільки РСК країни сам із собою не має змісту), а поза діагоналлю — числові оцінки рівня співпраці між різними парами держав.

У класичній матричній грі (game in normal form) “матриця” звичайно відбиває виграші гравців при тих чи інших комбінаціях стратегій [5], [6]. У нашому випадку, оскільки кількість стратегій дуже велика (наприклад, “інвестувати X% бюджету в активні наступальні інструменти, Y% — в оборонні”), складно безпосередньо будувати велику багатовимірну матрицю виграшів. Тому запропоновано спростити підхід: виділити з усього різноманіття стратегій їхній *узагальнений результат* у вигляді рівня співпраці R. Далі вже на основі R обчислюють агреговані індекси для кожного гравця, які унаочнюють, наскільки вигідно чи небезпечно тому вести активну діяльність у цьому мережевому середовищі.

Наприклад, якщо країна “A” підтримує високий рівень співпраці з більшістю потужних держав, вона отримує відчутні переваги для нарощування кіберстійкості (спільні рішення, обмін технологіями) та збільшення кібербезпеки (отримання термінових попереджень про нові уразливості). Натомість брак кооперації, або її зниження, може стимулювати більш агресивний сценарій, коли країна намагається розвивати власну наступальну потужність чи вдаватися до кібершантажу.

Роль індексів у модельованій грі та їх розрахунок

Щоби відобразити основні “виходи” з моделі (фактично — *виграші* гравців), у роботі використовуються три індекси:

1. **Індекс кібербезпеки (cybersecurity_index)**

$$\text{cybersecurity}_{\text{index}} = \frac{\bar{X}_{(\text{рядкове})}}{\sigma(\mathbf{R})},$$

де $\bar{X}_{(\text{рядкове})}$ — середнє значення відповідного рядка (або, залежно від реалізації, середнє по рядках і потім усереднення), а $\sigma(\mathbf{R})$ — стандартне відхилення усіх елементів матриці **R** (за винятком діагоналей). Він відбиває рівень **“пасивного” або “захисного” виграшу**: чим краща співпраця зі сторонами, тим більше шансів на регулярний обмін патчами, попередженнями та оперативну допомогу в разі кібератаки. Нормалізація на стандартне відхилення робить цей показник чутливим до “розкиду” рівнів співпраці.

2. **Індекс кіберстійкості (cyberstability_index)**

$$\text{cyberstability\_index} = \frac{\bar{X}_{(\text{стовпчикове})}}{\max(\mathbf{R}) - \min(\mathbf{R})},$$

де $\bar{X}_{(\text{стовпчикове})}$ — середнє значення відповідного стовпця матриці (для конкретної країни як “приймача” співпраці), а $\max(\mathbf{R}), \min(\mathbf{R})$ — найбільший і найменший елементи поза діагоналлю. Умовно відображає, **наскільки стабільним є оточення** країни: якщо в матриці немає значних розривів (максимум і мінімум не надто відрізняються), а рівень співпраці розподілений рівномірно, то країна має кращу здатність “пристосовуватися” і відновлюватися, тобто ніде не виникає “провалів” співпраці, що перешкоджали б її діяльності.

3. **Індекс кіберпотужності (cyberpower_index)**

$$\text{cyberpower\_index} = \frac{\bar{X}_{(\text{загальне})}}{\sigma(\mathbf{R})},$$

де $\bar{X}_{(\text{загальне})}$ — середнє значення всіх елементів **R** (крім діагоналі), а $\sigma(\mathbf{R})$ — стандартне відхилення тих самих елементів. Показує “середню” залученість країни в мережу співпраці, порівняно з тим, наскільки нестабільною вона є загалом. Високий cyberpower_index може свідчити, що країна перебуває в хорошій позиції, щоб **впливати** на цифровий простір — адже вона поєднує розгалужені партнерські зв’язки зі стабільністю та певною однорідністю оточення.

На відміну від традиційних ігор, де кожному гравцю визначають один (або кілька) точних числових значень виграшу для кожної комбінації стратегій, у нашому підході кожен із трьох індексів є **узагальненим** відображенням виграшу країни через певну призму (захист,

стійкість, потужність). Це дає змогу оцінити **багатовимірність** “результату” участі країни у складному кіберсередовищі.

Усі ці аспекти доповнюють “систему координат” нашої моделі, де матриця співпраці РСК і три “ігрові” індекси (кібербезпека, кіберстійкість, кіберпотужність) дають змогу кількісно оцінити, що втрачає чи здобуває гравець, коли зближується або дистанціюється від інших держав у кіберпросторі. Такий підхід, хоч і не завжди дає повну картину реальної політики, дозволяє виявити тенденції та сценарії, що допомагають розробляти більш стійкі (а часом і кооперативні) стратегії.

