КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1078
УДК 621.391:004.056.5

Ахрамович Володимир Миколайович
доктор технічних наук, професор
професор кафедри кібербезпеки
Державний університет "Київський авіаційний інститут"
ORCID: 0000-0002-0086-9131
12z@ukr.net

Ахрамович Вадим Володимирович
завідувач комп'ютерним центром
Національна академія статистики, обліку та аудиту
ORCID: 0009-0003-2787-8745
12zstzi@gmail.com

Санченко Володимир Іванович
аспірант
Державний університет "Київський авіаційний інститут"
ORCID: 0009-0009-3967-9683
volodymyr.sanchenko@gmail.com

Арєшков Мирослав Максимович
аспірант
Державний університет "Київський авіаційний інститут"
ORCID: 0009-0000-4739-3268
MyroclavK6@gmail.com

БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ В УМОВАХ НЕВИЗНАЧЕННОСТІ

Анотація. У сучасних умовах цифровізації питання захисту інформації в різних типах комп'ютерних мереж набуває особливої актуальності. Постійна поява нових загроз, динамічність інформаційних потоків та непередбачувана поведінка атакувальників створюють середовище з високим рівнем невизначенності. Це ускладнює застосування традиційних методів оцінки ризиків та проектування систем захисту. У статті розглядаються теоретичні та практичні підходи до забезпечення безпеки мереж в умовах невизначенності. Проаналізовано методи моделювання ризиків з використанням ймовірнісних та нечітких моделей, окреслено роль адаптивних алгоритмів і машинного навчання для виявлення загроз. Запропоновано концептуальну основу для побудови комплексних систем захисту, здатних до самонавчання та адаптації у мінливому середовищі. Особливого значення набуває використання математичних моделей, здатних враховувати неповноту даних і нечіткість у визначенні параметрів безпеки. Поєднання ймовірнісного аналізу, методів нечіткої логіки та алгоритмів машинного навчання дозволяє формувати адаптивні системи, які можуть своєчасно реагувати на нові загрози. Моделювання ризику в умовах невизначеності дозволяє кількісно оцінювати ефективність заходів захисту мереж. Fuzzy-підхід та нечіткі змінні дають змогу враховувати неповну або нечітку інформацію про потенційні загрози. Адаптивні моделі виявляються більш ефективними у порівнянні зі статичними, зменшуючи максимальний ризик атак Використання сценарного моделювання (DoS, MITM) допомагає виявити критичні точки мережі та планувати оптимальні заходи захисту. Формування теоретико-практичних засад забезпечення безпеки мереж в умовах невизначеності, а також обґрунтування методів, що дозволяють підвищити стійкість інформаційних систем до непередбачуваних атак і знизити ризики втрати даних.

Ключові слова: безпека мереж, математичні моделі, нечіткі моделі, формалізація невизначеності та ризику, моделювання ризиків, рівень загроз, методологія дослідження, багаторівневі моделі захисту, сценарії атак.

ВСТУП

Інформаційна безпека є критично важливою складовою функціонування сучасних комп'ютерних мереж, які об'єднують користувачів, сервіси та інфраструктуру у глобальному масштабі. Зростання кількості кіберзагроз, поява складних атак (APT, MITM, DDoS), а також невизначеність щодо їхніх джерел і наслідків формують нові виклики для дослідників та практиків у сфері безпеки.

Загальна картина: невизначеність як фундаментальна характеристика сучасних мереж та їх складових [1, 2, 3, 4, 5]. У сучасних дослідженнях підкреслюється, що мережеве середовище характеризується невизначеністю на кількох рівнях: неповнота/шум у даних телеметрії, змінність поведінки користувачів і атакувальників, а також імовірнісні залежності між компонентами системи. Для аналізу таких систем пропонуються підходи, що поєднують ймовірнісні, нечіткі та епістемічні моделі ризику.

Легковагова криптографія – стандартизація і практичне застосування. Що роблять дослідники**:** через обмежені ресурси кінцевих пристроїв (малі CPU, RAM, батареї) значна увага приділяється LWC – алгоритмам, оптимізованим під апаратні/програмні обмеження. Ключові результати**:** NIST провів процес стандартизації LWC і у 2023 році оприлюднив звіт про оцінювання фіналістів, що завершився вибором (ASCON тощо) як еталонних рішень для певних застосувань IoT. Це створює підґрунтя для широкого впровадження LWC у практичних системах.

Практичний висновок – при розробці безпеки для середовищ з обмеженими ресурсами слід віддавати пріоритет алгоритмам, які пройшли незалежну оцінку та мають оптимальне співвідношення «безпека/витрати».

ML/AI для виявлення аномалій у мережах – огляд тенденцій і обмежень**.** Стан досліджень – численні огляди (survey) показують швидке зростання робіт, що застосовують ML/DL для виявлення аномалій у IoT (як класичні алгоритми, так і глибокі мережі). Роботи класифікують методи за типом ознак, режимом навчання (supervised/unsupervised) та розміщенням обробки (edge/gateway/cloud). Обмеження: потреба в маркованих даних, висока обчислювальна вартість для деяких DL-підходів, ризик overfitting та уразливість моделей до adversarial прикладів. Рішення в літературі: гібридні підходи (легкі моделі на шлюзі та важкі моделі в хмарі), transfer learning для обмежених наборів даних, використання інкрементального/онлайн-навчання для врахування дрифтів у поведінці.

Нечіткі, ймовірнісні та гібридні моделі ризику – робота з невизначеністю**.** Опис напрямку – у зв'язку з неповнотою та нечіткістю даних багато робіт застосовують Fuzzy Logic, Bayesian підходи та стохастичні моделі для оцінки ризиків та прийняття рішень у безпеці. Fuzzy-підходи часто використовують для агрегації кількісних і якісних показників та побудови політик реагування. Сильні сторони: дають можливість формалізувати експертні знання, оперувати нечіткими входами та будувати адаптивні правила. Слабкі сторони: інтерпретованість і валідація моделей складніша, потреба у тонкому налаштуванні правил та верифікації в реальних сценаріях.

