Кіберзахист як ключовий елемент відсічі збройної агресії у кіберпросторі в системі кібероборони держави

Cyber Protection as a Key Element of Repelling Armed Aggression in Cyberspace within the State Cyber Defense System

Олег Семененко [A]

Corresponding author: Заслужений діяч науки і техніки України, д. військ. н., професор, заступник начальника інституту з наукової роботи, e-mail: aosemenenko@ukr.net, ORCID ID: https://orcid.org/0000-0001-6477-3414

Володимир Рудницький [B]

доктор технічних наук, професор, головний науковий співробітник, e-mail: rvn_2008@ukr.net, ORCID ID: https://orcid.org/0000-0003-3473-7433

Руслан Нетребко [D]

старший викладач, Житомирський військовий інститут імені С. П. Корольова, e-mail: netr_rv@ukr.net, ORCID ID: https://orcid.org/0000-0003-3212-5249

Володимир Ткач [C]

Старший науковий співробітник, e-mail: volodymyr.tkach@viti.edu.ua, ORCID ID: https://orcid.org/0000-0003-0013-7368

Ольга Шугалій [C]

старший науковий співробітник, e-mail: olga.shugaliy@gmail.com, ORCID ID: https://orcid.org/0000-0002-6587-0096

Андрій Карпенко [C]

науковий співробітник, e-mail: andriy.karpenko@viti.edu.ua, ORCID ID: https://orcid.org/0000-0002-8372-6303

Oleh Semenenko [A]

Corresponding author: Honored Worker of Science and Technology of Ukraine, Dr of Military Sciences, Professor, Deputy Head of the Institute for scientific work, e-mail: aosemenenko@ukr.net, ORCID ID: https://orcid.org/0000-0001-6477-3414

Volodymyr Rudnytskyi [B]

Dr of Technical Sciences, Professor, Chief Researcher, e-mail: rvn_2008@ukr.net, ORCID ID: https://orcid.org/0000-0003-3473-7433

Ruslan Netrebko [D]

Senior Lecturer, Zhytomyr Military Institute named after S. P. Korolev, e-mail: netr_rv@ukr.net, ORCID ID: https://orcid.org/0000-0003-3212-5249

Volodymyr Tkach [C]

Senior Researcher, e-mail: volodymyr.tkach@viti.edu.ua, ORCID ID: https://orcid.org/0000-0003-0013-7368

Olha Shuhalii [C]

Senior Researcher, e-mail: olga.shugaliy@gmail.com, ORCID ID: https://orcid.org/0000-0002-6587-0096

Andrii Karpenko [C]

Research Officer, e-mail: andriy.karpenko@viti.edu.ua, ORCID ID: https://orcid.org/0000-0002-8372-6303

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, м. Черкаси, Україна
[C] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна
[D] Житомирський військовий інститут імені С. П. Корольова, м. Житомир, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine
[C] Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
[D] Korolov Zhytomyr Military Institute, Zhytomyr, Ukraine

Received: April 19, 2026 | Revised: April 28, 2026 | Accepted: April 30, 2026

УДК 004.056:355.45

DOI: https://doi.org/10.33445/sds.2026.16.2.4

Мета роботи. Обґрунтувати визначальну роль кіберзахисту як ключового елементу відсічі збройній агресії у кіберпросторі та визначити його місце у системі кібероборони держави в умовах сучасних гібридних загроз.

Метод дослідження. Застосовано системний підхід, структурно-функціональний аналіз, метод концептуального моделювання, а також елементи порівняльного аналізу сучасних міжнародних підходів до кібербезпеки.

Результати. Обґрунтовано кіберзахист як системоутворюючий елемент кібероборони держави, що забезпечує стійкість, безперервність і керованість інформаційно-комунікаційних систем в умовах постійної кібернетичної агресії. Запропоновано концептуальну модель взаємозв'язку кіберзахисту, адаптивності та кіберстійкості.

Теоретична цінність. Розширено наукове розуміння кіберзахисту як механізму відсічі агресії, уточнено його місце в системі кібероборони та розвинено існуючі теоретичні підходи.

Purpose. To substantiate the decisive role of cyber protection as a key element of repelling armed aggression in cyberspace and to determine its place within the state cyber defense system under conditions of contemporary hybrid threats.

