УДК: 004.01/.08+004.942 DOI: **10.33099/2311-7249/2025-53-2-51-59**

***ГОРГУЛЕНКО Владислав Андрійович,***
Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна,
https://orcid.org/0000-0001-6382-5075

***КОЛОМІЄЦЬ Богдан Іванович,***
Навчально-науковий випробувальний полігон високотехнологічного озброєння та військової техніки, Черкаси, Україна,
https://orcid.org/0009-0008-6812-1155

# ФАКТОРИ ВПЛИВУ НА ЕФЕКТИВНІСТЬ ВЕДЕННЯ КІБЕРБОРОТЬБИ В ІНТЕРЕСАХ ЗАСТОСУВАННЯ ЗБРОЙНИХ СИЛ

***Метою статті*** *є дослідження внутрішніх і зовнішніх факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил для виявлення та розкриття тих із них, усунення яких є першочерговим завданням.*

***Методи дослідження****. Під час проведення дослідження було застосовано методи SWOT-аналізу та математичну модель ієрархії з теорії системного аналізу. За допомогою методу SWOT-аналізу було сформовано множину внутрішніх та зовнішніх факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил, а використання математичної моделі ієрархії дало змогу провести їх ранжування та знайти ті фактори, усунення яких, з досить високою ймовірністю, є першочерговим.*

***Отримані результати дослідження.*** *У статті запропоновано проводити дослідження факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил в два етапи: формування множини факторів впливу на підвищення ефективності ведення кіберборотьби – проблем; виявлення та розкриття фактору (факторів), вирішення якого (яких) є обґрунтовано першочерговим. У результаті проведеного аналізу внутрішніх та зовнішніх факторів складено SWOT-матрицю факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил. Використання цього методу дало змогу не тільки сформувати множину факторів, а й визначити характер їхнього впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил. Для виконання другого етапу дослідження факторів впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил, з огляду на її раціональність, було обрано SWOT-стратегію Weaknesses-Opportunities. Виявлено зв'язки між елементами множини внутрішніх та зовнішніх факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил, складено спрямований граф взаємозв'язків. На основі спрямованого графу побудовано бінарну матрицю досяжності факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил. За допомогою застосування математичної моделі ієрархії до досліджуваної системи було отримано ранжовану ієрархію факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил, що складається з восьми рівнів, кожен з яких містить один або декілька факторів. Ієрархія є впорядкованою за критерієм пріоритетності для усунення (вирішення) версією спрямованого графу взаємозв'язків між факторами, що досліджувалися. За результатами дослідження шуканими факторами є: відсутність методичного апарату планування та управління діями сил і засобів кіберборотьби (управлінський фактор) та можливість використання наукового та інтелектуального потенціалу для удосконалення форм і способів ведення протиборства у кіберпросторі.*

***Елементи наукової новизни.*** *Запропоновано методичний підхід аналізу внутрішніх і зовнішніх факторів впливу на підвищення ефективності ведення кіберборотьби, який, на відміну від інших відомих, дав змогу врахувати природу факторів та отримати їх ранжовану ієрархію.*

***Теоретична й практична значущість викладеного у статті.*** *Цінністю отриманих результатів дослідження є визначення і розкриття внутрішнього та зовнішнього факторів, вирішення яких може привести до підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил.*

***Ключові слова:*** *ефективність, застосування збройних сил, кібербезпека, кіберборотьба, кібероборона, кіберпростір, метод аналізу ієрархій, факторний аналіз.*

## Вступ

**Постановка проблеми.** Сьогодні кібероборона є однією з невід'ємних складових забезпечення національної безпеки держави [1–2]. Відповідно, кіберборотьба являє собою процес виконання збройними силами та іншими складовими сил оборони, сили і засоби яких є носіями спроможностей з ведення протиборства у кіберпросторі, власне військових заходів з кібероборони як у мирний час, так і під час правового режиму воєнного стану (особливого періоду) [3]. Ефективне ведення кіберборотьби

передбачає досягнення успіху виділеним комплектом сил і засобів у тріаді завдань «кіберзахист – кіберрозвіка – кібервплив» [4–5]. Для оцінювання зазначеної ефективності наразі існує досить сформований науковий доробок, наприклад [6–10], який дає змогу кількісно характеризувати ступінь відповідності результатів тих чи інших кібердій завданням на їх виконання. Зокрема, у дослідженні [8] мірою ефективності ведення кіберборотьби запропоновано прийняти математичні сподівання $\widetilde{M}(P_i),\ i=\overline{1,n},\ \sum_{i=1}^{n}P_i=1,\ n=6$, яке характеризує перебування захищеної інформаційно-комунікаційної системи (далі – ІКС) $S$ (об'єкта кіберборотьби) у її можливих станах $S_1,\ldots,S_6$, фізичний зміст яких описано в авторській математичній моделі. Водночас, одним із провідних та вкрай нагальних питань сучасної воєнної науки в цілому є не лише оцінювання, а й підвищення ефективності застосування військ (сил). На ефективність ведення кіберборотьби в інтересах застосування збройних сил впливає низка зовнішніх та внутрішніх факторів, які не дають змоги повною мірою реалізовувати наявний потенціал спроможностей з ведення протиборства у кіберпросторі. Враховуючи це, актуальним науковим завданням є дослідження факторів (умов та чинників), які впливають на ефективність ведення кіберборотьби в інтересах застосування збройних сил.

