УДК: 004.056 DOI: **10.33099/2311-7249/2026-55-1-100-107**

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

МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ВЕДЕННЯ КІБЕРБОРОТЬБИ В ІНТЕРЕСАХ ЗАСТОСУВАННЯ УГРУПОВАНЬ ВІЙСЬК (СИЛ) В ОПЕРАЦІЯХ

Метою статті *є удосконалення методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях за рахунок використання окремих положень теорії стохастичних диференціальних рівнянь на етапі формування вихідних даних для оцінювання ефективності.*

Методи дослідження*. Під час проведення дослідження щодо удосконалення методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях були використані наукові методи системного аналізу, аналітичного математичного моделювання, методи теорії марківських випадкових процесів, теорії матриць, а також теорії стохастичних диференціальних рівнянь.*

Отримані результати дослідження. *Наведено удосконалену методику оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях. Експериментально перевірено працездатність удосконаленої методики на тестовому наборі вихідних даних. Результати чисельного експерименту свідчать, що удосконалена методика є працездатною та дозволяє підвищити адекватність моделювання перебігу та результатів ведення кіберборотьби на 5–10%, в залежності від величини впливу випадкових факторів на функціонування конкретної інформаційно-комунікаційної системи.*

Елементи наукової новизни. *Удосконалена методика оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях, на відміну від існуючих, дозволяє враховувати вплив випадкових факторів на перебіг та результати ведення кіберборотьби за рахунок застосування окремих положень теорії стохастичних диференціальних рівнянь на етапі уточнення вихідних даних. Ядром удосконаленої методики є розроблена авторська математична модель функціонування захищеної інформаційно-комунікаційної системи в умовах ведення кіберборотьби.*

Теоретичне та практичне значення викладеного у статті. *Теоретичною значимістю результатів дослідження є прикладне застосування окремих положень теорії стохастичних диференціальних рівнянь для моделювання перебігу реального випадкового процесу – функціонування захищеної інформаційно-комунікаційної системи в умовах ведення кіберборотьби. Практична цінність отриманого наукового результату полягає у можливості використання удосконаленої методики під час прогнозування перебігу та результатів кібердій (кіберборотьби) посадовими особами відповідних органів військового управління, до сфери діяльності яких входить планування операцій у кіберпросторі.*

Ключові слова: *інформаційна безпека, інформаційні технології, оцінювання ефективності, кіберборотьба, математична модель, моделювання, прогнозування, штучний інтелект.*

Вступ

Постановка проблеми. Локальним війнам та збройним конфліктам сучасності дедалі більше стають притаманними риси асиметричності та гібридності. Кіберпростір беззаперечно є доменом збройного протиборства [1–6]. В низці держав, як-от Україні, спеціальні підрозділи для ведення протиборства у кіберпросторі (кіберборотьби) перебувають на етапі формування та набуття спроможностей; в деяких (наприклад, США) таких військових формувань існують та досить результативно застосовуються за призначенням вже тривалий час. Технології та засоби кіберзахисту, кіберрозвідки та кібервпливу удосконалюються в унісон з розвитком інформаційних технологій. Форми і способи протиборства у кіберпросторі постійно видозмінюються для досягнення поставлених воєнних цілей. Як наслідок, постає проблема оцінювання ефективності ведення кіберборотьби з точки зору системного підходу. Вирішення цієї проблеми дозволить здійснювати прогнозування під час планування кібероперацій та більш раціонально розподіляти ресурси (сили і засоби кіберборотьби) для виконання конкретних кібердій.

Аналіз останніх досліджень і публікацій. В роботі [7] проведено аналіз наявного науково-методичного апарату, який може бути використано для оцінювання ефективності кіберборотьби. Було встановлено, що наразі немає однієї методики (методу), за допомогою якої можна було б цілісно оцінювати ефективність ведення воєнних дій у кіберпросторі, наявні лише часткові методики, які є концептуально різними за описаними в них підходами.

З-поміж актуальних наукових праць, в яких розглядаються пов’язані з означеною в статті наукові проблеми можна виділити:

статтю [8], в якій висвітлено результати дослідження сучасних викликів і загроз, що виникають у зв'язку з кібербезпекою критичної інфраструктури, а

також визначено стратегії та технології, необхідні для її ефективного захисту;

роботу [9], де авторами запропоновано підхід до виявлення кібератак в інформаційних мережах з випадковим моментом їх появи, що дає змогу збільшити ефективність кіберзахищеності інформаційних мереж та інформації;

працю [10], автори якої всебічно проаналізували ландшафт кіберзагроз для технологічно менш розвинених суб'єктів кіберборотьби та запропонували адаптовану систему моделювання загроз для вирішення їхніх унікальних вразливостей та потреб;

в публікації [11] розкрито основні положення розробленої моделі управління кіберзахистом, яка допомагає оцінювати оптимальність процесів із захисту власної інформаційної та кіберінфраструктури, а також контролювати ефективність кіберзахисту.