Нечітко-гнучкі IDS та гібридні архітектури – практичні реалізації. Приклади – останні роботи показують успішну інтеграцію нечіткої логіки з нейромережами або класичними ML для покращення виявлення атак в IoT-протоколах (наприклад, захист RPL у сенсорних мережах). Такі гібриди дозволяють поєднати експертні правила з автоматичними ознаками. Висновок: гібридні IDS мають великий потенціал для

середовищ з невизначеністю, особливо коли ресурсно-важкі обчислення винесені на шлюзи/хмару, а на пристроях залишаються легкі предобробки та базові критерії.

Оцінка ризику та менеджмент – агреговані підходи для IoT. Напрямки – останні огляди та моделі ризику для IoT пропонують багаторівневі та багатовимірні фреймворки, що враховують залежності між активами, функціональністю та зовнішніми загрозами. Розвиваються методи кількісної оцінки (ентропійні підходи, кореляційний аналіз) та інтеграції з бізнес-цілями. Проблеми – стандартизація методів оцінки ризику для IoT все ще неповна; багато моделей залишаються концептуальними або вимагають значного обсягу даних для параметризації.

Реалізовані практики: Zero Trust, мікросегментація та оновлення безпеки. Тенденції: у практиці захисту рекомендовано застосовувати принципи Zero Trust (докладна автентифікація кожного з'єднання, мікросегментація) та автоматизовані процеси керування оновленнями. Це особливо важливо в умовах невизначеності, коли статичні політики можуть швидко застаріти. (поширено в сучасних оглядах і практиці).

Постановка проблеми. У сучасних комп'ютерних і корпоративних мережах неможливо наперед визначити всі параметри, що характеризують як внутрішні процеси, так і зовнішні впливи. Фактори невизначеності охоплюють широкий спектр явищ: від нестабільності каналів зв'язку й коливань навантаження до непередбачуваної поведінки користувачів і атакувальників. У зв'язку з цим задача забезпечення інформаційної безпеки набуває характеру оптимізаційної задачі в умовах неповної та суперечливої інформації. Задачі, які потрібно визначити:

- захист мереж в умовах невизначеності;
- необхідність рівень загроз, при неповній або суперечливій інформації;
- потреба в адаптивних системах, здатних змінювати параметри в режимі реального часу.

Аналіз останніх досліджень і публікацій. У статті [1] проведено дослідження системи захищеності ком'ютера його складових в умовах невизначеності. Для цього складено: кортеж нечітких множин із складових ком'ютера; проведено його моделювання; розраховані рівні ризиків; рівні захищеності ком'ютера, агрегація результатів, функції належності. Для обрахунків параметрів, використані методи трапеції та трикутника. Розрахунки ілюстровані графічним матеріалом.

В статті [2] досліджується система захисту соціальної мережі від компонентів мережі в умовах невизначеності. Основна увага приділяється нечіткості даних, побудові моделей нечітких множин, оцінці ризиків і рівня безпеки мережевих об'єктів. Запропонований підхід дозволяє розробляти ефективні рішення для прийняття управлінських рішень у контексті кібербезпеки. Представлено алгоритм для побудови кортежа параметрів захисту та їх моделювання за допомогою функцій членства. Методи агрегування результатів і розрахунків із використанням трапецієподібних і трикутних функцій розглядаються окремо. Для цієї мети було скомпільовано наступне: кортеж нечітких множин із компонентів мережі; Було проведено моделювання; Розраховувалися рівні ризику; рівні мережевої безпеки, агрегування результатів, функції членства.

В статті [3] представлено метод кількісного дослідження ризиків, що базується на аналізі й оцінюванні ризиків інформаційних систем. Запропонований підхід дозволяє використовувати широкий спектр параметрів, які забезпечують створення гнучких засобів оцінювання. Цей метод дає можливість розраховувати ризики як на основі статистичних даних, так і на основі експертних оцінок, зроблених в умовах невизначеності та слабкоформалізованого середовища.

Розроблені методи забезпечують представлення результатів у числовій і словесній формах. Наприклад, можливе використання лінгвістичних змінних, які часто застосовують для опису складних систем, що характеризуються параметрами не лише у кількісному, але й у якісному вигляді. Ризики інформаційних систем можуть бути описані через концептуальну модель нечітких множин, яка враховує невизначеність, неточність і суб'єктивність під час їхнього оцінювання.

В статті [4] запропоновано метод оцінювання ймовірності виникнення атак у MANET, що базується на апараті нечіткої логіки. Метод включає побудову кортежу нечітких множин, який описує основні параметри мережі (вразливості вузлів, рівень довіри, поведінкові аномалії тощо), моделювання ризиків з урахуванням експертних оцінок, визначення функцій належності та агрегування результатів для отримання інтегрального показника захищеності.

В статті [5] проведено дослідження системи захисту корпоративної мережі з урахуванням її архітектурних та функціональних складових в умовах часткової або повної невизначеності Для досягнення поставленої мети було побудовано кортеж нечітких множин, що описують найважливіші аспекти функціонування та захисту корпоративної мережі. У кортеж включено як технічні характеристики (наприклад, інтенсивність інформаційного потоку, рівень захисту, параметри витоку даних, активність фаєрволу, роботу системи резервного копіювання тощо), так і організаційні складові (розмежування доступу, політика автентифікації, ідентифікація користувачів, аудит тощо). Кожен з параметрів отримав відповідну нечітку інтерпретацію у вигляді лінгвістичних змінних: "низький", "середній", "високий" рівень.

В статті [6] відмічається, що один з актуальних напрямків, що розвиваються в області інформаційної безпеки, пов'язаний з використанням Honeypots (віртуальних приманок, онлайн-пасток), а вибір критеріїв для визначення найбільш ефективних Honeypot і їх подальшої класифікації є актуальним завданням. Представлені основні продукти, в яких реалізовані технології віртуальної приманки. Вони часто використовуються для вивчення поведінки, підходів і методів, які використовує стороння сторона для отримання несанкціонованого доступу до ресурсів інформаційної системи. Онлайн-хуки можуть імітувати будь-який ресурс, але частіше вони виглядають як справжні продакшн-сервери та робочі станції.

В статті [7] розглядається один із нових та перспективних підходів до вирішення проблеми оцінювання кібербезпеки на об'єктах критичної інфраструктури з використанням теорії нечітких множин, наприклад, для оцінки ризиків інформаційної безпеки. На практиці трапляються ситуації, коли на розрахунок кінцевих результатів істотно впливають невідповідності висновків або помилки експертів. Тому, щоб мінімізувати такі похибки, пропонується методи фазирування інтервалів шляхом перетворення їх у нечіткі числа.