**Аналіз останніх досліджень і публікацій.** Аналіз впливу факторів на ефективність функціонування складних систем (зокрема, військового призначення) є відомим способом наукового обґрунтування рекомендацій щодо її підвищення. Не виключенням зазначеному є також система підготовки й ведення кіберборотьби як підсистема загальної системи забезпечення кібербезпеки держави. Зокрема, стаття [11] висвітлює результати дослідження Р. Грищука, Р. Жовноватюка та Г. Носової щодо розкриття факторів впливу на природу виникнення гібридних загроз у кіберпросторі. У роботі [12] автором надано перелік умов та чинників, які впливають на спроможності Збройних Сил України (далі – ЗС України) у кібердомені, за декількома з яких сьогодні вже запропоновано науково-обґрунтовані рішення. На вивчення системних і персоніфікованих факторів впливу щодо процесу забезпечення кібербезпеки органів державної влади і критичної інфраструктури спрямовано увагу в праці О. Потія, О. Бакалинського, Д. Мялковського та Д. Верби [13]. В останній, колективом авторів обґрунтовано, що саме запровадження чіткої вертикалі системи кіберзахисту є ключовим для наближення до нормативного рівня кібербезпеки органів державної влади і об'єктів критичної інфраструктури держави. Дослідженням факторів, які пливають на розвиток форм і способів застосування сил оборони в умовах гібридизації збройних конфліктів займалися О. Семененко, С. Митченко, О. Водчиць, Ю. Добровольський, Р. Тарасов та Є. Лисенко [14].

Разом із тим, дослідженню факторів, які впливають на підвищення ефективності ведення кіберборотьби саме як форми воєнних (бойових) дій в контексті наростаючої гібридності сучасної війни надано значно менше уваги, що додатково підтверджує актуальність поставленого наукового завдання.

**Метою статті** є дослідження внутрішніх і зовнішніх факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил для виявлення та розкриття тих із них, усунення яких є першочерговим завданням.

## Виклад основного матеріалу дослідження

Здебільшого, дослідження факторів впливу спрямовані на пошук, виявлення та розкриття певної проблеми (сукупності проблем), вирішення (усунення) якої дало б змогу підвищити ефективність функціонування складної системи або окремих її підсистем. Такий підхід зумовлений обмеженістю в ресурсах, яка притаманна і для системи кіберборотьби ЗС України зокрема. Відповідно, дослідження щодо впливу факторів доцільно проводити за двома етапами, а саме:

1. Формування множини факторів впливу на підвищення ефективності ведення кіберборотьби – проблем.

2. Виявлення та розкриття фактору (факторів), вирішення якого (яких) є обґрунтовано першочерговим.

У процесі першого етапу, для пошуку та формулювання множини факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил пропонується скористатися методом SWOT-аналізу. Цей метод зарекомендував себе як дієвий засіб стратегічного планування розвитку складних систем. Перевагою SWOT-аналізу є те, що на відміну від решти відомих методів, які набули широкого використання в дослідженні факторів впливу на ефективність функціонування систем, що він передбачає диференціацію умов і чинників на категорії: сильні (strengths) та слабкі (weaknesses) сторони – внутрішні фактори, можливості (opportunities) та загрози (threats) – зовнішні фактори. Така його особливість дає змогу не тільки сформувати перелік (множину) факторів, а й визначити характер їхнього впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил.

Результатом виконання другого етапу має стати ранжована ієрархія факторів впливу, в якій елементом вищого рівня буде шуканий фактор (фактори), усунення якого (яких), з досить високою ймовірністю, є першочерговим для підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил. Тобто має місце задача ранжування та вибору альтернатив. Результативність та доцільність використання, у процесі вирішення таких задач, методу аналізу ієрархій (далі – МАІ), розробленого Т. Сааті [15–17], який за своєю сутністю є не тільки одним із методів дослідження впливу факторів, а й потужним інструментом ранжування альтернатив та прийняття складних багатокритеріальних рішень,

підтверджується, зокрема, у роботах [18–20]. Втім, за MAI ранжування альтернативних рішень здійснюється шляхом оцінювання ваги критеріїв, які зі свого боку є однаковими для кожної альтернативи. Альтернативами вирішення поставленого наукового завдання є ніщо інше, ніж фактори впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил. Підібрати такі критерії оцінювання альтернатив, які були б притаманні кожному із зазначених факторів, без викривлення й втрати оригінального змісту, є досить складно з огляду на їхню неоднорідність. Зважаючи на це, виконати другий етап пропонується за допомогою використання математичної моделі ієрархії.

*Перший етап (SWOT-аналіз факторів).* Загалом, метод SWOT-аналізу використовується під час стратегічного планування для відповіді на три базові запитання, які виникають під час аналізу функціонування складної системи, а саме:

з'ясування поточного стану системи шляхом оцінювання сильних і слабких сторін, можливостей та загроз;

виокремлення сильних сторін та можливостей, які майбутній стан системи може використати, а також слабких сторін і загроз, які він може пом'якшити;

прийняття рішення щодо побудови стратегії зміни стану складної системи.

*Сильні сторони (Strengths)*. Система кіберборотьби в ЗС України сьогодні є такою, що розвивається. Перш за все, в структурі Міністерства оборони України (далі – МО України) наявний головний елемент – сили і засоби безпосередньо призначені для підготовки (зокрема планування) кібероперацій та ведення кіберборотьби як під час операцій, так і в окремому порядку. З 2014 року по теперішній час згадані сили і засоби набули досить різнопланового досвіду з відсічі агресії у кіберпросторі та деструктивного впливу на кіберінфраструктуру противника. Підрозділи ЗС України, що фактично є носіями спроможностей з ведення протиборства у кіберпросторі постійно поповнюються підготовленими фахівцями за рахунок військових закладів вищої освіти. Окрім цього, в ЗС України наявна дієва мережа центрів захисту інформації та кібербезпеки, яка перешкоджає несанкціонованим втручанням в роботу ІКС та виведення їх зі сталого функціонування, а також – чіткі вимоги щодо захисту інформації на об'єктах інформаційної діяльності ЗС України. Враховуючи означене, сильними сторонами існуючої системи підготовки й ведення кіберборотьби є:

наявність сил і засобів – носіїв спроможностей з ведення протиборства у кіберпросторі;

набутий досвід ведення кіберборотьби під час відсічі збройної агресії у кіберпросторі;

налагоджений процес підготовки (навчання) військових фахівців з кібербезпеки та захисту інформації;

дієва мережа центрів захисту інформації та кібербезпеки;

чіткі вимоги до захисту інформації на об'єктах інформаційної діяльності.

