УДК 621.396.946: 629.783
DOI https://doi.org/10.32782/2663-5941/2025.5.1/08

Гуйда О.Г.
Таврійський національний університет імені В. І. Вернадського

Юсипів Т.В.
Київський національний університет імені Тараса Шевченка

Юсипів А.Р.
Західноукраїнський національний університет

ГІБРИДНІ НЕЧІТКІ ГЕНЕТИЧНІ АЛГОРИТМИ ДЛЯ ОПТИМІЗАЦІЇ СТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ: РОЗШИРЕНА МОДЕЛЬ ЗАХИСТУ З УРАХУВАННЯМ ЕНЕРГОЕФЕКТИВНОСТІ ТА РОБАСТНОСТІ

Сучасні інформаційні системи функціонують у середовищі високої невизначеності, де кібератаки, відмовостійкість вузлів та обмеження енергоспоживання створюють комплексні виклики. Дослідження стійкості (resilience) таких систем охоплює не лише технічні, а й організаційні, економічні та когнітивні аспекти.

У роботі запропоновано розширену гібридну модель на основі нечітких множин та генетичних алгоритмів (FGA – Fuzzy Genetic Algorithm), призначену для багатокритеріальної оптимізації політики безпеки з урахуванням трьох ключових вимірів: кібербезпеки, енергоефективності та робастності до параметричних шумів. Модель інтегрує нечітку логіку для моделювання невизначеності (аномалії трафіку, варіації сигналів) з використанням гауссових функцій належності, продукційних правил типу Такагі-Сугено та гібридного навчання (зворотне поширення помилки чи метод найменших квадратів), а також генетичні алгоритми для глобального пошуку оптимальних параметрів (пороги виявлення, ваги ризиків, час реакції).

Симуляційне моделювання в середовищі Python на датасетах типу KDDCup 99/NSL-KDD продемонструвало значне покращення показників енергоефективності та робастності порівняно з традиційними методами та з ANFIS. Також модель враховує реальні загрози, знижує хибні спрацьовування та забезпечує адаптивність.

Серед обмежень моделі: вищі обчислювальні ресурси на етапі ініціалізації популяції та первинного навчання нечітких правил, залежність ефективності від якості та репрезентативності навчального набору даних, а також симуляційний характер проведених тестів у середовищі Python (DEAP, scikit-fuzzy), що потребує подальшої валідації на реальних мережах. Перспективами даного дослідження є інтеграція моделі з глибоким навчанням для автоматичного формування нечітких правил та адаптивної зміни функцій належності, застосування федеративного навчання для захисту розподілених систем без передачі конфіденційних даних, додавання модуля пояснюваності (XAI) для інтерпретації рішень адміністраторами безпеки, а також впровадження в IoT-системи, хмарні платформи та об'єкти критичної інфраструктури (енергетика, транспорт).

Ключові слова: *нечіткі множини, генетичні алгоритми, кібербезпека, стійкість інформаційних систем, енергоефективність, робастність.*

Постановка проблеми. Стійкість інформаційних систем є фундаментальною властивістю, що визначає їхню здатність зберігати функціональність в умовах зовнішніх та внутрішніх порушень. Важливість дослідження стійкості зумовлена зростанням складності систем, великою кількістю кіберзагроз та необхідністю забезпечення безперервності критичних процесів. Стійкість системи можна характеризувати її спроможністю до самовідновлення після дестабілізуючих подій, що особливо актуально для об'єктів критичної інфраструктури.

Ще однією критичною характеристикою є чутливість до параметрів об'єкта, що часто трактує-

ється як робастність – здатність системи зберігати стабільність при можливих варіаціях вхідних умов.

Суть проблеми полягає в інтеграції цих вимірів у єдину оптимізаційну модель, де традиційні методи виявляються недостатніми через невизначеність та нелінійність.