В статті [8] для моделювання ризику інформаційної безпеки підприємства запропоновано нечіткі моделі надавати у вигляді нечітких мереж. Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збиток організації. Використовуваний в методиці механізм отримання оцінок ризику на основі нечіткої логіки дозволяє отримати чисельне значення ризику, лінгвістичний опис ступеня ризику, а також рівень впевненості експерта у виникненні ризикової події.

Монографія [9] присвячена теоретико-методологічним і практичним аспектам розробки методів ідентифікації аномальних станів та методології побудови систем виявлення вторгнень. У роботі проведено аналіз засобів виявлення зловживань та

аномалій. Значну увагу приділено формалізації процесу створення mi-вимірних параметричних, атакуючих, еталонних, поточних та детекційних середовищ. Це є підґрунтям для створення засобів, які дозволять автоматизувати процес детектування в слабоформалізованому нечітко визначеному середовищі аномальний стан, що породжується кібератаками, у заданий проміжок часу шляхом контролю поточного стану множини визначених параметрів.

Монографія [10] присвячена теоретико-методологічним і практичним аспектам оцінювання ризиків інформаційної безпеки. У роботі проведено аналіз базових понять, методів, моделей, засобів та міжнародних нормативних документів, пов'язаних з оцінюванням і управлінням ризиками. Значну увагу приділено розробленню методів модифікації порядку лінгвістичної змінної при перевизначенні еталонів параметрів, а також оцінювання ризиків безпеки ресурсів інформаційних систем в реальному часі з використанням CVSS метрик, які містяться у відкритих базах даних уразливостей.

В статті [11] відзначається, що одним з методів оцінки ризиків інформаційної безпеки є обґрунтований вибір і здійснення протидії загрозам. Ситуативна нечітка модель OWA багатокритеріальна. Вирішення проблеми вибору заходів протидії зниженню інформаційної безпеки пропонуються ризики. Запропонована модель дає можливість модифікувати пов'язані ваги критеріїв на основі інформаційної ентропії щодо ситуації агрегації. Перевагою модель полягає в постійному вдосконаленні вагових коефіцієнтів критеріїв і агрегації експертів. думки в залежності від параметра, що характеризує ситуацію агрегації.

В роботі [12] досліджується поєднання оцінку ризику (RA) і нечіткої логіки (FL), де: «Оцінка ризику – це загальний процес ідентифікації, аналізу та оцінки ризику. Ідентифікація ризику включає розуміння джерел ризику, сфер впливу, подій та їх причини та можливі наслідки. Мета полягає в тому, щоб створити вичерпний перелік ризиків, включаючи ризики, які можуть бути пов’язані з втраченими можливостями, і ризики, пов’язані з прямим контролем організації. Комплексний огляд дозволяє повністю розглянути потенціал вплив ризику на організацію».

У статті [13] розроблено підхід на основі аналізу оболонок даних (DEA) для вирішення MOSPP з нечіткими параметрами (FMOSPP) для врахування реальних ситуацій, коли вхідні-вихідні дані включають невизначеність трикутної форми членства. Цей підхід до встановлення зв'язку між MOSPP і DEA є більш гнучким для реального практичного застосування. У зв'язку з цим кожна дуга в FMOSPP розглядається як одиниця прийняття рішень з безліччю нечітких входів і виходів. Потім отримують дві нечіткі оцінки ефективності, що відповідають кожній дузі. Ці нечіткі оцінки ефективності об'єднані для визначення унікальної нечіткої відносної ефективності.

В статті [14] розглядаються різнітипи шкідливих атак, такі як електронні віруси, шкідливе програмне забезпечення, шкідливий код, та інші кіберзагрози, в першу чергу, які впливають на інформаційні системи. Системні адміністратори не знають типу та рівня атаки. Коли зловмисники зламують комп'ютерні системи, і вони не впевнені в діях, які необхідно вжити для захисту. Тому – наукові цілі визначити ці типи кібератак за допомогою теорії нечітких множині випустити попередження для адміністраторів, спонукаючи їх до вжиття необхідних дій.

В статті [15] описується кібербезпека промислової системи управління яка є дуже складна і складна тема дослідження, з огляду на інтеграцію цих систем у національні критичні інфраструктури. Системи управління зараз з'єднані між собою в промислові мережі і часто підключені до Інтернет. У цьому контексті вони стають мішенями різних

кібератак зловмисників таких як хакери, промислові шпигуни тощо та розвідувальні служби. Автори пропонують спосіб моделювання профілів зловмисників і оцінки рівня успіху нападу, проведений у заданих умовах. Автори використовують нечіткий підхід для створення профілів зловмисників на основі атрибутів зловмисника, такі як знання, техресурсів і мотивації.

В літературних джерелах [1,3,6,7,9-15] не розглядаються безпека мереж в умовах невизначенності, що являється недоліком, в [2] розглядаються окремий тип мереж-соціальні, в [4] розглядаються окремий тип мереж – MANET, в [5] проведено дослідження системи захисту корпоративної мережі, в [8] для моделювання ризику інформаційної безпеки підприємства запропоновано нечіткі моделі надавати у вигляді нечітких мереж. Загальним недоліком [2,4,5,8] являється використання одного типу математичних моделей та розгляд якогось конкретного типу мереж.

Мета статті. Формування теоретико-практичних засад забезпечення безпеки мереж в умовах невизначенності, а також обґрунтування методів, що дозволяють підвищити стійкість інформаційних систем до непередбачуваних атак і знизити ризики втрати даних.

ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ

Модель інформаційного захисту в умовах невизначеності. Введемо показник ризику R, рівня загроз T, ефективності захисту E. Формалізація невизначеності через функції належності нечітких множин. Побудова узагальненої моделі:

$$R=f\,(T,E,U), \tag{1}$$

де U – параметри невизначеності (шум у даних, відсутність інформації, суперечливі оцінки).

Постановка задачі. Формалізуємо задачу через введення базових показників: T(t) – рівень загроз у момент часу t; E(t) – ефективність системи захисту в момент часу t; U(t) – параметри невизначеності, що характеризують шум, неповноту або нечіткість даних; R(t) – інтегральний показник ризику.

