**International Science Journal of Engineering & Agriculture**
2024; 3(5): 8-17
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20240305.02
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

# Удосконалений метод оцінки стійкості гетерогенних комп'ютерних мереж військового призначення в умовах активної дії дестабілізуючих факторів

**Ярослав Вячеславович Мельник**
Центр імітаційного моделювання, Національний університет оборони України, Київ, Україна
ORCID 0000-0002-2919-9119

**Для цитування цієї статті:**
Мельник Ярослав Вячеславович. Удосконалений метод оцінки стійкості гетерогенних комп'ютерних мереж військового призначення в умовах активної дії дестабілізуючих факторів. International Science Journal of Engineering & Agriculture. Vol. 3, No.5, 2024, pp. 8-17. doi: 10.46299/j.isjea.20240305.02.
**Надійшла до редакції:** 16 вересня 2024 р.; **Схвалено:** 30 вересня 2024 р.;
**Опубліковано:** 01 жовтня 2024 р.

**Анотація:** У роботі представлено методологічний підхід до оцінки стійкості гетерогенних комп'ютерних мереж. Метод передбачає використання сучасних математичних моделей та алгоритмів для оцінки вразливостей мережі, імітаційного моделювання її поведінки під впливом різних загроз та розробки рекомендацій щодо підвищення її стійкості. Критично важливим завданням для забезпечення безпеки та надійності функціонування військових систем, а особливо з початком агресії російської федерації проти України, є способи оцінки стійкості гетерогенних комп'ютерних мереж військового призначення в умовах активної дії противника. Запропонований метод оцінки стійкості гетерогенних комп'ютерних мереж військового призначення передбачає застосування перколяційних (в якості теоретичної основи використовується теорія перколяції) алгоритмів, які дозволяють моделювати динаміку мереж в умовах впливу зовнішніх загроз, таких як кібератаки або фізичних пошкоджень. Це забезпечує більш точну оцінку стійкості гетерогенних комп'ютерних мереж що є критично важливим для військових операцій, де швидка адаптація до умов що змінюються є необхідною умовою. Даний підхід дозволяє також врахувати відсутність достовірної інформації про показники стійкості складових мережі, які належать цивільним провайдерам послуг інтернету. Крім того, метод включає аналіз живучості системи, що дозволяє виявляти вразливі місця та своєчасно вживати заходів для їх усунення. Це важливо для підтримання безперервності функціонування мережі, особливо в умовах гібридних загроз, що характеризуються складністю і непередбачуваністю. Комп'ютерне моделювання запропонованого удосконаленого методу в математичному та програмному забезпеченні системи управління зв'язком військового призначення свідчить про підвищення ефективності функціонування як комп'ютерної мережі, так і системи зв'язку в цілому.

**Ключові слова:** стійкість, завадозахищеныть, гетерогенна комп'ютерна мережа, перколяційний кластер, локальна обчислювальна мережа, інформаційно-комунікаційні системи.

## 1. Вступ

Дослідження, яке виконане свідчать про значно зростаючі вимоги до підвищення оперативності процесів управління військами та озброєнням, темпу операцій (бойових дій), при значному скороченню часу циклу управління. При цьому підвищення ефективності виконання завдань військами не можливе без впровадженням сучасних інформаційних

технологій у роботу системи управління з'єднань, об'єднань та органів військового управління всіх рівнів Збройних Сил України та зразки озброєння і військової техніки та як наслідок формування єдиного інформаційного простору.

На створення єдиного інформаційного простору впливають особливості побудови сучасних автоматизованих систем управління військами, що вимагають побудови територіально розподілених комп'ютерних мереж, які повинні забезпечувати доступність та достовірність передачі необхідної інформації. Для цього необхідний розвиток складних гетерогенних комп'ютерних мережі (як компонента інформаційно-комунікаційної системи) сегменти яких можуть перебувати в різних регіонах країни на значній відстані один від одного. Створення окремої локальної мережі для кожної гетерогенної комп'ютерної мережі не представляється можливим, як з економічних, так і з технічних причин. Отже, необхідна інтеграція з існуючою комунікаційною мережею загального користування і, як наслідок з мережею Інтернет. Це призводить до появи великого ризику виходу елементів мережі з ладу в результаті впливу навмисних і навіть ненавмисних перешкод (експлуатаційних відмов, бойових та інших пошкоджень, кібератак тощо).

Слід також зазначити активний розвивиток широкого спектру нових методів і технологій кібернетичного впливу, як на окремі засоби обчислювальної техніки, так і на інформаційно-комунікаційні системи та автоматизовані системи військового управління.