Водночас, питання оцінювання ефективності ведення кіберборотьби (як цілісного процесу виконання заходів з кіберзахисту, кіберрозвідки та кібервпливу) в інтересах застосування угруповань військ (сил) в операціях залишається відкритим. Незважаючи на те, що у формалізованому вигляді та у відкритому доступі методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях наразі немає, результати аналізу досвіду ведення кіберборотьби, організаційно-штатної структури органів військового управління, військових частин та підрозділів кіберборотьби, а також існуючого науково-методичного апарату оцінювання результативності окремих її елементів, можна зробити висновок про те, що в дійсності ефективність ведення кіберборотьби оцінюється за певною методикою (методиками). З огляду на це, завданням дослідження є удосконалення такої методики.

Метою статті є удосконалення методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях за рахунок використання окремих положень теорії стохастичних диференціальних рівнянь на етапі формування вихідних даних для оцінювання ефективності.

Виклад основного матеріалу дослідження

Передумовою удосконалення методики є необхідність оцінювання перебігу та результатів кіберборотьби як цілісної системи, що складається з кіберзахисту, кіберрозвідки та кібервпливу, а також формування Командування Кіберсил Збройних Сил України як основного актора ведення збройного протиборства у кіберпросторі. Удосконалена методика оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях складається з трьох взаємопов'язаних етапів, які включають: формування вихідних даних, математичне моделювання та оцінювання ефективності.

Об'єктом дослідження методики є перебіг та результати процесу ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях.

Дослідження щодо удосконалення методики проводилося з припущенням про марківський характер процесу ведення кіберборотьби та про скінченну (дискретну) кількість можливих станів функціонування захищених інформаційно-комунікаційних систем (далі – ІКС). ІКС розглядаються як об'єкти ведення кіберборотьби та середовище протікання цього процесу. Використання марківських ланцюгів для дослідження фізичних систем з дискретними станами та безперервним часом є достатньо відомим підходом для прогнозування динаміки випадкових процесів за відомими початковими умовами.

Саме у вигляді такого ланцюга можна навести процес функціонування захищеної ІКС в умовах ведення кіберборотьби. Так, враховуючи трирівневу архітектуру побудови кіберпростору, в якому функціонують захищені ІКС, а саме: фізичний мережевий рівень; логічний мережевий рівень; рівень кіберперсони, а також три складові кіберборотьби (кіберзахист; кіберрозвідка; кібервплив), було визначено набір можливих станів, в яких може функціонувати захищена ІКС [12]: S_1 – сталий (штатний) режим функціонування ІКС; S_2 – противником проведено кіберрозвідку (сканування системи на наявність вразливостей кіберінфраструктури); S_3 – нанесено кібервплив на фізичний мережевий рівень ІКС; S_4 – нанесено кібервплив на логічний мережевий рівень ІКС; S_5 – нанесено кібервплив на рівень кіберперсони ІКС; S_6 – активний кіберзахист та відновлення ІКС до режиму сталого (штатного) функціонування. Розмічений граф станів функціонування захищеної ІКС наведено на рис. 1.

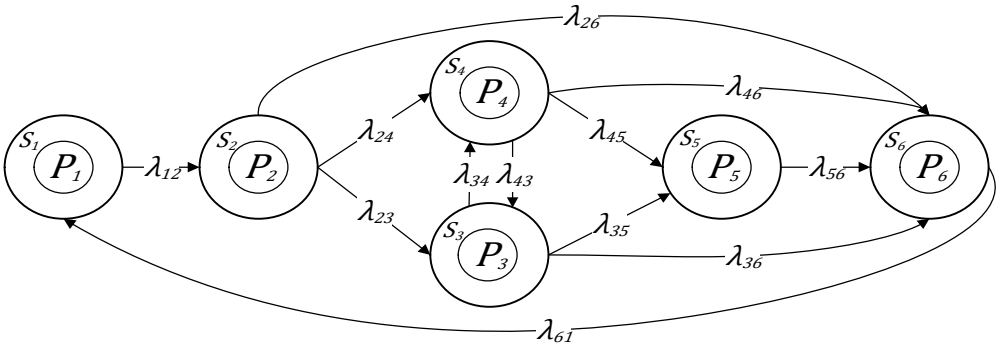

Рисунок 1 – Граф станів захищеної інформаційно-комунікаційної системи в умовах ведення кіберборотьби

На відміну від запропонованого графу у статті [12], метою якої було детальне висвітлення основних положень саме математичної моделі функціонування захищеної ІКС (яка є невід'ємною частиною методики), наведений вище граф станів більш адекватно відображає сутність функціонування таких систем. Він враховує можливість нанесення противником кібервпливу напряму на логічний мережевий рівень ІКС.

Відповідно, показниками ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях обрано ймовірності $P_i(t)$, перебування ІКС у станах S_i на деякому інтервалі часу T, які розраховуються шляхом вирішення системи лінійних диференціальних рівнянь Колмогорова для ймовірностей станів. У свою чергу ймовірності станів можуть бути інтерпретовані як середній відносний час перебування захищеної ІКС у станах.

Eman 1. Перший етап удосконаленої методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях призначено для формування вихідних даних.

