УДК 004.056
DOI https://doi.org/10.15589/znp2025.4(502).47

# ОПТИМІЗАЦІЯ СТРАТЕГІЙ КІБЕРЗАХИСТУ: ЕКОНОМІЧНИЙ АНАЛІЗ РАЦІОНАЛЬНОСТІ В СУЧАСНИХ КІБЕРВІЙНАХ

# CYBERSECURITY STRATEGIES OPTIMIZATION: ECONOMIC ANALYSIS OF RATIONALITY IN MODERN CYBERWARS

**Yaroslava Yu. Yakovenko**[1]
yaroslavayakovenko@gmail.com
ORCID: 0000-0001-5042-2701

**Roman V. Shaptala**[2]
r.shaptala@gmail.com
ORCID: 0000-0002-4367-5775

**Я. Ю. Яковенко**[1],
доктор філософії

**Р. В. Шаптала**[2],
доктор філософії, асистент

*[1] Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk*
*[2] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv*
*[1] Кременчуцький національний університет імені Михайла Остроградського, м. Кременчук*
*[2] Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ*

**Анотація.** *Мета*. Дослідження присвячене вивченню принципів, що лежать в основі сучасних національних стратегій кібервійни, та комплексному аналізі їх ефективності. Дослідницька складова спрямована на деконструкцію військових доктрин провідних держав через призму синтезу класичних економічних інструментів, зокрема теорії ігор та аналізу витрат-вигод, з емпіричними даними, отриманими з кейс-стаді масштабних кіберконфліктів. *Методика*. Застосовано комбінацію якісних методів, зокрема порівняльний аналіз для системного зіставлення національних моделей кіберсил (США, Китай, Іран, рф, Україна) за критеріями централізації, ролі недержавних стейкхолдерів та моделі фінансування. Метод кейс-стаді використано для поглибленого вивчення масштабних кібератак, таких як Stuxnet, NotPetya та атаки на Київстар, що дозволяє наочно продемонструвати концепції асиметрії, неконтрольованої ескалації та каскадних економічних збитків у ланцюгах постачання. Системний підхід забезпечує інтеграцію теоретичних концепцій (модель Гордона-Лоеба, теорія ігор) у єдиний фрейм задля пояснення стратегічних рішень. *Результати*. Встановлено, що архітектура національних кіберсил є раціональним рішенням унікальної оптимізаційної задачі, що збалансовує бюджетні обмеження, бажаний рівень контролю та толерантність до ризику. Виявлено та обґрунтовано парадокс кіберзброї на прикладі NotPetya, де атака призвела до стратегічного економічного провалу через неконтрольовані негативні екстерналії, що завдали збитків усім, включно з союзниками агресора. Детально проаналізовано асиметрію витрат між атакуючим та захисником як ключовий економічний фактор, що пояснює перманентність кіберконфліктів низької інтенсивності. *Наукова новизна*. Уперше запропоновано комплексний підхід, який розглядає національні моделі кібервійни не як суто військові доктрини, а як стратегії, що є відповіддю на унікальні внутрішні та зовнішні виклики. Особливу увагу приділено концепції «краудсорсингової оборони» на прикладі української IT-армії як нової, економічно ефективної моделі ведення кібервійни, що дозволяє експоненційно масштабувати можливості держави за рахунок мобілізації глобального волонтерського руху. *Практична значимість*. Результати дослідження можуть бути використані для формування національних стратегій кібероборони, оптимізації бюджетного розподілу у сфері кібербезпеки та розробки моделей державно-громадського партнерства у цифровій сфері. Запропонований підхід здатен підвищити стійкість держави до кібератак та сприяти формуванню економічно збалансованої системи кіберзахисту.
**Ключові слова:** кібербезпека; економіка кібербезпеки; теорія ігор; діджиталізація; теорія прийняття рішень.

**Abstract.** *Purpose*. The study aims to examine the principles underlying modern national cyberwar strategies and to comprehensively analyse their effectiveness. The research component seeks to deconstruct the military doctrines of leading states through the synthesis of classical economic tools – specifically game theory and cost-benefit analysis – combined with empirical data from case studies of large-scale cyber conflicts. *Method*. A combination of qualitative methods is applied. Comparative analysis is used to systematically compare national models of cyber forces (the USA, China, Iran, the russian federation, and Ukraine) according to the criteria of centralisation, the role of non-state

stakeholders, and financing models. The case study method is employed for an in-depth examination of large-scale cyberattacks such as Stuxnet, NotPetya, and the cyberattack on Kyivstar, allowing clear illustration of the concepts of asymmetry, uncontrolled escalation, and cascading economic losses in supply chains. The system approach ensures the integration of theoretical concepts (Gordon–Loeb model, game theory) into a unified framework for explaining strategic decision-making. *Results*. The study shows that the architecture of national cyber forces represents a rational solution to a unique optimisation problem that balances budget constraints, the desired level of control, and risk tolerance. The cyberweapons paradox is identified and substantiated using the NotPetya case, where the attack led to a strategic economic failure due to uncontrolled negative externalities that inflicted losses on all parties, including the aggressor's allies. The cost asymmetry between the attacker and the defender is analysed in detail as a key economic factor explaining the persistence of low-intensity cyber conflicts. *Scientific novelty*. For the first time, a comprehensive approach is proposed that views national models of cyberwarfare not as purely military doctrines but as strategic responses to unique internal and external challenges. Particular attention is given to the concept of "crowdsourcing defence" exemplified by the Ukrainian IT Army as a new, cost-effective model of conducting cyberwarfare, enabling the exponential scaling of a state's cyber capabilities through the mobilisation of a global volunteer movement. *Practical importance*. The findings can be applied in the development of national cyber defence strategies, optimisation of budget allocation in the cybersecurity domain, and design of public–private partnership models in the digital sphere. The proposed framework can enhance a state's resilience to cyberattacks and support the creation of an economically balanced and sustainable cyber defence system.

