УДК 004.056.5:351
**DOI:** 10.31673/2412-9070.2023.064448

**Я. В. МЕЛЬНИК**, здобувач;
**В. Б. БІЛАВКА**, аспірант,
Національний університет оборони України, Київ

# МОДЕЛЬ КІЛЬКІСНОГО ОЦІНЮВАННЯ СТІЙКОСТІ ГЕТЕРОГЕННИХ КОМП'ЮТЕРНИХ МЕРЕЖ ЗА УМОВ ПОШИРЕННЯ ВПЛИВУ ЛОГІЧНОЇ ЗАВАДИ НА ОСНОВІ ТЕОРІЇ ПЕРКОЛЯЦІЇ

***Тенденції останніх років, особливо з початком агресії рф проти України, свідчать про дедалі вищі вимоги до підвищення оперативності процесів керування органами державної влади зі значним скороченням часу циклу керування. При цьому удосконалення ефективності виконання завдань неможливе без упровадження сучасних інформаційних технологій у роботу на всіх рівнях державного керування, та, як наслідок, формування єдиного інформаційного простору. У статті розглянуто особливості створення сучасних автоматизованих систем керування, що потребують побудови територіально розподілених, при цьому неоднорідних (гетерогенних) комп'ютерних мереж, які мають забезпечувати доступність та вірогідність передавання необхідної інформації, зокрема за умов поширення впливу логічної завади (навмисних — кібератак із боку хакерів та ненавмисних дій користувача, системного адміністратора та ін.), що також впливають на формування єдиного інформаційного простору. Опрацьовано підходи до забезпечення властивості стійкості гетерогенних комп'ютерних мереж, які зі свого боку використовують обладнання провайдерів послуг інтернету за умов зовнішніх та внутрішніх дестабілізувальних факторів. Запропоновано математичну модель оцінювання стійкості гетерогенних комп'ютерних мереж критичного призначення за умов впливу логічної завади. Водночас як теоретична основа застосовано теорію перколяції. Такий підхід дає змогу брати до уваги відсутність вірогідної інформації про показники стійкості складових мережі, які належать різним (непідконтрольних органам державного керування) провайдерам послуг інтернету. Комп'ютерне моделювання на основі запропонованої математичної моделі свідчить про підвищення ефективності комп'ютерної мережі загалом.***

**Ключові слова:** стійкість; телекомунікаційна мережа загального користування; гетерогенна комп'ютерна мережа; перколяційний кластер; математична модель.

## *ВСТУП*

На створення єдиного інформаційного простору впливають особливості побудови сучасних систем керування, що потребують формування територіально розподілених мереж та розвитку складних гетерогенних комп'ютерних мереж (ГКМ). При цьому сегменти цієї ГКМ можуть перебувати в різних регіонах країни на значній відстані один від одного. Створення окремої локальної мережі для кожної ГКМ не є можливим як з економічних, так і з технічних причин. Отже, потрібна інтеграція з наявною телекомунікаційною мережею загального користування і, як наслідок, із мережею «Інтернет». Це зумовлює появу великого ризику виходу елементів мережі з ладу через вплив навмисних і навіть ненавмисних завад: експлуатаційних відмов, бойових та інших пошкоджень, кібератак. Наслідком виходу з ладу лише одного важливого елемента мережі може стати руйнування комп'ютерної мережі та неможливість здійснювати обмін даними, що зі свого боку може призвести до тимчасової втрати системи керування загалом. Водночас найбільш небезпечними є дії від реалізації кібератак, оскільки вони виникають епізодично, можуть мати груповий або адресний характер та спричинити тимчасову втрату керування. Отже, напрям досліджень, пов'язаний із побудовою складних гетерогенних комп'ютерних мереж, є сучасним та актуальним.

**Постановка проблеми.** У процесі проєктування та експлуатації гетерогенних комп'ютерних мереж цілком логічним є завдання оцінити їх стійкість. А отже, створення математичної моделі оцінювання стійкості ГКМ за умов активної дії поширення впливу логічної завади є нагальним та своєчасним.

**Аналіз останніх досліджень і публікацій.** Останніми роками значно зросла увага стосовно досліджень і публікацій щодо оцінювання стійкості неоднорідних складних технічних систем та концептуальних засад побудови стійких розподілених інформаційних систем.

