# Концептуальні підходи до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення

# Conceptual Approaches to the Assessment of the Effectiveness of Cyber Warfare in Military Information and Communication Systems

**Олексій Соломицький** [A]
**Corresponding author:** доктор військових наук, професор, начальник відділу – заступник начальника управління, e-mail: solosa1@gmail.com, ORCID ID: https://orcid.org/0000-0001-8061-8895

**Ярослав Янковий** [B]
ад'юнкт інституту стратегічних комунікацій, e-mail: ya.yankovyi@gmail.com, ORCID ID: https://orcid.org/0009-0007-1718-3607

**Юзеф Добровольський** [C]
кандидат технічних наук, доцент, заступник начальника кафедри, e-mail: kataza@i.ua, ORCID ID: https://orcid.org/0000-0002-1077-1402

**Артем Семененко** [D]
Курсант Військовий інститут Київського національного університету імені Тараса Шевченка, e-mail: aretemsemen1612@gmail.com, ORCID ID: https://orcid.org/0009-0006-2753-5648

**Алевтина Гетьман** [F]
старший науковий співробітник, e-mail: getman2017@gmail.com, ORCID ID: https://orcid.org/0000-0002-6397-7412

**Володимир Мусієнко** [F]
старший науковий співробітник, e-mail: volodymyr.musienko@viti.edu.ua, ORCID ID: https://orcid.org/0000-0002-4909-6045

**Oleksii Solomitskyi** [A]
**Corresponding author:** Dr of Military Sciences, Professor, Head of Research Branch, e-mail: solosa1@gmail.com, ORCID ID: https://orcid.org/0000-0001-8061-8895

**Yaroslav Yankovyi** [B]
PhD researcher at the Institute of Strategic Communications, e-mail: ya.yankovyi@gmail.com, ORCID ID: https://orcid.org/0009-0007-1718-3607

**Yuzef Dobrovolskyi** [C]
Candidate of Technical Sciences, Associate Professor, e-mail: kataza@i.ua, ORCID ID: https://orcid.org/0000-0002-1077-1402

**Artem Semenenko** [D]
Cadet Military Institute of Taras Shevchenko National University of Kyiv, e-mail: aretemsemen1612@gmail.com, ORCID ID: https://orcid.org/0009-0006-2753-5648

**Alevtyna Hetman** [F]
Senior Research Fellow, e-mail: getman2017@gmail.com, ORCID ID: https://orcid.org/0000-0002-6397-7412

**Volodimir Musienko** [F]
Doctor of Philosophy, e-mail: volodymyr.musienko@viti.edu.ua, ORCID ID: https://orcid.org/0000-0002-4909-6045

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Національний університет оборони України, м. Київ, Україна
[C] Кафедра військової підготовки Державного університету Київський авіаційний університет", м. Київ, Україна
[D] Військовий інститут Київського національного університету імені Тараса Шевченка, Київ, Україна
[F] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] National Defense University of Ukraine, Kyiv, Ukraine
[C] Department of Military Training, State University "Kyiv Aviation University", Kyiv, Ukraine
[D] Military Institute of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[F] Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Kyiv, Ukraine

**Received:** February 17, 2026 | Revised: February 27, 2026 | Accepted: February 28, 2026

**УДК** 004.056:355.4:519.87

**DOI:** https://doi.org/10.33445/sds.2026.16.1.24

**Мета роботи.** Аналіз, узагальнення, систематизація та порівняння концептуальних підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення, зокрема інформаційних технологій та математичних моделей.

**Метод дослідження.** Загальнонаукові теоретичні методи дослідження: аналіз, узагальнення, систематизація та порівняння, які дозволяють комплексно досліджувати ключові риси та відмінності концептуальних підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення.

**Практична цінність дослідження.** Визначається можливістю використання результатів дослідження під час розроблення та вдосконалення систем підтримки ухвалення рішень, математичних моделей конкретних

**Purpose.** To analyze, generalize, systematize, and compare conceptual approaches to assessing the effectiveness of conducting cyber warfare in military information and communication systems, including relevant information technologies and mathematical models.