Не зважаючи на впровадження різних методів, спрямованих на підвищення рівня захищеності інформаційних ресурсів в ІКС, наслідки кібервпливу, як у світі так і в Україні, залишаються достатньо високими та становлять проблему світового рівня. У зв'язку з цим, виникає нагальна потреба забезпечення ефективного функціонування ГКМ військово призначення в умовах експлуатаційних відмов, бойових та інших пошкоджень, наприклад, кібератак.

Доведено те, що гетерогенні комп'ютерні мережі (ГКМ) військового призначення є складовою або підсистему системи зв'язку та автоматизованого управління військами ЗС України. Варте зазначити те, що використання обладнання цивільних провайдерів послуг інтернету для ГКМ військового призначення надає нові можливості щодо збільшення основних показників ефективності мережі, але створює об'єктивні умови для розробки нових підходів оптимізації будь яких завдань.

У даній роботі пропонується удосконалений метод оцінки стійкості гетерогенних комп'ютерних мереж військового призначення, який базується на інтеграції різних видів аналізу, моделювання загроз та оптимізації захисних стратегій. Це дозволяє не лише оцінювати поточний стан мережі, але й передбачати можливі наслідки дестабілізацій та розробляти ефективні заходи для їхнього попередження або мінімізації шкоди.

## 2. Об'єкт і предмет дослідження

**Об'єкт дослідження** – процес функціонування гетерогенних комп'ютерних мережам військового призначення [1] в умовах зовнішніх та внутрішніх дестабілізуючих факторів.

Гетерогенні комп'ютерні мережі військового призначення, що функціонують в умовах зовнішніх та внутрішніх дестабілізуючих факторів це досить складні інфраструктури, які поєднують різні типи програмного та апаратного забезпечення, комунікаційних технологій і протоколів для забезпечення надійного функціонування військових підрозділів. Такі мережі інтегрують різнорідні системи, включаючи провідні та безпровідні мережі, супутникові канали зв'язку, мобільні пристрої, сенсори, системи управління військами та зброєю, а також елементи штучного інтелекту [3].

**Предмет дослідження** – стійкість гетерогенних комп'ютерних мережам військового призначення, які в своїм складі використовують обладнання провайдерів послуг інтернету та функціонують в умовах зовнішніх та внутрішніх дестабілізуючих факторів.

## 3. Мета та задачі дослідження

Метою дослідження є доведення наукового результату, а саме, удосконаленого методу оцінки стійкості гетерогенних комп'ютерних мереж військового призначення в умовах активної дії дестабілізуючих факторів. Теоретичним підґрунтям методу є складова теорія випадкових графів – теорія перколяції.

Тому, для виконання мети дослідження було визначено такі задачі:

Визначення зовнішніх (кібератаки, електромагнітні перешкоди, фізичне знищення в наслідок ураження противником) та внутрішніх (технічні збої в роботі обладнання, помилки конфігурації, програмного та апаратного забезпечення, а також людські фактори) дестабілізуючих факторів, що впливають на функціонування гетерогенних комп'ютерних мереж військового призначення.

Аналіз сучасних підходів до оцінки стійкості комп'ютерних мереж, виявлення їхніх обмежень та недоліків у контексті військового призначення гетерогенних мереж.

Формулювання нових підходів до оцінки стійкості мереж, які враховують специфіку гетерогенних архітектури, різних типів загроз та умови управління військами оперативного рівня. Розробка математичних моделей та алгоритмів для інтеграції цих підходів.

Використання імітаційного моделювання для створення реалістичних сценаріїв дії дестабілізуючих факторів на мережу та тестування стійкості запропонованих рішень в умовах загроз що змінюються.

Проведення серії експериментів та симуляцій для перевірки стійкості мереж у різних сценаріях, оцінка результатів та їх порівняння з існуючими методами.

Розробка рекомендацій щодо практичного впровадження удосконаленого методу оцінки стійкості в систему управління військовими оперативного рівня для підвищення їхньої ефективності в умовах ведення операцій (бойових дій).

Актуальність забезпечення властивості стійкості гетерогенним комп'ютерним мережам військового призначення, які в своїм складі використовують обладнання провайдерів послуг інтернету та будуть функціонувати в умовах непрогнозованої зміни сегментів, обумовленої активними діями противника та іншими чинниками доведена та не викликає сумніву.

## 4. Аналіз літератури

В межах даного дослідження з використанням методу статистичного моделювання Монте-Карло виконана оцінка інтегрального показника стійкості ГКМ військового призначення, які будувалися на основі так званих класичних підходів (ці методики описані в [4,5,6], при моделюванні обране чотири варіанти). В деяких випадках ГКМ була нестійкої, а узагальнений показника стійкості ГКМ – імовірність функціонування мережі (імовірність стійкості) дорівнює 0,67. А це не відповідає сучасним вимогам до систем зв'язку військово призначення (рис. 1).