Не існує конкретного імені або особи, яку можна було б назвати засновником теорії стійкості інформаційних систем, але існують багато дослідників та вчених, які зробили значний внесок у розвиток цієї галузі. Так, Рита Руби Альберт та Альберт-Ласло Барабазі [1] розглядають останні досягнення в галузі складних мереж, зосереджуючись на статистичній механіці мережної топології та динаміки. Автори описують основні моделі й аналітичні інструменти, що охоплюють випадкові графіки, мережі «малого світу» та мережі без масштабу, а також взаємодію між топологією та надійністю мережі проти збоїв і кібератак. У подальших дослідженнях Альберт-Ласло Барабазі [2] досяг прогресу в розумінні складних мереж, які

характеризують взаємодію між складовими системи. Ці мережі збиралися та розвивалися завдяки додаванню та видаленню вузлів і зв'язків, динамічних процесів, які зрештою визначали їх топологію. Він довів, що мережі, які з'являються в різноманітних системах, мають спільні топологічні та динамічні характеристики, що вказує на існування надійних принципів самоорганізації та еволюційних законів, які керують взаємозв'язаним природним і соціальним світом навколо нас.

Серед вітчизняних учених теорія стійкості інформаційних систем набула подальшого розвитку в роботах професорів Барабаша О. В. і Кравченка Ю. В. [3], які зробили внесок у розвиток понятійного апарату і розв'язали проблему забезпечення стійкості для конкретних технічних систем. Барабаш О. В. уперше формалізував і довів основну відмінність стійкості функціонування від функціональної стійкості.

Отже, стійкість гетерогенних інформаційних систем розглядається як складна галузь досліджень, в яку зроблено вагомий внесок багатьма вченими в усьому світі.

Водночас сучасні дослідження і публікації не зважають на теперішні зміни в середовищі функціонування гетерогенних інформаційних систем критичного призначення та на потребу в побудові територіально розподілених, при цьому неоднорідних (гетерогенних) комп'ютерних мереж, які мають забезпечувати доступність і вірогідність передавання потрібної інформації, зокрема за умов впливу логічної завади.

**Формулювання мети статті.** Метою статі є обґрунтування та розроблення математичної моделі оцінювання стійкості гетерогенних комп'ютерних мереж критичного призначення за умов активної дії логічної завади. Теоретичним підґрунтям математичної моделі є складова теорії випадкових графів — теорія перколяції.

Варто звернути увагу на те, що стійкість ГКМ критичного призначення — це її властивість виконувати завдання за призначенням за умов впливу:

- експлуатаційних відмов, зумовлених вичерпанням ресурсу, фізичним старінням та конструктивними недоліками;
- бойових та інших пошкоджень (наприклад, кібератак та завад), які не мають експлуатаційного характеру.

Чисельні показники стійкості як мережі загалом, так і її сегментів мають імовірнісний зміст:

- імовірність стійкості мережі;
- імовірність стійкості сегмента мережі.

Отже, актуальність забезпечення властивості стійкості гетерогенних комп'ютерних мереж критичного призначення, які у своєму складі використовують обладнання провайдерів послуг інтернету та здатні функціонувати за умов непрогнозованої зміни сегментів, зумовленої впливом логічної завади, цілком доведено та не викликає сумніву.

## *ОСНОВНА ЧАСТИНА*

У межах запропонованого дослідження з використанням методу статистичного моделювання Монте-Карло здійснено оцінювання інтегрального показника стійкості наявних ГКМ критичного призначення, які будувалися на основі так званих класичних підходів (описано в [4-8], у процесі моделювання вибрано чотири варіанти). Час від часу ГКМ була нестійкою та не відповідала сучасним вимогам стійкості мереж загалом.

Дослідження теорії моделювання складних технічних систем із метою визначення адекватного підходу для вирішення завдання побудови стійких ГКМ підтверджують ідею, яка є в основі наукових результатів статті. Сутність цього в такому: процес передавання пакетів із потрібною інформацією з одного локального сегмента мережі до іншого, може бути подано як «протікання» корисного трафіку від постачальника до споживача. Для опису процесів просочування доцільно використовувати теорію перколяції — складову теорії випадкових графів.