Загальну модель ризику можна подати як функціональну залежність:

$$R(t) - f\,(T(t), E(t), U(t)) \tag{2}$$

Мета дослідження полягає у визначенні такої структури функції FFF, яка б адекватно відображала вплив усіх трьох компонентів на результативність системи захисту. При цьому ставляться такі завдання: формалізація невизначеності шляхом використання методів нечіткої логіки [6, 7, 8, 9, 10] ймовірнісних підходів або їхніх гібридів; аналіз стабільності моделі: виявлення умов, за яких система захисту залишається у працездатному стані навіть при коливаннях параметрів T(t) і U(t); оптимізація параметрів захисту: знаходження таких значень E(t), що мінімізують ризик R(t) у середньому або гарантовано для найгіршого сценарію.

Таким чином, задача захисту мереж в умовах невизначеності формулюється як багатокритеріальна оптимізаційна проблема:

$$\min_{E(t)} R(t) \quad за\ умов U(t) \in \Omega \tag{3}$$

де: Ω – множина можливих сценаріїв невизначеності, за умов:

$$E(t) \in \Omega_E, \quad T(t) \in \Omega_T, \; U(t) \in \Omega_U, \tag{4}$$

де: Ω_E – допустима область параметрів системи захисту (ресурси, обчислювальна складність, пропускна складність), Ω_T – множина можливих сценаріїв загроз, Ω_U – множина можливих раалізацій невизначенності.

Критерії оптимальності можуть бути визначені у кілької формах:

1. Мінімізація середнього риску (expected risk)

$$\min_{E(t)} \max_{U(t) \in \Omega_E} R(t)$$

де математичне сподівання береться за математичним розподілом невизначеності

2. Мінімізація максимального ризику (worst-case)

$$\min_{E(t)} \max_{U(t) \in \Omega_U} R(t)$$

3. Багатокритеріальна оптимізація – одночасна мінімізація ризику $R(t)$ та вартості/ресурсоємності захисту $C(E(t))$:

$$\min(R(t), \quad C(E(t))$$

Математична інтерпретація невизначеності. Для формалізації невизначеності U(t) пропонується використовувати

- Ймовірнісний підхід: $U(t) \sim P(u), \quad u \in \Omega_U$,

де: $P(u)$ – апріорний або емпіричний розподіл шуму/помилок.

- Нечіткий підхід: невизначені параметри подаються як нечіткі множини з функціями належності: $\mu_U(u) : \Omega_U \to [0,1]$, що дозволяє враховувати «ступінь можливості» реалізації того чи іншого сценарію.
- Гібридні моделі: поєднання ймовірнісних і нечітких підходів, де розподіли мають додаткові функції належності (fuzzy-probabilistic risk models).

Динамічна модель ризику. З урахуванням часової змінності параметрів модель ризику можна подати як диференціальне рівняння:

$$\frac{dR(t)}{dt} = \alpha T(t) - \beta E(t) + \gamma U(t),$$

де: α – коефіцієнт впливу інтенсивності загроз, β – коефіцієнт ефективності системи захисту, γ – коефіцієнт чутливості до невизначеності. Аналіз цієї моделі дозволяє визначати стійкість системи при різних сценаріях T(t) та U(t), а також обґрунтовувати вимоги до адаптивних алгоритмів.

Ймовірнісні моделі. Ймовірнісні методи застосовуються тоді, коли невизначеність можна інтерпретувати як випадковість із відомим або апроксимованим розподілом [11,12,13]. Формалізація ризику: R(t)=P(A)·L(A), де P(A) – ймовірність реалізації атаки A, а L(A) – потенційні збитки.

Приклад. Якщо ймовірність DDoS-атаки на сервер становить P=0.3, а очікувані збитки від недоступності сервісу дорівнюють L=100 одиниць, тоді ризик:R=0.3×100=30.

Ймовірнісні моделі добре працюють, якщо є статистика атак та поведінкових партнерів, але їхня обмеженість полягає у складності збору достовірних даних.

Нечіткі моделі (Fuzzy Logic). У випадках, коли дані неповні або якісні («високий ризик», «низький рівень захисту»), доцільно використовувати нечітку логіку. Функції належності. Для змінної рівень загроз T можна визначити нечіткі множини:
«низкий» рівень загроз:

$$\mu_{low}(T) = \max(0,1-\frac{T}{50}),$$ «середній»:

$$\mu_{mid}(T) = \max(0,1-|\frac{T-50}{25}|),$$ «високий»:

$$\mu_{higt}(T) = \min(1,\frac{T}{50}).$$ Fuzzification

Нехай T=40, тоді: $\mu_{low}(40)=0.2$, $\mu_{mid}(40)=0.6$, $\mu_{higt}(40)=0.8$

Це означає, що стан загроз на 20% залежить від «низького», на 60% – від «середнього» та на 80% – від «високого» рівня. Правила нечіткого виведення. Приклад: IF (загроза = «висока») AND (ефективність захисту = «низька») THEN (ризик = «критичний»). IF (загроза = «середня») AND (ефективність = «середня») THEN (ризик = «помірний»).

Defuzzification. Для отримання чіткого значення ризику застосовується метод центру ваги (centroid):

$$R^* = \frac{\int r\mu_R(r)dr}{\int \mu_R(r)dr}$$

Приклад fuzzification/defuzzification. Нехай: T=40 (загроза середня), E=60 (ефективність захисту достатня). Правила дають два висновки: ризик «помірний» з вагою 0.6; ризик «низький» з вагою 0.4. Після дефазифікації (метод центру ваги) отримаємо: $R^* \approx 35$(за шкалою від 0 до 100). Таким чином, ризик оцінюється як середній із тенденцією до зниження.

Гібридні моделі. Гібридні підходи поєднують ймовірнісні оцінки (на основі історичних даних) та нечіткі правила (експертні знання) [14, 15]. Наприклад, ймовірність атаки P(A) задається статистично, а її «серйозність» оцінюється нечіткими термами («низька», «середня», «висока»). Результат: система здатна працювати і з даними, і з якісними оцінками експертів. Таким чином, ймовірнісні моделі забезпечують точність при наявності статистики, нечітка логіка дозволяє працювати з нечіткими оцінками, а гібридні моделі поєднують обидва підходи для підвищення адаптивності системи захисту.