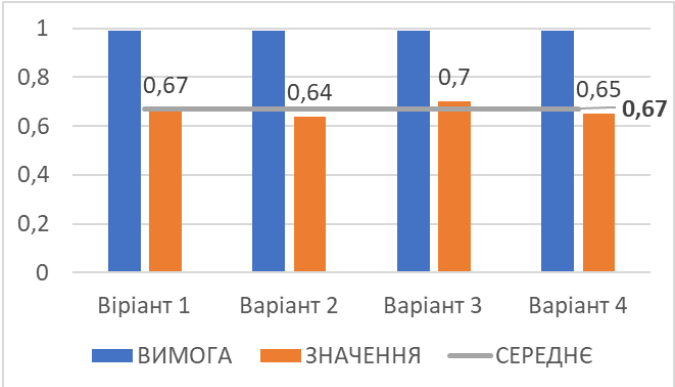


**Рис.1.** Результати моделювання.

Дослідження показало обмеженість використання існуючих наукових та інженерних підходів при забезпеченні гетерогенним комп'ютерним мережам військового призначення такої властивості, як стійкість. Іншими словами існує невідповідність між обмеженістю наукового апарату за темою розробки сучасних комп'ютерних мереж загального призначення та необхідністю забезпечення властивості стійкості гетерогенним комп'ютерним мережам військового призначення, які діють умовах експлуатаційних відмов, активної дії противника та мають в своїм складі обладнання цивільних провайдерів послуг інтернету.

## 5. Методи досліджень

Запропонований удосконалений метод оцінки стійкості гетерогенних комп'ютерних мереж (ГКМ) базується на фундаментальних принципах теорії перколяції, яка ефективно описує поведінку складних систем. Сутність теорії перколяції в наступному: процес передачі пакетів з потрібною інформацією, з одного локального сегменту мережі до іншого, може бути представлений у вигляді "просочування" корисного трафіку від джерела інформації до споживача інформації. Застосування цього підходу до оцінки стійкості ГКМ дозволяє кількісно оцінити їх здатність зберігати функціональність при впливі дестабілізуючих факторів.

У роботі використовуються наступні основні методи:

Методи теорії перколяції для аналізу та оцінки перколяційних процесів: Теорія перколяції використовується для моделювання стійкості елементів ГКМ. Основною ідеєю є визначення критичної щільності з'єднань у мережі, після якої відбувається руйнування мережі на окремі, незв'язані між собою сегменти (елементи).

Теорія графів для моделювання топології ГКМ. Модель мережі будується як граф, де вершини представляють вузли, а ребра – канали зв'язку між ними. Що дозволяє застосовувати методи графів для аналізу з'єднаності мережі, її стійкості та вразливості до випадкових (random attack) та спрямованих атак (targeted attack).

Методи математичного моделювання, а саме імовірнісні моделі перколяції та моделі на основі дискретних процесів. Імовірнісні методи використовуються для моделювання випадкових процесів видалення або відмов вузлів і з'єднань. Що дозволяє оцінювати ймовірність руйнування мережевої структури [14] та втрат зв'язності в умовах дії дестабілізуючих факторів. У свою чергу застосування дискретних стохастичних процесів дозволяє моделювати поширення відмов у мережі під дією атак чи збоїв, а також визначати умови, за яких відбудеться критичне порушення роботи мережі.

Методи імітаційного моделювання використовуються для вивчення впливу різних типів дестабілізуючих факторів (кібератаки, фізичні руйнування, електромагнітні перешкоди) на структуру мережі та аналізу сценарію катастрофічних відмов. Імітаційні сценарії дозволяють дослідити, як мережа руйнується і як вона може адаптуватися до втрат особливо під час одночасного виходить з ладу велика кількість вузлів або з'єднань.

5. Емпіричні методи, а саме експериментальні дослідження стійкості. Проведення експериментів на реальних або лабораторних мережах для перевірки теоретичних результатів. Це дозволяє оцінити реальну стійкість системи в умовах впливу дестабілізуючих факторів [9].

Використання теорії перколяції в поєднанні з цими методами дає змогу глибше зрозуміти поведінку ГКМ під дією дестабілізуючих факторів та розробити ефективні інструменти їх захисту і адаптації.

## 6. Результати досліджень

Стійкість гетерогенних комп'ютерних мереж, особливо військового призначення, є ключовим показником здатності мережі функціонувати під впливом певних дестабілізуючих факторів (кібератак, фізичних пошкоджень, електромагнітних впливів). Іншими словами

стійкість це здатність системи зв'язку і автоматизації управління військами (АУВ) виконувати завдання в умовах впливу різноманітних факторів. Слід також розуміти що для системи зв'язку стійкість поєднує такі властивості як надійність, живучість, кіберзахищеність та завадозахищеність.