**Method.** General scientific theoretical research methods were employed, including analysis, generalization, systematization, and comparison, which enable a comprehensive examination of the key features and differences among conceptual approaches to assessing the effectiveness of conducting cyber warfare in military information and communication systems.

**Practical implications.** It is determined by the possibility of applying the research results in the development and improvement of decision support systems, mathematical models of specific cyber warfare processes, the planning of cyber defense

процесів ведення кіберборотьби, планування заходів кібероборони та оцінювання ефективності дій у межах сучасних гібридних воєнних конфліктів.

**Майбутні дослідження.** полягають у впровадженні отриманих результатів у практику моделювання та оцінювання ефективності перебігу та результатів ведення кіберборотьби органами військового управління усіх ланок управління.

**Тип статті.** Теоретичний.

***Ключові слова:*** інформаційна безпека, інформаційні технології, інформаційний простір кіберборотьба, кібербезпека, кіберзахист, кібероборона, кіберпростір, кібервплив, кіберрозвідка, оцінювання ефективності, прогнозування, математична модель, моделювання, штучний інтелект.

measures, and the assessment of the effectiveness of actions within the framework of contemporary hybrid military conflicts.

**Future research.** Consist in the implementation of the obtained results into the practice of modeling and assessing the effectiveness of the course and outcomes of conducting cyber warfare by military command authorities at all levels of command.

**Paper type.** Theoretical.

***Key words:*** Artificial Intelligence, Information Security, Information Technologies, Information Space, Cyber Warfare, Cybersecurity, Cyber Defense, Cyber Protection, Cyberspace, Cyber Influence, Cyber Intelligence, Effectiveness Evaluation, Forecasting, Mathematical Model, Modelling.

## *Вступ*

В умовах зростання ролі кіберпростору як окремого операційного середовища сучасних воєнних конфліктів особливої актуальності набуває проблема оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення. Інформаційно-комунікаційні системи військового призначення виступають критично важливим елементом системи управління військами, забезпечення розвідки, зв'язку, обміну даними та прийняття управлінських рішень, що безпосередньо впливає на результативність виконання бойових завдань. У зв'язку з цим кіберборотьба розглядається не лише як допоміжний інструмент впливу, а як повноцінна складова протиборства, спрямована на зниження функціональної спроможності інформаційно-комунікаційних систем противника та забезпечення стійкості власних систем.

Складність оцінювання ефективності ведення кіберборотьби зумовлена високою динамічністю середовища кіберпростору, невизначеністю параметрів впливу, наявністю випадкових та незалежних чинників, а також багатофакторністю процесів функціонування інформаційно-комунікаційних систем військового призначення. Традиційні підходи до оцінювання ефективності, що базуються на статичних показниках або детермінованих моделях, не в повній мірі враховують стохастичний характер кібервпливів та нелінійну динаміку змін станів системи. У зв'язку з цим виникає потреба у розробленні науково обґрунтованих методичних підходів, які дозволять комплексно оцінювати ефективність ведення кіберборотьби з урахуванням змін рівня працездатності, кіберстійкості та здатності системи до відновлення в умовах інтенсивного кібервпливу противника.

Таким чином, формування формалізованого підходу до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення є актуальним науковим завданням, вирішення якого сприятиме підвищенню обґрунтованості управлінських рішень, оптимізації розподілу ресурсів кіберзахисту та підвищенню загальної стійкості військових систем управління в умовах сучасного збройного протиборства.

Для цього необхідним є аналіз, узагальнення, систематизація та порівняння концептуальних підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення, зокрема інформаційних технологій та математичних моделей.

Метою статті є аналіз, узагальнення, систематизація та порівняння концептуальних підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення, зокрема інформаційних технологій та математичних моделей.

## *Теоретичні основи дослідження*

З метою визначення ступеня наукової розробленості проблематики оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення, а також виявлення ключових підходів, результатів і наявних наукових прогалин, у межах

дослідження проведено комплексний аналіз вітчизняних та іноземних наукових праць, нормативно-правових документів і аналітичних матеріалів.