Method. The study employs a systems approach, structural-functional analysis, conceptual modeling, as well as elements of comparative analysis of modern international cybersecurity frameworks.

Results. The study substantiates cyber protection as a system-forming element of state cyber defense, ensuring resilience, continuity, and controllability of information systems under persistent cyber aggression. A conceptual model linking cyber protection, adaptability, and cyber resilience is proposed.

Theoretical value. The research advances the conceptualization of cyber protection from a risk-management tool to a mechanism of repelling aggression, refining its role within cyber defense systems and extending existing theoretical approaches.

Практична цінність. Результати можуть бути використані для формування політики кібероборони, стратегій кіберстійкості, захисту критичної інфраструктури та інтеграції у військове планування.
Майбутні дослідження. Доцільно зосередитись на розробленні кількісних показників, формалізації моделі та її емпіричній перевірці.
Тип статті. Теоретична.

Ключові слова: кіберборотьба, кібербезпека, кіберзахист, кібервплив, кіберпростір, кібероборона, інформаційно-комунікаційні системи, відсіч збройної агресії у кіберпросторі, система кібероборони держави.

Practical value. The findings can support the development of cyber defense policies, resilience strategies, and protection of critical infrastructure, as well as integration into military planning.
Future research. Further studies should focus on quantitative indicators, model formalization, and empirical validation.
Article type. Theoretical.

Key words: Cyber Warfare, Cybersecurity, Cyber Protection, Cyber Influence, Cyberspace, Cyber Defense Information and Communication Systems, Armed Aggression in the Cyberspace Repelling, State Cyber Defense System.

Вступ

Сучасний етап розвитку безпекового середовища характеризується стрімкою трансформацією сутності явища та особливостей перебігу збройних конфліктів сьогодення, у яких кіберпростір виступає не лише допоміжним, а самостійним середовищем протиборства. Застосування кіберзасобів дозволяє досягати стратегічних ефектів без прямого використання традиційних військових інструментів, що зумовлює зростання ролі кібероперацій у загальній системі національної безпеки.

Особливого значення ця тенденція набуває в умовах збройної агресії проти України, де кіберпростір активно використовується для здійснення комплексного впливу на державні інституції, критичну інфраструктуру та інформаційне середовище. Кібератаки супроводжують бойові дії, підсилюючи їх ефект та створюючи додаткові загрози функціонуванню держави.

У цих умовах ключовим фактором протидії виступає здатність держави забезпечити стійкість своїх інформаційно-комунікаційних систем. Саме ця здатність визначає, чи зможе держава зберегти керованість, функціонування критичної інфраструктури та стабільність суспільних процесів. Незважаючи на це, у більшості наукових досліджень кіберзахист продовжує розглядатися як допоміжний або технічний елемент, що забезпечує лише захист від загроз. Такий підхід є обмеженим, оскільки не враховує його реальної ролі у відсічі агресії.

Таким чином, виникає необхідність у формуванні нового концептуального підходу, в межах якого кіберзахист розглядатиметься як ключовий елемент системи кібероборони держави, що забезпечує відсіч збройній агресії у кіберпросторі.

Теоретичні основи дослідження

Розвиток наукових підходів до дослідження кіберпростору як середовища протиборства призвів до формування кількох базових категорій, серед яких ключове місце займають кіберборотьба, кібероборона, кіберзахист та кібервплив.

Кіберборотьба розглядається як сукупність дій, спрямованих на досягнення переваги у кіберпросторі шляхом впливу на інформаційні та комунікаційні системи противника. Вона включає як наступальні, так і оборонні компоненти, що забезпечують комплексний характер протиборства. Кібервплив, у свою чергу, спрямований на досягнення інформаційно-психологічних ефектів, впливаючи на свідомість населення, прийняття рішень та функціонування державних інститутів. Кібероборона держави є інтегрованою системою, що поєднує різні елементи забезпечення безпеки у кіберпросторі, включаючи організаційні, технічні, правові, військові, політичні, економічні та інші компоненти.

У рамках існуючих підходів кіберзахист визначається як:

система заходів захисту інформаційних ресурсів;

технічний рівень забезпечення безпеки;

механізм реагування на інциденти.

Однак такі підходи не враховують того, що у сучасних умовах ключовим є не факт відбиття окремої атаки (удару), а здатність системи функціонувати в умовах постійного впливу загроз.