Синхронізація концепцій: як індекси поєднуються з теорією ігор

Попри те, що моделі з індексами не завжди мають класичну форму “гравець × стратегія → payoff”, вони дають змогу:

1. Визначити чинники, що впливають на виграш: зміна рівня співпраці (наприклад, укладення нових угод між країнами) підвищує або знижує окремі індекси.

2. Оцінити мотивацію гравців: країна, що відчуває нестачу співпраці, може почати активно шукати нових партнерів, аби збільшити cyberpower_index чи cybersecurity_index.

3. Передбачити наслідки “зради” чи “зниження взаємної довіри”: якщо одна країна почне вести приховані наступальні операції проти свого формального партнера, це може знизити РСК в парі “країна А — країна В”, а відтак погіршити індекси А або В.

4. Виявити потенційну рівновагу: хоча стаття не обмежується формальним пошуком рівноваги Неша, самі індекси можуть слугувати орієнтиром, у якому напрямку країни можуть робити кроки, щоб покращити спільні позиції (наближення до умовної “Парето-ефективності” в кооперативному сенсі).

Таким чином, введення **матриць РСК** і трьох **ігрових індексів** дає змогу в стислій формі відобразити складну багатосторонню взаємодію в кіберпросторі й перейти до практичних розрахунків, де на прикладі конкретних країн буде продемонстровано, як ці індекси працюють на симульованих даних.

У класичному формулюванні теорії ігор кожен гравець (країна) має певну множину стратегій, а результат (виграш/корисність) кожного гравця залежить від сукупності стратегій усіх учасників. Подача гри може бути здійснена у нормальній (матриці виграшів) або у розширеній формі (дерево гри).

Для наступних міркувань щодо побудови ігрової моделі, як приклад розглянемо “Дилему в’язня” в кіберпросторі. Часто взаємодію кількох країн у сфері кібербезпеки порівнюють із дилемою в’язня: якщо обидві держави співпрацюють (наприклад, відкривають доступ до ключових кіберзагроз, оперативно обмінюються сигнатурами малварі), вони отримують кращий сукупний результат. Однак у деяких випадках кожна зі сторін може “зрадити” (не розкривати повну інформацію, приховувати вразливості, щоб використати їх самостійно), сподіваючись на більшу вигоду. Стається так звана “пастка некооперативності”. Щоб запобігти їй, можуть розроблятися механізми перевірки, спільного аудиту чи міжнародних договорів — у такому випадку наявність механізмів покарання сприяє виникненню *кооперативних* результатів навіть у грі, яка потенційно може мати антагоністичний характер [27], [29], [30].

Вихідні дані та формування матриць співпраці

Для апробації запропонованого підходу було обрано 5 країн в тому числі об'єднана Європа як інтегрована спільнота країн ЄС, які відіграють помітну роль у глобальному кіберпросторі. Це США, Китай, Україна, Європа (умовно як інтегрована спільнота країн ЄС) та Японія.

Вихідні дані представлено у вигляді матриць співпраці РСК розміру 5×5. Кожна матриця відображає, наскільки держава **і** схильна до співпраці зі своїми потенційними партнерами (або суперниками) у кіберсфері. Числа в діапазоні від 0 до 10 інтерпретують:

© Гайдук О. В., Звєрєв В. П. (2025). Ігрові індекси в інформаційних технологіях забезпечення міжнародних комунікацій: кіберстійкість, кіберпотужність та кібербезпека. Сучасний захист інформації, 1(61), 44–59. https://doi.org/10.31673/2409-7292.2025.016955.

– **0** — відсутність (або неможливість) взаємодії, зокрема випадки “країна сама з собою” на діагоналі;

– **1–4** — слабка або обмежена співпраця (фрагментарний обмін інформацією);

– **5–7** — помірний рівень співпраці (спільні навчання, консультативна підтримка);

– **8–10** — високий рівень співпраці (глибока інтеграція в обмін даними, спільні проєкти, формальні угоди).

На практиці такі оцінки можуть бути отримані шляхом експертного опитування або на основі емпіричних індикаторів (кількість спільних кібернавчань, угод про взаємну допомогу, ступінь відкритості “threat intelligence” тощо).