Упродовж останніх років спостерігається значне пожвавлення наукового інтересу до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних систем оборонного та безпекового призначення як окремої складової сучасних воєнних дій [1–14]. Ця тенденція обумовлена як еволюцією кіберзагроз, так і потребою військового управління в інструментарії для підтримки ухвалення рішень у складних умовах інформаційної та кібернетичної невизначеності.

Певна частина сучасних публікацій присвячена структуризації та формалізації кіберпростору як об'єкта моделювання [1–7]. Дослідники прикладних аспектів оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних систем оборонного та безпекового призначення пропонують багаторівневі моделі, що інтегрують фізичний, логічний та когнітивний рівні кіберінфраструктури, дозволяючи відбити як технічні характеристики мереж, так і поведінкові аспекти користувачів та операторів систем [8–12]. Це узгоджується з фундаментальними підходами теорії складних систем та теорії інформації, де кіберпростір розглядається як складний адаптивний континуум взаємодій.

Окремим напрямом досліджень у сфері кіберборотьби є вивчення та удосконалення (розвиток) існуючої терміносистеми (термінології), яка наразі дещо не відповідає вимогам сьогодення [13; 14].

Водночас, питання аналізу, узагальнення, систематизації та порівняння основних сучасних комп'ютерних інформаційних технологій та математичних моделей для оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення залишаться відкритим.

## *Методологія дослідження*

Методологічну основу дослідження становить поєднання системного, структурно-функціонального та міждисциплінарного підходів до аналізу процесів ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення. Такий підхід зумовлений складністю кіберпростору як середовища протиборства, яке характеризується високим рівнем динамічності, багатофакторністю та взаємозалежністю технічних, організаційних і інформаційних компонентів.

У процесі дослідження застосовано комплекс загальнонаукових методів. Метод **аналізу** використовувався для вивчення наукових праць і нормативно-аналітичних матеріалів, що стосуються моделювання кібероперацій, кіберзахисту та оцінювання ефективності функціонування інформаційно-комунікаційних систем у кіберпросторі. Метод **узагальнення** дозволив виокремити основні напрями розвитку наукових підходів до оцінювання ефективності кіберборотьби та сформувати узагальнену систему класифікації відповідних моделей.

Метод **систематизації** застосовано для впорядкування наявних концептуальних підходів до моделювання кіберпротиборства за їх функціональними та методологічними ознаками. Це дало змогу виділити групи моделей, що ґрунтуються на різних математичних та інформаційно-технологічних інструментах, зокрема імітаційному моделюванні, агентно-орієнтованих підходах, мережевому аналізі, стохастичних процесах та теорії ігор.

Метод **порівняльного аналізу** використано для визначення ключових характеристик і обмежень кожного з підходів до моделювання кібердій. Порівняння здійснювалося за такими критеріями, як здатність моделі враховувати невизначеність середовища, можливість аналізу стратегічної взаємодії сторін, рівень деталізації опису кіберінфраструктури та придатність до використання в системах підтримки ухвалення рішень.

Крім того, застосовано **елементи концептуального моделювання**, що дозволили сформувати узагальнену аналітичну схему взаємозв'язку між різними типами математичних

моделей і інформаційно-технологічних підходів до дослідження кіберпротиборства. У межах цього підходу кіберпростір розглядається як складна система взаємодії технічних, інформаційних та організаційних елементів, що функціонує в умовах постійної зміни станів та впливу випадкових факторів.

Таким чином, застосований методологічний інструментарій дозволив комплексно дослідити сучасні концептуальні підходи до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення, визначити їхні ключові характеристики, можливості застосування та методологічні обмеження.

## *Результати*

Симбіоз передових комп'ютерних інформаційних технологій з усталеним та строго доведеним математичним апаратом дослідження операцій дозволив сформувати низку взаємопов'язаних та, водночас, концептуально різних підходів до моделювання, а як наслідок і прогнозування, перебігу та результатів ведення воєнних (бойових) дій у кіберпросторі. Наразі можна виділити такі групи підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення:

інформаційно-технологічні підходи до моделювання кібердій;

агентно-орієнтовані математичні моделі;

мережеві та графові моделі кіберпростору;

математичні моделі на основі теорії ймовірностей та випадкових процесів;

ігрові та оптимізаційні моделі кіберпротиборства;

інтегровані та міждисциплінарні підходи до моделювання воєнних дій в кіберпросторі.