Методологічною основою дослідження є системний підхід, який дозволяє розглядати кібероборону як цілісну систему взаємопов'язаних елементів. Структурно-функціональний аналіз застосовано для визначення ролі кіберзахисту у цій системі, а концептуальне моделювання – для формування узагальненої моделі його функціонування.

Крім того, використано порівняльний аналіз міжнародних підходів до кібербезпеки, зокрема рекомендацій National Institute of Standards and Technology та European Union Agency for Cybersecurity.

Постановка проблеми

Наявне протиріччя між традиційним трактуванням кіберзахисту як допоміжного елементу та його фактичною роллю у забезпеченні стійкості держави в умовах агресії. Це протиріччя проявляється у:

недооцінці його стратегічного значення;

обмеженому використанні у військовому плануванні;

відсутності чіткої концепції його ролі у кібероборони.

Вирішення означеної проблеми потребує переосмислення сутності кіберзахисту та визначення його місця у системі кібероборони.

Результати

Кіберзахист є системоутворюючим елемент системи кібероборони держави. У системі кібероборони держави кіберзахист виконує функцію базового елемента, що забезпечує її цілісність та здатність до функціонування в умовах агресивного впливу. На відміну від інших компонентів кіберборотьби, які можуть мати ситуативний або операційний характер, кіберзахист має безперервний характер і діє незалежно від фази конфлікту.

Системоутворююча роль кіберзахисту проявляється у трьох ключових вимірах.

По-перше, він забезпечує структурну стійкість інформаційно-комунікаційних систем оборонного та безпекового призначення, що означає здатність зберігати свою архітектуру та функціональні зв'язки під впливом деструктивних факторів. Це досягається через впровадження принципів сегментації, резервування, відмовостійкості та розподіленості.

По-друге, кіберзахист забезпечує функціональну безперервність, яка передбачає здатність систем виконувати свої ключові функції навіть за умов часткового порушення їх роботи. У цьому контексті важливу роль відіграють механізми відновлення, дублювання та динамічного перерозподілу ресурсів.

По-третє, він формує операційну керованість, тобто здатність органів управління зберігати контроль над процесами та приймати рішення в умовах кібернетичного впливу.

Таким чином, кіберзахист не лише забезпечує захист інформаційно-комунікаційних систем оборонного та безпекового призначення, але й визначає здатність держави до протидії агресії в цілому.

Узагальнення зазначеного дозволяє сформулювати (запропонувати) визначення кіберзахисту, з точки зору його розгляду як ключового елемента відсічі збройної агресії у кіберпросторі в системі кібероборони держави. Кіберзахист як відсіч збройній агресії у кіберпросторі – це системно організована, безперервна та адаптивна діяльність, спрямована на зрив досягнення цілей противника шляхом забезпечення стійкості, керованості та функціональної безперервності інформаційно-комунікаційних систем держави в умовах цілеспрямованого кібервпливу.

Запропоноване визначення має кілька принципових відмінностей від традиційних підходів.

По-перше, запропоноване визначення акцентує не на процесі захисту, а на результаті – відсічі агресії.

По-друге, запропоноване визначення підкреслює активний характер кіберзахисту, який полягає не лише у реагуванні, але й у створенні умов, за яких воєнна агресія у кібервпросторі втрачає ефективність.

По-третє, запропоноване визначення інтегрує технічні, організаційні та управлінські аспекти в єдину систему.

З урахуванням вище зазначеного можливо формалізувати роль кіберзахисту в системі кібероборони держави. Для формалізації ролі кіберзахисту доцільно представити процес протидії агресії в кіберпросторі у вигляді узагальненої моделі.

Процес відсічі збройної агресії у кіберпросторі можна представити у вигляді функціональної залежності:

$$R = f(C, S, A, T), \quad (1)$$

де C – рівень кіберзахисту;
S – стійкість системи кібероборони держави;
A – адаптивність;
T – інтенсивність появи (надходження) кіберзагроз.

Аналіз цієї моделі дозволяє зробити кілька висновків, а саме:

за низького рівня C система кібероборони держави переходить у стан деградації;

зростання C забезпечує нелінійне підвищення кіберстійкості інформаційно-комунікаційних систем оборонного та безпекового призначення;

адаптивність виступає мультиплікатором ефективності кіберзахисту.

Таким чином, кіберзахист виступає ключовою змінною, що визначає результат відсічі збройної агресії у кіберпросторі системою кібероборони держави.