Гетерогенність (тобто неоднорідність) комп'ютерних мереж полягає у відмінностях між елементами інфраструктури мережі, оскільки вони мають різні характеристики надійності, захищеності, пропускної спроможності та важливості.

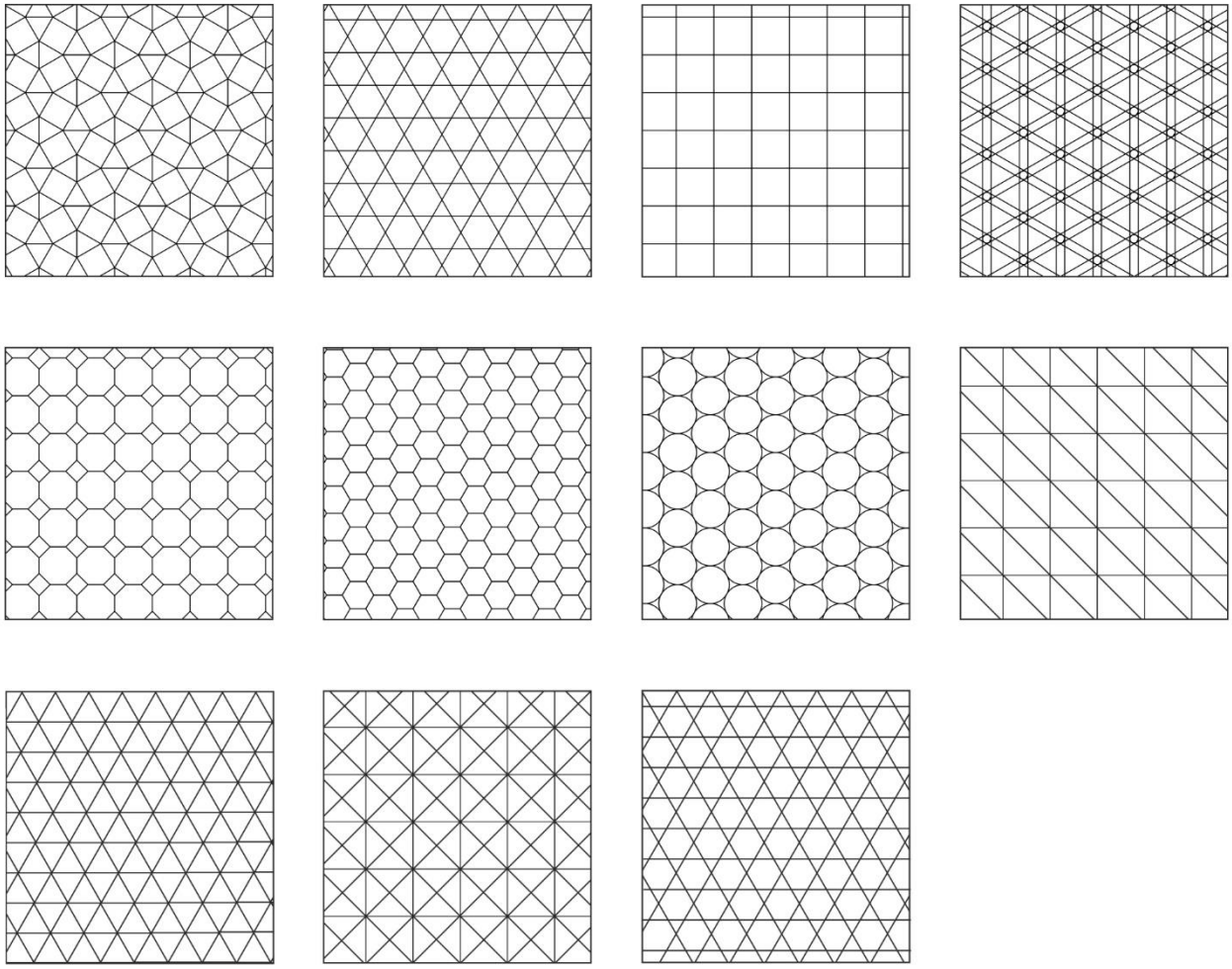

**Рис. 1**. Приклади регулярних решіток різної конфігурації.

На відміну від регулярних решіток (малюнок 1) та довільно-масштабованих графів які добре вивчені та побудовані відповідно до відомих правил, реальні структури ГКМ не мають регулярних структур або структур [15], визначених конкретними правилами, що ускладнює, а в деяких випадках унеможливлює, знаходження узагальненого аналітичного рішення.