Інформаційно-технологічні підходи до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення. Одним із найпоширеніших напрямів є використання імітаційного моделювання на основі спеціального математичного та програмного забезпечення комп'ютерних середовищ, які відтворюють структуру кіберпростору у вигляді мережевих топологій, інформаційних потоків та взаємодії програмно-апаратних компонентів. Такі моделі дозволяють досліджувати сценарії ведення кіберборотьби (кіберзахист, кіберрозвідка, кібервплив), поширення шкідливого програмного забезпечення, вплив відмов окремих вузлів на стійкість системи в цілому. У межах цього підходу кіберпростір зазвичай подається як багаторівнева система, що включає фізичний рівень (обладнання та канали зв'язку), логічний рівень (протоколи, сервіси, програмні компоненти) та когнітивний рівень (користувачі, оператори, процеси прийняття рішень). Моделювання взаємодії між цими рівнями дає змогу аналізувати комплексний характер кібердій, зокрема поєднання технічних, організаційних та інформаційно-психологічних

Важливе місце посідають агентно-орієнтовані математичні моделі воєнних (бойових) дій у кіберпросторі, у яких учасники кіберпротиборства (атакуючі, захисники, нейтральні користувачі) подаються у вигляді автономних агентів із визначеними правилами поведінки. Такі моделі дозволяють досліджувати адаптивні стратегії, ескалацію протистояння та ефекти колективної поведінки в умовах невизначеності. Особливо цінним є те, що агентно-орієнтовані моделі можуть відтворювати асиметричний характер воєнних конфліктів у кіберпросторі, коли сторони мають різні ресурси, цілі та рівні доступу до інформації.

Мережеві та графові моделі кіберборотьби. Значна частина наукових досліджень у сфері кіберборотьби та кібероборони (кіберзахисту) ґрунтується на поданні систем (інформаційно-комунікаційних систем, автоматизованих систем управління військами та зброєю, систем підтримки прийняття рішень), що функціонують в кіберпросторі у вигляді графів, де вершини відповідають вузлам мережевої топології, а ребра – каналам зв'язку або логічним взаємозв'язкам. Такий підхід дозволяє формалізувати задачі виявлення критичних вузлів, оцінювання живучості мереж, аналізу каскадних відмов та оптимізації захисних заходів.

У військовому контексті графові моделі застосовуються для оцінювання вразливості систем управління військами та озброєнням, логістичних інформаційних систем, а також для аналізу наслідків цілеспрямованих кібервпливів на окремі елементи кіберінфраструктури. Особливу увагу приділяють динамічним графам, у яких структура мережі змінюється з часом, що відповідає реальним умовам бойових дій та активної протидії з боку противника.

Математичні моделі на основі теорії ймовірностей та теорії випадкових процесів. З огляду на високий рівень невизначеності, яка притаманна кіберпростору, дедалі ширше застосовуються стохастичні (ймовірнісні) математичні моделі. Вони дозволяють враховувати випадковий характер виявлення вразливостей інформаційної та кіберінфраструктури, успішності кібератак, часу реагування систем кіберзахисту, а також поведінки користувачів. У межах цього підходу використовується математичний апарат теорії марковських випадкових процесів, стохастичні диференціальні рівняння, а також моделі систем масового обслуговування.

Стохастичні моделі оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення є особливо корисними для аналізу довготривалих процесів кіберпротиборства, коли важливо оцінити не лише миттєвий ефект кібератаки, а й накопичувальний вплив на боєздатність системи, що функціонує в кіберпросторі. Вони також дають змогу формалізувати ризики та ймовірності досягнення противником певних цілей за різних сценаріїв розвитку подій.

Ігрові та оптимізаційні моделі кіберпротиборства. Взаємодія сторін у кіберпросторі часто має характер стратегічного протистояння, що робить доцільним застосування математичного апарату теорії ігор. Ігрові моделі дозволяють аналізувати вибір оптимальних стратегій кібератаки та кіберзахисту, розподіл обмежених ресурсів, а також умови досягнення рівноваги між сторонами.