Приклад програмної реалізації

Для автоматизації процесу було реалізовано демонстраційний код на мові Python. Модульні бібліотеки (наприклад, NumPy) дають змогу працювати з багатовимірними масивами, тоді як візуалізація може здійснюватися за допомогою бібліотек Matplotlib, NetworkX або інших засобів відтворення графів.

```
1. Завантаження (або оголошення) матриць
2. import numpy as np
3.
4. # Матриця для США
5. matrix_usa = np.array([
6.     [0, 2, 3, 4, 5],
7.     [2, 0, 3, 4, 5],
8.     [3, 3, 0, 4, 5],
9.     [4, 4, 4, 0, 5],
10.    [5, 5, 5, 5, 0]
11. ])
12. # Аналогічно визначаються matrix_china, matrix_ukraine тощо
13. Розрахунок середніх і стандартного відхилення
14. def calculate_indices(matrix):
15.     flat_matrix = [item for row in matrix for item in row if item != 0]
16.     # Середнє значення
17.     mean_matrix = np.mean(flat_matrix)
18.     # Макс і мін
19.     max_val = np.max(flat_matrix)
20.     min_val = np.min(flat_matrix)
21.     # Стандартне відхилення
22.     std_val = np.std(flat_matrix)
23.
24.     # Кіберстійкість (по стовпцях)
25.     col_means = matrix.mean(axis=0)  # середні значення кожного стовпця
```

```
    cyberstability_index = np.mean(col_means) / (max_val - min_val)

    # Кібербезпека (по рядках)
    row_means = matrix.mean(axis=1)
    cybersecurity_index = np.mean(row_means) / std_val

    # Кіберпотужність (середнє/стд)
    cyberpower_index = mean_matrix / std_val

    return (cyberstability_index, cybersecurity_index, cyberpower_index)
Застосування до набору країн
matrices = [matrix_usa, matrix_china, matrix_ukraine, matrix_europe, matrix_japan]
countries = ["США", "Китай", "Україна", "Європа", "Японія"]

for i, m in enumerate(matrices):
    stability, security, power = calculate_indices(m)
    print(f"{countries[i]}:")
    print(f"  Індекс кіберстійкості  = {stability:.2f}")
    print(f"  Індекс кібербезпеки   = {security:.2f}")
    print(f"  Індекс кіберпотужності= {power:.2f}\n")
```

У результаті програма виводить набір числових показників для кожної країни. Очікується, що США та Китай матимуть вищі або більш збалансовані індекси завдяки значній залученості в мережу міжнародної кібервзаємодії, а менші за розміром чи ресурсами країни (наприклад, Україна чи окремі європейські держави) можуть мати нижчі показники потужності, проте вищу стійкість або безпеку за умови тісної кооперації з партнерами.

Результати та їх інтерпретація

Після виконання коду кожна країна отримує три умовні ключові метрики, які свідчать про (1) її "пасивну" здатність захищатися (кібербезпека), (2) спроможність відновлюватися й не втрачати функціоналу (кіберстійкість), (3) уміння ініціювати власні проєкти та мати вплив (кіберпотужність).

1. Кібербезпека (cybersecurity_index)

- Вищі значення: свідчать про краще "середовище" співпраці, що дає змогу країні отримувати допомогу, експертну підтримку, спільно розробляти захисні рішення.

- Нижчі значення: сигналізують, що країна або не має достатньо союзників, або її мережа контактів складається з партнерів із низьким рівнем взаємодії.

2. Кіберстійкість (cyberstability_index)

- Високий показник означає, що країна не надто залежить від "пікових" коливань співпраці. Навіть якщо з однією з країн партнерство слабне, то є розгалужена система контактів.

- Низький показник застерігає про ризик “вузького горла”: втрата одного ключового партнера призведе до серйозного спаду загальної захищеності.

3. Кіберпотужність (cyberpower_index)

- Висока кіберпотужність інтерпретується як здатність держави активно впливати на дигітальний простір, утворювати коаліції, проводити кібератаки або розвідувальні операції.

- Низька кіберпотужність означає, що країна або новачок у цій сфері, або свідомо більше орієнтована на суто оборонні заходи, не претендуючи на лідерство.

У практичному сенсі аналітик може, спираючись на ці метрики, формувати рекомендації щодо нарощування тих чи інших напрямів співпраці. Наприклад, якщо Індекс кібербезпеки занадто низький, варто ініціювати спільні проєкти з партнерами; якщо бракує кіберпотужності, можливо, потрібні інвестиції в наступальні дослідницькі програми чи поглиблене вивчення тактик противника.

