TECHNICAL SCIENCES AND TECHNOLOGIES
DOI: https://doi.org/10.25140/2411-5363-2025-3(41)-237-253
УДК 004.2

Юрій Іванович Підлісний
аспірант кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: ypodlesny@ukr.net. **ORCID:** https://orcid.org/0009-0001-9783-3898. **ResearcherID:** LSL-1170-2024

НЕЧІТКА ЛОГІКА В ОЦІНЮВАННІ РИЗИКІВ БЕЗПЕКИ IoT: ПОБУДОВА ПРАВИЛ І РЕАЛІЗАЦІЯ

У статті запропоновано нову модель оцінювання ризиків інформаційної безпеки в середовищі Інтернету речей (IoT), яка базується на методах нечіткої логіки типу Mamdani. З метою підвищення точності аналізу ризиків враховано не лише технічні характеристики пристроїв, а й контекст їхнього функціонування – зокрема рівень критичності функцій, вразливість та захищеність каналів зв'язку. Розроблена модель реалізована у MATLAB з використанням Fuzzy Logic Toolbox. Проведено моделювання фрагмента гетерогенної IoT-мережі та виконано візуалізацію результатів. Отримані результати порівняно з традиційною методологією EBIOS, що дозволило виявити переваги запропонованого підходу, зокрема плавність переходів між рівнями ризику та кращу адаптивність до змін контексту. Запропонована модель може бути використана для автоматизованого аналізу ризиків у динамічних і критичних IoT-системах.

Ключові слова: *Інтернет речей; оцінювання ризиків; нечітка логіка; Fuzzy Logic Toolbox; Mamdani; інформаційна безпека; EBIOS.*
Рис. 5. Бібл.: 16. Табл.: 3.

Актуальність теми дослідження. Інтернет речей (Internet of Things, IoT) стрімко трансформує сучасний цифровий ландшафт, забезпечуючи взаємодію мільярдів пристроїв у різних сферах – від розумного дому й медицини до промисловості та критичної інфраструктури. За прогнозами аналітичних агентств, до 2030 року кількість підключених IoT-пристроїв перевищить 25 млрд, що створює безпрецедентний обсяг трафіку, даних і взаємодій між компонентами цих систем.

Разом із розширенням функціональності та масштабуванням IoT-систем зростає і поверхня атак. Багато пристроїв характеризуються обмеженими обчислювальними ресурсами, відсутністю оновлень безпеки та базовими або відсутніми механізмами захисту, що робить їх вразливими до широкого спектра кібератак – від простих DoS-атак до складних сценаріїв компрометації конфіденційних даних і атак типу «людина посередині» (MITM).

Особливо небезпечною є ситуація в умовах високої динамічності IoT-мереж, коли топологія, поведінка пристроїв і рівень ризику постійно змінюються. Традиційні методи оцінювання ризиків, які базуються на детермінованих підходах, виявляються недостатньо ефективними в таких умовах. Їм бракує здатності опрацьовувати неповну, нечітку або суперечливу інформацію, що часто є характерною для реальних IoT-сценаріїв.

У цьому контексті виникає потреба у використанні інтелектуальних підходів до оцінювання ризиків, зокрема методів нечіткої логіки, які дозволяють враховувати невизначеність, суб'єктивну експертну оцінку та гнучко реагувати на зміни в мережі. Побудова ефективної системи оцінювання ризиків на основі нечіткої логіки відкриває нові можливості для забезпечення надійності та адаптивності безпеки IoT-середовищ.

Постановка проблеми. Забезпечення кібербезпеки в середовищі Інтернету речей (IoT) є надзвичайно складним завданням через розподілений характер мереж, різнорідність пристроїв та обмежені ресурси їхньої обчислювальної потужності. Традиційні підходи до аналізу ризиків, зокрема методи, що базуються на строгих числових оцінках або стандартизованих шкалах (наприклад, CVSS, ISO/IEC 27005) – передбачають наявність повної, точної та формалізованої інформації про активи, вразливості, загрози й контекст функціонування. У реальних умовах IoT ці вимоги часто є недосяжними.

Проблема ускладнюється наявністю:

– *невизначеності в даних* щодо ймовірності атак та їх впливу;

– *суб'єктивності в експертних оцінках* і відсутності формальних правил ухвалення рішень;

– *динамічної природи IoT-середовища,* яке швидко змінюється та адаптується.