У військових дослідженнях особливу увагу приділяють динамічним та стохастичним іграм, які враховують зміну стратегій у часі та неповну інформацію про дії противника. Такі моделі є корисними для обґрунтування рішень щодо інвестування в засоби кіберзахисту, вибору пріоритетних напрямів кібероборони та оцінювання ефективності превентивних заходів у кіберпросторі.

Інтегровані та міждисциплінарні підходи до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення. Сучасні тенденції свідчать про перехід від ізольованих моделей до інтегрованих підходів, які поєднують передові комп’ютерні інформаційні технології та математичні моделі. Такі моделі призначені для охоплення технічних, організаційних та когнітивних аспекти кібердій (кіберборотьби), а також їхній зв’язок із військовими операціями (бойовими діями) в інших операційних середовищах.

Інтегровані моделі використовуються, зокрема, для аналізу гібридних воєнних конфліктів, у яких кібердії поєднуються з інформаційно-психологічними операціями та традиційними воєнними (кінетичними) засобами. Вони дозволяють досліджувати системні ефекти, які не можуть бути виявлені в межах вузькоспеціалізованих підходів.

Узагальнена характеристика описаних вище підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення наведена в табл. 1.

**Таблиця 1:** Узагальнена характеристика концептуальних підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення

| Підхід до моделювання | Основний інструментарій | Ключові можливості | Обмеження |
|---|---|---|---|
| **Імітаційне моделювання** | Комп'ютерні симуляції, цифрові двійники | Аналіз сценаріїв кібератак, тестування заходів захисту | Високі вимоги до даних і обчислювальних ресурсів |
| **Агентно-орієнтовані моделі** | Автономні агенти, правила поведінки | Дослідження адаптивних стратегій і асиметрії | Складність калібрування моделей |
| **Мережеві (графові) моделі** | Теорія графів, мережевий аналіз | Оцінка вразливостей та живучості систем | Обмежена можливість врахування людського фактору |
| **Стохастичні моделі** | Теорія ймовірностей, випадкові процеси | Урахування невизначеності та ризиків | Складність інтерпретації результатів моделювання |
| **Ігрові моделі** | Теорія ігор, оптимізація | Аналіз стратегічної взаємодії сторін | Потреба у припущеннях щодо раціональності |
| **Інтегровані та міждисциплінарні моделі** | Поєднання імітаційних, стохастичних, ігрових і когнітивних моделей | Комплексний аналіз кібердій у взаємозв'язку з іншими операційними середовищами | Висока складність побудови та практичної реалізації |

***Джерело:*** Складено автором.

Наведені в таблиці підходи до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення не є самодостатніми та ізольованими, а розглядаються як інструментальна основа систем підтримки ухвалення рішень у сфері кібероборони. Інтегровані та міждисциплінарні моделі забезпечують можливість комплексного оцінювання обстановки в кіберпросторі, прогнозування наслідків різних варіантів дій та обґрунтування управлінських рішень в умовах невизначеності та дефіциту часу. Поєднання імітаційних, стохастичних і ігрових підходів дозволяє формувати сценарії розвитку кіберпротиборства, оцінювати ефективність альтернативних стратегій та підтримувати вибір раціональних заходів реагування на кіберзагрози з урахуванням їхнього впливу на загальну стійкість системи управління військами та ефективність виконання завдань за призначенням.

## *Обговорення*

Проведений аналіз концептуальних підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення свідчить про багатовекторність сучасних наукових досліджень у цій сфері. Систематизація існуючих моделей показує, що жоден із підходів не забезпечує універсального інструментарію для комплексного аналізу кіберпротиборства, оскільки кожен з них орієнтований на дослідження окремих аспектів функціонування кіберпростору.