**Key words:** cybersecurity; economics of cybersecurity; game theory; digitalization; decision-making theory.

## ПОСТАНОВКА ЗАДАЧІ

В умовах, коли кіберпростір став частиною інфраструктури для функціонування держав, економік та суспільств, технологічний прогрес постійно супроводжується системними вразливостями, а відтак – критичні сфери (комунікації, торгівля, транспорт тощо) знаходяться під безпосередньою загрозою інформаційних та кібервійн.

При цьому центральним аспектом для розуміння розширення театру воєнних дій за рахунок появи кіберпростору на додачу до чотирьох традиційних (земля, вода, повітря, космос) виступає необхідність розмежування інформаційних та кібервійн. Якщо перші являють собою «контентну війну», націлену впливати на індивідуальну, масову чи групову свідомість через семантичні повідомлення, що призводить до навмисного психологічного впливу чи дезінформації [1], то кібервійни характеризуються чітким цілеспрямованим деструктивним впливом на фізичну інфраструктуру і системи управління [2]. Зрозуміло, що з початком Інтернет-епохи інформаційні війни вийшли на новий рівень охоплення, інтенсивності та ефективності. Водночас, з огляду на те, що інструментарій кібервійн – не семантичні повідомлення, а програмні коди, призначені для порушення функціонування або перехоплення керування фізичною інфраструктурою, то об'єктами таких атак стають технологічні лінії, виробництва та інфраструктури соціального, воєнного та фінансового призначення на національному рівні.

З огляду на вищенаведене, можемо констатувати подвійну природу сучасних конфліктів, які відбувається одночасно в межах когнітивної (переконання) і фізичної (інфраструктура) сфер, прикладом якої виступає війна рф проти України. Відповідно, ефективна національна оборона має поєднувати протидію агресору на полі бою, в інформаційному і кіберпросторі. Більш того, з новими викликами нині стикається і архітектура міжнародної безпеки, яка історично базувалася на принципах Вестфальської системи. Мається на увазі, що Вестфальська система міжнародних відносин, яка сформувалася у XVII столітті на принципах суверенітету держав, їхній територіальній цілісності та принципі невтручання у внутрішні справи, втрачає актуальність у кіберпросторі, де держава не може гарантувати безпеку своєї інфраструктури та громадян, покладаючись лише на фізичний контроль над своєю територією. Таким чином, кіберпростір формує фундаментальний виклик основам міжнародного права та стабільності, вимагаючи нових аналітичних підходів для розуміння логіки дій у цій новій реальності.

## АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Науковий дискурс щодо кібербезпеки та кібервійни є багатогранним і розвивається на перетині кількох дисциплін, включаючи комп'ютерні науки, міжнародні відносини, економіку та право. Аналіз сучасних публікацій дозволяє виділити кілька ключових напрямів дослідження. Частину досліджень, зокрема роботи Хана З. Ф. [2] присвячено теоретичному осмисленню кібервійни як нового феномену міжнародної безпеки, у той час як Ланде Д. та Даник Ю. [1] досліджують роль штучного інтелекту в посиленні маніпулятивного впливу та автоматизації атак, що ще більше ускладнює атрибуцію та реагування.

Важливим теоретичним інструментом є теорія ігор, яка моделює стратегічну взаємодію між атакуючим та захисником. Роботи в цьому напрямі, зокрема Арсе Д. [3], підкреслюють ключову економічну особливість кіберконфлікту – асиметрію витрат: захисник змушений захищати всі потенційні вектори

атаки, тоді як атакуючому достатньо знайти лише одну вразливість.

Окремий інтерес представляють емпіричні дослідження економічних наслідків кібератак [4, 5]. Крім того, окремі дослідники, як-от Вайс М. та Крігер Н. [6], аналізують складну взаємодію між державними структурами, такими як USCYBERCOM, та приватним сектором, вказуючи на значний вплив бізнес-інтересів на формування державної політики. Існують також порівняльні дослідження [7], що описують організаційні структури кіберсил різних країн, проте вони часто обмежуються військово-політичним аналізом.

## ВІДОКРЕМЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Попри наявність окремих досліджень національних моделей кіберсил та економічних теорій кібербезпеки, у науковій літературі бракує комплексного аналізу, який би систематично застосовував економічну логіку (оптимізація витрат, управління ризиками, асиметрія) для порівняння та пояснення, чому різні держави обирають настільки відмінні архітектури своїх кіберсил. Існуючі роботи або описують моделі, або аналізують економічні теорії, але не поєднують їх для створення пояснювального фрейму. Дана стаття має на меті заповнити цю прогалину, стверджуючи, що кожна національна модель є не просто військовою доктриною, а раціональним економічним рішенням унікальної оптимізаційної задачі, що стоїть перед конкретною державою.

## МЕТА ДОСЛІДЖЕННЯ

Мета дослідження – провести порівняльний аналіз архітектур національних кіберсил через призму економічних теорій для виявлення раціональних засад, що лежать в основі їхніх стратегій, та оцінити ефективність інструментів деескалації кіберконфліктів.

## МЕТОДИ, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Об'єктом дослідження є процеси формування та функціонування національних систем кібербезпеки в умовах глобального геополітичного протистояння та мілітаризації кіберпростору.

Предметом дослідження є економічні та стратегічні принципи, що визначають архітектуру, доктрини та операційну діяльність національних кіберсил, а також економічні наслідки їх застосування.