Висновки та перспективи подальших досліджень

У межах цієї роботи розглянуто застосування теорії ігор до проблематики міжнародної кібербезпеки. Запропоновано низку індексів (кібербезпеки, кіберстійкості, кіберпотужності), які дають змогу в кількісному форматі оцінювати взаємодію держав у кіберпросторі та виявляти, наскільки ефективно країни співпрацюють чи, навпаки, перебувають у стані конфронтації. Класичні уявлення теорії ігор (рівновага Неша, максимін, Парето-оптимальність, повторювані ігри) можуть бути адаптовані до контексту кіберконфліктів та міжнародної кооперації. Введено поняття матриці співпраці РСК, що відбиває рівень взаємної довіри та готовності держав до обміну інформацією, технологіями та спільного реагування на кіберзагрози.

Розроблено методику обчислення трьох умовних ігрових індексів — кібербезпеки (cybersecurity_index), кіберстійкості (cyberstability_index) та кіберпотужності (cyberpower_index) — на базі матричних оцінок РСК. Продемонстровано програмну реалізацію на Python, що дає змогу швидко виконувати розрахунки для різних конфігурацій держав.

На прикладі умовних п’яти країн (США, Китай, Україна, Європа, Японія) імітовано сценарії з різним рівнем співпраці. Виявлено, що високі показники індексу кібербезпеки частіше пов’язані з розгалуженими зв’язками з партнерами, а високі значення кіберстійкості — із більш рівномірним розподілом зв’язків. Кіберпотужність тісно корелює з “загальною” інтеграцією країни в міжнародне кіберсередовище.

Перевагами моделі є відносна простота, інтеграція багатосторонніх факторів взаємодії та можливість масштабувати на більшу кількість гравців. До обмежень належить експертний характер оцінок РСК, відсутність явної “динаміки” (у часі), а також складнощі з формальним пошуком “точок рівноваги”, оскільки індекси є агрегованими метриками, а не безпосередніми виграшами в класичному сенсі.

Розроблений підхід може бути основою для створення аналітичних панелей (dashboards), де інтегруються реальні дані (кількість спільних кібернавчань, операцій із запобігання кібератакам, угоди про обмін розвідувальними даними тощо). Такі панелі допоможуть кібердипломатам, а також державним інституціям та структурам сил оборони і безпеки краще розуміти поточну динаміку та ухвалювати виважені рішення щодо посилення або перегляду рівнів співпраці.

Завдяки кількісній оцінці з’являється можливість більш прозорого обговорення “хто кому й наскільки довіряє” у кіберпросторі. Це, в свою чергу, може прискорити укладення двосторонніх і багатосторонніх угод про кіберзахист, спільний обмін даними про загрози та координацію відповідей на кібератаки. Запропонована модель може суттєво доповнити згадані міжнародні індекси (GCI від ITU, NCSI та інші) за рахунок “міждержавного” компонента,

© Гайдук О. В., Звєрєв В. П. (2025). Ігрові індекси в інформаційних технологіях забезпечення міжнародних комунікацій: кіберстійкість, кіберпотужність та кібербезпека. Сучасний захист інформації, 1(61), 44–59. https://doi.org/10.31673/2409-7292.2025.016955.

підсвічуючи той факт, що кібербезпека багато в чому є результатом взаємодії, а не суто внутрішніх зусиль країни.

Проведене дослідження демонструє, що поєднання інструментарію теорії ігор із кількісною оцінкою рівня співпраці між державами відкриває нові можливості для розуміння міжнародної кібербезпеки та кібердипломатії. Реалізована модель виявилася корисною для ідентифікації сильних і слабких ланок у кіберзахисті, а також для формування рекомендацій щодо розширення чи оптимізації партнерських зв'язків.

Хоча сучасні кіберконфлікти характеризуються високою динамічністю, комплексом геополітичних, економічних і технологічних чинників, запропонований ігровий підхід здатен окреслити орієнтири щодо того, як змінюється "виграш" кожної країни під впливом різних параметрів колективної (або конфліктної) взаємодії. Це важливо як для суто дослідницьких цілей, так і для практичної кібердипломатії, планування оборонних стратегій та налагодження міжнародних механізмів стримування й покарання кіберагресорів. Робота закладає основу для майбутніх досліджень і прикладних розробок, покликаних усунути невизначеність і забезпечити якісну комунікацію між державами у галузі кіберзахисту, що, своєю чергою, сприятиме глобальній стабільності та безпеці в цифрову епоху.

Перелік посилань

1. О. Корченко, Є. Іванченко, О. Бакалинський, Д. Мялковський, Д. Зубков, Метод оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури держави. Наукоємні технології 61 (1), 3-20.

2. О. Гайдук. Кібердипломатія як парадигма нового підходу до міжнародних відносин: досвід країн світу, науково-академічні практики та кібербезпека міжнародних комунікацій. Монографія "Стратегічні комунікації в умовах війни: погляд від волонтера до науковця". Національна Академія Служби Безпеки України, Київ, 2024.