*Слабкі сторони (Weaknesses)*. Нині однією із основних слабких сторін наявної системи підготовки й ведення кіберборотьби є те, що згадані вище сили і засоби розділено за різними органами військового управління (далі – ОВУ), які не є однією командною вертикаллю. Більше того, сьогодні практично відсутній методичний апарат щодо планування та управління діями сил і засобів кіберборотьби. Незважаючи на обґрунтовану необхідність наявності мережі кіберполігонів для моделювання та випробування кібертехнологій (кіберзброї), полігонна база за напрямом кіберборотьби вимагає розширення. Останнє тісно пов'язане із невизначеністю вимог (загальних, тактико-технічних та ін.) до кіберзброї та норм забезпечення нею підрозділів кіберборотьби. Також, на ефективність ведення кіберборотьби негативно впливає недосконаліть механізму залучення цивільних фахівців з кібербезпеки до виконання завдань з відсічі агресії у кіберпросторі під час правового режиму воєнного стану (особливого періоду).

Відповідно, до слабких сторін системи підготовки й ведення кіберборотьби слід віднести:

розділ сил і засобів кіберборотьби серед ОВУ різних командних вертикалей;

відсутність методичного апарату планування та управління діями сил і засобів кіберборотьби – управлінський фактор;

відсутність полігонної бази (мережі кіберполігонів) – фактор інфраструктури;

невизначеність вимог до кіберзброї та норм забезпечення нею – технологічний фактор;

механізм залучення цивільних фахівців з кібербезпеки є недосконалим – фактор персоналу.

*Можливості (Opportunities)*. Зовнішніми факторами, які можуть сприяти досягненню системою підготовки й ведення кіберборотьби ЗС України визначених цілей та завдань є наступні:

чіткий розподіл повноважень складових сектора безпеки й оборони України щодо ведення протиборства у кіберпросторі, окреслення меж відповідальності ЗС України за цим напрямом;

збільшення фінансування з державної економіки;

мобілізація цивільних фахівців з кібербезпеки до підрозділів кіберборотьби;

розвиток нормативно-правової бази щодо протиборства у кіберпросторі;

використання наукового та інтелектуального потенціалу для удосконалення форм і способів ведення протиборства у кіберпросторі;

співпраця з державами-партнерами щодо перейняття передових кібертехнологій.

*Загрози (Threats)*. Відповідно, загрозами системи підготовки й ведення кіберборотьби, з огляду на розглянуті вище фактори, є:

економічний (фінансовий) фактор набуття спроможностей з ведення протиборства у кіберпросторі та закупівлі (розроблення) кіберзброї;

недооцінювання важливості створення Кіберсил як окремого роду військ (сил) ЗС України – організаційний фактор;

заволодіння противником технологічною перевагою – технологічний фактор.

Проаналізувавши внутрішні та зовнішні фактори впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил авторами складено відповідну SWOT-матрицю (табл. 1).

Таблиця 1

SWOT-матриця факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил

| | | | | |
|---|---|---|---|---|
| Внутрішні фактори | Сильні сторони (Strengths) | | Слабкі сторони (Weaknesses) | |
| | $S_1$ | наявність сил і засобів – носіїв спроможностей з ведення протиборства у кіберпросторі; | $W_1$ | розділ сил і засобів кіберборотьби серед ОВУ; |
| | $S_2$ | набутий досвід ведення кіберборотьби під час відсічі збройної агресії у кіберпросторі; | $W_2$ | відсутність методичного апарату планування та управління діями сил і засобів кіберборотьби – управлінський фактор; |
| | $S_3$ | налагоджений процес підготовки (навчання) військових фахівців з кібербезпеки та захисту інформації; | $W_3$ | відсутність полігонної бази (мережі кіберполігонів) – фактор інфраструктури; |
| | $S_4$ | дієва мережа центрів захисту інформації та кібербезпеки; | $W_4$ | невизначеність вимог до кіберзброї та норм забезпечення нею – технологічний фактор; |
| | $S_5$ | чіткі вимоги до захисту інформації на об'єктах інформаційної діяльності. | $W_5$ | механізм залучення цивільних фахівців з кібербезпеки є недосконалим –фактор персоналу. |
| Зовнішні фактори | Можливості (Opportunities) | | Загрози (Threats) | |
| | $O_1$ | чіткий розподіл повноважень щодо ведення протиборства у кіберпросторі, окреслення меж відповідальності ЗС України; | $T_1$ | економічний (фінансовий) фактор набуття спроможностей з ведення протиборства у кіберпросторі та закупівлі (розроблення) кіберзброї; |
| | $O_2$ | збільшення фінансування з державної економіки; | | |
| | $O_3$ | мобілізація цивільних фахівців з кібербезпеки до підрозділів кіберборотьби; | $T_2$ | недооцінювання важливості створення Кіберсил як окремого роду військ (сил) ЗС України – організаційний фактор; |
| | $O_4$ | розвиток нормативно-правової бази щодо протиборства у кіберпросторі; | | |
| | $O_5$ | використання наукового та інтелектуального потенціалу для удосконалення форм і способів ведення протиборства у кіберпросторі; | $T_3$ | технологічна перевага противника – технологічний фактор. |
| | $O_6$ | співпраця з державами-партнерами щодо перейняття передових кібертехнологій. | | |