1.1. Особливістю існуючої статистики, яку можна використати під час формування вихідних даних методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях є наявність таких даних як кількість переходів та час перебування в стані лише для обчислення середніх значень інтенсивностей першого (θ_{12}) та останнього (θ_{61}) переходів між станами ІКС:

$$\theta_{ij} = \frac{N_{ij}}{T_i}, \qquad (1)$$

де θ_{ij} – середня інтенсивність переходу з S_i в S_j, $\theta_{ij} \in \{\theta_{12}, \theta_{61}\}$;

N_{ij} – к-сть переходів зі стану S_i в S_j;

T_i – час перебування в стані S_i, діб.

Решта інтенсивностей переходів захищеної ІКС в умовах ведення кіберборотьби ($\theta_{ij} \notin \{\theta_{12}, \theta_{61}\}$) можуть бути представленими лише орієнтовними числовими інтервалами на основі історичних даних про функціонування захищених ІКС:

$$\theta_{ij} \in \left[\lambda_{ij}^{min}, \lambda_{ij}^{max}\right], \qquad (2)$$

де λ_{ij}^{min} – нижня межа числового інтервалу;

λ_{ij}^{max} – верхня межа числового інтервалу.

Середні значення таких інтенсивностей пропонується обчислювати середнім арифметичним верхньої та нижньої межі статистичних інтервалів:

$$\theta_{ij} = \frac{\lambda_{ij}^{min} + \lambda_{ij}^{max}}{2}. \qquad (3)$$

1.2. Слід зазначити, що захищена ІКС являє собою складну людино-машинну систему зі значним впливом випадкових факторів, що й власне обумовило застосування положень теорії стохастичних диференціальних рівнянь для апроксимації наявних статистичних даних щодо ведення кіберборотьби. Зокрема, підтверджено високу збіжність наявної статистики для першого та останнього переходів (θ_{12} та θ_{61}) з результатами їх апроксимації відомою у сфері фінансової математики стохастичною моделлю Васічека. На основі цього зроблено припущення про високу збіжність й інших інтенсивностей переходів.

1.3. Модель Васічека є однофакторною стохастичною моделлю, що описує динаміку випадкового процесу з поверненням до середнього рівня. Таким випадковим процесом є кіберборотьба, а середнім θ_{ij} – обчислені в блоці 1.1 середні значення інтенсивностей переходів ІКС між станами. Модель Васічека описується стохастичним диференціальним рівнянням (СДР) виду:

$$d\lambda_{ij}(t) = \alpha\left(\theta_{ij} - \lambda_{ij}(t)\right)dt + \sigma dW(t), \qquad (4)$$

де λ_{ij} – інтенсивність переходу зі стану S_i в S_j;

α – швидкість повернення λ_{ij} до θ_{ij}, $0 < \alpha \leq 1$;

σ – величина впливу випадкових факторів на відповідну інтенсивність переходу, $\sigma > 0$;

$W(t)$ – вінерівський стохастичний процес з незалежними приростами, $W(0) = 0$, $\Delta W(t) = \sqrt{\Delta t}\xi$, $\xi \sim \mathrm{N}(0,1)$.

Параметр α характеризує швидкість повернення до середнього значення, а σ – власне величину впливу випадкових факторів на відповідну інтенсивність переходу. Параметри α та σ варіюються залежно від рівня підготовленості персоналу захищеної ІКС як складної людино-машинної системи та його готовності до протидії заходам кіберборотьби. $W(t)$ є вінерівським стохастичним процесом, який являє собою математичну модель випадкового шуму з незалежними приростами, нульовим математичним сподіванням та одиничною дисперсією. Отже, модель Васічека може бути використаною для уточнення інтенсивностей переходів ІКС між станами.

1.4. Вирішувати СДР, яким представляється модель Васічека пропонується чисельним методом Ейлера-Маруями, за допомогою якого можна побудувати N незалежних траєкторій розв'язку моделі Васічека на інтервалі часу T з кроком Δt. Чисельний метод Ейлера-Маруями є рекурсією виду:

$$\lambda_{ij}^{(n)}(t_{k+1}) = \lambda_{ij}^{(n)}(t_k) + \alpha\left(\theta_{ij} - \lambda_{ij}^{(n)}(t_k)\right)\Delta t + \\ + \sigma\sqrt{\Delta t}\xi_k^{(n)}, \qquad (5)$$

де t_k – крок на інтервалі $[0, T]$, $t_k = k\Delta t$, $k = 0,1,\dots,{}^{T}/_{\Delta t}$;

n – реалізація моделі Васічека, $n = 1, \dots, N$;

$\xi_k^{(n)}$ – незалежна нормальна випадкова величина для кроку k реалізації n.

Eman 2. Другий етап удосконаленої методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях присвячено математичному моделюванню

функціонування захищеної ІКС в умовах ведення кіберборотьби.

2.1. Як було попередньо зазначено, фізичний зміст можливих станів захищеної ІКС враховує як трирівневу структуру кіберпростору, так і сутність кіберборотьби, яка полягає у комплексі заходів з кіберзахисту, кіберрозвідки та кібервпливу. Кіберзахист знайшов своє відображення у станах S_1 та S_6, кіберрозвідка – у стані S_2, а кібервплив, відповідно, у станах S_3, S_4, S_4.