3. Von Neumann, J., & Morgenstern, O. Theory of Games and Economic Behavior. Princeton University Press, 1944.

4. Osborne, M. J. An Introduction to Game Theory. Oxford University Press, 2003.

5. Basar, T., & Olsder, G. J. Dynamic Noncooperative Game Theory. SIAM, 1999.

6. Tambe M., Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned. Cambridge University Press, 2011.

7. Charles A. Holt and Alvin E. Roth, The Nash equilibrium: A perspective Department of Economics, University of Virginia, Charlottesville, VA 22904-4182; Department of Economics and Harvard Business School, Harvard University, Cambridge, MA 02138 January 28, 2004.

8. Fiorenzo Mornati, Pareto optimality in the work of pareto. Revue européenne des sciences sociales T. 51, No. 2, Numéro spécial du cinquantenaire: autour de pareto (2013), pp. 65-82 (18 pages).

9. Nisarg Shah, Game Theory : Zero-Sum Games, The Minimax Theorem https://www.cs.toronto.edu /~nisarg/teaching/304f17/slides/CSC304-L5.pdf https://www.cs.toronto.edu/~nisarg/teaching/304f19/slides/304f19-L6.pdf

10. Kaifu Zhang, Timothy Van, Theorem of the Maximin and Applications to Bayesian Zero-Sum Games, Feb 2010 Economics and Political Sciences; Centre for Economic Policy Research.

11. Amadi Emmanuuel Chukwudi, Eze Udoka, Ikerionwu Charles. Game Theory Basics and Its Application in Cyber Security. Advances in Wireless Communications and Networks. Vol. 3, No. 4, 2017, pp. 45-49. doi: 10.11648/j.awcn.20170304.13

12. Chukwudi, Amadi & Eze, Udoka & Ikerionwu, Charles. (2017). Game Theory Basics and Its Application in Cyber Security. Advances in Wireless Communications and Networks. 3. 45-49.

13. Індекс кібервразливості Cyber Exposure Index – Cyber Exposure Development Environment

14. Рейтинг безпеки Bitsight Bitsight Cyber Security Ratings | Bitsight

15. Худинцев, Микола & Жилін, Артем & Davydiuk, Andrii. (2021). Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог). Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України ISBN: 978-966-136-887-2.

16. Національний індекс кібербезпеки. Академія електронного урядування (eGA) https://ega.ee/project/national-cyber-security-index/

17. Глобальний індекс кібербезпеки (GCI) Міжнародного союзу електрозв'язку https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

18. Інструмент оцінки національних стратегій кібербезпеки ENISA https://www.enisa.europa.eu/ tools/national-cybersecurity-strategies-evaluation-tool

19. Cyber Readiness Index (CRI) Potomac Institute for Policy Studies https://www.belfercenter.org/publication/cyber-readiness-index-20

20. Cybersecurity Capacity Maturity Model for Nations Global Cyber Security Capacity Centre https://gcscc.ox.ac.uk/the-cmm

21. Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. "National Cyber Power Index 2020." September 2020 https://www.belfercenter.org/publication/national-cyber-power-index-2020

22. Національний індекс кіберпотужності (NCPI) 2022 https://www.belfercenter.org/publication/national-cyber-power-index-2022

23. Cam Sivesind, Cyber Powers: Ranking the Top 30 Nations by Capabilities, Intent Sep 27, 2022.

24. 10 Guards, 30 наймогутніших кібердержав світу https://10guards.com/ua/blog/2022/10/10/the-worlds-30-cyber-superpowers/

25. Індекс кібер можливостей та національної потужності – Cyber Capabilities and National Power (CCNP), https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/

26. Çifci, Hasan, Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework. 10.21203/rs.3.rs-2159915/v1, 2022. https://www.researchgate.net/publication/364451490_Comparison_of_National-Level_Cybersecurity_and_Cyber_Power_Indices_A_Conceptual_Framework

27. Axelrod, R. *The Evolution of Cooperation.* Basic Books, 1984.

28. Eric Rasmusen's book, Games and Information: An Introduction to Game Theory. First Edition: 1989, 344 pp., ISBN: 0-631- 15709-3. Second edition: 1994, 478 pp., ISBN: 1-55786- 502- 7. Third Edition, ISBN: 0631215573, 2001. Fourth Edition, 2006, ISBN:1405136669.

29. Lin, H. S., & Zegart, A. B. (Eds.) *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.* Brookings Institution Press, 2019.

30. Kamhoua, C. A., Kwiat, K., & Hurley, P. (Eds.) *Game Theory and Machine Learning for Cyber Security.* CRC Press, 2020.

Надійшла 20.02.2025