Як було попередньо означено, перевагою використання методу SWOT-аналізу для дослідження факторів впливу на ефективність функціонування складних систем, є можливість визначення не лише їх множини, а й характеру впливу, який вони здійснюють. Цю можливість реалізовано шляхом диференціації факторів впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил за категоріями: сильні та слабкі сторони, можливості та загрози. Для визначення стратегії переведення системи підготовки й ведення кіберборотьби з поточного стану в необхідний (підвищення ефективності) необхідно обрати одну з можливих, а саме:

стратегія S-O – акцент на сильні сторони для використання наявних можливостей;

стратегія W-O – подолання слабких сторін шляхом реалізації можливостей;

стратегія S-T – протидія загрозам за допомогою сильних сторін;

стратегія W-T – уникнення загроз, приведення до мінімуму слабких сторін.

Для подальшого дослідження факторів впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил, з огляду на її раціональність, було обрано стратегію W-O.

*Другий етап (побудова ранжованої ієрархії факторів).* Вихідною множиною елементів для побудови ієрархії є внутрішні фактори – слабкі сторони поточного стану системи підготовки й ведення кіберборотьби, а також зовнішні – можливості. Якщо зв'язки між елементами цієї

множини $H$ визначені, то описати її можливо у вигляді спрямованого графу та квадратної бінарної матриці залежності $B$ розмірністю $n \times n$, де $n$ – кількість факторів, які є взаємозалежними між собою. Матриця $B$ позначає наявність (або відсутність) залежності між складовими множини $H$ факторів впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил. Отже, елемент матриці залежності $b_{ij}$, $i = \overline{1,n}$, може приймати значення:

$$b_{ij} = \begin{cases} 1, \text{ якщо } i\text{-ий фактор залежить від } j\text{-го;} \\ 0, \text{ якщо } i\text{-ий фактор не залежить від } j\text{-го.} \end{cases} \quad (1)$$

Знаючи зв'язки між елементами множини $H$ факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил та, використовуючи вираз (1), авторами заповнено матрицю залежності $B$ (табл. 2).

Таблиця 2

Матриця залежності факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил

| | $W_1$ | $W_2$ | $W_3$ | $W_4$ | $W_5$ | $O_1$ | $O_2$ | $O_3$ | $O_4$ | $O_5$ | $O_6$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $W_1$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $W_2$ | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $W_3$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $W_4$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| $W_5$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| $O_1$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $O_2$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $O_3$ | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| $O_4$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $O_5$ | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| $O_6$ | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |

Відповідно до наданої вище матриці залежності, авторами складено спрямований граф взаємозв'язків між елементами множини $H$ факторів впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил (рис. 1).

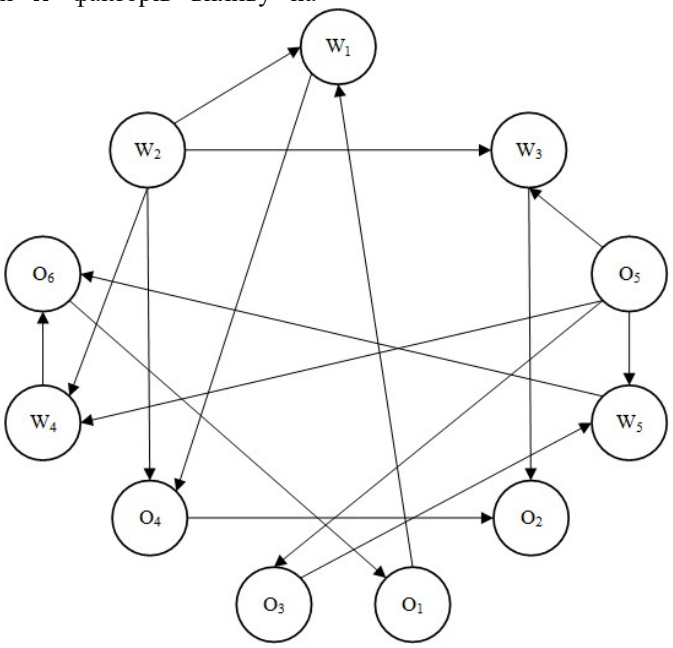


Рисунок 1 – Спрямований граф взаємозв'язків між факторами

Наступним кроком є побудова бінарної матриці досяжності $(I + B)$ відповідній матриці $B$ розмірності. Це можна реалізувати шляхом піднесення її у деякий ступінь $k$, за якого виконуватиметься рівність:

$$(I + B)^{k-1} \leq (I + B)^k = (I + B)^{k+1}. \quad (2)$$

де: $I$ – одинична матриця;

$(I + B)^k = (I + B)^{k+1}$ – матриця досяжності.

Сформувати матрицю досяжності можна й іншим шляхом, за допомогою спрямованого графу (рис. 1). У такому разі елементи матриці досяжності $d_{ij}$, $i = \overline{1,n}$, прийматимуть значення:

$$d_{ij} = \begin{cases} 1, \text{ якщо з } i\text{-го є маршрут до } j\text{-го;} \\ 0, \text{ якщо з } i\text{-го немає маршруту до } j\text{-го.} \end{cases} \quad (3)$$

Втім, за обома наданими вище варіантами побудови матриці досяжності, за незмінних вихідних даних її зміст буде однаковим (табл. 3) [розроблено авторами].