Для вирішення задач статті було обрано теорію перколяції складова теорії графів. Теорія перколяції [8], аналізує перехід систем з різнорідним (хаотичним) розподілом елементів від зв'язаного стану до ізольованого та є потужним інструментом для визначення стійкості ГКМ до відмов. Основна ідея полягає у визначенні критичного порогу перколяції на основі топології мережі, особливостей дестабілізуючих факторів і різнотипності її компонентів. Величина порогу перколяції визначається за допомогою методу статистичного моделювання Монте-Карло. Поріг перколяції [12] (поріг "просочування" для регулярних решіток визначений та має певне критичне значення (як приклад, для квадратичної решітки він складає 0,5927)) в загальному розумінні це мінімальна концентрація елементів при якій в безмежній системі (наприклад решітці чи графі) вперше виникає нескінченний кластер, який пов'язує усі елементи системи. Цей кластер має назву перколяційний [11]. Отже в нашому випадку у ГКМ

під перколяційним кластером розуміється кластер функціональних елементів, з'єднаних лініями зв'язку, який включає принаймні один граничний вузол від кожної територіально рознесеною ГКМ. ГКМ моделюємо як нескінченний граф [13] $Y\ (S, L)$, де $S = \{s_1, s_2, \dots, s_n\}$ – вузли мережі, а $L = \{l_1, l_2, \dots, l_n\}$ це канали зв'язку. Межові вузли $R_l = \{r_i\}$ – це вузли що мають підключення або інтегрується до зовнішньої мережі (інтернету), та відповідають вимогам $R_l \subset S$. Вузли мережі також можуть мати різні характеристики, показники надійності та захищеності, тому задають:

$p_{\text{над}}$ – надійність вузла $r_i$,

$p_{\text{зах}}$ – захищеність вузла $r_i$.

Вся сукупність вузлів однієї ЛОМ утворює межі, з яких визначається множина $G$.

$$G = \{g_j\}, |g_j| > 0, |G| \geq 2, \tag{1}$$

де g — межа, r — ключовий вузол, та відповідає вимогам $g_j \subset r_i$. Один ключовий вузол належить строго одній межі $\cap_j g_j = \emptyset$. При цьому кластер $W$ вважається перколяційним у тому і тільки в тому випадку, якщо він містить хоча б однин вузол з кожної межі.

$$W \bigcap_j g_j \neq \emptyset, \tag{2}$$

В умовах активної дії дестабілізуючих факторів ймовірність збереження з'єднань $p_{\text{зз}}$ між територіально рознесеними сегментами ГКМ [10] за певний інтервал часу, протягом якого вузли, які вийшли з ладу не можуть бути відновлені, визначається як імовірність збережеться зв'язку між множинами межових вузлів ГКМ [7], через які здійснюється доступ (інтеграція) з Інтернет. Узагальнена блок-схема удосконаленого методу оцінки стійкості ГКМ представлений на малюнку 2.

З початку проводимо ініціалізацію мережі, визначаємо топології мережі та відповідні ймовірнісні характеристики (коефіцієнти) вузлів і каналів та задаємо вихідні дані (блок 1 малюнок 2). Структура ГКМ представляємо у вигляді нескінченного (безмежного) графу, вузлами $s_i$ якого є елементи мережі, а ребрами $l_i$ – зв'язки між ними. Вузли локальних сегментів, за допомогою яких відбувається інтеграція з мережею Інтернет, визначають множину $G$ відповідно до формули (1). Далі задаються імовірності надійності $p_{\text{над}}$ та захищеності $p_{\text{зах}}$ вузла та визначаємо максимальну стійкість вузла $p_{\text{ст}}$ до впливу дестабілізуючих факторів (3).