Математичні нечіткі моделі та методи з прикладами використання ймовірнісних і нечітких підходів в мережах IoT. У процесі моделювання захисту інформації в мережах IoT під невизначеністю доцільно поєднувати ймовірнісні методи та нечіткі моделі, оскільки класичний детермінований підхід не враховує неповноти даних, варіативності поведінки атак та складності оцінки ризиків. Нечітка логіка дає змогу врахувати невизначеність у параметрах, які неможливо точно виміряти (наприклад, "низький рівень атаки", "середній рівень завантаження"). Функції належності: для змінної

«рівень завантаження IoT-мережі» (U) вводяться нечіткі множини: Low, Medium, High. Типові функції належності мають вигляд: графічні залежності – (рис. 1,2):

$$\mu_{Low}(U)=\begin{cases}1, & U\le 20\\ \dfrac{40-U}{20}, & 20<U\le 40\\ 0, & U>40\end{cases}$$

$$\mu_{Medium}(U)=\begin{cases}0, & U\le 20\\ \dfrac{U-20}{20}, & 20<U\le 40\\ \dfrac{60-U}{20}, & 40<U\le 60\\ 0, & U>60\end{cases}$$

$$\mu_{High}(U)=\begin{cases}0, & U\le 40\\ \dfrac{U-40}{20}, & 40<U\le 60\\ 1, & U>60\end{cases}$$

Приклад fuzzification. Нехай завантаження U=45%. Тоді:

$\mu_{Low}(45)=0,\ \mu_{Medium}(45)=\dfrac{60-45}{20}=0,75\ \ \mu_{High}(45)=\dfrac{45-40}{20}=0,25$ отже, значення U=45 описується нечіткою комбінацією Medium (0.75) та High (0.25).

Defuzzification. Для визначення чіткого значення ризику R^* застосовується метод центру ваги:

$$R^*=\frac{\int x\mu\ (x)dx}{\int \mu\ (x)dx}$$

У простій дискретній постановці:

$$R^*=\frac{\sum_i x_i\mu(x_i)}{\sum_i \mu(x_i)}$$

Приклад. Нехай значення ризику для Medium=0.75 при x=0.5а для High=0.25 при x=0.8. Тоді:

$$R^*=\frac{0,5*0,75+0,8*0,25}{0,75+0,25}=0,575$$ (рис. 3).

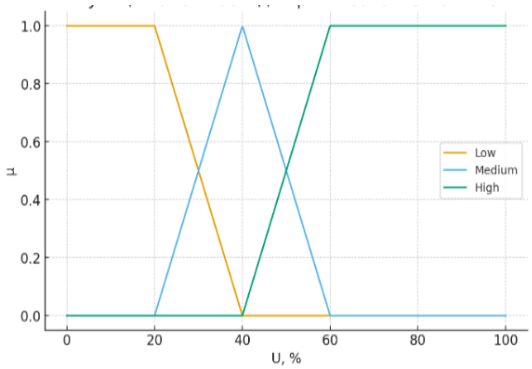

Рисунок 1. Функції належності μLow(U),μMedium(U),μHigh(U)

ISSN 2663 – 4023

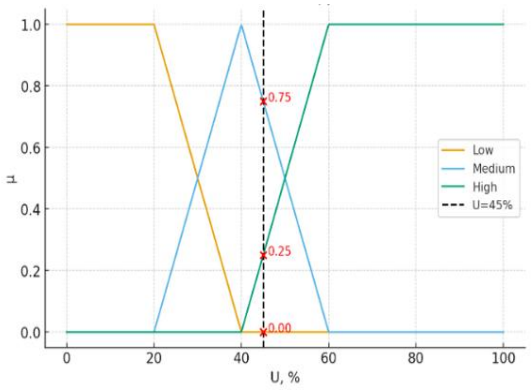

Рисунок 2. Fuzzification прикладу при U=45%

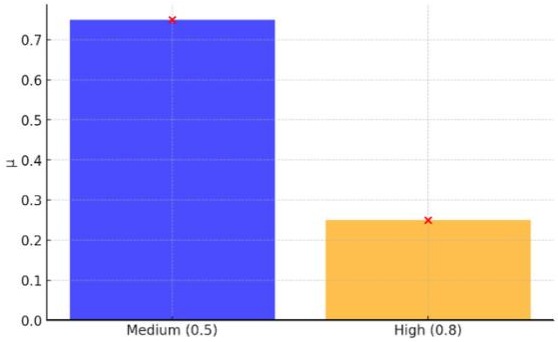

Рисунок 3. Defuzzification методом центру ваги $R^* = 0,575$

Таким чином, поєднання ймовірнісного підходу (для відомих частот атак) та нечітких моделей (для нечітко вимірюваних параметрів) забезпечує більш гнучку та адекватну оцінку безпеки IoT-систем.

Методи підвищення безпеки. У сучасних мережах IoT застосування традиційних механізмів захисту є недостатнім через високу динаміку загроз, обмеженість ресурсів та значний рівень невизначеності. Тому все більшого поширення набувають адаптивні та інтелектуальні методи підвищення безпеки, які інтегрують як класичні підходи, так і новітні технології.

IDS/IPS-системи. Системи виявлення та запобігання вторгненням (Intrusion Detection/Prevention Systems) забезпечують моніторинг трафіку та ідентифікацію аномалій. Signature-based IDS – визначає загрози за відомими шаблонами атак. Anomaly-based IDS – використовує статистичні та машинні моделі для виявлення нетипової поведінки. IPS – не тільки виявляє, але й блокує шкідливий трафік у реальному часі. Поєднання IDS/IPS з fuzzy- та probabilistic-аналізом дає змогу мінімізувати хибні спрацьовування та підвищити ефективність при обмежених ресурсах IoT.

Концепція Zero Trust. Модель Zero Trust базується на принципі «ніколи не довіряй, завжди перевіряй». Основні механізми: багатофакторна автентифікація (MFA); постійна верифікація користувачів і пристроїв; мікросегментація мережі (обмеження доступу лише до потрібних ресурсів); мінімальні привілеї (Least Privilege Access).

Для IoT ця концепція дозволяє ізолювати пристрої, які можуть бути скомпрометовані, і знизити ймовірність розповсюдження атаки по всій мережі.