2.2. Для графу станів функціонування захищеної ІКС в умовах ведення кіберборотьби існує матриця густини ймовірностей (тобто інтенсивностей) переходів:.

$$\lambda_{ij} = \begin{pmatrix} -\lambda_{12} & \lambda_{12} & 0 & 0 & 0 & 0 \\ 0 & -(\lambda_{23}+\lambda_{24}+\lambda_{26}) & \lambda_{23} & \lambda_{24} & 0 & \lambda_{26} \\ 0 & 0 & -(\lambda_{34}+\lambda_{35}+\lambda_{36}) & \lambda_{34} & \lambda_{35} & \lambda_{36} \\ 0 & 0 & \lambda_{43} & -(\lambda_{43}+\lambda_{45}+\lambda_{46}) & \lambda_{45} & \lambda_{46} \\ 0 & 0 & 0 & 0 & -\lambda_{56} & \lambda_{56} \\ \lambda_{61} & 0 & 0 & 0 & 0 & -\lambda_{61} \end{pmatrix}, \quad (6)$$

Матриця повинна відповідати вимогам, які висуваються до генераторних матриць марківських ланцюгів безперервного часу. А саме: позадіагональні елементи більші або дорівнюють нулю; діагональні елементи дорівнюють сумі позадіагональних елементів відповідного рядка зі знаком мінус; сума елементів матриці в кожному рядку рівна нулю. У формалізованій постановці вимоги матриці інтенсивностей переходів ІКС набувають вигляду:

$$\lambda_{ij} \geq 0 \; i \neq j, \qquad \lambda_{ii} = -\sum_{j \neq i} \lambda_{ij}\,, \qquad \sum_{j} \lambda_{ij} = 0 \;\; \forall i. \quad (7)$$

2.3. Наступним кроком моделювання є складання системи лінійних диференціальних рівнянь Колмогорова для ймовірностей станів захищеної ІКС в умовах ведення кіберборотьби. Система рівнянь формується за відомими правилами відповідно до матриці інтенсивностей. Кожне рівняння відповідає за моделювання в часі ймовірності конкретного стану захищеної ІКС.

2.4. Далі необхідно обчислити значення матриці інтенсивностей переходів захищеної ІКС в умовах ведення кіберборотьби (6) за допомогою отриманих на кроці 1.4 реалізацій стохастичної моделі Васічека чисельним методом Ейлера-Маруями. Чисельне значення інтенсивності переходу зі стану S_i у стан S_j на момент часу t визначається монтекарлівською оцінкою математичного сподівання серед N реалізацій:

$$\lambda_{ij}(t) \approx \widetilde{\mathbb{M}}\big[\lambda_{ij}(t)\big] = \frac{1}{N}\sum_{n=1}^{N} \lambda_{ij}^{(n)}(t)\,. \quad (8)$$

Відповідно, елементом матриці інтенсивностей обирається оцінка математичного сподівання на момент часу $t = T$:

$$\lambda_{ij} \approx \widetilde{\mathbb{M}}\big[\lambda_{ij}(t = T)\big]. \quad (9)$$

При цьому, моделювання інтенсивностей, які позначають переходи пов'язані з виявленням вразливостей та ураженням ІКС пропонується проводити з початковим значенням $\lambda_{ij}(0) = \lambda_{ij}^{max}$, а тих інтенсивностей, які позначають переходи пов'язані з відновленням ІКС – з початковим значенням $\lambda_{ij}(0) = \lambda_{ij}^{min}$.

Приклади розв'язку стохастичної моделі Васічека чисельним методом Ейлера-Маруями ($N = 1000$, $T = 0$) та обчислення інтенсивності переходу λ_{ij} для підстановки в матрицю (6) наведені на рис. 2 та 3.

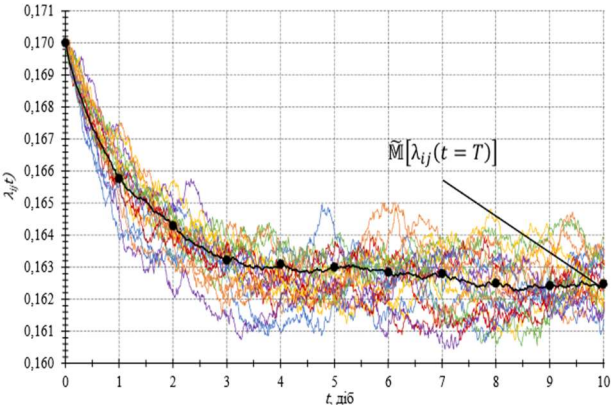

Рисунок 2 – Приклад розв'язку СДР моделі Васічека з параметрами:
$\alpha = 0{,}8;\ \theta_{ij} = 0{,}15;\ \sigma = 0{,}01;\ \lambda_{ij}(0) = 0{,}17.$
Результат: $\lambda_{ij} \approx 0{,}1625$