$$p_{\text{ст}} = p_{\text{над}} * p_{\text{зах}}, \tag{3}$$

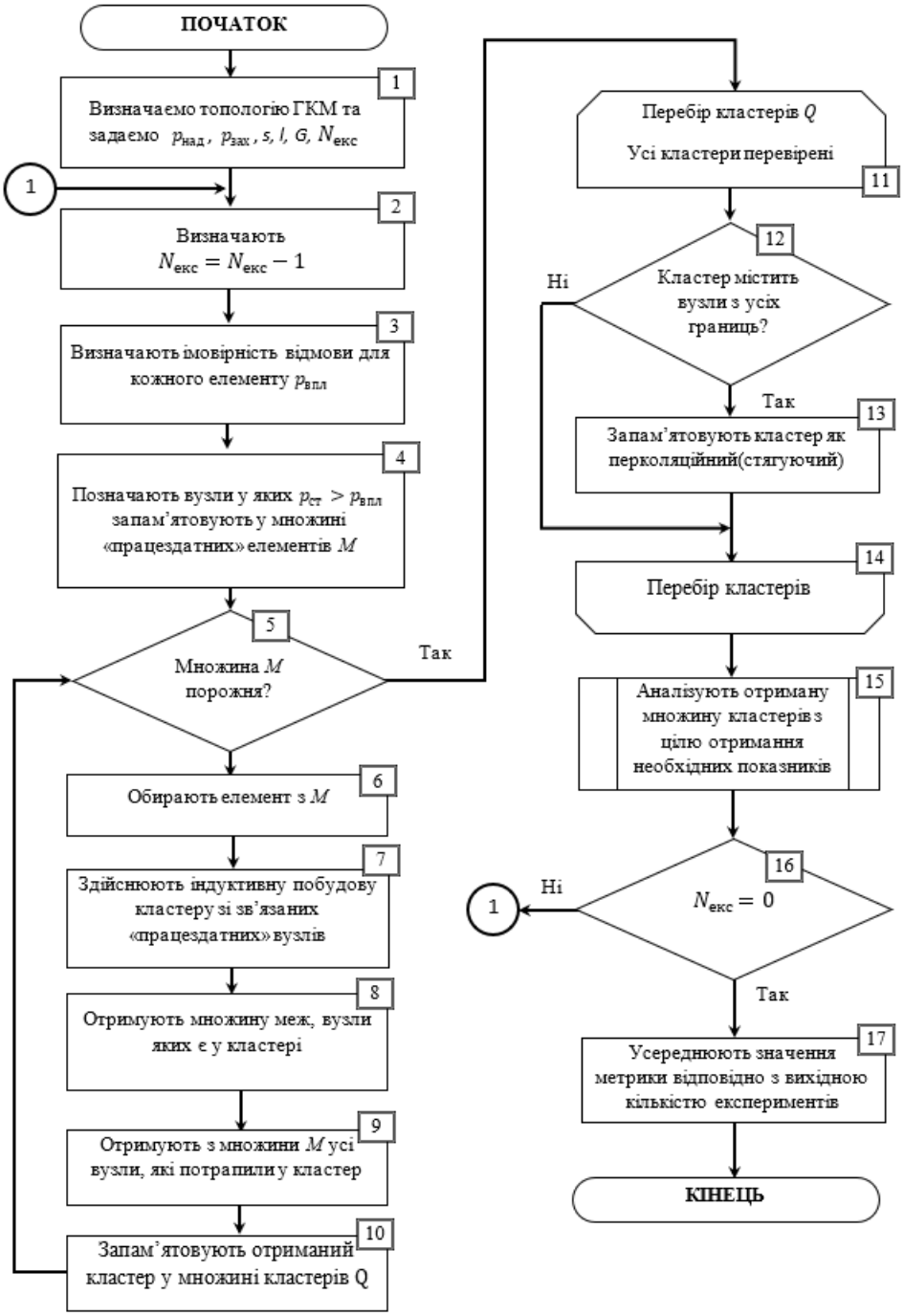


**Рис 2.** Блок-схема узагальненого удосконаленого методу оцінки стійкості ГКМ військового призначення в умовах активної дії дестабілізуючих факторів.

За допомогою методу статистичного планування визначається кількість необхідних експериментів $N_{\text{екс}}$, та обчислюється за формулою довірчого інтервалу (4):

$$N_{\text{екс}} = ( Z_{\frac{\alpha}{2}} * \delta/E)^2, \quad (4)$$

де $Z_{\frac{\alpha}{2}}$ – значення стандартного нормального розподілу для заданого рівня надійності, δ – стандартне відхилення результатів експериментів, $E$ – максимальна допустима похибка.

Далі зменшуємо кількість експериментів на одиницю (блок 2 малюнка 2).

Кожному окремому вузлу мережі за рівномірним законом розподілу встановлюється $p_{\text{впл}}$. (блок 3 малюнок 2). Вузли, у яких, імовірність стійкості вища за імовірність впливу $p_{ст} > p_{впл}$ запам’ятовують у множині працездатних вузлів $M$, які можуть брати участь у забезпеченні трафіку між абонентами (блок 4 малюнок 2). За допомогою системи множин що не перетинаються отримуємо відповідну множину кластерів, які у своєму складі мають працездатні зв'язані між собою вузли.[8,11] Реалізація на практиці має наступний вигляд. Обирають перший будь-який вузол з множини $M$ (блок 6 малюнок 2) та створюють множину $H$, в яку входять ці вузли. Обраний вузол видаляють з множини $M$ (блок 9 малюнок 2). Для кожного вузла що був доданий в множину $H$ послідовно обирають дану процедура допоки існують усі зв’язані з черговим вузлом вузли (блок 7 малюнок 2). Дану процедуру повторюють поки множина $M$ не стане порожнім (блок 5 малюнок 2). При побудові множини $H$ перевіряється належність вузла до певної межі, і у позитивному випадку, зберігають ідентифікатор межі. Зберігають усі отримані кластери множини $H$ у множині кластерів $Q$ (блок 10 малюнок 2).