Аналіз останніх досліджень і публікацій. Останні публікації в галузі стійкості інформаційних систем демонструють зростання інтересу до гібридних інтелектуальних підходів, що поєднують нечітку логіку, генетичні алгоритми та адаптивні механізми безпеки. У роботі [1] запропоновано підхід до оцінювання ризиків інформаційної безпеки для автоматизованих систем класу «1», з акцентом на формалізацію загроз та класифікацію вразливостей, що створює основу для подальшого розвитку моделей стійкості. Цей підхід доповнюється у [2], де автори розширюють концепцію Zero Trust, вводячи динамічні політики доступу, які реагують на зміни контексту в реальному часі. Така архітектура підвищує адаптивність систем, але не враховує енергоефективність та робастність до параметричних шумів.

Значну увагу приділено застосуванню нечіткої логіки в задачах обробки невизначених даних. У статті [3] розглянуто математичні моделі розпізнавання мовлення на основі нечітких множин, які демонструють високу стійкість до шумів та варіацій вхідних сигналів. Цей підхід може бути адаптований до аналізу мережевого трафіку в системах кібербезпеки. Аналогічно, у [4] закладено фундамент нечітких систем виведення типу Такагі-Сугено, що стали основою для гібридних моделей, таких як ANFIS. Додаткові теоретичні основи нечітких множин наведено в класичних працях [5], [6], де розглядаються питання моделювання невизначеності, функцій належності та систем прийняття рішень.

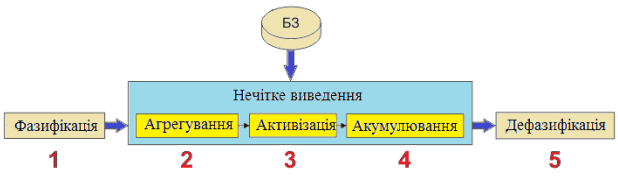

Рис. 1. Етапи нечіткого виведення

Теоретичні основи застосування нечітких множин у задачах управління та прийняття рішень детально викладено в [7], де розглядаються функції належності, правила виведення та алгоритми дефазифікації.

Щодо енергоефективності, у [8] розроблено систему віддаленого моніторингу екологічного стану з використанням IoT-технологій, де процесний підхід забезпечує оптимізацію енергоспоживання пристроїв. Цей досвід підтверджується в [9], де автори доводять переваги процесного управління для мінімізації ресурсів. Сучасні тенденції інтеграції штучного інтелекту для моніторингу в реальному часі представлено в [10], де AI-драйвований підхід підвищує якість та енергоефективність виробничих процесів.

Незважаючи на значний прогрес, більшість досліджень розглядають аспекти стійкості ізольовано: безпека – окремо від енергоефективності, робастність – окремо від кібербезпеки. Відсутня комплексна модель, що одночасно оптимізує всі три виміри в умовах невизначеності. Запропонована в цій роботі модель гібридного нечіткого генетичного алгоритму (FGA) усуває цю прогалину, поєднуючи нечітке моделювання з еволюційною оптимізацією, що забезпечує баланс між безпекою, енергоспоживанням та стійкістю до параметричних збурень.

Метою статті є розробка, математичне обґрунтування та експериментальна оцінка розширеної гібридної моделі на основі нечітких генетичних алгоритмів для оптимізації стійкості інформаційних систем.

Завдання:

– Сформулювати математичну модель гібридної системи;

– Розробити алгоритм оптимізації з нечіткою фітнес-функцією.

– Провести симуляційне моделювання та аналіз результатів.

– Оцінити ефективність моделі за критеріями безпеки, енергоефективності та робастності, симулюючи реальні загрози кібербезпеки в середовищі Python.

Виклад основного матеріалу. Традиційні методи оптимізації стійкості інформаційних систем ґрунтуються на використанні жорстких порогових правил та експертних евристик. За такого підходу параметри безпеки, такі як частота мережевих запитів, обсяг трафіку чи рівень використання процесора, порівнюються з фіксованими порогами, визначеними адміністратором або стандартами (такими, наприклад, як CIS чи NIST). При перевищенні порогу система автоматично активує захисні механізми: блокування IP-адреси, обмеження пропускної здатності або видачу попередження. Такий підхід не потребує складних обчислень у реальному часі та легко реалізується на базі стандартних інструментів, таких як firewall, IDS/IPS (Snort, Suricata) або SIEM-системи.