Таблиця 3

Матриця досяжності факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил

| | $W_1$ | $W_2$ | $W_3$ | $W_4$ | $W_5$ | $O_1$ | $O_2$ | $O_3$ | $O_4$ | $O_5$ | $O_6$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $W_1$ | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| $W_2$ | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| $W_3$ | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $W_4$ | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| $W_5$ | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| $O_1$ | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| $O_2$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $O_3$ | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| $O_4$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| $O_5$ | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $O_6$ | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |

Шукана ранжована ієрархія факторів впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил може бути побудована на основі матриці досяжності шляхом поділу вершин спрямованого графа (факторів) на підмножини рівнів. Для цього необхідно в ітеративному порядку визначати досяжні $R(h_i)$ й попередні $A(h_i)$ вершини для кожного фактору (табл. 4) [розроблено авторами].

Таблиця 4

Перша ітерація побудови ранжованої ієрархії факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил

| $h_i$ | $R(h_i)$ | $A(h_i)$ | $R(h_i) \cap A(h_i)$ |
|---|---|---|---|
| $W_1$ | $W_1$, $O_2$, $O_4$ | $W_1$, $W_2$, $W_4$, $W_5$, $O_1$, $O_3$, $O_5$, $O_6$ | $W_1$ |
| $W_2$ | $W_1$, $W_2$, $W_3$, $W_4$, $O_1$, $O_2$, $O_4$, $O_6$ | $W_2$ | $W_2$ |
| $W_3$ | $W_3$, $O_2$ | $W_2$, $W_3$, $O_5$ | $W_3$ |
| $W_4$ | $W_1$, $W_4$, $O_1$, $O_2$, $O_4$, $O_6$ | $W_2$, $W_4$, $O_5$ | $W_4$ |
| $W_5$ | $W_1$, $W_5$, $O_1$, $O_2$, $O_4$, $O_6$ | $W_5$, $W_3$, $O_5$ | $W_5$ |
| $O_1$ | $W_1$, $O_1$, $O_2$, $O_4$ | $W_2$, $W_4$, $W_5$, $O_1$, $O_3$, $O_5$, $O_6$ | $O_1$ |
| $O_2$ | $O_2$ | $W_1$, $W_2$, $W_3$, $W_4$, $W_5$, $O_1$, $O_2$, $O_3$, $O_4$, $O_5$, $O_6$ | $O_2$ |
| $O_3$ | $W_1$, $W_5$, $O_1$, $O_2$, $O_3$, $O_4$, $O_6$ | $O_3$, $O_5$ | $O_3$ |
| $O_4$ | $O_2$, $O_4$ | $W_1$, $W_2$, $W_4$, $W_5$, $O_1$, $O_3$, $O_4$, $O_5$, $O_6$ | $O_4$ |
| $O_5$ | $W_1$, $W_3$, $W_4$, $W_5$, $O_1$, $O_2$, $O_3$, $O_4$, $O_5$, $O_6$ | $O_5$ | $O_5$ |
| $O_6$ | $W_1$, $O_1$, $O_2$, $O_4$, $O_6$ | $W_2$, $W_4$, $W_5$, $O_3$, $O_5$, $O_6$ | $O_6$ |

На кожному кроці ітерації, факторами поточного рівня будуть ті, для яких виконуватиметься рівність:

$$A(h_i) = R(h_i) \cap A(h_i), \qquad (4),$$

тобто рівнем ієрархії вважатимемо множину тих вершин, які є недосяжними з решти вершин множини $H$. Як видно з табл. 4, вершинами (факторами) першого рівня ієрархії є:

$W_2$ – відсутність методичного апарату планування та управління діями сил і засобів кіберборотьби – управлінський фактор;

$O_5$ – використання наукового та інтелектуального потенціалу для удосконалення форм і способів ведення протиборства у кіберпросторі.

Виконавши описаний вище підхід, було сформовано ранжовану ієрархію факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил (рис. 2) [розроблено авторами].

Ранжована ієрархія факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил складається з восьми рівнів, кожен з яких містить один або декілька факторів з множини $H$. Отримана за допомогою (1)–(4) та наведена на рис. 2 схема ієрархії є впорядкованою за критерієм пріоритетності для усунення (вирішення) версією спрямованого графу взаємозв'язків між факторами, що досліджуються (рис. 1). Пріоритетність усунення (вирішення) фактору (факторів) чисельно дорівнює порядковому номеру рівня ранжованої ієрархії, на якому він (вони) знаходяться згідно зі схемою.

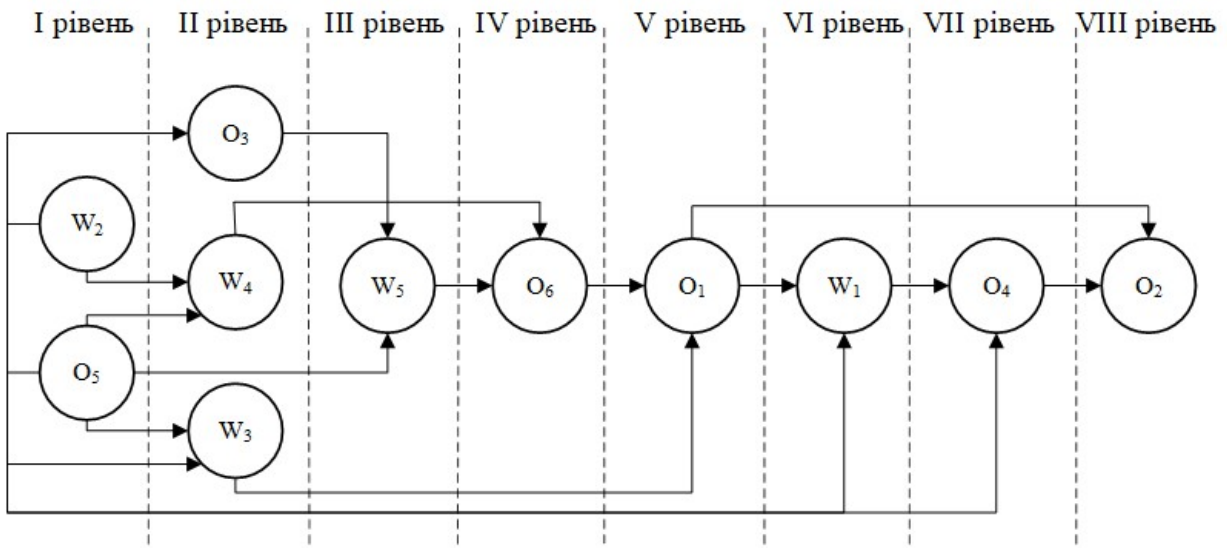


Рисунок 2 – Ранжована ієрархія факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил

Відповідно, шуканими факторами, усунення яких, з досить високою ймовірністю, є першочерговим для підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил є:

W2 – відсутність методичного апарату планування та управління діями сил і засобів кіберборотьби (управлінський фактор);

O5 – можливість використання наукового та інтелектуального потенціалу для удосконалення форм і способів ведення протиборства у кіберпросторі.

## Висновки й перспективи подальших досліджень

Отже, під час дослідження внутрішніх і зовнішніх факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил за допомогою методу SWOT-аналізу було сформовано їх множину, а використання математичної моделі ієрархії дало змогу провести ранжування та знайти ті фактори, усунення яких, з досить високою ймовірністю, є першочерговим завданням для підвищення зазначеної ефективності. Такими факторами виявилися: відсутність методичного апарату планування та управління діями сил і засобів кіберборотьби (управлінський фактор) та можливість використання наукового й інтелектуального потенціалу для удосконалення форм і способів ведення протиборства у кіберпросторі.

Ранжована ієрархія факторів впливу на підвищення ефективності ведення кіберборотьби в інтересах застосування збройних сил показала, що множина усіх таких факторів, за критерієм пріоритетності їхнього усунення, поділяється на вісім рівнів, порядковий номер кожного з яких чисельно дорівнює пріоритету усунення фактору (факторів) цього рівня.

Перспективою подальших досліджень є розроблення (удосконалення) методичного апарату (методів, моделей, методик та алгоритмів) планування та управління діями сил і засобів кіберборотьби, а також наукове обґрунтування розвитку форм і способів її ведення в інтересах застосування збройних сил.

## Список бібліографічних посилань

**1. Сніцаренко П. М.** Про сутність кібероборони як виду воєнних дій. *Наука і оборона*. 2024. № 3 (26). С. 45–54. DOI: 10.33099/2618-1614-2024-26-3-45-54. **2. 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. DOI: 10.15849/IJASCA.250330.03. **3. Robinson M., Jones K., Janicke H.** Cyber warfare: Issues and challenges. *Computers & Security*. 2015. № 49. P. 70–94. DOI: 10.1016/j.cose.2014.11.007. **4. Горгуленко В. А.** Кіберборотьба у воєнних конфліктах сучасності: передовий досвід, тенденції та закономірності розвитку. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 2 (50). С. 11–28. DOI: 10.33099/2311-7249/2024-50-2-11-28. **5. Грищук Р. В., Даник Ю. Г.** *Основи кібернетичної безпеки*: монографія. Житомир : ЖНАЕУ, 2016. 636 с. **6. Богданович В. Ю., Грищук Р. В., Левченко О. В.** Система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: Військові та технічні науки*. 2017. № 4(74). С. 21–37. **7. Korobiichuk I., Hryshchuk R., Mamarev V., Okhrimchuk V., Kachniarz M.** Cyberattack Classificator Verification. *Advances in Intelligent Systems and Computing*. 2018. Vol. 635. P. 402–411. DOI: 10.1007/978-3-319-64474-5_34. **8. Горгуленко В. А.** Математична модель визначення ймовірнісних станів інформаційно-комунікаційної системи в умовах ведення кіберборотьби. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2025. № 1 (52). С. 77–84. DOI: 10.33099/2311-7249/2025-52-1-77-84. **9. Madewell A. C., Johnson P. C.** Quantifying the Operational Resilience of Systems Operating in Cyberspace. *Military Operations Research*. 2022. № 27 (3). P. 5–22. DOI: 10.5711/1082598327305. **10. Горгуленко В. А.** Аналіз