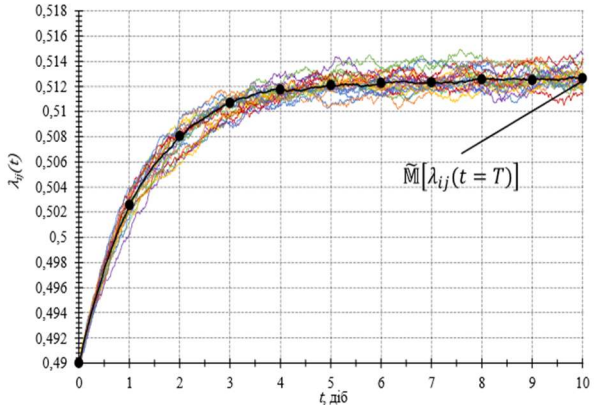

Рисунок 3 – Приклад розв'язку СДР моделі Васічека з параметрами:
$\alpha = 0{,}8;\ \theta_{ij} = 0{,}5;\ \sigma = 0{,}1;\ \lambda_{ij}(0) = 0{,}49.$
Результат: $\lambda_{ij} \approx 0{,}513$

Eman 3 присвячено безпосередньо оцінюванню ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях. Для наочності буде проведено чисельний експеримент з оцінювання ефективності на наборі тестових даних.

3.1. Спочатку здійснюється наповнення матриці інтенсивностей переходів захищеної ІКС значеннями отриманими за допомогою чисельного вирішення моделі Васічека (4) за чисельною схемою (5), з урахуванням дотримання вимог, які висуваються до даного типу матриць (7).

Чисельні значення матриці вище розраховані за схемою (5) з параметрами: $\alpha = 0{,}3$; $\sigma = 0{,}0025$. Параметри θ_{ij} та $\lambda_{ij}(0)$, а також λ_{ij} для кожного позадіагонального елемента матриці наведені в табл. 1 (діагональні елементи обчислюються за правилом матриці).

Таблиця 1

Розрахунок позадіагональних елементів матриці інтенсивностей

	θ_{ij}	$\lambda_{ij}(0)$	λ_{ij}
λ_{12}	0,4	0,5	0,413
λ_{23}	0,15	0,23	0,162
λ_{24}	0,25	0,38	0,264
λ_{26}	0,5	0,42	0,504
λ_{34}	0,12	0,175	0,131
λ_{35}	0,23	0,4	0,264
λ_{36}	0,45	0,24	0,448
λ_{43}	0,17	0,27	0,183
λ_{45}	0,3	0,49	0,317
λ_{46}	0,4	0,34	0,405
λ_{56}	0,35	0,5	0,365
λ_{61}	0,6	0,4	0,598

Приклад наповнення матриці інтенсивностей переходів тестовими значеннями:

$$\lambda_{ij} = \begin{pmatrix} -0{,}413 & 0{,}413 & 0 & 0 & 0 & 0 \\ 0 & -0{,}93 & 0{,}162 & 0{,}264 & 0 & 0{,}504 \\ 0 & 0 & -0{,}843 & 0{,}131 & 0{,}264 & 0{,}448 \\ 0 & 0 & 0{,}183 & -0{,}905 & 0{,}317 & 0{,}405 \\ 0 & 0 & 0 & 0 & -0{,}365 & 0{,}365 \\ 0{,}598 & 0 & 0 & 0 & 0 & -0{,}598 \end{pmatrix}$$

3.2. Наступним кроком є заповнення системи лінійних диференціальних рівнянь Колмогорова для ймовірностей станів захищеної ІКС в умовах ведення кіберборотьби чисельними значеннями з матриці інтенсивностей:

$$\frac{dP_1(t)}{dt} = -0{,}413P_1(t) + 0{,}598P_6(t);$$
$$\frac{dP_2(t)}{dt} = -0{,}93P_2(t) + 0{,}413P_1(t);$$
$$\frac{dP_3(t)}{dt} = -0{,}843P_3(t) + 0{,}162P_2(t) + 0{,}183P_4(t);$$
$$\frac{dP_4(t)}{dt} = -0{,}905P_4(t) + 0{,}264P_2(t) + 0{,}131P_3(t);$$
$$\frac{dP_5(t)}{dt} = -0{,}365P_5(t) + 0{,}264P_3(t) + 0{,}317P_4(t);$$
$$\frac{dP_6(t)}{dt} = -0{,}598P_6(t) + 0{,}504P_2(t) + 0{,}448P_3(t) + 0{,}405P_4(t) + 0{,}365P_5(t).$$

Після цього проводиться розв'язання системи рівнянь будь-яким з відомих методів (метод Ейлера, метод Рунге-Кутти та ін.).

3.3. Блок 3.3 висвітлює розв'язок системи лінійних диференціальних рівнянь Колмогорова для ймовірностей станів (так званий розв'язок задачі Коші), якою представляється математична модель функціонування ІКС в умовах ведення кіберборотьби для варіанту вихідних даних (рис. 4).