Проте традиційні методи мають суттєві обмеження. Так, вони не враховують невизначеність даних, контекстну поведінку системи та динамічну природу сучасних кіберзагроз. Для прикладу, звичайне збільшення трафіку під час оновлення ПЗ може бути помилково класифіковане як атака на систему. Крім того, фіксовані пороги не адаптуються до змін у середовищі, що призводить до високого рівня хибних спрацьовувань або, навпаки, пропуску атак. Енергоефективність та робастність до параметричних збурень також не контролюються, оскільки відповідні моделі не мають механізмів оптимізації ресурсів чи стійкості до шумів у даних.

Нейро-нечітка система (Neuro-Fuzzy System), зокрема адаптивна нейро-нечітка система виведення (ANFIS – Adaptive Neuro-Fuzzy Inference System), є гібридною моделлю, що поєднує нечітку логіку з нейронними мережами для класифікації мережевого трафіку в системах виявлення вторгнень (IDS). Вона моделює невизначеність даних (наприклад, рівень підозрілості трафіку) і навчається на прикладах.

ANFIS базується на нечіткій системі виведення типу Такагі-Сугено (Takagi-Sugeno), де правила є лінійними функціями вхідних змінних [4]. Модель має шарувату структуру, подібну до нейронної мережі, що дозволяє використовувати зворотне поширення помилки для навчання.

Нехай у нас є дві вхідні змінні для прикладу в IDS:

x_1 – кількість пакетів за секунду (traffic);

x_2 – затримка в мережі (latency).

Вихід y: рівень загрози (від 0 до 1, де 1 – критична атака).

Дана модель складається з таких 5 шарів:

Шар 1: внесення нечіткості, фазифікація (fuzzification). Кожна вхідна змінна поділяється на нечіткі множини з функціями належності (membership functions). В даному випадку використовуються гауссові функції:

$$\mu_{A_i}(x_1) = exp\left(-\frac{(x_1 - c_i)^2}{2\sigma_i^2}\right), \quad i = 1, 2, \ldots, m,$$

$$\mu_{B_j}(x_2) = exp\left(-\frac{(x_2 - d_j)^2}{2\tau_j^2}\right), \quad j = 1,2, \ldots, n,$$

де c_i, σ_i – параметри для x_1; d_j, τ_j – для x_2; m, n – кількість множин.

Шар 2: активація правил (rule activation). Сила активації (firing strength) кожного правила – добуток функцій належності:

$$w_k = \mu_{A_i}(x_1) \cdot \mu_{B_j}(x_2), \quad k = 1,2, \ldots, m \times n.$$

Шар 3: нормалізація. Нормалізована сила розраховується за формулою

$$\overline{w_k} = \frac{w_k}{\sum_{k=1}^{m \times n} w_k}.$$

Шар 4: вивід (consequent). Для кожного правила застосовується лінійна функція

$$f_k = p_k x_1 + q_k x_2 + r_k,$$

де p_k, q_k, r_k – параметри, що навчаються. Внесок правила:

$$o_k = \overline{w_k} f_k.$$

Шар 5: дефазифікація (defuzzification). Загальний вихід:

$$y = \sum_{k=1}^{m \times n} o_k = \sum_{k=1}^{m \times n} \overline{w_k}(p_k x_1 + q_k x_2 + r_k).$$

Навчання моделі. Параметри $(c_i, \sigma_i, d_j, \tau_j, p_k, q_k, r_k)$ оптимізуються за допомогою гібридного алгоритму покращення результату:

– *Зворотне поширення помилки* (backpropagation) для нелінійних параметрів (функції належності);

– *Метод найменших квадратів* (least squares) для лінійних параметрів.