Для досягнення поставленої мети було використано комплекс загальнонаукових та спеціальних методів дослідження: 1) порівняльний аналіз застосовувався для системного зіставлення організаційних моделей кіберсил Сполучених Штатів Америки, Китаю, Ірану, російської федерації та України. Порівняння проводилося за такими уніфікованими критеріями, як ступінь централізації управління, роль недержавних акторів, інтеграція з традиційними збройними силами та модель фінансування, що дозволило виявити ключові відмінності та спільні риси в їхніх підходах; 2) метод кейс-стаді використовувався для поглибленого аналізу окремих кібероперацій та дозволив на емпіричних прикладах проілюструвати теоретичні концепції, такі як асиметрія витрат, неконтрольована ескалація, прямі та непрямі економічні збитки, а також негативні екстерналії; 3) системний підхід забезпечив інтеграцію концепцій з різних галузей знань – економічної теорії (аналіз витрат-вигод, модель Гордона-Лоеба), теорії ігор, міжнародних відносин та комп'ютерних наук – в єдиний аналітичний фрейм

Застосування зазначених методів у комплексі дозволило забезпечити валідність та надійність отриманих результатів, а також всебічно розкрити економічну логіку, що лежить в основі сучасних стратегій ведення кібервійни.

## ОСНОВНИЙ МАТЕРІАЛ

Основними характерними рисами кібервійни є наступні [1, 6]: 1) анонімність (за рахунок використання, зламаних мереж, проксі-серверів та інших методів маскування, що ускладнює точне визначення джерела атаки); 2) невизначеність точки старту (початку атаки може передувати проникнення в систему задовго до атаки, що розмиває межі між шпигунськими та атакувальними діями); 3) знищення лог-файлів та інших цифрових слідів присутності; 4) транскордонність, що ускладнює розслідування та атрибуцію.

Вищеперелічені особливості суперечать принципу міжнародного гуманітарного права (jus ad bellum та jus in bello або право на війну та право війни), оскільки неможливість чіткої ідентифікації агресора ускладнює притягнення держави-агресора до відповідальності і унеможливлює політику стримування.

Перші дві риси забезпечують так звану «правдоподібну заперечуваність» (англ. plausible deniability), тобто відбувається здійснення ворожих дій без ризику спровокувати формальну військову відповідь чи міжнародні санкції, які при цьому досягають стратегічних цілей – дестабілізації, шпигунства, завдання економічних збитків. Іншими словами, створюється «сіра зона» перманентного конфлікту низької інтенсивності. З економічної точки зору, правдоподібна заперечуваність є механізмом зниження очікуваних витрат на агресію шляхом мінімізації ймовірності відплати. Кібератаки на енергетичну інфраструктуру України у 2015–2016 рр. являють собою ілюстративний приклад даної стратегії. Попри те, що їх приписували хакерським групам, пов'язаним з рф, відсутність прямих, а не опосередкованих доказів, не дозволив формуванню casus belli («привід для війни») для союзників України, що наочно демонструє виклик поствестфальській системі. Ситуацію ускладнює і наднаціональний характер всесвітньої мережі та унікальна структура управління нею, коли

недержавна організація ICANN (Internet Corporation for Assigned Names and Numbers), відстоюючи парадигму «один світ – один Інтернет», відкидає право держав регулювати національні сегменти Інтернету. Фактично це призводить до того, що відсутні міжнародно-правові механізми регулювання та захисту від кібердій, спрямованих проти конкретних держав, а превентивні заходи малоефективні.

Тут варто відзначити ще одну характерну рису кібервоєн – асиметричність, коли менш розвинуті у військовому чи економічному плані держави можуть створити високорівневу кіберзброю і протистояти розвиненим країнам, створюючи ілюзію вирівнювання сил. Разом з цим, розвинені країни з високотехнологічним виробництвом, потужним наукомістким сектором та значною інтеграцією інформаційних технологій усе частіше стають мішенями для кібератак з огляду на розвиток робототехніки, біотехнологій, хмарних обчислень. Більш того, посилення взаємопов'язаності елементів технологічних об'єктів підвищує імовірність «колапсних відмов», коли атака на окремий елемент може призвести до колапсу цілої системи.

Відповідно, з огляду на стратегічну важливість кіберпростору, провідні світові держави активно розбудовують мережі спеціалізованих військових та розвідувальних структур. Порівняльний аналіз моделей США, Китаю, Ірану та рф, наведений у табл.1, демонструє відмінні стратегічну культуру, політичну систему та геополітичні амбіції кожної країни щодо кіберзахисту.

Підхід США до організації кіберсил характеризується високим ступенем централізації, інституціоналізації та глибокою інтеграцією у традиційні військові структури. Центральним елементом цієї системи є Кіберкомандування Сполучених Штатів (USCYBERCOM), створене у 2009 році та підвищене у 2018 році до статусу повноцінного єдиного бойового командування Міністерства оборони. До цього цифрова служба захисту (DDS – Defence Digital Service, ЦСЗ) як підрозділ федерального уряду був уповноважений залучати перевірених хакерів до проникнення в урядові мережі. Так, у квітні 2016 року розпочався проєкт, отримавший назву «Хакни Пентагон», який виявив слабкі місця у кіберзахисті, зокрема продемонструвавши, що комп'ютери, які вважалися видимими у внутрішніх мережах ставали джерелами витоку даних. Паралельно Цифрова служба США (USDS – United States Digital Service) почала залучати цифрових фахівців для поширення смарт-технологій у федеральних агенціях та співпрацювати з офісом Кіберкомандування армії США, зокрема в рамках проєкту «Джин Ерсо» для розробки системи зламування, спрямованої для протидії безпілотникам на передовій у 2018 році. Нині USCYBERCOM відповідає за весь спектр військових операцій у кіберпросторі – від захисту інформаційних мереж Пентагону до проведення наступальних кібероперацій на підтримку бойових командувань по всьому світу. Таким чином, американська модель – високовитратна та з високим рівнем контролю, що відображає високу оцінку прямого командування та готовність нести значні постійні витрати для інституційної інтеграції. Економічна логіка тут полягає у мінімізації операційного ризику та максимізації синергії.