Для подальшого дослідження доцільно надати розширену класифікацію кіберзахисту як ключового елемента відсічі збройної агресії у кіберпросторі в системі кібероборони держави.

Кіберзахист доцільно розглядати як багатовимірну систему, що включає кілька взаємопов’язаних типів.

За функціональною роллю:

1) превентивний кіберзахист спрямований на запобігання виникненню інцидентів. Його ефективність визначається рівнем підготовленості систем до потенційних загроз;

2) реактивний кіберзахист реалізується у процесі виявлення та реагування на атаки. Він забезпечує локалізацію загроз і мінімізацію наслідків;

3) адаптивний кіберзахист передбачає здатність систем змінювати свою поведінку залежно від характеру загроз. Це найбільш перспективний напрям, що базується на використанні аналітики та автоматизації.

За рівнем реалізації:

1) технічний рівень, який полягає у інфраструктурних рішеннях;

2) організаційний рівень, який полягає у процедурах та системі управління організацією кіберзахисту;

3) стратегічний, який полягає у плануванні та політиці;

4) нормативний, який полягає у правовому забезпеченні кіберзахисту.

За об’єктами:

критична інфраструктура;

військові системи;

державні інформаційні ресурси;

інформаційне середовище.

Комплексність цієї класифікації підтверджує, що кіберзахист охоплює більшість рівнів функціонування системи кібероборони держави в умовах відсічі збройної агресії у кіберпросторі.

Засоби кіберзахисту є інструментами загальної системи кібероборони держави, саме вони формують практичну основу реалізації відсічі збройної агресії у кіберпросторі.

Технічні засоби забезпечують безпосередній захист інфраструктури, включаючи системи виявлення вторгнень, засоби контролю доступу та криптографічний захист інформації (даних).

Аналітичні засоби дозволяють прогнозувати та виявляти загрози на ранніх етапах, що суттєво підвищує ефективність реагування.

Організаційні засоби визначають порядок взаємодії суб'єктів системи кібероборони держави (системи забезпечення кібербезпеки України), забезпечуючи узгодженість дій щодо кіберзахисту інформаційно-комунікаційних системи оборонного та безпекового призначення.

Нормативні засоби створюють правову основу функціонування системи кібероборони України.

Синергія зазначених засобів кіберзахисту забезпечує досягнення головного результату – зниження ефективності воєнної агресії противника у кіберпросторі.

Системну роль кіберзахисту у загальній системі кібероборони держави наведено у табл.

Таблиця: Роль кіберзахисту у загальній системі кібероборони держави

Компонент	Рівень	Функція	Результат	Залежність
Кіберборотьба	Операційний	Активна протидія	Нейтралізація	Висока
Кібервплив	Стратегічний	Вплив	Дестабілізація	Середня
Кіберзахист	*Базовий*	*Стійкість*	*Відсіч*	*Ключова*

Джерело: розроблено авторами

Наведена вище таблиця демонструє той факт, що кіберзахист є фундаментом загальної системи кібероборони держави.

Результати аналізу практики кіберзахисту під час відсічі збройної агресії у кіберпросторі(кейс-стаді) підтверджують наведені вище теоретичні положення, а саме:

кібератаки на енергетичну інфраструктуру України показали, що навіть у разі проникнення противника ефективний кіберзахист дозволяє відновити функціонування систем;

Wiper-атаки 2022 року продемонстрували важливість резервування та відновлення файлових структур інформаційно-комунікаційних систем критичної інфраструктури держави;

DDoS-атаки на початку широкомасштабного вторгнення в Україну у 2022 році підтвердили значення масштабованості та розподіленості систем кіберзахисту.

У всіх випадках кіберзахист забезпечував саме відсіч збройної агресії у кіберпросторі, а не лише реагування на кіберінциденти.

Доцільним у контексті мети дослідження є аналіз організації кіберзахисту в Україні. Система кіберзахисту України має багаторівневу структуру, що включає державні, військові та спеціалізовані органи, зокрема Державна служба спеціального зв'язку та захисту інформації України та Служба безпеки України.

Особливістю системи організації кіберзахисту в Україні є:

інтеграція різних секторів (зокрема приватного та державного);

орієнтація на реальні загрози кібербезпеці;

розвиток міжнародної взаємодії з державами-партнерами щодо питань кбіероборони.