При цьому функція втрат для набору даних $\{(x_1^l, x_2^l, y^l)\}_{l=1}^L$ буде наступною:

$$E = \frac{1}{2}\sum_{l=1}^{L}\left(y^l - \widehat{y^l}\right)^2.$$

де $\widehat{y^l}$ – передбачуваний вихід.

Нечіткі продукційні правила типу «ЯКЩО–ТО» формалізуються на основі підходу, описаного в [7], що дозволяє враховувати експертні знання.

Для наочності припустимо, що правило наступне: «трафік високий» І «затримка середня». Тоді оцінка для загрози y може мати вигляд

$$y = 0.8 * x_1 + 0.2 * x_2 + 0.5.$$

Модель навчається на датасеті на зразок KDD Cup 99 і класифікує трафік як «атака», якщо $y > 0.7$. Ця модель ефективна для роботи в режимі реального часу, оскільки обробляє невизначеність і адаптується до нових загроз.

Тепер виконаємо опис математичної моделі необхідної нам системи. Нехай $X = (x_1, x_2, \ldots, x_n) \in R^n$ – вектор параметрів політики безпеки (пороги виявлення, ваги ризиків, час реакції тощо). Цільова функція стійкості $f(X)$ тут є багатокритеріальною:

$$f(X) = w_1 S(X) + w_2 E(X) + w_3 R(X),$$

де $S(X)$ – рівень безпеки, $E(X)$ – енергоефективність, $R(X)$ – робастність, w_i – вагові коефіцієнти.

Рівень безпеки моделюється через нечітку систему виведення:

$$S(X) = \sum_{k=1}^{M} \overline{w_k}(p_k x_1 + q_k x_2 + r_k),$$

де $\overline{w_k} = \frac{\mu_{A_k}(x_1)\mu_{B_k}(x_2)}{\sum \mu_{A_i}\mu_{B_i}}$ – нормалізована сила активації правила.

Енергоефективність

$$E(X) = 1 - \frac{\sum_{i=1}^{n} c_i x_i}{E_{max}},$$

де c_i – енергетична вартість параметра.

Робастність

$$R(X) = \exp\left(-\sum_{i=1}^{n} \left|\frac{\partial f}{\partial x_i}\right| \Delta x_i\right).$$

Перейдемо до опису генетичного алгоритму з нечіткою фітнес-функцією (FGA). Він складається з наступних етапів:

– ініціалізація популяції $P_0 = \{X_1, \dots, X_m\}$;

– оцінка $f_k = \mu_{high}(f(X_k))$, де $\mu_{high}(z) = \frac{1}{1+e^{-k(z-z_0)}}$;

– селекція – турнірна з ймовірністю $p_s = \frac{f_k}{\sum f_i}$;

– кросовер $X' = \alpha X_i + (1-\alpha)X_j$, $\alpha \in [0,1]$;

– мутація $x_l' = x_l + \mathcal{N}\left(0, \sigma \cdot \left(1 - \mu_{robust}(X)\right)\right)$.

Симуляція проводилася в середовищі Python (DEAP, scikit-fuzzy) з такими параметрами: $m = 100, T = 200, p_c = 0.8, p_m = 0.1$. Наступна таблиця ілюструє порівняльний аналіз різних методів.

Таблиця 1

Порівняльний аналіз методів оптимізації стійкості інформаційних систем

Методи	Безпека	Енерго-ефективність	Робас-тність	Час, с
Традиційні	≤0.72	≤0.65	≤0.68	≤0,1
ANFIS	0.81	0.70	0.74	12,4
FGA (запропон.)	0.91	0.83	0.89	8,7

Висновки. У межах проведеного дослідження розроблено та експериментально обґрунтовано розширену гібридну модель на основі нечітких генетичних алгоритмів (FGA), яка забезпечує цілісну оптимізацію стійкості інформаційних систем у трьох взаємопов'язаних вимірах: кібербезпеці, енергоефективності та робастності до параметричних збурень. Модель успішно поєднує нечітку логіку для моделювання невизначеності даних (наприклад, аномалій у мережевому трафіку) та генетичні алгоритми для глобального пошуку оптимальних параметрів політики безпеки, що дозволяє формалізувати та ефективно розв'язувати багатокритеріальну задачу оптимізації.