Перебирають усі кластери з множини $Q$ (блоки 11-14 малюнок 2) і перевіряють, чи містить відповідний кластер вузли усіх меж (блок 12 малюнок 2). Далі визначають кластер який містить хоча б по одному вузлу з кожної межі та зберігають у множині перколяційних кластерів $D$. Множину $D$ аналізують та отримуються потрібні метрики (блок 15 малюнок 2), а саме розмір працездатного кластеру, імовірність збереження зв’язку між межами локальних сегментів, імовірність утворення зв'язку між випадково обраним вузлом ГКМ і межами локальних сегментів.

На кінцевому етапів зменшують кількість експериментів $N_{\text{екс}}$ на одиницю, допоки $N_{\text{екс}} > 0$, переходять на наступний крок 2 (блок 16 малюнок 2). Цикл завершується у випадку коли $N_{\text{екс}} = 0$, тоді усереднюють отримані на кожному циклі метрики та закінчують виконання розрахунку (блок 17 малюнок 2).

## 7. Перспективи подальшого розвитку досліджень

Вибір ГКМ військового призначення як об'єкта дослідження та використання теорії перколяції в якості методу оцінки стійкості обґрунтований низкою переваг, які роблять цей підхід зручним і вигідним у контексті розробленої удосконаленої методики. Оскільки удосконалений метод адаптований до ГКМ, дозволяє моделювати вплив дестабілізуючих факторів та дозволяє підвищити ефективність управління військами (силами).

Подальший розвиток удосконаленого методу оцінки стійкості військових комп’ютерних мереж на основі теорії перколяції повинен бути спрямований на інтеграцію новітніх технологій, таких як машинне навчання, адаптивні алгоритми та кіберзахист, а також на врахування нових типів загроз і розширення моделі для більш складних систем. Що дозволить підвищити ефективність і надійність функціонування військових мереж в умовах активної дії дестабілізуючих факторів.

## 8. Висновки

Підсумовуючи, слід зазначити що ГКМ військового призначення є складними системами, що включають різні типи вузлів і каналів зв'язку, кожен з яких має свої специфічні характеристики надійності, пропускної здатності та захищеності. Їх ефективна робота критично залежить від здатності функціонувати під впливом дестабілізуючих факторів. Удосконалений метод оцінки стійкості, заснований на теорії перколяції, дозволяє ефективно моделювати процес ураження ГКМ в умовах деструктивних впливів, таких як кібератаки, фізичні атаки, збої обладнання або перебої в зв'язку. Він дозволяє визначити критичні елементи мережі, вихід з ладу яких призводить до деградації або повної втрати працездатності системи. Математична модель враховує не лише надійність окремих вузлів і каналів, але й

рівень їх захищеності від зовнішніх атак. Це дає змогу комплексно оцінювати стійкість мережі як з точки зору технічної надійності, так і кіберзахищеності. Гнучкість і адаптивність запропонованого методу дозволяє застосовувати його для різних типів мереж, їх масштабів і умов функціонування. Він легко інтегрується в реальні військові системи та здатний швидко адаптуватися до змін у топології мережі або під час дестабілізуючих впливів. Застосування цього методу у ГКМ військового призначення підвищує ефективність управління мережевими ресурсами, оптимізує захист від загроз і забезпечить стабільність функціонування мереж в умовах активних дій дестабілізуючих факторів.

---

**Список літератури:**

1) Антонов В.М. *Комп'ютерні мережі військового призначення* / В.М. Антонов, О.Ю. Пермяков – К.: МК-Прес, 2005. – 320 с.

2) Довгий С.О. *Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання.* / Довгий С.О., Воробієнко П.П., Гуляєв К.Д. – К.: Азимут-Україна. 2013. – 608 с.

3) *Елементи дослідження складних систем військового призначення*: [навч. посіб.] / О.М. Загорка, С.П. Мосов, А.І. Сбітнев, П.І. Стужук. – К.: НАОУ, 2005. – 100 с.

4) Мельник Я.В., Мурасов Р.К., Кононенко С.М. Застосування теорії перколяції для оцінювання стійкості гетерогенних мереж в умовах кібератак. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2017. № 2 (29). С.54-58.