існуючого науково-методичного апарату з метою розроблення методики розподілу сил і засобів кіберборотьби. *Системи обробки інформації*. 2025. № 1(180). С. 14–25. DOI: 10.30748/soi.2025.180.02. **11. Грищук Р. В., Жовноватюк Р. М., Носова Г. Д.** Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2019. № 3 (36). С. 53–58. DOI: 10.33099/2311-7249/2019-36-3-53-58. **12. Горгуленко В. А.** Фактори, що впливають на спроможності Збройних Сил України у кібердомені. *Військові інновації у сучасних війнах* : зб. тез доповідей міжнародного академічного форуму. (Київ, 18–19 квіт. 2024 р.). Київ. 7БЦ. 2024. С. 157–158. **13. Потій О. В., Бакалинський О. О., Мялковський Д. В., Верба Д. В.** Аналіз системних і персоніфікованих факторів організаційно-ресурсних умов діяльності із забезпеченості кібербезпеки органів державної влади і критичної інфраструктури України. *Безпека інформації*. 2022. № 3 (28). С. 107–118. DOI: 10.18372/2225-5036.28.17366. **14. Семененко О., Митченко С., Водчиць О., Добровольський Ю., Тарасов Р., Лисенко Є.** Аналіз факторів, що впливають на розвиток форм і способів застосування сил оборони України в умовах гібридизації збройних конфліктів. *Social Development and Security*. 2023. № 5 (13). С. 75–92. DOI: 10.33445/sds.2023.13.5.9. **15. Saaty T. L.** Applications of analytical hierarchies. *Mathematics and Computers in Simulation*. 1979. № 21 (1). P. 1–20. DOI: 10.1016/0378-4754(79)90101-0. **16. Saaty T. L.** Some mathematical concepts of the analytic hierarchy process. *Behaviormetrika*. 1991. № 29 (18). P. 1–9. DOI: 10.2333/bhmk.18.29_1. **17. Saaty T. L.** The analytic hierarchy and analytic network measurement processes: Applications to decisions under Risk. *European Journal of Pure and Applied Mathematics.* 2008. № 1 (1). P. 122–196. DOI: 10.29020/nybg.ejpam.v1i1.6. **18. Potomkin M. M., Semenenko O. M., Kliat Y. O. & Sedliar A. A.** Comparing the Results of Alternative Ranking Obtained by Several Variants of the Analytic Hierarchy Process. *Cybernetics and Systems Analysis*. 2024. № 60. P. 970–977. DOI: 10.1007/s10559-024-00733-z. **19. Потьомкін М. М., Седляр А. А., Дейнега О. В., Зварич А. О.** Комплексне використання принципу Парето та методу аналізу ієрархій для підвищення обґрунтованості результатів ранжування альтернатив. *Кібернетика та системний аналіз*. 2021. № 3 (57). С. 97–105. **20. Вартанян В. М., Штейнбрехер Д. О.** Застосування методу аналізу ієрархій для побудови стратегії управління знаннями високотехнологічних проектів. *Радіоелектронні і комп'ютерні системи*. 2019. № 2 (90). DOI: 10.32620/reks.2019.2.11.

## INFLUENCING FACTORS ON THE EFFECTIVENESS OF CYBER WARFARE IN THE INTERESTS OF ARMED FORCES USAGE

***HORHULENKO Vladyslav,*** Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine, https://orcid.org/0000-0001-6382-5075

***KOLOMIIETS Bohdan,*** Educational and Scientific Testing Ground for High-Tech Weapons and Military Equipment, Cherkasy, Ukraine, https://orcid.org/0009-0008-6812-1155

***Formulation of the problem in general.*** *Effective cyber warfare involves achieving success with a dedicated set of forces and means in the triad of tasks «cyber defence, cyber intelligence, cyber influence». A fairly well-established body of scientific work currently assesses this effectiveness. At the same time, one of the leading and extremely urgent issues of modern military science is not only the assessment, but also the increase in the effectiveness of the armed forces' usage, particularly cyber warfare troops.*

***Research methods.*** *The SWOT-analysis method and a mathematical hierarchy model from the theory of systems analysis were applied during the research. Using the SWOT-analysis method, a set of internal and external factors influencing the effectiveness of cyber warfare in the interests of armed forces usage was formed, and implementation of the mathematical hierarchy model made it possible to rank them and find those factors, the solution of which, with a reasonably high probability, is of primary importance for increasing the specified effectiveness.*

***Literature review.*** *Analysing factors that influence the effectiveness of complex systems (particularly military systems) is a well-known way to form substantiated recommendations for improvement. Still, much less attention has been paid to the study of influencing factors on the effectiveness of cyber warfare as a form of military (combat) actions in the context of the increasing hybridity of modern warfare.*

***Research results.*** *The article suggests a study of the factors influencing the effectiveness of cyber warfare in the interests of armed forces usage in two stages: formation of a set of factors influencing the effectiveness of cyber warfare – problems; identification and disclosure of a key factor (factors), the solution of which is reasonably of primary importance. As a result of internal and external factors analysis, a SWOT-matrix of factors influencing the effectiveness of cyber warfare in the interests of armed forces usage was compiled. The use of this method made it possible not only to form a set of factors, but also to determine the nature of their influence on the effectiveness of cyber warfare in the interests of armed forces usage. To carry out the second stage of the study of factors influencing the effectiveness of cyber warfare in the interests of armed forces usage, given its rationality, a SWOT–strategy Weaknesses-Opportunities was chosen. Connections between elements of the set of internal and external factors of influencing the effectiveness of cyber warfare in the interests of armed forces usage were identified, and a directed graph of relationships was compiled. Based on the directed graph, a binary matrix of factors influencing the effectiveness of cyber warfare in the interests of armed forces usage accessibility was constructed. By applying the hierarchy mathematical model to the studied system, a ranked hierarchy of factors influencing the effectiveness of cyber warfare in the interests of armed forces usage was obtained, consisting of eight levels, each of which contains one or more factors. The suggested hierarchy is a version of the directed graph of relationships between the studied factors, ordered by the priority criterion for elimination (resolution).*

*According to the study results, factors that have been searched for are: the lack of a methodological apparatus for planning and managing the actions of cyber warfare forces and means (management factor) and the possibility of using scientific and intellectual potential to improve forms and methods of the confrontation in cyberspace.*

***Research novelty.*** *The novelty of the research results lies in the suggested methodological approach for internal and external factors that influence the effectiveness of cyber warfare analysis, which, unlike the known ones, made it possible to consider the nature of the factors and obtain their ranked hierarchy.*

***Theoretical and practical significance.*** *The value of the research results is the identification and disclosure of internal and external factors, the solution of which can lead to increased effectiveness of cyber warfare in the interests of armed forces usage.*

***Conclusions and future work.*** *The ranked hierarchy of factors influencing the effectiveness of cyber warfare in the interests of armed forces usage showed that the set of all such factors, according to the criterion of their elimination priority, is divided into eight levels, the serial number of each of which is numerically equal to the priority of elimination of this level factor(s). A promising area for further research is the development (improvement) of methodological apparatus (methods, models, techniques and algorithms) for planning and managing the cyber warfare forces. It means combat actions and scientific substantiation of the forms and methods of their conduct and development.*