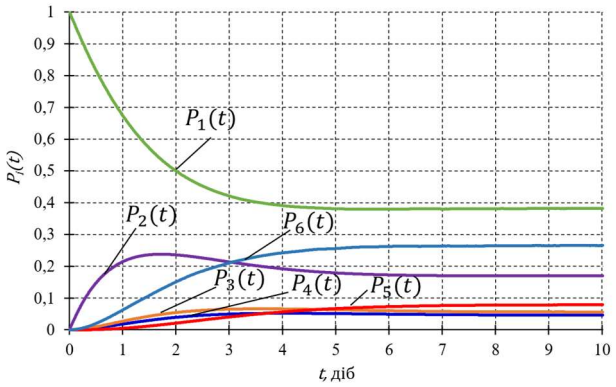

Рисунок 4 – Розв'язок системи лінійних диференціальних рівнянь математичної моделі ІКС

Показані на графіку траєкторії відображають розподіл ймовірностей станів захищеної ІКС в умовах ведення кіберборотьби та інтервалі часу в десять діб. Показники ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях, якими обрано ймовірності перебування захищеної ІКС наведено в табл. 2.

Таблиця 2

Показники ефективності ведення кіберборотьби (для тестового варіанту вихідних даних)

Ймовірність стану	Значення показника ефективності
$P_1(t=10)$	0,383
$P_2(t=10)$	0,170
$P_3(t=10)$	0,047
$P_4(t=10)$	0,056
$P_5(t=10)$	0,079
$P_6(t=10)$	0,265

Розв'язок системи рівнянь показує, що за заданих вихідних даних захищена ІКС близько 40% часу (що становить майже 4 доби з загальних 10-ти) буде функціонувати у сталому режимі; відновлення ІКС до режиму сталого функціонування займе дещо більше чверті усього часу (що становить дещо більше 2,5 діб); решта ймовірностей станів захищеної ІКС в умовах ведення кіберборотьби також висвітлена в таблиці вище. Обов'язковою умовою розв'язку системи диференціальних рівнянь Колмогорова є дотримання вимоги щодо суми ймовірностей станів на кожному моменті часу t, яка повинна дорівнювати одиниці:

$$\sum_i P_i(t) = 1. \qquad (10)$$

Структурно-логічну схему удосконаленої методики проілюстровано на рис. 5.