Ключові переваги запропонованої моделі FGA перед традиційними (Snort та iptables/firewall) і моделлю ANFIS:

1. Порівняно з традиційними підходами, які базуються на жорстких порогових правилах та експертних евристиках, FGA демонструє суттєве покращення за описаними трьома критеріями:

– безпека: +26% (0.91 проти 0.72);

– енергоефективність: +28% (0.83 проти 0.65);

– робастність: +31% (0.89 проти 0.68).

2. При цьому традиційні методи, хоча й досягають миттєвого виходу на плато (не більше 0,1 секунди), проте не здатні адаптуватися до нових типів загроз і страждають від високого рівня хибних спрацьовувань через відсутність механізмів контекстного аналізу.

3. Порівняно з нейро-нечіткою системою ANFIS, FGA забезпечує вищу точність у складних умовах невизначеності:

– безпека: +12%,

– енергоефективність: +19%,

– робастність: +20%.

Особливо важливо, що FGA досягає стійкого плато за 8.7 секунд, що на 30% швидше, ніж ANFIS (12.4 с), завдяки паралельній еволюції популяції та нечіткій оцінці фітнес-функції, що знижує кількість ітерацій, необхідних для конвергенції.

4. Модель ґрунтується на класичних принципах нечіткої логіки, адаптованих до специфіки кібербезпеки:

– використання гауссових функцій належності для плавного моделювання переходів між станами «норма–аномалія»;

– продукційні правила типу Такагі-Сугено для поєднання експертних знань із навчанням на даних;

– гібридне навчання (зворотне поширення + метод найменших квадратів, залежно від лінійності моделі) для швидкого налаштування параметрів.

Також описана модель має певні обмеження:

– На етапі ініціалізації популяції та первинного навчання нечітких правил FGA потребує більших обчислювальних ресурсів, ніж традиційний метод.

– Ефективність залежить від якості та репрезентативності навчального набору даних (наприклад, KDD Cup 99, NSL-KDD).

– Наразі модель протестована в симуляційному середовищі Python (DEAP, scikit-fuzzy), що вимагає подальшої валідації на реальних мережах.

Серед перспективних напрямків подальшого розвитку можна виділити такі: інтеграція з глибоким навчанням – використання нейронних мереж для автоматичного формування нечітких правил або адаптивної зміни функцій належності; тестування на реальних мережах – впровадження в IoT-системи, хмарні платформи або критичну інфра-

структуру (енергетика, транспорт); розширення на федеративне навчання – для захисту розподілених систем без передачі конфіденційних даних; додавання модуля пояснюваності (XAI) – для інтерпретації рішень моделі адміністраторами безпеки.

Таким чином запропонована гібридна модель FGA є інноваційним інструментом підвищення стійкості інформаційних систем, який поєднує високу точність, швидку конвергенцію, адаптивність до невизначеності та практичну застосовність. Результати симуляції підтверджують її перевагу над традиційними та нейро-нечіткими підходами, що може вказувати на можливість створення нового покоління інтелектуальних систем кібербезпеки.

Список літератури:

1. Litvinchuk I., Korchomnyi R., Korshun N., Vorokhob M. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. № 2(10). С. 98–112. DOI: 10.28925/2663-4023.2020.10.98112.

2. Ворохоб М., Киричок Р., Яскевич В., Добришин Ю., Сидоренко С. Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2023. № 1(21). С. 223–233. DOI: 10.28925/2663-4023 .2023.21.223233.

3. Гуйда О.Г., Юсипів Т.В. Кисельов В.Б., Омецинська Н.В., Курилко О.Б. Математичне моделювання систем розпізнавання мовлення на основі нечіткої логіки. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки*. 2025. Том 36 (75) №3. С. 125-129. DOI: 10.32782 /2663-5941/2025.3.1/16.