Штучний інтелект і машинне навчання (AI/ML). Інтелектуальні методи забезпечують адаптивність і прогнозування атак. ML-класифікатори (SVM, Random

Forest, нейронні мережі) виявляють нові атаки без потреби у відомих сигнатурах. Deep Learning використовується для аналізу великих обсягів IoT-трафіку та виявлення складних атак (наприклад, DDoS з ботнетів). Reinforcement Learning дозволяє адаптувати політики доступу залежно від поведінки користувачів і пристроїв. Особливо ефективним є поєднання AI/ML з нечіткою логікою для прийняття рішень у ситуаціях неповноти даних.

Багаторівневі моделі захисту. Забезпечення кіберзахисту IoT досягається завдяки побудові багаторівневих систем, що поєднують (рис. 4):

Мережевий рівень – фільтрація трафіку, VPN, IDS/IPS. Прикладний рівень – контроль доступу, шифрування даних, захист API. Користувацький рівень – автентифікація, політики управління ідентичностями. Аналітичний рівень – AI/ML-модулі для виявлення аномалій та прогнозування атак.

Модель Defense-in-Depth (захист у глибину) забезпечує стійкість навіть у разі прориву одного з рівнів.

Висновок. Поєднання IDS/IPS-систем, Zero Trust-політики, AI/ML-алгоритмів та багаторівневих архітектур формує адаптивну систему безпеки IoT, здатну ефективно функціонувати в умовах невизначеності та обмежених ресурсів.

Рисунок 4. Багаторівнева модель підвищення безпеки в IoT, де кожен рівень відповідає за свій захисний контур: від мережевих механізмів до AI/ML-аналітики

1. Мережевий рівень (фільтрація, VPN, IDS/IPS). Основний захист трафіку та сегментація мереж. Використання брандмауерів, систем виявлення та запобігання вторгненням. Захищене з’єднання через VPN.
2. Прикладний рівень (шифрування, контроль доступу). Захист даних під час зберігання й передавання. Використання легковагових криптографічних алгоритмів у середовищах IoT. Обмеження доступу на рівні сервісів.
3. Користувацький рівень (автентифікація, політики доступу). Ідентифікація користувачів та пристроїв (паролі, сертифікати, багатофакторна автентифікація). Застосування політик доступу на основі ролей (RBAC/ABAC). Виявлення підозрілої поведінки користувачів.
4. Аналітичний рівень (AI/ML, виявлення аномалій). Використання машинного навчання для аналізу поведінки мережі. Адаптивні алгоритми для реагування на нові, невідомі атаки. Прогнозування ризиків на основі історичних і потокових даних.

Така модель дозволяє комбінувати класичні методи захисту (мережеві фільтри, шифрування) з інтелектуальними (AI/ML) (табл. 1), забезпечуючи стійкість навіть в умовах високої невизначеності загроз.

Таблиця 1

Порівняння рівнів

Рівень	Основні завдання	Методи захисту	Приклади реалізації
Мережевий	Захист трафіку, запобігання проникненню	Фільтрація, VPN, IDS/IPS, мікросегментація	Snort, Suricata, OpenVPN
Прикладний	Захист даних і сервісів	Шифрування (AES, LWC), контроль доступу	TLS/DTLS, ASCON (LWC)
Користувацький	Ідентифікація та конт-роль дій користу-вачів/пристроїв	MFA, RBAC/ABAC, поведінковий аналіз	Google Authenticator, Okta
Аналітичний	Виявлення аномалій, адаптація до нових загроз	AI/ML, fuzzy logic, аналіз потокових даних	TensorFlow IDS, Azure Sentinel

Приклади сценаріїв та моделювання. У цьому підрозділі демонструється практичне застосування математичних моделей для оцінки безпеки мереж в умовах невизначеності. Для ілюстрації розглянемо два типові сценарії атак та вплив рівня захисту на показник ризику R.

Сценарій 1: DoS-атака. Розглянемо мережу з обмеженими ресурсами. При недостатньому резервуванні пропускної здатності ризик переходить у критичну зону вже при завантаженні 65%. Формально, залежність ризику від завантаження мережі L та рівня невизначеності U можна описати як:

$$R = f(L,U) = \frac{LU}{1-L(1-U)}$$

де: $0 \le L \le 1, 0 \le U \le 1$

Ця формула дозволяє врахувати нечіткі оцінки навантаження та неповну інформацію про атаки (fuzzification).

Сценарій 2: MITM-атака в MANET. Для мобільної ad-hoc мережі (MANET) невизначеність маршрутів та обмежена безпека каналів збільшують ймовірність перехоплення даних. Ризик можна моделювати як:

$$R = q(P_v, S) = P_v(1-S)$$

де: Pv – ймовірність перехоплення пакету, S – коефіцієнт захисту (0 – відсутність захисту, 1 – максимальний захист).

Моделювання показує, що збільшення рівня захисту значно знижує ризик навіть при високій невизначеності маршруту. Для наочності проведено три експерименти:

Залежність ризику R від рівня невизначеності U. Використано fuzzy-підхід для представлення нечітких оцінок. Крива демонструє, що при підвищенні невизначеності ризик зростає нелінійно (рис. 5).

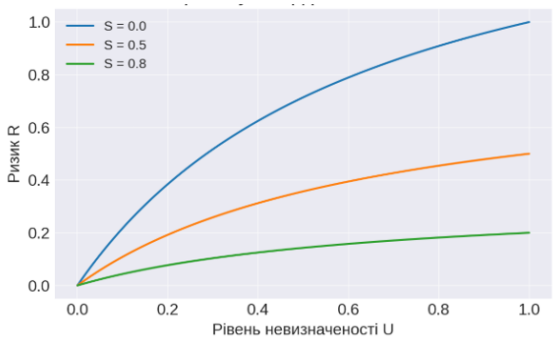

Рисунок 5. Криві R(U) для різних рівнів захисту

Вплив рівня захисту на сценарій атаки DoS / MITM. Моделювання показує, як підвищення коефіцієнта захисту S зменшує максимальний ризик атаки (рис. 6).