Важливою особливістю американської моделі є тісний зв'язок між військовими та розвідувальними операціями. Водночас, для захисту цивільної сфери

**Таблиця 1.** Порівняльна структура національних кіберсил [1; 2; 6; 8]

| Критерій порівняння | США | Китай | Іран | рф |
|---|---|---|---|---|
| Основне командування | USCYBERCOM (Єдине бойове командування) | Сили стратегічної підтримки НВАК (PLASSF) | Кіберсили Корпусу вартових Ісламської революції (IRGC) | Війська інформаційних операцій (МО рф) |
| Загальна модель | Військово-центрична, інтегрована | Централізована військова з елементами цивільно-військової фузії | Асиметрична, ідеологізована, керована КВІР | Керована спецслужбами, гібридна |
| Ключові підпорядковані підрозділи | Кіберкомандування Армії, Флоту, ВПС, Морської піхоти | Департамент мережевих систем | Організація пасивної оборони (NPDO) | Центри кіберзахисту військових округів |
| Відповідальні розвідувальні агентства | Агентство національної безпеки (NSA), Центральне розвідувальне управління (CIA) | Міністерство державної безпеки (MSS) | Міністерство розвідки (VAJA) | Федеральна служба безпеки (ФСБ), Головне управління Генштабу (ГРУ), Служба зовнішньої розвідки (СЗР) |
| Роль недержавних гравців | Переважно контрактники з приватного сектору (оборона) | «Альянс червоних хакерів» (RHA) – керована державою мережа | «Басідж» – цивільне воєнізоване ополчення, що залучає кіберволонтерів | Проксі-хакерські групи, що діють за вказівкою спецслужб |

існує окрема структура – Агентство з кібербезпеки та захисту інфраструктури (CISA), що діє в межах Міністерства національної безпеки. CISA відповідає за захист критичної інфраструктури країни та координацію заходів у цивільному секторі, що розмежовує військові та внутрішні завдання.

Китай демонструє унікальний підхід, оскільки 2015 році в рамках масштабної військової реформи було створено Сили стратегічної підтримки Народно-визвольної армії Китаю (PLASSF), що об'єднали під єдиним командуванням космічні, кібернетичні та радіоелектронні війська з метою досягнення переваги в інформаційній сфері. Відмінною рисою китайської моделі є активне залучення недержавних гравців, зокрема «Альянсу червоних хакерів» (Red Hacker Alliance), неформальною, але керованою державою мережею патріотично налаштованих хакерів як у самому Китаї, так і в китайській діаспорі по всьому світу. Така модель дозволяє зберігати певний рівень правдоподібної заперечуваності. З економічної точки зору, це гібридна модель витрат з меншим рівнем контролю. Вона використовує «безкоштовну» або низьковитратну працю (патріотичні хакери) для певних завдань, максимізуючи охоплення та правдоподібну заперечуваність, тобто відбувається оптимізація масштабу та економічної ефективності за рахунок ідеального операційного контролю.

Розвиток кібернетичних можливостей Ірану є прикладом асиметричної стратегії, сформованої як реакція на власну вразливість та зовнішній тиск, адже Іран розглядає кібератаки як інструмент національної сили, що дозволяє протистояти більш потужним супротивникам, таким як США та Ізраїль. Іранська модель, що спирається на Корпус вартових Ісламської революції та ополчення «Басідж», є прикладом економічно ефективної стратегії для держави з обмеженими економічними ресурсами, що дозволяє асиметрично проектувати силу проти багатших супротивників.

Російська модель організації кіберсил, на відміну від американської, значною мірою спирається на можливості спецслужб, а ключову роль у проведенні агресивних кібероперацій відіграють розвідувальні відомства. Така структура, де провідна роль належить розвідці, а не єдиному військовому командуванню, свідчить про те, що росія розглядає кібероперації насамперед як інструмент гібридної війни, шпигунства та політичного впливу, а не як окремий вид бойових дій, інтегрований у загальновійськові операції за американським зразком.

Кожна з цих архітектур є економічно раціональним рішенням для унікальної оптимізаційної задачі відповідної країни, що збалансовує бюджет, бажаний рівень контролю, толерантність до ризику атрибуції та наявний людський капітал

Щодо українського кіберфронту, то постійні атаки на державні установи, критичну інфраструктуру та медіапростір змусили Україну виробити власну модель національної кібероборони, що характеризується унікальною синергією між формальними державними структурами, що створювалися та реформувалися в умовах війни, та децентралізованим, глобальним волонтерським рухом, що став потужною відповіддю громадянського суспільства на агресію.

Якщо на початковому етапі російської агресії у 2014 році українська система кіберзахисту була фрагментованою, то у 2016 році було ухвалено першу «Стратегію кібербезпеки України», яка офіційно визнала кібероборону важливим елементом національної оборони. Після ухвалення у 2017 році Закону України «Про основні засади забезпечення кібербезпеки України» було розподілено повноваження між ключовими суб'єктами національної системи кібербезпеки (Держспецзв'язку було визначено відповідальним за кіберзахист державних інформаційних ресурсів та об'єктів критичної інфраструктури; Нацполіція зосередилася на боротьбі з кіберзлочинністю; СБУ отримала повноваження у сфері контррозвідки, боротьби з кібертероризмом та кібершпигунством. Варто зазначити, що згодом було проведено реформу і в Збройних Силах України з переформатуванням у 2020 році Командування Військ зв'язку та кібернетичної безпеки ЗСУ.