Основний об'єкт дослідження теорії перколяції — стягувальний або перколяційний кластер, тобто кластер, який з'єднує дві протилежні сторони системи. Теорія перколяції вивчає умови створення та властивості перколяційного кластера. Більшість результатів теорії перколяції здобуто в результаті комп'ютерного моделювання. При цьому доводилося проводити тисячі комп'ютерних випробувань на великих об'єктах. Багаточисленне моделювання показало, що такий процес є критичним, тобто існує поріг, подолання якого змінює ймовірність утворення кластера з 0 до 1.

Значення порога перколяції визначається за допомогою методу статистичного моделювання Монте-Карло. Задаємо кожному вузлу випадкове число $p$, що позначає максимальну стійкість вузла до деструктивного впливу завади. Пов'язані між собою вузли, які працюють після деструктивного впливу завади, утворюють функціонувальні кластери. Після впливу завади вузли, що працюють, можуть зберігати перколяційний кластер. За допомогою комп'ютерного моделювання виявлено закономірність, наприклад, перколяційний кластер у квадратній решітці вперше утворюється при $p = p_{зб} \approx 0{,}593$, де $p_{зб}$ — імовірність збереження перколяційного кластера, та було здобуто залежність кількості стійких вузлів від розміру решітки, яка має значення для подальших результатів [9].

У телекомунікаційних мережах загального користування неможливо передбачити стійкість того чи іншого вузла до завади. Це пов'язано з тим, що

невідомі характеристики вузла (наприклад, вони можуть змінитися внаслідок оновлення програмного забезпечення) і неможливо передбачити ступінь впливу через відкритість та загальнодоступність мережі загального користування.

### *Модель кількісного оцінювання стійкості гетерогенних комп'ютерних мереж критичного призначення за умов впливу логічної завади*

Для аналізу завади, яка значно підвищує ймовірність відмови елементів ГКМ, потрібно знати структуру ГКМ. Для організації територіально розподілених компонентів інформаційних систем органів державної влади використовуються ресурси мережі зв'язку загального користування, які також мають зв'язок з глобальною мережею «Інтернет». Існує багато варіантів альтернативних маршрутів для передавання інформаційних пакетів між компонентами ГКМ, при цьому в певний момент часу пакети передаються за маршрутами, заздалегідь погодженими з постачальником телекомунікаційних послуг (віртуальними каналами). Такі канали виділяються для передавання трафіку з певними параметрами і використовують частину доступних елементів. Для різних типів трафіку може бути зарезервовано різні віртуальні канали. Водночас рішення щодо введення в маршрут того або іншого вузла ухвалюються самим вузлом на основі його поточного стану та необхідних ресурсів. Також існує значна невизначеність у характеристиках трафіку, який передається мережами загального користування, і навантаженні, яке ним створюється на вузли ГКМ. Отже, виникає протиріччя між потребою оцінити поширення логічної завади і відсутністю аналітичних методів розв'язання.

Змоделювавши процес перколяції на структурі всіх вузлів, які можуть брати участь у процесі передавання інформаційних потоків, можна дістати різні конфігурації передавання маршрутів між ключовими вузлами ГКМ. Імовірність уведення вузла має бути вищою за критичну ймовірність створення перколяційного кластера [9]. Для кожної отриманої конфігурації можна провести аналіз поширення завади з однієї або кількох точок впливу. Для цього кожному вузлу, що увійшов у перколяційний кластер, надається комплексний показник стійкості до завади $k$. На основі цього показника або за будь-яким іншим правилом, випадково вибирається одна або кілька точок впливу логічної завади. Далі розпочинають процес моделювання її поширення. При цьому закон вибору наступного вузла може змінюватися залежно від виду завад, які були змодельовані.

У дослідженнях поширення комп'ютерних епідемій застосовуються моделі кінцевих автоматів SIS (може бути заражений – заражений – може бути заражений) і SIR (може бути заражений – заражений – видалений). Залежно від типу логічної завади і способу її поширення задаються різні ймовірнісні та тимчасові характеристики переходу з одного стану в інший. Розглядаються ефекти імунізації, різні параметри переходу з одного стану SIS/SIR в інший, поширення по різних застосунках передавання даних (імейли, вебвузли, p2p-мережі тощо) швидкість відновлення антивірусного програмного забезпечення, а також інші параметри [10].