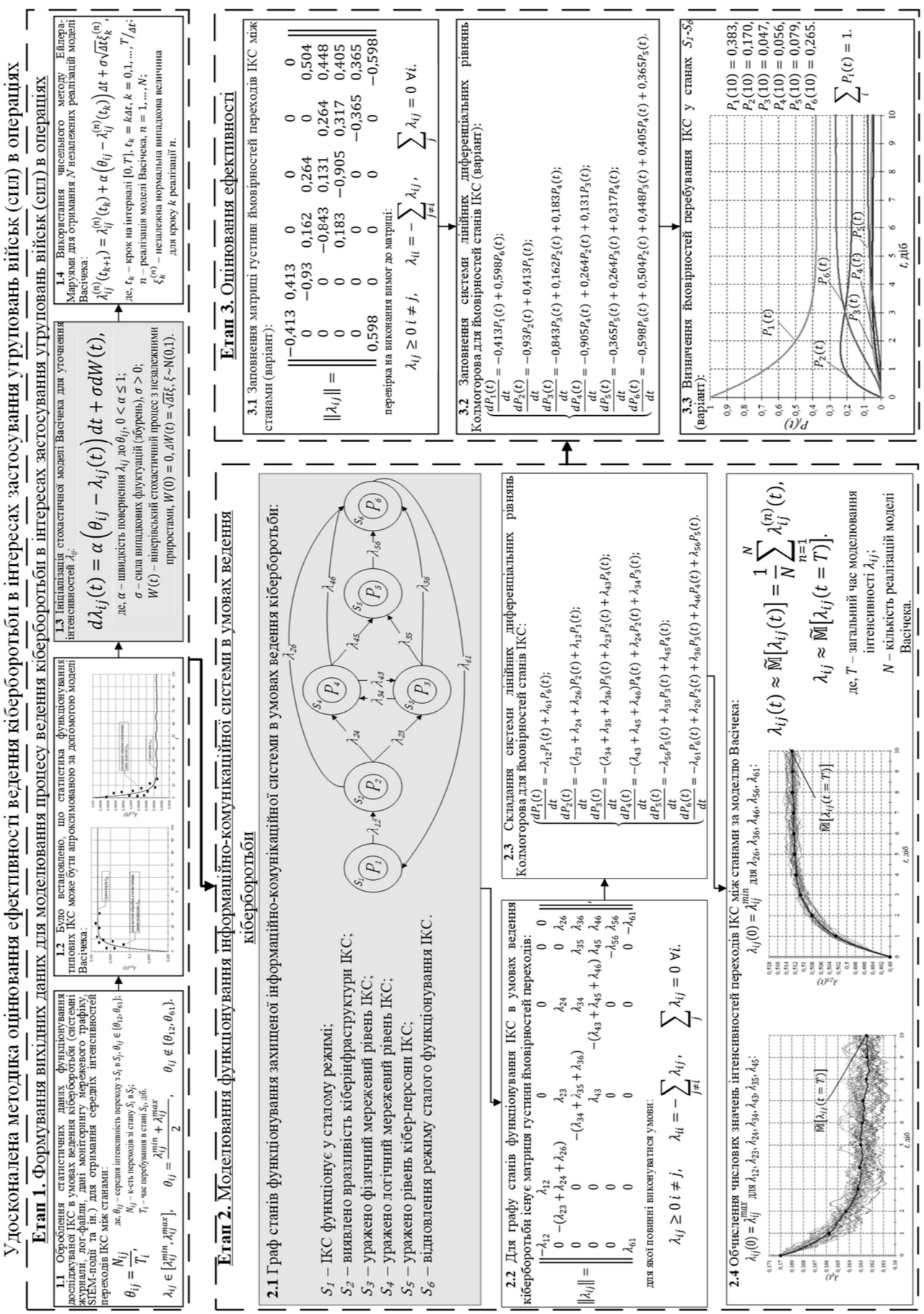

Рисунок 5 – Структурно-логічна схема удосконаленої методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях

Висновки

Отже, у статті було викладено основні положення удосконаленої методики оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях. Методика складається з трьох взаємопов'язаних етапів: формування вихідних даних для оцінювання ефективності; математичне моделювання функціонування захищеної інформаційно-комунікаційної системи в умовах ведення кіберборотьби; власне оцінювання ефективності ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях. Удосконалена методика на відміну від існуючих дозволяє враховувати вплив випадкових факторів на перебіг та результати ведення кіберборотьби за рахунок застосування положень теорії стохастичних диференціальних рівнянь на етапі уточнення вихідних даних. Методика є універсальною та гнучкою у використанні, оскільки з одного боку враховує трирівневу архітектуру побудови практично усіх сучасних захищених інформаційно-комунікаційних систем, а з іншого – є вкрай чутливою до зміни параметрів (вихідних даних), які є унікальними для кожної окремої системи.

Практична цінність отриманого наукового результату полягає у можливості використання удосконаленої методики під час прогнозування перебігу та результатів кібердій (кіберборотьби) посадовими особами відповідних органів військового управління, до сфери діяльності яких входить планування операцій у кіберпросторі.

Виграш від використання удосконаленої методики полягає у підвищенні адекватності математичного моделювання, а як наслідок і прогнозування, перебігу та результатів ведення кіберборотьби в інтересах застосування угруповань військ (сил) в операціях, за рахунок використання окремих положень теорії стохастичних диференціальних рівнянь на етапі формування вихідних даних для оцінювання ефективності. Чисельне представлення підвищення зазначеної адекватності, за попередніми результатами моделювання, знаходиться в межах 5–10%, в залежності від величини впливу випадкових факторів на функціонування конкретної інформаційно-комунікаційної системи.

Перспективи і напрями подальших досліджень. Враховуючи те, що предметом цього дослідження є методика оцінювання ефективності ведення кіберборотьби, перспективою подальших дослідженням за означеним напрямом є розроблення нового та удосконалення існуючого науково-методичного доробку для підвищення такої ефективності. Одним із найактуальніших способів підвищення ефективності ведення кіберборотьби є впровадження технологій штучного інтелекту (нейронних мереж, генетичних алгоритмів тощо) у виконання заходів з кіберзахисту, кіберрозвідки й кібервпливу.

Конфлікт інтересів. Автор повідомляє про відсутність конфліктів інтересів, що впливають на результати дослідження.

Фінансування. Фінансування дослідження не здійснювалося.

Доступність даних. Дослідження виконано з використанням виключно відкритих даних, доступних у публічних джерелах.

Використання засобів штучного інтелекту (далі – ШІ). Автор підтверджує, що не використовував засоби ШІ при створенні цієї статті.

Список бібліографічних посилань

1. Грищук Р. В., Даник Ю. Г. *Основи кібернетичної безпеки*: монографія. Житомир : ЖНАЕУ, 2016. 636 с. **2. 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. DOI: https://doi.org/10.33099/2311-7249/2024-50-2-5-10. **3. Грабар І. Г., Грищук Р. В., Молодецька К. В.** *Безпекова синергетика: кібернетичний та інформаційний аспекти*: монографія. Житомир. ЖНАЕУ, 2019. 280 с. **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: https://doi.org/10.33099/2311-7249/2024-50-2-11-28. **5. 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. DOI: https://doi.org/10.30748/zhups.2025.83.11. **6. Калайда Ю.П.** Гібридні кібератаки в умовах українсько-російської кібервійни. *Інформація і право*. 2025. № 4 (55). С. 205–214. DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346481. **7. 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: https://doi.org/10.30748/soi.2025.180.02. **8. 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. DOI: https://doi.org/10.33099/2311-7249/2025-54-3-75-83. **9. Хорошко В., Шелест М., Ткач Ю.** Багатоальтернативне виявлення кібератак в інформаційних мережах. *Безпека інформації*. 2021. № 3 (27). С. 136–140. DOI: https://doi.org/10.18372/2225-5036.27.16515. **10. Kumar S. , Nagar G.** Threat Modeling for Cyber Warfare Against Less Cyber-Dependent *Adversaries*. 2024. Vol. 23 No. 1. *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, 27–28 June 2024, P. 257–264. DOI: https://doi.org/10.34190/eccws.23.1.2462. **11. 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). DOI: https://doi.org/10.1093/cybsec/tyaf020. **12. 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: https://doi.org/10.33099/2311-7249/2025-52-1-77-84.