Разом з цим, найбільш унікальним елементом української моделі є феномен масового кіберволонтерства, втіленням якого стала ІТ-армія України, створена одразу після повномасштабного вторгнення рф у 2022 році для скоординованих DDoS-атак та інших видів кібератак на ресурси російських державних органів (сайти кремля, держдуми), бізнес-корпорацій («Газпром», «Лукойл») та банків («Сбербанк», ВТБ). Відповідно, Україна продемонструвала як держава, що зазнала нападу, може експоненційно масштабувати свої кібернетичні можливості, що створює потужну асиметричну перевагу. Іншими словами, можемо стверджувати появу нової економічної моделі «краудсорсингової оборони», яка різко знижує витрати держави на проведення наступальних операцій, мобілізуючи глобальний пул волонтерської праці.

Яскравим підтвердженням еволюції кіберзагроз як інструменту гібридної війни слугує аналіз динаміки атак на критичну інфраструктуру України в період 2023–2024 років. Статистичні дані демонструють непропорційне зростання кількості зареєстрованих інцидентів на 70 % порівняно з попереднім періодом, що суттєво перевищує середньосвітові показники [9].

Особливо показовим прикладом цілеспрямованого деструктивного впливу є масштабна кібератака на ПрАТ «Київстар» у грудні 2023 року. Цей інцидент, який з високою достовірністю (92 %) атрибутовано російській APT-групі Sandworm, мав надзвичайно високий рівень складності (9,2/10 за шкалою MITRE ATT&CK) [10]. Кібератака продемонструвала значний

каскадний ефект: окрім припинення надання послуг зв'язку для понад 24 мільйонів користувачів, було порушено роботу банківських терміналів та систем оповіщення про повітряну тривогу. Таким чином, атака на один телекомунікаційний вузол спричинила системний збій, що виходить далеко за межі комерційних збитків і має ознаки стратегічної операції, спрямованої на дестабілізацію критичних державних функцій.

Визначальні характеристики кібервійни – її перманентність, асиметричність та складність у досягненні стабільного стримування – можливо ефективно пояснити через економічну призму. Державні та недержавні актори суб'єкти, від USCYBERCOM до хакерських груп, діють як раціональні суб'єкти, що прагнуть максимізувати свою корисність (геополітичний вплив, прибуток) за наявних обмежень (витрати, ризики) [7]. При цьому інструментом оцінки ефективності кібератаки є не її технічна витонченість, а економічний вплив, що охоплює прямі фінансові втрати, системні збої та втрату довіри [6]. Глобальна вартість кіберзлочинності, що оцінюється у понад 1 трильйон доларів, підкреслює макроекономічний масштаб цієї проблеми [11].

Економічні рішення щодо національних витрат на кібербезпеку є багатоаспектним питанням, що вимагає застосування аналітичних моделей. Перший інструмент – аналіз витрат і вигод (Cost-Benefit Analysis, CBA). Раціональна інвестиція в кібербезпеку відбувається тоді, коли гранична вигода (зменшення ризику) дорівнює або перевищує граничні витрати на захід безпеки [12]. Зрозуміло, що це вимагає ідентифікації та кількісної оцінки прямих витрат (обладнання, програмне забезпечення, персонал) та непрямих витрат (втрата довіри), а потім оцінки зменшення очікуваних збитків від інвестицій [13].

Більш досконалим інструментом для оптимізації інвестицій є модель Гордона-Лоеба. Ключове положення цієї моделі полягає в тому, що, як правило, економічно недоцільно інвестувати більше ніж приблизно 37 % від очікуваних збитків від порушення безпеки [6]. Іншими словами, модель показує, що інвестиції слід спрямовувати на активи з помірною вразливістю та високою цінністю, а не лише на найбільш вразливі, що у комплексі дозволяє уникнути надмірних інвестицій, аби досягти «ідеальної» безпеки.

Нарешті, з точки зору теорії ігор [14] критичною економічною особливістю кіберконфлікту є асиметрія витрат між атакуючим та захисником, яка часто грає на користь атакуючого. Кіберконфлікт можна моделювати як некооперативну гру, де гравці (держави) приймають рішення для максимізації своїх виграшів (безпека, вплив) з огляду на очікувані дії своїх супротивників. Мається на увазі, що захисник повинен захищати всі потенційні вразливості, тоді як атакуючому достатньо знайти лише одну слабкість (проблема «найслабшої ланки» з точки зору захисника) [9]. Дана асиметрія змушує захисників постійно збільшувати витрати, тоді як атакуючі часто можуть досягти своїх цілей з набагато меншими ресурсами [14]. Певною мірою це пояснює, чому навіть наддержави зі значними бюджетами на кіберзахист залишаються вразливими.

Порівняльний аналіз, наведений у табл. 3 демонструє, що кібератака може бути точною, як у випадку Operation Orchard, або мати неконтрольоване глобальне поширення, як Stuxnet; спрямована на стратегічні військові об'єкти або на цивільну критичну інфраструктуру, як BlackEnergy. Розуміння цієї багатоаспектності є необхідною умовою для розробки адекватних стратегій захисту та міжнародних норм регулювання.

Ще один приклад – кібератака на Україну NotPetya у 2017 році, що є прикладом люстрації економічних концепцій прямих та непрямих витрат, а також негативних екстерналій, оскільки це був «вайпер», замаскований під програму-вимагач, спрямований на саботаж, а не на отримання прибутку [15].