У найпростішому, алгоритм поширення за моделлю SIR такий. За одиницю часу моделювання з кожного ураженого вузла завада поширюється на один сусідній вузол. При цьому вибирається вузол із найменшим показником $k$. Моделювання завершується, коли не залишається вузлів для ураження.

Модель поширення завади:

**1.** Сформувати перколяційний кластер на основі графа всіх альтернативних маршрутів передавання повідомлень між множинами ключових вузлів.

**2.** Присвоїти кожному вузлу сформованого кластера випадкове число $\alpha \in [0,1]$.

**3.** Вибрати джерела інформаційних потоків логічної завади і стоку конструктивного трафіку, який витискається.

**4.** Знайти вузли, пов'язані з вузлами, які уражені логічною завадою.

**5.** «Пропустити» логічну заваду в той вузол, в якому випадкове число $\alpha$ набуває найменшого або найбільшого (залежно від фізичного змісту показника) значення.

**6.** Блокувати вузол: вузли в ділянках, що повністю оточено вузлами з логічною завадою, втрачають активність.

**7.** Закінчити витиснення, коли логічна завада займе або блокує всі можливі вузли.

У процесі моделювання на вибраній реалізації структури ГКМ виконують розрахунки руху поверхні, що розділяє сфери впливу ушкоджених сторін і тих, що працюють, у міру того, як логічна завада поширює свій вплив на вузли та канали ГКМ. Зі збільшенням деструктивних інформаційних потоків логічна завада здатна повністю охопити ділянки, заповнені необмеженим конструктивним трафіком і заявками на обслуговування.

Нехай, як обмеження, логічна завада не може витиснути конструктивний трафік із сегментів ГКМ, обладнаних захищеним (єдиним) шлюзом. Згідно з наведеним алгоритмом кластер, що витісняє та містить логічну заваду, росте відповідно до локальних властивостей решіток, вибираючи вузли з найменшим (найбільшим) значенням $\alpha$. Заборона витиснення із заблокованих ділянок додає в модель нелокальні властивості, оскільки, маючи

локальний канал спостереження, відповісти на запитання, чи є ця ділянка заблокованою, не можливо і потрібно провести глобальний моніторинг.

Після отримання структури можливого альтернативного варіанта передавання інформаційних повідомлень, окрім моделювання поширення завади, також можна оцінити ймовірність збереження зв'язків, як це описано раніше.

Щоб оцінити стійкість ГКМ було розраховано метрики для структури гетерогенної мережі (рис. 1, *а*) та її незначної модифікації, що полягає в додаванні кількох зв'язків (рис. 1, *б*). Різними цифрами на рис. 1 зазначено різні локальні мережі, поєднані між собою відповідними лініями зв'язку. Здобуті залежності оцінювання стійкості від імовірності стійкості вузлів ГКМ наведено на рис. 2. Для кожного кроку часу моделювання визначають імовірність ураження вузла $p_{ур}$ як відношення кількості уражених вузлів до загальної кількості вузлів та ймовірність:

$$p_в = 1 - p_{ур}.$$

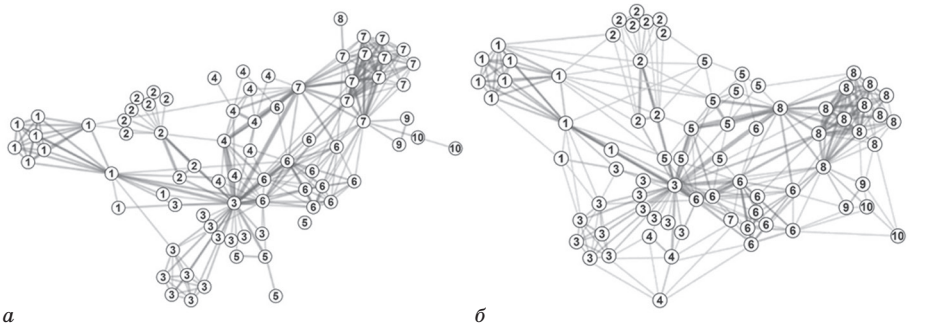
Отже, можна здійснити оцінювання ймовірності збереження зв'язків між ключовими вузлами ГКМ у певний момент часу впливу ненавмисних або навмисних завад та DDoS-атак.