Імітаційні та інформаційно-технологічні моделі є ефективними для аналізу сценаріїв розвитку кіберінцидентів і дослідження поведінки складних технічних систем. Агентно-орієнтовані підходи дозволяють моделювати адаптивні стратегії учасників кіберпротиборства та відтворювати асиметричний характер сучасних конфліктів у кіберпросторі. Водночас мережеві та графові моделі забезпечують можливість формалізації структури інформаційно-

комунікаційних систем і оцінювання їхньої вразливості до цілеспрямованих кібервпливів.

Стохастичні та ігрові моделі створюють методологічні передумови для аналізу невизначеності, ризиків та стратегічної взаємодії сторін. Разом з тим їх практичне застосування пов'язане з необхідністю формалізації значної кількості параметрів і припущень щодо поведінки системи.

Отримані результати підтверджують доцільність використання інтегрованих підходів до моделювання кібероперацій, які поєднують різні математичні та інформаційно-технологічні методи. Така інтеграція створює методологічну основу для подальшого розвитку інструментів оцінювання ефективності кібердій у складних умовах сучасного збройного протиборства.

## *Висновки*

В умовах трансформації характеру сучасних збройних конфліктів та інтеграції кіберпростору до переліку повноцінних операційних доменів ведення воєнних дій особливої наукової та практичної актуальності набуває оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення. Інформаційно-комунікаційні системи військового призначення сьогодні становлять основу функціонування систем управління військами, забезпечують циркуляцію розвідувальної інформації, підтримують процеси планування операцій, координацію сил і засобів, а також формують інформаційну основу для прийняття управлінських рішень у реальному масштабі часу. Втрата їх працездатності або зниження функціональної спроможності внаслідок кібервпливу безпосередньо впливає на здатність військових формувань виконувати покладені завдання та досягати визначених цілей.

Кіберборотьба у такому контексті виступає не лише як сукупність окремих заходів кіберзахисту або активних кібервпливів, а як системний процес протиборства, що охоплює дії щодо порушення функціонування інформаційно-комунікаційних систем противника, одночасно із забезпеченням стійкості, живучості та відновлюваності власних систем. Відповідно, оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення повинно враховувати як результати активних і пасивних заходів, так і зміну станів системи під впливом сукупності зовнішніх та внутрішніх факторів. Особливістю такого оцінювання є необхідність аналізу динамічних процесів, що відбуваються в умовах неповної інформації, випадковості подій, різнорідності кібератак та багатоваріантності сценаріїв розвитку обстановки.

Додаткову складність становить те, що процеси функціонування інформаційно-комунікаційних систем військового призначення мають нелінійний характер і залежать від значної кількості взаємопов'язаних параметрів, включаючи інтенсивність кібервпливів, швидкість реагування підрозділів кіберзахисту, рівень резервування ресурсів, здатність до локалізації та відновлення пошкоджених компонентів. Традиційні підходи, засновані на статичних або детермінованих показниках, не забезпечують достатньої глибини аналізу та не дозволяють адекватно відобразити стохастичну природу кіберпротиборства. У зв'язку з цим виникає потреба у формалізованих методичних підходах, що ґрунтуються на математичному моделюванні динаміки станів системи та враховують випадкові й незалежні чинники впливу.

Таким чином, розроблення науково обґрунтованих підходів до оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення є важливим завданням сучасної військової науки. Його вирішення сприятиме підвищенню обґрунтованості управлінських рішень, оптимізації розподілу сил і засобів у кіберпросторі, підвищенню рівня кіберстійкості військових систем управління та забезпеченню належного рівня інформаційної переваги в умовах збройного протиборства.

Оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення є ключовим елементом сучасної військової науки, що забезпечує можливість структурованого аналізу, прогнозування і підтримки ухвалення рішень у складних умовах кіберпротиборства. Систематизація сучасних підходів до Оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення дала змогу розкрити позитивні риси кожного з них, а також наявні обмеження. Таким чином, керуючись сформульованим у статті оглядом сучасних комп'ютерних інформаційних технологій та основних типів математичних моделей кіберборотьби, є можливість розроблення спеціалізованих вузькопрофільних моделей кібердій, що будуть більш адекватно відповідати процесу, який необхідно моделювати.