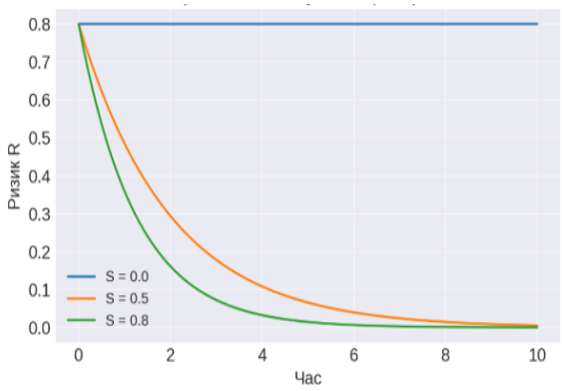

Рисунок 6. Ризик R як функція часу для різних рівнів захисту

Порівняння статичної та адаптивної моделей. Статична модель не враховує зміни поведінки атакуючих і реагує лише після факту атаки. Адаптивна модель підлаштовується під поведінку атак і зменшує пікові значення ризику (рис. 7).

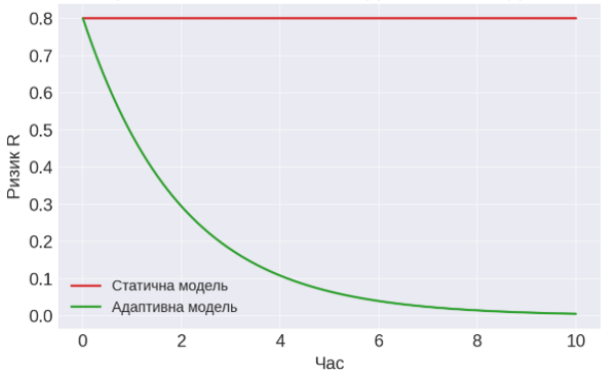

Рисунок 7. Порівняння R(t) для статичної та адаптивної моделей

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Моделювання ризику в умовах невизначеності дозволяє кількісно оцінювати ефективність заходів захисту мереж. Fuzzy-підхід та нечіткі змінні дають змогу враховувати неповну або нечітку інформацію про потенційні загрози. Адаптивні моделі виявляються більш ефективними у порівнянні зі статичними, зменшуючи максимальний ризик атак. Використання сценарного моделювання (DoS, MITM) допомагає виявити критичні точки мережі та планувати оптимальні заходи захисту.

Напрями подальшого дослідження. Розробка і тестування гібридних архітектур (edge/gateway/cloud) з автоматичним масштабуванням рівня захисту залежно від стану вузлів. Створення відкритих репозиторіїв/датасетів, що відображають реальні умови невизначеності (шум, пропуски, асиметричні атаки). Інтеграція нечітких та стохастичних метрик у ML-пайплайни для кращої інтерпретації невизначеності. Оцінка енергетичної ефективності захисних стратегій у реальних розгортаннях (емпіричні виміри). Дослідження стійкості ML-моделей в умовах targeted/adversarial атак у IoT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Akhramovych, V., & Akhramovych, V. (2025). Method for calculating the information protection indicator of a computer under uncertainty. *Information Technology and Security, 13*(1), 55–68. https://doi.org/10.20535/2411-1031.2025.13.1.328898
2. Akhramovych, V., Laptiev, O., Ilienko, A., & Akhramovych, V. (2024). Method for calculating information protection in social networks using fuzzy sets. *Bezpeka Informatsii, 30*(3), 358–364.
3. Akhramovych, V., Akhramovych, V., Brailovskyi, M., Pepa, Y., & Laptieva, T. (2025). Quantitative risk assessment using fuzzy set methods. *Information Systems and Technologies Security, 1*(9), 18–25.
4. Akhramovych, V., & Akhramovych, V. (2025). Method for calculating the probability of attacks in MANET networks under uncertainty. *Information Technology and Security, 13*(2), 334–345. https://doi.org/10.20535/2411-1031.2025.13.1.328898
5. Ilienko, A., & Akhramovych, V. (2025). Method for calculating corporate network protection under uncertainty. *Cybersecurity: Education, Science, Technique, 1*(29), 480–492.
6. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S., Kurchenko, O., Laptiev, O., Sievierinov, O., & Tkachuk, S. (2021). Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. *Eastern-European Journal of Enterprise Technologies, 111*(3/9), 63–83. https://doi.org/10.15587/1729-4061.2021.225346
7. Yevseiev, S. P., Shmatko, O. V., & Romashchenko, N. V. (2019). Algorithm for assessing information security risk based on a fuzzy set approach. *Modern Information Systems, 3*(2), 73–79. https://doi.org/10.18372/2225-5036.29.18068
8. Kochetkov, O. V., Haur, T. O., & Mashin, V. M. (2019). Information security risk assessment system based on fuzzy logic. *Scientific Works of O.S. Popov Odesa National Academy of Telecommunications, 1*, 97–104. https://doi.org/10.33243/2518-7139-2019-1-1-97-104
9. Korchenko, A. O. (2019). *Methods for identifying anomalous states in intrusion detection systems*. Komprint. https://nubip.edu.ua/sites/default/files/u34/monografiya_korchenko_anna_1.pdf
10. Imamverdiyev, Y. N., & Derakshande, S. A. (2021). Fuzzy OWA model for information security risk management. *Automatic Control and Computer Sciences, 45*(1), 20–28.
11. Shapiro, A. F. (n.d.). *Risk assessment applications of fuzzy logic*. Casualty Actuarial Society; Canadian Institute of Actuaries; Society of Actuaries.
12. Bagheri, M., Ebrahimnejad, A., Razavyan, S., Hosseinzadeh, F., & Malekmohammadi, N. (2021). Solving fuzzy multi-objective shortest path problem based on data envelopment analysis approach. *Complex & Intelligent Systems, 7*, 725–740. https://doi.org/10.1007/s40747-020-00234-4
13. Sastry, V. N., Janakiraman, T. N., & Mohideen, S. I. (2003). New algorithms for multi-objective shortest path problem. *Opsearch, 40*(4), 278–298.
14. Pricop, E., & Mihalache, S. F. (2019). Fuzzy approach to modelling cyber attack patterns in industrial control systems. In *Proceedings of the International Conference on Electronics, Computers and Artificial Intelligence (ECAI 2019)* (pp. 1–6).
15. Milić, S. D. (2019). Fuzzy-decision algorithms for cyber security analysis of advanced SCADA and remote monitoring systems. In *Advances in information security and privacy* (Chapter 7). https://doi.org/10.4018/978-1-7998-2910-2.ch007