TECHNIQUE FOR EVALUATING THE EFFECTIVENESS OF CONDUCTING CYBER WARFARE IN SUPPORT OF THE EMPLOYMENT OF FORCE GROUPINGS IN OPERATIONS

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

The article's purpose *is to refine the methodology for assessing the effectiveness of cyber warfare in support of the deployment of military formations (forces) in operations, by applying certain principles of stochastic differential equations during the stage of generating input data for effectiveness assessment*

Research methods. *During the research on improving the technique for evaluating the effectiveness of conducting cyber warfare in support of the employment of force groupings in operations, scientific methods of system analysis, analytical mathematical modelling, methods of the theory of Markov random processes, matrix theory, and the theory of stochastic differential equations were used.*

Literature review. *The issue of evaluating the effectiveness of conducting cyber warfare (as a holistic process of implementing cyber defence, cyber intelligence, and cyber influence measures) in support of the employment of force groupings in operations remains open.*

Research results. *The main scientific result of the research is the improved technique for evaluating the effectiveness of conducting cyber warfare in support of the employment of force groupings in operations. In addition, the performance of the improved technique was experimentally verified on a test set of initial data. The results of the numerical experiment showed that the improved technique y is workable.*

Research novelty. *The improved technique for evaluating the effectiveness of conducting cyber warfare in support of the employment of force groupings in operations, unlike existing ones, allows for taking into account the influence of random factors on the course and results of conducting cyber warfare by applying certain provisions of the theory of stochastic differential equations at the stage of refining the initial data. The core of the improved technique is the author's mathematical model of the functioning of a protected information and communication system in the conditions of cyber warfare.*

Theoretical and practical significance. *The theoretical significance of the research results is the practical application of certain provisions of the theory of stochastic differential equations for modelling the course of a real random process – the functioning of a protected information and communication system in the conditions of conducting cyber warfare. The practical value of the obtained scientific result lies in the possibility of using an improved technique to predict the course and outcomes of cyber actions (cyber warfare) by officials of relevant military command bodies whose sphere of activity includes planning operations in cyberspace.*

Conclusions and future work. *The technique is universal and flexible in use, since on the one hand it takes into account the three-level architecture of the construction of almost all modern protected information and communication systems, and on the other hand it is extremely sensitive to changes in parameters (input data), which are unique for each individual system. The prospect of further research in this area is to increase the effectiveness of conducting cyber warfare.*

Keywords: *artificial intelligence, cyber warfare, effectiveness evaluation, forecasting, information technologies, information security, mathematical model, modelling.*

References

1. Hryschuk, R. V., Danyk, Yu. H., (2016). *Fundamentals of cyber security*: a monograph. Zhytomyr: ZhNAEU. **2. 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. DOI: https://doi.org/10.33099/2311-7249/2024-50-2-5-10. **3. Hrabar, I.H., Hryshchuk, R.V., & Molodetska, K.V.** (2019). *Bezpekova synerhetyka: kibernetychnyi ta informatsiinyi aspekty*. Hryshchuk, R. V. (Ed.). Zhytomyr: ZhNAEU. **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: https://doi.org/10.33099/2311-7249/2024-50-2-11-28. **5. 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*, 83 (1), 89-97. DOI: https://doi.org/10.30748/zhups.2025.83.11. **6. Kalaida, Yu. P.,** (2025). Hybrid cyberattacks in the conditions of the ukrainian-russian cyberwar. *Informatsiia i parvo*. 55 (4), 206-214. DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346481.

7. 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: https://doi.org/10.30748/soi.2025.180.02.

8. Murasov, R., Pharaon, S., Huk, O., (2025) Critical infrastructure cybersecurity: assessment and management of cyberattack risks. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, 54 (3), 75-83. DOI: https://doi.org/10.33099/2311-7249/2025-54-3-75-83.

9. Khoroshko, V., Shelest, M., Tkach, Yu., (2021). Multialternative detection of cyberattacks in information networks. *Ukrainian Scientific Journal of Information Security*, 27 (3), 136-140. DOI: https://doi.org/10.18372/2225-5036.27.16515.

10. Kumar, S., Nagar, G., (2024). Threat Modeling for Cyber Warfare Against Less Cyber-Dependent Adversaries. *23, 1 : Proceedings of the 23rd European Conference on Cyber Warfare and Security*, 27–28 June 2024, 257-264. DOI: https://doi.org/10.34190/eccws.23.1.2462. **11. 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*, 11 (1). DOI: https://doi.org/10.1093/cybsec/tyaf020. **12. 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: https://doi.org/10.33099/2311-7249/2025-52-1-77-84.

Рукопис надійшов до редакції *23.01.2026*
Рукопис прийнято до друку після рецензування *26.03.2026*
Дата публікації *30.04.2026*