5) Мельник Я.В., Пермяков О.Ю., Кільменінов О.А. Застосування перколяційних алгоритмів для оцінки надійності гетерогенних мереж військового призначення. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2019. № 1 (34). С.23-27. URL: https://doi.org/10.33099/2311-7249/2019-34-1-23-28

6) Мельник Я.В., Куртсеітов Т.Л., Мурасов Р.К. Обчислення надійності системи критичної інфраструктури шляхом декомпозиції її як складної системи К.: НУОУ. ISSN 2522-9842 *Journal of Scientific Papers "Social Development and Security",* Vol. 12, No. 5, 2022. С.84-92. DOI: 10.33445/sds.2022.12.5.8

7) Савченко В.А., Моделювання кібератак засобами теорії графів // В.А. Савченко, О.Й. Мацько, С.В. Легомінова, І.С. Полторак, В.В. Марченко // *Сучасний захист інформації* №4(40), 2019. – С. 6-11.

8) Тарасевич Ю.Ю. Перколяция: теория, приложения, алгоритмы. Либроком, 2018. 116 с.

9) Толюпа С.В. *Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз* / Лукова-Чуйко Н.В., С.В. Толюпа, В.С. Наконечний, Браіловський М.М.: монографія. – К.: Формат, 2021. – 407 с.

10) Analysis of Social Network Parameters and the Likelihood of its Construction / V. Savchenko, V. Akhramovych, A. Tushych, I. Sribna, I. Vlasov *// International Journal of Emerging Trends in Engineering Research.* Volume 8 No. 2 (February 2020). pp. 271 – 276.

11) Broadbent S.K., Hammersley J.M. Percolation processes I. Crystals and mazes // *Proceedings of the Cambridge Philosophical Society* 53, 629-641

12) Don R. Baker, Gerald Paul, Sameet Sreenivasan, and H. Eugene Stanley. Continuum percolation threshold for interpenetrating squares and cubes. Phys. Rev. E, 66(4):046136, Oct 2002.

13) Fractal functions and their application to source data coding / Zamrii I., Sobchuk V., Laptiev O., Savchenko V., Shkapa V., Kovalenko V. and Kotok V. ARPN Journal of Engineering and Applied Sciences. Vol. 17, No. 4, February 2022. pp.424-435.

14) Kravchenko Y., O. Afanasyeva, M. Tyshchenko,S. Mykus, "Intellectualisation of Decision Support Systems For Computer Networks: Production-Logical F-Inference", International conference Information Technology and Interactions, IT&I-2020, CEUR Workshop Proceedings, 2021, 2845, pp. 117–126.

15) Kravchenko, Y., Leshchenko, O., Dakhno, N., Pliushch, O.,Trush, O., Yermakov, Y. Development of Model of Artificial Ecosystem on the Basis of Genetic Algorithm. 2022 IEEE 4th

International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 199–203.

## An improved method of assessing the stability of heterogeneous military computer networks in conditions of active action of destabilizing factors

**Yaroslav Melnyk**
Simulation Centre, National Defense University of Ukraine, Kyiv, Ukraine
ORCID 0000-0002-2919-9119

**Abstract:** The work presents a methodological approach to assessing the stability of heterogeneous computer networks. The method involves the use of modern mathematical models and algorithms for assessing the network's vulnerabilities, simulating its behavior under the influence of various threats, and developing recommendations for increasing its stability. A critically important task for ensuring the security and reliability of the operation of military systems, and especially with the beginning of the aggression of the Russian Federation against Ukraine, are methods of assessing the stability of heterogeneous computer networks of military purpose in conditions of active enemy action. The proposed method of assessing the stability of heterogeneous military computer networks involves the use of percolation (percolation theory is used as a theoretical basis) algorithms that allow modeling the dynamics of networks under the influence of external threats, such as cyber attacks or physical damage. This provides a more accurate assessment of the resilience of heterogeneous computer networks, which is critical for military operations where rapid adaptation to changing conditions is a must. This approach also allows us to take into account the lack of reliable information about the stability indicators of network components belonging to civilian Internet service providers. In addition, the method includes an analysis of the system's survivability, which allows you to identify vulnerabilities and take measures to eliminate them in a timely manner. This is important for maintaining the continuity of the network, especially in the conditions of hybrid threats, which are characterized by complexity and unpredictability. Computer modeling of the proposed improved method in the mathematical and software support of the military communications management system indicates an increase in the efficiency of the functioning of both the computer network and the communications system as a whole.

**Keywords:** stability, survivability, heterogeneous computer network, percolation cluster, local computing network, information and communication systems.