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Volodymyr Akhromovych
Doctor of Technical Sciences, Professor
Professor of the Department of Cybersecurity
State University «Kyiv Aviation Institute»
ORCID: 000-0002-0086-9131
12z@ukr.net

Vadym Akhromovych
Head of the Computer Center
State Academy of Statistics, Accounting and Audit
ORCID: 0009-0003-2787-8745
12zstzi@gmail.com

Volodymyr Sanchenko
Postgraduate Student
State University «Kyiv Aviation Institute»
ORCID: 0009-0009-3967-9683
volodymyr.sanchenko@gmail.com

Myroslav Areshkov
Postgraduate student
State University «Kyiv Aviation Institute»
ORCID: 0009-0000-4739-3268
MyroclavK6@gmail.com

COMPUTER NETWORK SECURITY IN CONDITIONS OF UNCERTAINTY

Abstract. In the modern era of digitalization, the issue of information protection in various types of computer networks is becoming increasingly relevant. The constant emergence of new threats, the dynamic nature of information flows, and the unpredictable behavior of attackers create an environment with a high level of uncertainty. This complicates the application of traditional methods of risk assessment and security system design. This article examines theoretical and practical approaches to ensuring network security under uncertainty. Methods of risk modeling using probabilistic and fuzzy models are analyzed, and the role of adaptive algorithms and machine learning in threat detection is outlined. A conceptual framework is proposed for building comprehensive protection systems capable of self-learning and adapting to a changing environment. Special emphasis is placed on the use of mathematical models capable of accounting for incomplete data and fuzziness in defining security parameters. The combination of probabilistic analysis, fuzzy logic methods, and machine learning algorithms enables the development of adaptive systems that can respond promptly to emerging threats.

Risk modeling under uncertainty allows for a quantitative assessment of the effectiveness of network protection measures. The fuzzy approach and fuzzy variables make it possible to consider incomplete or imprecise information about potential threats. Adaptive models prove to be more effective compared to static ones, reducing the maximum risk of attacks. The use of scenario modeling (DoS, MITM) helps identify critical network points and plan optimal protection measures. The work contributes to the formation of theoretical and practical foundations for ensuring network security under uncertainty and substantiates methods that enhance the resilience of information systems to unpredictable attacks and reduce the risks of data loss.

Keywords: network security, mathematical models, fuzzy models, uncertainty and risk formalization, risk modeling, threat level, research methodology, multilayer protection models, attack scenarios.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Akhramovych, V., & Akhramovych, V. (2025). Method for calculating the information protection indicator of a computer under uncertainty. *Information Technology and Security*, *13*(1), 55–68. https://doi.org/10.20535/2411-1031.2025.13.1.328898
2. Akhramovych, V., Laptiev, O., Ilienko, A., & Akhramovych, V. (2024). Method for calculating information protection in social networks using fuzzy sets. *Bezpeka Informatsii*, *30*(3), 358–364.
3. Akhramovych, V., Akhramovych, V., Brailovskyi, M., Pepa, Y., & Laptieva, T. (2025). Quantitative risk assessment using fuzzy set methods. *Information Systems and Technologies Security*, *1*(9), 18–25.
4. Akhramovych, V., & Akhramovych, V. (2025). Method for calculating the probability of attacks in MANET networks under uncertainty. *Information Technology and Security*, *13*(2), 334–345. https://doi.org/10.20535/2411-1031.2025.13.1.328898
5. Ilienko, A., & Akhramovych, V. (2025). Method for calculating corporate network protection under uncertainty. *Cybersecurity: Education, Science, Technique*, *1*(29), 480–492.
6. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S., Kurchenko, O., Laptiev, O., Sievierinov, O., & Tkachuk, S. (2021). Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. *Eastern-European Journal of Enterprise Technologies*, *111*(3/9), 63–83. https://doi.org/10.15587/1729-4061.2021.225346
7. Yevseiev, S. P., Shmatko, O. V., & Romashchenko, N. V. (2019). Algorithm for assessing information security risk based on a fuzzy set approach. *Modern Information Systems*, *3*(2), 73–79. https://doi.org/10.18372/2225-5036.29.18068
8. Kochetkov, O. V., Haur, T. O., & Mashin, V. M. (2019). Information security risk assessment system based on fuzzy logic. *Scientific Works of O.S. Popov Odesa National Academy of Telecommunications*, *1*, 97–104. https://doi.org/10.33243/2518-7139-2019-1-1-97-104
9. Korchenko, A. O. (2019). *Methods for identifying anomalous states in intrusion detection systems*. Komprint. https://nubip.edu.ua/sites/default/files/u34/monografiya_korchenko_anna_1.pdf
10. Imamverdiyev, Y. N., & Derakshande, S. A. (2021). Fuzzy OWA model for information security risk management. *Automatic Control and Computer Sciences*, *45*(1), 20–28.
11. Shapiro, A. F. (n.d.). *Risk assessment applications of fuzzy logic*. Casualty Actuarial Society; Canadian Institute of Actuaries; Society of Actuaries.
12. Bagheri, M., Ebrahimnejad, A., Razavyan, S., Hosseinzadeh, F., & Malekmohammadi, N. (2021). Solving fuzzy multi-objective shortest path problem based on data envelopment analysis approach. *Complex & Intelligent Systems*, *7*, 725–740. https://doi.org/10.1007/s40747-020-00234-4
13. Sastry, V. N., Janakiraman, T. N., & Mohideen, S. I. (2003). New algorithms for multi-objective shortest path problem. *Opsearch*, *40*(4), 278–298.
14. Pricop, E., & Mihalache, S. F. (2019). Fuzzy approach to modelling cyber attack patterns in industrial control systems. In *Proceedings of the International Conference on Electronics, Computers and Artificial Intelligence (ECAI 2019)* (pp. 1–6).
15. Milić, S. D. (2019). Fuzzy-decision algorithms for cyber security analysis of advanced SCADA and remote monitoring systems. In *Advances in information security and privacy* (Chapter 7). https://doi.org/10.4018/978-1-7998-2910-2.ch007

Отримано редакцією журналу / Received: 17.01.26
Прорецензовано / Revised: 02.02.26
Схвалено до друку / Accepted: 26.03.26