Кібератака NotPetya – негативна екстерналія, яку вона створила для світової економіки. Шкідливе програмне забезпечення поширилося з початкових цілей в Україні (через програмне забезпечення M. E. Doc) на транснаціональні корпорації. Згадане кейс-стаді розкриває парадокс економіки кібервійни: «успішна» тактична кібератака може бути «провальною» стратегічною економічною зброєю. Метою, ймовірно, було завдати шкоди економіці та інститутам України [17], але на кожен 1 долар прямої економічної шкоди,

**Таблиця 2.** Економічні моделі для прийняття рішень щодо інвестицій у кібербезпеку [1; 3; 7; 12; 13; 14]

| Модель | Принцип | Ключові змінні | Застосування | Обмеження |
|---|---|---|---|---|
| Аналіз витрат і вигод (CBA) | Інвестувати, де гранична вигода граничних витрат | Прямі/непрямі витрати, ймовірність ризику, очікувані збитки | Фундаментальне прийняття рішень | Складність кількісної оцінки непрямих витрат та ймовірностей |
| Модель Гордона-Лоеба | Оптимізувати інвестиції на основі вразливості та потенційних збитків | Потенційні збитки, вразливість, інвестиції | Надає верхню межу для раціональних витрат | Статична модель, припускає раціональних акторів, специфічні функції ймовірності порушення |
| Теорія ігор (Атакуючий-Захисник) | Моделювати стратегічну взаємодію між раціональними супротивниками | Матриці виграшів, стратегії, витрати для атакуючого/захисника | Прогнозує рівноважні результати, інформує динамічний захист | Припускає раціональність, часто вимагає повної інформації, обчислювальна складність |

**Таблиця 3.** Аналіз кейс-стаді кібератак [4; 6; 7]

| Критерій | Stuxnet | Operation Orchard | Black Energy |
|---|---|---|---|
| Рік виявлення | 2010 | 2007 | 2015 |
| Ймовірні виконавці | США та Ізраїль | Ізраїль | російська хакерська група (Sandworm) |
| Ціль | Ядерна програма Ірану (центрифуги в Натанзі) | Сирійські системи ППО та РЛС в районі Дейр-ез-Зор | Енергетична інфраструктура України (обленерго) |
| Призначення | Багатоцільова (шпигунство та диверсія) | Атакуюча (нейтралізація ППО) | Багатоцільова (шпигунство та диверсія) |
| Складність | Дуже складна (використання 4-х 0-day вразливостей, глибокі знання ПЛК Siemens) | Дуже складна (глибокі знання систем РЕБ та ППО) | Висока (соціальна інженерія, знання систем ICS/SCADA) |
| Область дії | Глобальна (побічне зараження >100,000 систем по всьому світу, хоча ціль була місцевою) | Місцева (конкретний ядерний об'єкт Аль-Кабір) | Регіональна (половина Івано-Франківської області) |
| Ключові характеристики | USB-носії, локальна мережа | Ймовірно, радіоелектронний характер | Фішингові листи з зараженими документами |

**Таблиця 4.** Економічні збитки від інциденту NotPetya (2017) [15; 16]

| Категорія витрат | Наслідки кібератаки | Постраждалі сторони | Оцінений фінансовий вплив |
|---|---|---|---|
| Прямі витрати (Україна) | Переривання бізнесу, знищення даних, витрати на відновлення | Уряд України, банки, інфраструктура | До 0.5 % ВВП (приблизно 560 млн дол.) |
| Непрямі витрати (глобальні та побічні ефекти) | Зупинка виробництва, збій логістики, втрата доходу | Maersk, Merck, FedEx та ін. | >10 млрд дол. глобально |
| Посилення в ланцюгу постачання | Втрата прибутку клієнтів постраждалих компаній | Клієнти компаній, що постраждали | Оцінено в 7.3 млрд дол. втрат прибутку клієнтів, 4-кратний мультиплікативний ефект |
| Довгострокові втрати | Втрата контрактів з постачальниками, підвищення страхових премій, обов'язкові інвестиції в безпеку | Початково інфіковані компанії та їхні партнери | Відображено у змінених відносинах у ланцюгу постачання |

завданої основній цілі (Україні), припадає приблизно 18 доларів побічної шкоди решті світу. Відповідно, подібні кібератаки у результаті занадто неконтрольовані, щоб бути ефективними інструментами політики.

Якщо виходити з того, що кіберзброя – складна система з визначеним життєвим циклом, який можна розглядати як «виробничий процес», то цей цикл багатоетапний за своєю суттю – від визначення проєкту та розвідки до вторгнення і атаки.

Якщо сучасна кіберзброя базується на експлойтах zero-day (вразливостях, невідомих розробнику програмного забезпечення), то екосистема, що їх створює, функціонує як складний, багаторівневий ринок. Відповідно, ціни визначаються не класичним співвідношенням попиту та пропозиції, а й дефіцитністю та впливом експлойту (так, наприклад, експлойт для iPhone може коштувати 5–7 млн дол., а експлойт для Windows -до 1 млн дол. [18]). Така ринкова структура створює критичну дилему для урядів, адже експлойт є цінним, але його вартість втрачається після розкриття та виправлення. Існування прибуткового сірого ринку експлойтів zero-day діє як економічний фактор, що спричинює «відтік мізків» з оборонної екосистеми та стимулює гонку озброєнь у кіберпросторі.

На тлі ескалації кіберконфліктів та відсутності дієвих міжнародно-правових механізмів стримування, у експертному середовищі починає формуватися дискусія щодо кібермиротворчості. Дана ідея логічна, якщо виходити з того, що, коли кібервійна виходить за межі шпигунства чи пропаганди і спрямовується на критичну національну інфраструктуру, то її наслідки можуть призвести до гуманітарних катастроф. Водночас економічні санкції залишаються одним з основних реальних інструментів, що використовуються для деескалації. Застосування санкцій за кібератаки стикається з рядом проблем, зокрема проблема атрибуції ускладнює остаточне покладання відповідальності. Автократичні режими, які стоять за значною частиною державно спонсорованої кіберактивності, часто є більш стійкими до економічного тиску. Крім того, підсанкційні держави все частіше використовують цифрові активи, такі як криптовалюти, для ухилення від санкцій, що підриває їхній вплив [19].

## ОБГОВОРЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

По-перше, архітектури національних кіберсил є раціональними рішеннями унікальних оптимізаційних задач. Кожна модель, представлена в Таблиці 1, є не просто військово-технічним вибором, а відображенням глибинних політико-економічних реалій та стратегічної культури країни.