Перспективою подальших досліджень за означеним у статті напрямом є впровадження отриманих результатів у практику моделювання та оцінювання ефективності перебігу та результатів ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення органами військового управління усіх ланок управління. Окремим перспективним напрямом дослідження є впровадження технологій штучного інтелекту в сфері оцінювання ефективності ведення кіберборотьби в інформаційно-комунікаційних системах військового призначення.

## *Фінансування*

Це дослідження не отримало конкретної фінансової підтримки.

## *Конкуруючі інтереси*

Автори заявляють, що у них немає конкуруючих інтересів.

## *Список використаних джерел*

1. Semenenko, O., Kirsanov, S., Movchan, A., Sliusarenko, M., & Horhulenko, V. (2025). Addressing the Legal Gaps in AI Regulation for National Security: The Case of Ukraine's Defense Sector. Law, State and Telecommunications Review, 17(2), 56–85. https://doi.org/10.26512/lstr.v17i2.56351.
2. Liu M., Shore M., Yeoh W., Jiang F., Zeadally S. Toward effective cybersecurity management: a hierarchical process model with performance assessment, Journal of Cybersecurity, 2025, Vol. 11 (1). https://doi.org/10.1093/cybsec/tyaf020.
3. S. Kumar, G. Nagar. Threat Modeling for Cyber Warfare Against Less Cyber-Dependent Adversaries. Vol. 23 No. 1 (2024): Proceedings of the 23rd European Conference on Cyber Warfare and Security, 27–28 June 2024, p. 257–264. https://doi.org/10.34190/eccws.23.1.2462.
4. Калайда Ю.П. Гібридні кібератаки в умовах українсько-російської кібервійни. Інформація і право. 2025. № 4 (55). С. 205–214. https://doi.org/10.37750/2616-6798.2025.4(55).346481.
5. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
6. Semenenko O., Palamarchuk S., Poberezhets T., Palamarchuk N., Mytchenko S. Cybersecurity in Modern Armed Conflicts: Threats and Responses. International Journal of Advances in Soft Computing and its Applications. 2025. № 17(1). P. 32. https://doi.org/10.15849/IJASCA.250330.03.
7. Грабар І. Г., Грищук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. Житомир. ЖНАЕУ, 2019. 280 с.
8. Хорошко В., Шелест М., Ткач Ю. Багатоальтернативне виявлення кібератак в інформаційних мережах. Безпека інформації. 2021. № 3 (27). С.136–140. https://doi.org/10.18372/2225-

5036.27.16515.
9. Мазулевський О. Є., Жолобович Н. В. Оцінка поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 3(51). С. 34–40. https://doi.org/10.33099/2311-7249/2024-51-3-34-40.
10. Park J., Kim D., Shin D. Design and Implementation of Simulation Tool for Cyber Battle Damage Assessment Using MOCE (Measure of Cyber Effectiveness). Journal of the Korea Institute of Information Security & Cryptology. 2019. Vol. 2 (29). P. 465–472. https://doi.org/10.13089/JKIISC.2019.29.2.465.
11. Мурасов Р. К., Фараон С. І., Гук О. М. Кібербезпека критичної інфраструктури: оцінювання та управління ризиками кібератак. Сучасні інформаційні технології у сфері безпеки та оборони. 2025. № 54 (3). С. 75–83. https://doi.org/10.33099/2311-7249/2025-54-3-75-83.
12. Даник Ю.Г., Шестаков В.І., Лабунець В.О. Аналіз, оцінка та прогнозування розвитку роботизації сучасних та подальших воєнних конфліктів. Збірник наукових праць Харківського національного університету Повітряних Сил. 2025. № 1 (83). С. 89–97. https://doi.org/10.30748/zhups.2025.83.11.
13. Сніцаренко П. М., Саричев Ю. О., Гордійчук В. В. Сутність кіберпростору та його взаємозв'язок із кібернетичним простором. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 2 (50). С. 5–10. https://doi.org/10.33099/2311-7249/2024-50-2-5-10.
14. Вдовенко С. Г, Даник Ю. Г, Фараон С. І. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. Комп'ютерні науки та кібербезпека. 2019. № 1 (13). С. 17–29. https://doi.org/10.26565/2519-2310-2019-1-02.