***Keywords:*** *effectiveness, armed forces usage, cybersecurity, cyber warfare, cyber defence, cyberspace, hierarchy analysis method, factor analysis.*

## References

**1. Snitsarenko, P. M.,** (2024). About the essence of cyber defence as a type of military action. *Nauka i oborona*. 26 (3), 45-54. DOI: 10.33099/2618-1614-2024-26-3-45-54. **2. 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*. 17 (1), 32. DOI: 10.15849/IJASCA.250330.03. **3. Robinson, M., Jones, K., Janicke, H.,** (2015). Cyber warfare: Issues and challenges. *Computers & Security*. 49, 70-94. DOI: 10.1016/j.cose.2014.11.007. **4. Horhulenko, V. A.,** (2024). Cyber warfare in modern military conflicts: experience, trends and regularities of development. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 50 (2), 11-28. DOI: 10.33099/2311-7249/2024-50-2-11-28.

**5. Hryschuk, R. V., Danyk, Yu. H.,** (2016). *Fundamentals of cyber security*: a monograph. Zhytomyr: ZhNAEU. **6. Bohdanovych, V. Yu., Hryshchuk, R. V., Levchenko, O. V.,** (2017). System of criteria and indicators for assessing the effectiveness of the information security system. *Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriia: Viiskovi ta tekhnichni nauky.* 4(74), 21–37. **7. Korobiichuk, I., Hryshchuk, R., Mamarev, V., Okhrimchuk, V., Kachniarz, M.,** (2018). Cyberattack Classificator Verification. *Advances in Intelligent Systems and Computing*. 635, 402-411. DOI: 10.1007/978-3-319-64474-5_34. **8. Horhulenko, V. A.,** (2025). A mathematical model for determining probabilistic states of an information and communication system in the conditions of cyberwarfare. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony.* 52 (1), 77–84. DOI: 10.33099/2311-7249/2025-52-1-77-84. **9. Madewell A. C., Johnson P. C,** (2022). Quantifying the Operational Resilience of Systems Operating in Cyberspace. *Military Operations Research*. 27 (3), 5-22. DOI: 10.5711/1082598327305. **10. Horhulenko, V. A.,** (2025). Analysis of the existing scientific and methodological apparatus with the purpose of developing a technique for cyber forces assignment. *Systemy obrobky informatsii*. 180 (1), 14–25. DOI: 10.30748/soi.2025.180.02. **11. Hryshchuk, R. V., Zhovnovatiuk, R. M., Nosova, H. D.,** (2019). Hybrid threats in cyberspace: factors of influence on the nature of emergence. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 36 (3), 53-58. DOI: 10.33099/2311-7249/2019-36-3-53-58. **12. Horhulenko, V. A.,** (2024). Factors affecting the capabilities of the Armed Forces of Ukraine in a cyber domain. In: *Military innovations in the contemporary warfare: zb. tez dop. mizhnar. akad. forumu*. Kyiv, Ukraina, 18–19 kvitnia 2024. Kyiv: 7BC. **13. Potii, O. V., Bakalynsky, O. O., Myalkovsky, D. V., Verba, D. V.,** (2022). Analysis of systemic and personalised factors of organisational and resource conditions, cybersecurity endowment activities, bodies of state authority, and critical infrastructures of Ukraine. *Bezpeka informatsii*. 28 (3), 107-118. DOI: 10.18372/2225-5036.28.17366. **14. Semenenko, O., Mytchenko, S., Vodchyts, O., Dobrovolskyi, Yu., Tarasov, R., Lysenko, Ye.,** (2023). Analysis of factors affecting the development of forms and methods of use of the defence forces of Ukraine in the conditions of hybridisation of armed conflicts. *Social Development and Security*. 13 (5), 75-92. DOI: 10.33445/sds.2023.13.5.9. **15. Saaty, T. L.,** (1979). Applications of analytical hierarchies. *Mathematics and Computers in Simulation*. 21 (1), 1-20. DOI: 10.1016/0378-4754(79)90101-0. **16. Saaty, T. L.,** (1991). Some mathematical concepts of the analytic hierarchy process. *Behaviormetrika*. 29 (18), 1-9. DOI: 10.2333/bhmk.18.29_1. **17. Saaty, T. L.,** (2008). The analytic hierarchy and analytic network measurement processes: Applications to decisions under Risk. *European Journal of Pure and Applied Mathematics.* 1 (1), 122-196. DOI: 10.29020/nybg.ejpam.v1i1.6. **18. Potomkin, M. M., Semenenko, O. M., Kliat, Y. O. & Sedliar, A. A.,** (2024). Comparing the Alternative Ranking Results Obtained by Several Analytic Hierarchy Process Variants. *Cybernetics and Systems Analysis*. 60, 970–977. DOI: 10.1007/s10559-024-00733-z. **19. Potomkin, M. M., Sedliar, A. A. Deineha, O. V., Zvarych, A. O.,** (2021). Comprehensive use of the Pareto principle and the analytic hierarchy process to increase the substantiation of alternative ranking results. *Kibernetyka ta systemnyi analiz*. 57 (3), 97-105. **20. Vartanian, V. M., Shteinbrekher, D. O.,** (2019). Application of the hierarchy analysis technique for the design of high-technological projects' knowledge management strategy. *Radioelektronni i kompiuterni systemy*. 90 (2), 118-126. DOI: 10.32620/reks.2019.2.11.

*Рукопис надійшов до редакції* *15.06.2025*
*Рукопис прийнято до друку після рецензування* *01.07.2025*
*Дата публікації* *29.08.2025*