По-друге, асиметрія витрат, що моделюється теорією ігор, є ключовим економічним фактором, який пояснює перманентність кіберконфліктів. Як показано в Таблиці 2, захисник змушений інвестувати у комплексний захист, тоді як атакуючому достатньо знайти лише одну вразливість. Наведена фундаментальна асиметрія створює постійний економічний стимул для проведення атак низької та середньої інтенсивності, оскільки граничні витрати на атаку часто є значно нижчими за граничні витрати на всеохопний захист. Зокрема, це пояснює, чому навіть держави з величезними бюджетами на кібербезпеку залишаються вразливими і чому кіберпростір перебуває у стані постійного конфлікту, а не стабільного миру чи відкритої війни.

Нарешті, існування ринку експлойтів zero-day діє як економічний двигун гонки озброєнь у кіберпросторі. Для урядів це створює дилему: розкрити вразливість для її виправлення, тим самим підвищивши загальну безпеку, але втративши цінний наступальний інструмент, або зберегти її в таємниці для власних операцій, залишаючи власну інфраструктуру та громадян вразливими. Відповідно, ринкова динаміка прискорює гонку кіберозброєнь, оскільки держави змушені або купувати, або розробляти власні експлойти, щоб не відстати у військово-технологічному плані. Водночас, інструменти деескалації, такі як економічні санкції, мають обмежену ефективність через проблему атрибуції та використання підсанкційними режимами криптовалют для обходу обмежень.

## ВИСНОВКИ

Різноманітність архітектур національних кіберсил – від військово-центричної моделі США до цивільно-військової моделі Китаю – є раціональним рішенням для унікальної оптимізаційної задачі, що збалансовує витрати, контроль, ризики та наявні ресурси. Водночас інструменти деескалації, такі як економічні санкції, мають обмежену та умовну ефективність. Дослідження підтримує доцільність застосування економічних моделей (аналіз витрат-вигод, модель Гордона-Лоеба, теорія ігор) для прийняття рішень у сфері кібербезпеки. Водночас воно спростовує ідею про безмежну ефективність наступальних кібероперацій, вказуючи на їхні внутрішні економічні та стратегічні обмеження, пов'язані з ризиками неконтрольованої ескалації та побічної шкоди. Лише через комплексні зусилля в цих напрямах міжнародне співтовариство зможе зменшити ризики, пов'язані з мілітаризацією кіберпростору, та запобігти перетворенню цифрової епохи на епоху перманентної та неконтрольованої кібервійни.

## REFERENCES


[1] Lande, D., & Danyk, Y. (2025, January 6). Competitive artificial intelligence in information and cyber warfare. SSRN. https://doi.org/10.2139/ssrn.5084698

[2] Cyber Warfare and International Security: A New Geopolitical Frontier. (2025). *The Critical Review of Social Sciences Studies*, 3(2), 513–527. https://doi.org/10.59075/k9cbhz04

[3] Arce, D. (2022). Cybersecurity For Defense Economists. Defence and Peace Economics, 34(6), 705–725. https://doi.org/10.1080/10242694.2022.2138122

[4] Wang, W., Chen, X., Li, Y., & Zhu, C. (2024). Catch the Cyber Thief: A Multi-Dimensional Asymmetric Network Attack–Defense Game. *Applied Sciences*, 14(20), 9234. https://doi.org/10.3390/app14209234

[5] Kulkarni, A. N., & Fu, J. (2021). A Theory of Hypergames on Graphs for Synthesizing Dynamic Cyber Defense with Deception. 97–112. https://doi.org/10.1002/9781119723950.CH6

[6] Weiss, M., & Krieger, N. (2025). The political economy of cybersecurity: Governments, firms and opportunity structures for business power. *Contemporary Security Policy*, 46(3), 403–428. https://doi.org/10.1080/13523260.2025.2474867

[7] From Games to Gains: the Role of Game Theory and Gamification. World Wide Technology. Retrieved from: https://www.wwt.com/blog/from-games-to-gains-the-role-of-game-theory-and-gamification-in-cybersecurity-risk-management

[8] Eling, M., Elvedi, M., & Falco, G. (2022). The Economic Impact of Extreme Cyber Risk Scenarios. *North American Actuarial Journal*, 27(3), 429–443. https://doi.org/10.1080/10920277.2022.2034507

[9] KnowBe4 Report Reveals Critical Infrastructure Under Siege with Cyber Attacks Increasing

[10] 30 Percent in One Year. KnowBe4. 2024. Retrieved from: https://www.knowbe4.com/press/knowbe4-report-reveals-critical-infrastructure-under-siege-with-cyber-attacks-increasing-30-percent-in-one-year

[11] Melnyk T. (2023) Tse naibilsha u sviti khakerska ataka na telekom infrastrukturu». Pershe interviu prezydenta «Kyivstaru» pislia kiberataky, yaka paralizuvala operatora. Zhurnal Forbes Ukraine. Retrieved from: https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855 [in Ukrainian].