## *References*

1. Semenenko, O., Kirsanov, S., Movchan, A., Sliusarenko, M., & Horhulenko, V., (2025). Addressing the Legal Gaps in AI Regulation for National Security: The Case of Ukraine's Defense Sector. Law, State and Telecommunications Review, 17(2), 56–85. https://doi.org/10.26512/lstr.v17i2.56351.
2. Liu M., Shore M., Yeoh W., Jiang F., Zeadally S., (2025). Toward effective cybersecurity management: a hierarchical process model with performance assessment, Journal of Cybersecurity, Vol. 11 (1). https://doi.org/10.1093/cybsec/tyaf020.
3. Kumar, S., Nagar, G. Threat Modeling for Cyber Warfare Against Less Cyber-Dependent Adversaries. Vol. 23 No. 1 (2024): Proceedings of the 23rd European Conference on Cyber Warfare and Security, 27–28 June 2024, p. 257–264. https://doi.org/10.34190/eccws.23.1.2462.
4. Kalaida Yu. P., (2025) Hybrid cyberattacks in the conditions of the ukrainian-russian cyberwar. Informatsiia i pravo, vol. 55 (4), p. 206–214. https://doi.org/10.37750/2616-6798.2025.4(55).346481.
5. Hryschuk, R. V., Danyk, Yu. H., (2016). Fundamentals of cyber security: a monograph. Zhytomyr: ZhNAEU.
6. Semenenko O., Palamarchuk S., Poberezhets T., Palamarchuk N., Mytchenko S., (2025). Cybersecurity in Modern Armed Conflicts: Threats and Responses. International Journal of Advances in Soft Computing and its Applications. 2025. № 17(1). P. 32. https://doi.org/10.15849/IJASCA.250330.03.
7. Hrabar, I. H., Hryshchuk, R. V., & Molodetska, K. V. (2019). Bezpekova synerhetyka: kibernetychnyi ta informatsiinyi aspekty. Hryshchuk, R. V. (Ed.). Zhytomyr: ZhNAEU.
8. Khoroshko V., Shelest M., Tkach Yu., (2021). Multialternative detection of cyberattacks in information networks. Ukrainian Scientific Journal of Information Security, vol. 27 (3), p. 136–140. https://doi.org/10.18372/2225-5036.27.16515.

9. Mazulevskyi, O. Ye., Zholobovych, N. V., (2024). Assessment of the current state of cyber resilience, taking into account the situation in cyberspace. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 3(51), 34–40. https://doi.org/10.33099/2311-7249/2024-51-3-34-40.
10. Park J., Kim D., Shin D. Design and Implementation of Simulation Tool for Cyber Battle Damage Assessment Using MOCE (Measure of Cyber Effectiveness)., (2019). Journal of the Korea Institute of Information Security & Cryptology. Vol. 2 (29). P. 465–472. https://doi.org/10.13089/JKIISC.2019.29.2.465.
11. Murasov R., Pharaon S., Huk O., (2025) Critical infrastructure cybersecurity: assessment and management of cyberattack risks. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, vol. 54 (3), p. 75–83. https://doi.org/10.33099/2311-7249/2025-54-3-75-83.
12. Danyk Y., Shestakov V., Labunets V., (2025). Analysis, assessment, and forecasting of the development of robotics in contemporary and future military conflicts. Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl, vol. 83 (1), p. 89–97. https://doi.org/10.30748/zhups.2025.83.11.
13. Snitsarenko, P. M., Sarychev, Yu. O., Hordiichuk, V. V., (2024). On the essence of cyber space and its relationship with cybernetic space. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 50 (2). 5–10. https://doi.org/10.33099/2311-7249/2024-50-2-5-10.
14. Vdovenko, S. H, Danyk, Yu. H, Faraon, S. I., (2019). Definitive problems of the Terms of the Sphere of Cyber security and Cyber Defense and the Ways of their solution. Kompiuterni nauky ta kiberbezpeka. 13 (1). 17–29. https://doi.org/10.26565/2519-2310-2019-1-02.