Зазначені особливості забезпечують підвищену ефективність кіберзахисту як

інструменту відсічі збройної агресії у кіберпросторі.

Таким чином, проведений аналіз дозволяє стверджувати, що кіберзахист відіграє такі ключові функції у системі кібероборони держави:

1) визначає стійкість систем;

2) забезпечує безперервність функціонування інформаційно-комунікаційних систем оборонного та безпекового призначення;

3) знижує ефективність агресії у кіберпросторі.

Отже, кіберзахист виступає ключовим механізмом відсічі збройної агресії у кіберпросторі в системі кібероборони держави.

Обговорення

Отримані результати дослідження загалом підтверджують вихідну гіпотезу про системоутворюючу роль кіберзахисту в архітектурі кібероборони держави, однак їх інтерпретація потребує критичного співставлення з існуючими науковими підходами та уточнення низки концептуальних положень.

1. Співвідношення з усталеними теоретичними підходами

У роботі обґрунтовано перехід від ризик-орієнтованої парадигми до результат-орієнтованої (відсіч агресії). Така позиція є методологічно виправданою в умовах війни, проте вона містить певну *неявну передумову*: що управління ризиками не здатне забезпечити операційну ефективність у конфлікті. Це твердження є частково спрощеним.

Фактично сучасні підходи (зокрема NIST, ENISA) вже еволюціонують у напрямі resilience-based security, де акцент робиться не лише на мінімізації ризиків, а й на забезпеченні стійкості та безперервності. Таким чином, запропонована авторами концепція не є повністю альтернативною, а радше:

розширює існуючі моделі;

зміщує акценти з превенції на функціонування в умовах атаки.

Отже, твердження про принципову новизну підходу слід дещо пом’якшити або чіткіше позиціонувати як контекстуальну трансформацію (для умов збройної агресії), а не універсальну заміну існуючих моделей.

2. Логіка причинно-наслідкових зв’язків

У роботі встановлено залежність між рівнем кіберзахисту та здатністю системи до відсічі агресії. Однак тут наявна потенційна методологічна проблема:

кіберзахист розглядається як ключова змінна, тоді як інші фактори (кіберрозвідка, наступальні кібероперації, управління, людський фактор) фактично залишаються поза моделлю;

існує ризик надмірної редукції складної системи до одного домінуючого елемента.

Альтернативна інтерпретація:

кіберзахист є не стільки “визначальним”, скільки необхідною, але недостатньою умовою ефективної кібероборони.

Для посилення аргументації доцільно:

розширити модель, включивши щонайменше:

наступальні спроможності;

систему управління;

людський фактор;

або чітко обґрунтувати, чому саме кіберзахист виступає домінуючим елементом.

3. Концепт “відсічі агресії” у кіберпросторі

Ключовою теоретичною новацією є інтерпретація кіберзахисту як механізму «відсічі». Проте саме поняття “відсіч” у кіберпросторі має неоднозначний статус:

у класичному військовому розумінні відсіч передбачає примушення противника до припинення дій;

у кіберпросторі ж частіше йдеться про:

деградацію ефектів атак;

обмеження їх наслідків;

забезпечення функціонування систем.

Отже, виникає питання:

чи коректно ототожнювати стійкість системи з відсіччю агресії?

Альтернативна позиція:

кіберзахист забезпечує "операційну стійкість", але не завжди — "відсіч" у повному розумінні;

відсіч у кіберпросторі, ймовірно, є результатом комбінації оборонних і наступальних дій.

Це є важливою концептуальною "сліпою зоною", яку варто уточнити.

4. Оцінка запропонованої класифікації

Запропонована багатовимірна класифікація кіберзахисту (за функціями, рівнями, об'єктами) є логічно узгодженою та відповідає системному підходу. Водночас:

вона має описовий характер і не забезпечує можливості кількісної оцінки;

між рівнями (технічний, організаційний, стратегічний) відсутні чіткі критерії розмежування.

Для підвищення наукової цінності доцільно:

ввести метрики ефективності (KPI, KRI);

визначити індикатори переходу між рівнями зрілості;

інтегрувати класифікацію з відомими моделями (наприклад, maturity models).