[12] Peters A., MacConaghy P. (2021, January 29). Unpacking US Cyber Sanctions. Third Way. Retrieved from: https://www.thirdway.org/memo/unpacking-us-cyber-sanctions

[13] The Economics of Cybersecurity: Cost-Benefit Analysis – Bangalore. Retrieved from: https://skillogic.com/blog/the-economics-of-cybersecurity-cost-benefit-analysis/

[14] Gordon, L. (2016, March 22). Learn the Fundamentals of the Gordon-Loeb Cyber Investment Model in this Interview with Professor Gordon – ActiveCyber. Retrieved from: https://activecyber.net/learn-the-fundamentals-of-the-gordon-loeb-cyber-investment-model-in-this-interview-with-professor-gordon/

[15] Fugate, S., & Ferguson-Walter, K. (2019). Artificial intelligence and game theory models for defending critical networks with cyber deception. *AI Magazine*, 40(1), 49–62. https://doi.org/10.1609/aimag.v40i1.2849

[16] Johansmeyer T. NotPetya, Ukraine, and the limits of economic impact from cyber attacks. The Loop. Retrieved from: https://theloop.ecpr.eu/notpetya-ukraine-and-the-limits-of-economic-impact-from-cyber-attacks/

[17] Crosignani M., Macchiavelli M., Silva A. (2021, July) Pirates without Borders: The Propagation of Cyberattacks. *Federal Reserve Bank of New York Staff Reports*, no. 937. Retrieved from: https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf

[18] A Closer Look at NotPetya. Portnox. Retrieved from: https://www.portnox.com/cybersecurity-101/notpetya-attack/

[19] Khalil M. (2025, September 6). Zero-Day Exploit Statistics 2025: What Defenders Need. DeepStrike. Retrieved from: https://deepstrike.io/blog/zero-day-exploit-statistics-2025

[20] The Effectiveness of Economic Sanctions At Risk from Digital Asset Growth. U.S. GAO. Retrieved from: https://www.gao.gov/blog/effectiveness-economic-sanctions-risk-digital-asset-growth

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Lande, D., & Danyk, Y. (2025, January 6). Competitive artificial intelligence in information and cyber warfare. SSRN. https://doi.org/10.2139/ssrn.5084698

[2] Cyber Warfare and International Security: A New Geopolitical Frontier. (2025). *The Critical Review of Social Sciences Studies*, 3(2), 513–527. https://doi.org/10.59075/k9cbhz04

[3] Arce, D. (2022). Cybersecurity For Defense Economists. Defence and Peace Economics, 34(6), 705–725. https://doi.org/10.1080/10242694.2022.2138122

[4] Wang, W., Chen, X., Li, Y., & Zhu, C. (2024). Catch the Cyber Thief: A Multi-Dimensional Asymmetric Network Attack–Defense Game. *Applied Sciences*, 14(20), 9234. https://doi.org/10.3390/app14209234

[5] Kulkarni, A. N., & Fu, J. (2021). A Theory of Hypergames on Graphs for Synthesizing Dynamic Cyber Defense with Deception. 97–112. https://doi.org/10.1002/9781119723950.CH6

[6] Weiss, M., & Krieger, N. (2025). The political economy of cybersecurity: Governments, firms and opportunity structures for business power. *Contemporary Security Policy*, 46(3), 403–428. https://doi.org/10.1080/13523260.2025.2474867

[7] From Games to Gains: the Role of Game Theory and Gamification. World Wide Technology. Retrieved from: https://www.wwt.com/blog/from-games-to-gains-the-role-of-game-theory-and-gamification-in-cybersecurity-risk-management

[8] Eling, M., Elvedi, M., & Falco, G. (2022). The Economic Impact of Extreme Cyber Risk Scenarios. *North American Actuarial Journal*, 27(3), 429–443. https://doi.org/10.1080/10920277.2022.2034507

[9] KnowBe4 Report Reveals Critical Infrastructure Under Siege with Cyber Attacks Increasing

[10] 30 Percent in One Year. KnowBe4. 2024. Retrieved from: https://www.knowbe4.com/press/knowbe4-report-reveals-critical-infrastructure-under-siege-with-cyber-attacks-increasing-30-percent-in-one-year

[11] Мельник, Т. (2023) Це найбільша у світі хакерська атака на телеком інфраструктуру». Перше інтерв'ю президента «Київстару» після кібератаки, яка паралізувала оператора. *Журнал Forbes Ukraine*. Retrieved from: https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855

[12] Peters A., MacConaghy P. (2021, January 29). Unpacking US Cyber Sanctions. Third Way. URL: https://www.thirdway.org/memo/unpacking-us-cyber-sanctions

[13] The Economics of Cybersecurity: Cost-Benefit Analysis – Bangalore. URL: https://skillogic.com/blog/the-economics-of-cybersecurity-cost-benefit-analysis/

[14] Gordon, L. (2016, March 22). Learn the Fundamentals of the Gordon-Loeb Cyber Investment Model in this Interview with Professor Gordon – ActiveCyber. URL: https://activecyber.net/learn-the-fundamentals-of-the-gordon-loeb-cyber-investment-model-in-this-interview-with-professor-gordon/

[15] Fugate, S., & Ferguson-Walter, K. (2019). Artificial intelligence and game theory models for defending critical networks with cyber deception. AI Magazine, 40(1), 49–62. https://doi.org/10.1609/aimag.v40i1.2849

[16] Johansmeyer, T. NotPetya, Ukraine, and the limits of economic impact from cyber attacks. The Loop. URL: https://theloop.ecpr.eu/notpetya-ukraine-and-the-limits-of-economic-impact-from-cyber-attacks/

[17] Crosignani, M., Macchiavelli, M., Silva, A. (2021, July) Pirates without Borders: The Propagation of Cyberattacks. Federal Reserve Bank of New York Staff Reports, no. 937. URL: https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf

[18] A Closer Look at NotPetya. Portnox. Retrieved from: https://www.portnox.com/cybersecurity-101/notpetya-attack/

[19] Khalil, M. (2025, September 6). Zero-Day Exploit Statistics 2025: What Defenders Need. DeepStrike. URL: https://deepstrike.io/blog/zero-day-exploit-statistics-2025

[20] The Effectiveness of Economic Sanctions At Risk from Digital Asset Growth. U.S. GAO. URL: https://www.gao.gov/blog/effectiveness-economic-sanctions-risk-digital-asset-growth


Дата надходження статті до редакції: 27.10.2025
Дата затвердження статті до друку: 18.11.2025
Опубліковано: 30.12.2025