### *Висновки*

Запропоновано математичну модель кількісного оцінювання стійкості гетерогенних комп'ютерних мереж критичного призначення, які використовують у своєму складі обладнання провайдерів послуг інтернету за умов відсутності вірогідної інформації щодо показників стійкості сегментів мережі.

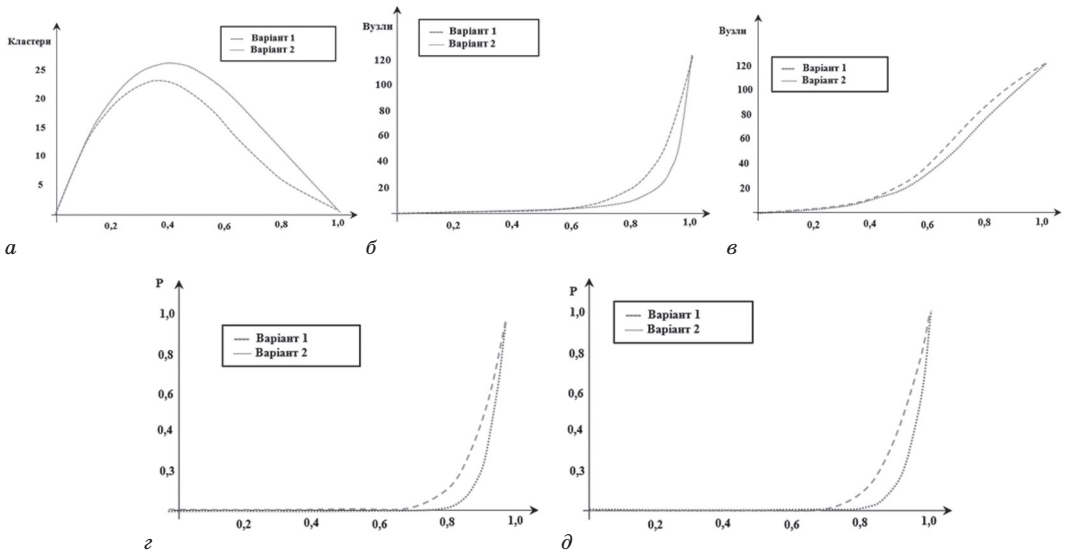
У результаті впливу логічної завади частина вузлів ГКМ переходить у непрацездатний стан, в якому неможливе передавання транзитного трафіку. Вузли, що залишились працездатними після впливу навмисних завад, пов'язані між собою та утворюють кластери, в яких можливе передавання інформаційних повідомлень.

Використання в математичній моделі принципів теорії перколяції дає змогу враховувати в мережі сегменти, некеровані з боку експлуатантів і функціонують за умов поширення логічної завади. Саму теорію перколяції було адаптовано до використання в ГКМ через визначення меж — вузлів територіально розподілених локальних сегментів ГКМ, за допомогою яких здійснюється підімкнення до Інтернету, що також дає можливість застосовувати її на довільних решітках.



*а* *б*

**Рис. 1. Структури гетерогенної комп'ютерної мережі: *а* — варіант 1; б — варіант 2**




*а* *б* *в* *г* *д*

**Рис. 2. Графіки залежності оцінювання стійкості від імовірності стійкості вузла для двох варіантів мережі: *а* — кількість кластерів; *б* — середній розмір кластера; *в* — максимальний розмір кластера; *г* — імовірність досяжності; *д* — імовірність збереження зв'язку**

Запропоновано математичну модель кількісного оцінювання стійкості гетерогенних комп'ютерних мереж критичного призначення за умов поширення впливу логічної завади. Водночас закон вибору наступного вузла може змінюватися залежно від виду завад, які були змодельовані.

Використання математичної моделі кількісного оцінювання стійкості дає змогу розробити ефективні практичні рекомендації щодо забезпечення стійкості гетерогенним комп'ютерним мережам критичного призначення.