5. Практична верифікація результатів

Посилання на кейси (енергетична інфраструктура, Wiper-атаки, DDoS) є доречним, однак їх використання має обмеження:

відсутня формалізована методика аналізу кейсів;

не визначено, які саме параметри кіберзахисту вплинули на результат;

можливий ефект підтверджувального упередження (обрані приклади підтверджують тезу).

Для посилення доказовості варто:

застосувати case study methodology з чіткими критеріями відбору;

порівняти випадки успішного та неуспішного кіберзахисту;

використати кількісні дані (час відновлення, втрати, масштаб впливу).

6. Обмеження дослідження

На основі аналізу можна виділити ключові обмеження:

1. Теоретичний характер моделі без емпіричної валідації.
2. Відсутність кількісних показників кіберстійкості.
3. Часткова редукція складної системи до одного домінуючого елементу.
4. Недостатня операціоналізація поняття "відсіч агресії".

Визнання цих обмежень підвищить академічну доброчесність і наукову вагу роботи.

7. Імплікації для теорії та практики

З теоретичної точки зору результати:

розширюють розуміння кіберзахисту як динамічної системи, а не набору засобів;

інтегрують його у контекст операційного мистецтва та стратегії.

З практичної точки зору:

обґрунтовується необхідність включення кіберзахисту до військового планування;

підкреслюється роль адаптивності та безперервності як ключових характеристик систем.

Водночас для реального впровадження необхідний перехід:

від концептуальної моделі → до інструментів оцінювання;

від якісних описів → до кількісних показників.

Запропонована у статті концепція є методологічно перспективною та відповідає сучасним трансформаціям безпекового середовища, однак потребує подальшої теоретичної конкретизації та емпіричної верифікації. Її наукова новизна полягає не стільки у повному запереченні існуючих підходів, скільки у їх переосмисленні в умовах високої інтенсивності кіберпротиборства та збройної агресії .

Для підвищення наукової якості роботи доцільно:

розширити модель системи кібероборони;

уточнити понятійний апарат;

забезпечити кількісну операціоналізацію ключових категорій;

посилити емпіричну базу дослідження.

Це дозволить перевести запропоновану концепцію з рівня теоретичного узагальнення до рівня прикладного інструменту стратегічного та операційного управління у сфері кібероборони.

Висновки

Отримані результати дозволяють критично переосмислити існуючі підходи до кіберзахисту.

У межах підходів, запропонованих National Institute of Standards and Technology та European Union Agency for Cybersecurity, кіберзахист розглядається як елемент управління ризиками. Основний акцент робиться на ідентифікації загроз, їх аналізі та мінімізації наслідків.

Такий підхід є ефективним у мирний час, однак має обмеження в умовах збройної агресії, де загрози мають системний і безперервний характер. Запропонована у статті концепція змінює фокус з управління ризиками на забезпечення результату – відсічі збройної агресії у кіберпросторі. Ключова відмінність полягає у переході:

від реактивності до стійкості;

від локального кіберзахисту до системної здатності функціонувати в умовах кібервпливів противника;

від мінімізації ризиків до зриву цілей противника.

Особливе значення має поняття адаптивності, яке дозволяє системі кібероборони змінювати свою поведінку залежно від характеру загроз. У цьому контексті кіберзахист виступає динамічною системою, що постійно еволюціонує. Крім того, результати дослідження свідчать про необхідність інтеграції кіберзахисту у планування військових операцій. Це означає, що він має розглядатися не лише як технічна функція, а як елемент оперативного мистецтва.

Для України ця концепція має особливе значення, оскільки кіберпростір є одним із ключових напрямів агресії російської федерації. У цих умовах ефективність кіберзахисту безпосередньо визначає здатність системи кібероборони держави до функціонування. Разом із тим, слід зазначити, що запропонований підхід потребує подальшого розвитку, зокрема у частині кількісної оцінки ефективності кіберзахисту та формалізації моделей його застосування.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. North Atlantic Treaty Organization. (2017). Талліннський посібник 2.0 з міжнародного права, застосовного до кібероперацій. Cambridge University Press.
2. National Institute of Standards and Technology. (2018). Рамкова основа для вдосконалення кібербезпеки критичної інфраструктури. URL: https://www.nist.gov