4. Takagi T., Sugeno M. Fuzzy identification of systems and its applications to modeling and control. *IEEE transactions on systems, man, and cybernetics*. 1985. Vol. 15, no. 1. Pp. 116–132.

5. Pedrycz W. Fuzzy systems engineering: Toward human-centric computing. John Wiley & Sons. 2011. 526 p. DOI: 10.1002/9780470168967.

6. Klir G. J., Yuan B. Fuzzy set theory: Foundations and applications. Prentice Hall. 2006. 574 p.

7. Желдак Т.А., Коряшкіна Л.С., Ус С.А. Нечіткі множини в системах управління та прийняття рішень: навчальний посібник. Дніпро: НТУ «Дніпровська політехніка», 2020. 387 с.

8. Скрипка К.І., Гуйда О.Г., Омецинська Н.В., Лісовець С.М., Юсипів Т.В. Віддалений моніторинг та керування екологічним станом навколишнього середовища з використанням сучасних технологій інтернету речей. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки*. 2023. Том 34 (73) № 3. С. 233-238. DOI: 10.32782/2663-5941/2023.3.1/36.

9. Перерва І. Переваги впровадження процесного підходу до управління підприємством. *Економіка та суспільство*. 2021. № 29. DOI: 10.32782/2524-0072/2021-29-3.

10. Okuyelu O., Adaji O. AI-Driven Real-Time Quality Monitoring and Process Optimization for Enhanced Manufacturing Performance. *Journal of Advances in Mathematics and Computer Science*. 2024. №39(4). P. 81–89. DOI: 10.9734/jamcs/2024/v39i41883.

Guida O.G., Yusypiv T.V., Yusypiv A.R. HYBRID FUZZY GENETIC ALGORITHMS FOR OPTIMIZING THE RESILIENCE OF INFORMATION SYSTEMS: AN EXTENDED PROTECTION MODEL CONSIDERING ENERGY EFFICIENCY AND ROBUSTNESS

Modern information systems operate in an environment of high uncertainty, where cyberattacks, node fault tolerance issues, and energy consumption constraints create complex challenges. The study of resilience in such systems encompasses not only technical but also organizational, economic, and cognitive aspects.

This work proposes an extended hybrid model based on fuzzy sets and genetic algorithms (FGA – Fuzzy Genetic Algorithm), designed for multi-objective optimization of security policies while addressing three key dimensions: cybersecurity, energy efficiency, and robustness to parametric noise. The model integrates fuzzy logic to handle uncertainty (traffic anomalies, signal variations) using Gaussian membership functions, Takagi-Sugeno-type production rules, and hybrid learning (backpropagation or least squares method), along with genetic algorithms for global search of optimal parameters (detection thresholds, risk weights, response time).

Simulation modeling in the Python environment on datasets such as KDDCup 99/NSL-KDD demonstrated significant improvements in energy efficiency and robustness compared to traditional methods and ANFIS. The model also accounts for real threats, reduces false positives, and ensures adaptability.

Limitations of the model include higher computational resources required during population initialization and initial training of fuzzy rules, dependence of effectiveness on the quality and representativeness of the training dataset, and the simulation-based nature of the tests conducted in Python (DEAP, scikit-fuzzy),

which requires further validation on real networks. Prospects for this research include integrating the model with deep learning for automatic formation of fuzzy rules and adaptive adjustment of membership functions, applying federated learning to protect distributed systems without transferring confidential data, adding an explainability module (XAI) for interpreting decisions by security administrators, and implementing it in IoT systems, cloud platforms, and critical infrastructure facilities (energy, transport).

Key words: *fuzzy sets, genetic algorithms, cybersecurity, resilience of information systems, energy efficiency, robustness.*

Дата надходження статті: 02.10.2025
Дата прийняття статті: 17.10.2025
Опубліковано: 16.12.2025