***Список використаної літератури***

*1.* ***Рубі Альберт Р., Альберт-Ласло Б.*** *Статистична механіка складних мереж // Огляд сучасної фізики. 2001. № 74. С. 57–74.*

*2.* ***Альберт-Ласло Б.*** *Поява масштабування в складних мережах // Довідник із графіків і мереж: від геному до Інтернету. 2005. №1. С. 69–84.*

*3.* ***Барабаш О. В., Кравченко Ю. В.*** *Функціональна стійкість — властивість складних технічних систем // Зб. наук. праць НАОУ. 2002. №40. С. 225–229.*

*4.* ***Венделл О.*** *Маршрутизація та комутація CCNA 200-120 // Офіційна бібліотека посібника з сертифікації. Cisco Press. 2013. 1600 с.*

*5.* ***Секейра Е.*** *Підключення мережних пристроїв Cisco, частина 1 (ICND1) Foundation Learning Guide, 4-е видання. // Офіційна бібліотека посібника з сертифікації. Cisco Press, 2016. 560 с.*

*6.* ***Тісо Д.*** *Підключення мережних пристроїв Cisco, частина 2 (ICND2) Foundation Learning Guide, 4-е видання // Офіційна бібліотека посібника з сертифікації. Cisco Press, 2018. 464 с.*

*7.* ***Секейра Е., Тісо Д.*** *Cisco CCNA Routing and Switching 200-120 Foundation Learning Guide Library //Офіційна бібліотека посібника з сертифікації. Cisco Press, 2020. 1200 с.*

*8.* ***Рівард Е.*** *CENT ICND1 100-101 Flash Cards and Exam Practic Pack // Офіційна бібліотека посібника з сертифікації. Cisco Press, 2023. 496 с.*

*9.* ***Мельник Я. В., Пермяков О. Ю., Кільменінов О. А.*** *Застосування перколяційних алгоритмів для оцінювання надійності гетерогенних мереж військового призначення // Сучасні інформаційні технології у сфері безпеки та оборони. 2019. №1(34). С. 23–27.*

*10.* ***Ван Х., Гао Дж.*** *Дослідження методу чисельного розрахунку щільності малих кластерів у моделі перколяції // Журнал прикладної математики та фізики. 2016. №4. С. 1507–1512.*

*Ya. V. Melnyk, V. B. Bilavka*

**MATHEMATICAL MODEL OF QUANTITATIVE ASSESSMENT OF STABILITY OF HETEROGENEOUS OF COMPUTER NETWORKS IN THE CONDITIONS OF THE PROPAGATION OF THE INFLUENCE OF A LOGICAL OBSTACLE ON THE BASIS OF THE PERCOLATION THEORY**

*The trends of recent years, especially with the beginning of the aggression of the Russian Federation against Ukraine, testify to the significantly increasing requirements for increasing the efficiency of the management processes of state authorities, with a significant reduction in the management cycle time. At the same time, increasing the efficiency of task performance is impossible without the introduction of modern information technologies into work at all levels of state administration, and, as a result, the formation of a single information space. The article examines the peculiarities of the construction of modern automated control systems, which require the construction of territorially distributed, at the same time, heterogeneous (heterogeneous) computer networks, which must ensure the availability and reliability of the transmission of the necessary information, including in the conditions of the spread of the influence of logical interference (intentional — cyber-attacks on the part of hackers and unintentional actions of the user, system administrator, etc.), which in turn affect the creation of a single information space. Developed approaches to ensure the stability of heterogeneous computer networks that, in turn, use the equipment of Internet service providers in conditions of external and internal destabilizing factors. A mathematical model for assessing the stability of heterogeneous computer networks of critical purpose, under the influence of logical interference, is proposed. At the same time, the theory of percolation is used as a theoretical basis. This approach makes it possible to take into account the lack of reliable information about the stability indicators of network components that belong to various Internet service providers (not under the control of state administration bodies). Computer modeling based on the proposed mathematical model indicates an increase in the efficiency of the computer network as a whole.*

**Keywords:** sustainability; public telecommunication network; heterogeneous computer network; percolation cluster; mathematical model.