3. National Institute of Standards and Technology. (2020). Засоби контролю безпеки та конфіденційності інформаційних систем (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5
4. European Union Agency for Cybersecurity. (2023). Звіт про кіберзагрози ENISA 2023. URL: https://www.enisa.europa.eu
5. European Union Agency for Cybersecurity. (2021). Кібербезпека та стійкість критичної інфраструктури. URL: https://www.enisa.europa.eu
6. International Telecommunication Union. (2020). Глобальний індекс кібербезпеки 2020. URL: https://www.itu.int
7. World Economic Forum. (2024). Глобальний огляд кібербезпеки 2024. URL: https://www.weforum.org
8. United Nations Institute for Disarmament Research. (2021). Звіт про кіберстабільність і міжнародну безпеку. URL: https://www.unidir.org
9. Microsoft. (2023). Звіт Microsoft про цифрову оборону 2023. URL: https://www.microsoft.com
10. IBM. (2023). Звіт про вартість витоку даних 2023. URL: https://www.ibm.com
11. CrowdStrike. (2024). Глобальний звіт про кіберзагрози 2024. URL: https://www.crowdstrike.com
12. Verizon. (2023). Звіт про розслідування витоків даних 2023. URL: https://www.verizon.com
13. FireEye. (2022). Звіт M-Trends 2022. URL: https://www.mandiant.com
14. Singer, P. W., & Friedman, A. (2014). Кібербезпека та кібервійна: що кожен повинен знати. Oxford University Press.
15. Rid, T. (2013). Кібервійна не відбудеться. Oxford University Press.
16. Libicki, M. C. (2009). Кіберстримування та кібервійна. RAND Corporation. URL: https://www.rand.org
17. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Системи управління інформаційною безпекою. Вимоги.
18. International Organization for Standardization. (2022b). ISO/IEC 27002:2022 Засоби контролю інформаційної безпеки.
19. North Atlantic Treaty Organization. (2022). Звіт про реалізацію Пакту кібероборони НАТО.
20. World Bank. (2022). Оцінка спроможностей кібербезпеки держав. URL: https://www.worldbank.org
21. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
22. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 15 бер. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
23. Державна служба спеціального зв'язку та захисту інформації України. Офіційні матеріали та аналітичні звіти. URL: https://cip.gov.ua
24. Служба безпеки України. Аналітичні матеріали з кібербезпеки. URL: https://ssu.gov.ua.

References

1. North Atlantic Treaty Organization. (2017). The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
2. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. U.S. Department of Commerce. URL: https://www.nist.gov
3. National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5
4. European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023.

URL: https://www.enisa.europa.eu
5. European Union Agency for Cybersecurity. (2021). Cybersecurity and Resilience of Critical Infrastructure. URL: https://www.enisa.europa.eu
6. International Telecommunication Union. (2020). Global Cybersecurity Index 2020. URL: https://www.itu.int
7. World Economic Forum. (2024). Global Cybersecurity Outlook 2024. https://www.weforum.org
8. United Nations Institute for Disarmament Research. (2021). Cyber Stability and International Security Report. URL: https://www.unidir.org
9. Microsoft. (2023). Microsoft Digital Defense Report 2023. URL: https://www.microsoft.com
10. IBM. (2023). Cost of a Data Breach Report 2023. URL: https://www.ibm.com
11. CrowdStrike. (2024). Global Threat Report 2024. URL: https://www.crowdstrike.com.
12. Verizon. (2023). Data Breach Investigations Report 2023. URL: https://www.verizon.com
13. FireEye. (2022). M-Trends 2022 Report. URL: https://www.mandiant.com
14. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
15. Rid, T. (2013). Cyber war will not take place. Oxford University Press.
16. Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation. URL: https://www.rand.org
17. International Organization for Standardization. (2022a). ISO/IEC 27001:2022 Information security management systems — Requirements.
18. International Organization for Standardization. (2022b). ISO/IEC 27002:2022 Information security controls.
19. North Atlantic Treaty Organization. (2022). Cyber Defence Pledge: Progress Report.
20. World Bank. (2022). Cybersecurity Capacity Review. URL: https://www.worldbank.org
21. Ukraine. (2021). Cybersecurity Strategy of Ukraine.
22. Ukraine. (2017). Law of Ukraine on the Basic Principles of Cybersecurity of Ukraine.
23. State Service of Special Communication and Information Protection of Ukraine. Official publications and analytical materials. URL: https://cip.gov.ua.
24. Security Service of Ukraine. Cybersecurity analytical materials. URL: https://ssu.gov.ua.