У зв'язку з цим постає науково-практична проблема: *як забезпечити ефективне оцінювання ризиків безпеки в IoT-системах в умовах неповноти, нечіткості та нестабільності вхідної інформації.*

Одним із перспективних напрямів розв'язання цієї проблеми є використання **нечіткої логіки** (fuzzy logic), яка дозволяє:

– *інтерпретувати якісні та лінгвістичні характеристики ризику* (наприклад, «висока вразливість», «низька ймовірність»);

– *моделювати логіку прийняття рішень експертів у вигляді нечітких правил типу IF–THEN*;

– *здійснювати оцінювання ризику навіть за умов невизначеності, суперечливості або часткової відсутності даних.*

Отже, необхідно розробити модель оцінювання ризику безпеки IoT-систем, яка базується на нечіткій логіці, формалізує експертні знання у вигляді нечітких правил та забезпечує інтерпретованість, адаптивність і точність у прийнятті рішень.

Аналіз останніх досліджень і публікацій. Упродовж останнього десятиліття проблема кібербезпеки в середовищі Інтернету речей (IoT) стала предметом активних наукових досліджень. Основна увага зосереджена на виявленні вразливостей, побудові моделей загроз, а також розробці методів аналізу ризиків для гетерогенних і динамічних IoT-систем.

У працях [1, 2] наголошується на особливостях безпеки IoT – численних точках входу, обмежених ресурсах пристроїв та складності централізованого управління безпекою.

Визначальним напрямом у сучасних підходах до оцінювання ризиків стала інтеграція методів штучного інтелекту, зокрема нечітких експертних систем. Так, у [3] і [4] запропоновано гібридні архітектури виявлення аномалій в IoT-мережах із використанням нечітких логічних блоків для покращення інтерпретованості рішень.

У роботах [5] та [6] описано системи оцінювання ризику на основі нечітких продукційних правил, що враховують не тільки рівень вразливості, але й контекст функціонування пристрою (наприклад, місце в мережі, критичність функції). При цьому автори підкреслюють переваги нечіткої логіки у роботі з неповною або якісною інформацією, а також у моделюванні людської експертної інтуїції.

Низка досліджень, зокрема [7; 8], акцентує увагу на необхідності створення адаптивних та масштабованих систем оцінки ризику**,** які могли б ефективно працювати в умовах високої динамічності та гетерогенності IoT-середовищ. Саме нечіткі системи розглядаються як одна з провідних технологій, здатних об'єднати формалізовані правила з експертними оцінками в єдину модель.

Попри значні досягнення, актуальною залишається проблема системної побудови бази нечітких правил, узгодження лінгвістичних змінних між різними джерелами знань та забезпечення пояснюваності результатів. У цьому контексті важливою науковою задачею є формалізація методики побудови нечіткої системи оцінювання ризиків IoT, орієнтованої на практичне застосування в реальних умовах.

Виділення недосліджених проблем. Хоча методи нечіткої логіки широко впроваджуються у практику оцінювання ризиків безпеки IoT-систем, досі залишаються відкритими ключові проблеми, що потребують подальших досліджень:

1. **Недостатня контекстуалізація ризиків.** Більшість наявних моделей зосереджуються на загальних загрозах без глибокого аналізу специфічного контексту роботи IoT-пристроїв, зокрема у промисловості, медичній сфері або смартмістах.

2. **Обмеженість у формалізації нечітких правил.** Існує проблема автоматизації та адаптації бази знань. Переважна більшість підходів використовує фіксовані (ручні) правила, що не враховують динаміку кіберзагроз у реальному часі.

3. **Інтеграція з іншими методами.** Недостатньо досліджено можливості інтеграції нечітких систем з іншими інтелектуальними підходами – такими як штучні нейронні мережі, генетичні алгоритми або баєсівські мережі – для покращення точності оцінювання ризиків.

4. **Масштабованість і продуктивність.** У більшості публікацій відсутній аналіз того, як нечіткі системи оцінювання ризиків працюють у великомасштабних IoT-мережах із тисячами пристроїв і взаємодіями в реальному часі.

5. **Відсутність стандартизації у формуванні вхідних параметрів.** Значення термів лінгвістичних змінних часто обираються довільно, що ускладнює відтворюваність та порівняння результатів між різними дослідженнями.

Таким чином, актуальним напрямом подальших досліджень є розробка адаптивної нечіткої моделі оцінювання ризиків, що враховує контекст функціонування IoT-систем, здатна динамічно оновлювати правила на основі змін у кіберсередовищі та легко масштабуватися під потреби різних сфер застосування.

Мета статті. Метою статті є розроблення підходу до оцінювання ризиків інформаційної безпеки в мережах Інтернету речей (IoT) на основі методів нечіткої логіки, зосереджуючи увагу на побудові бази нечітких правил, визначенні релевантних лінгвістичних змінних і формалізації процесу оцінювання ризиків у контексті динамічних та гетерогенних IoT-середовищ.

У межах досягнення цієї мети передбачається:

1. Провести аналіз існуючих методів оцінювання ризиків безпеки в IoT та виявити їхні обмеження в умовах невизначеності.

2. Сформулювати концептуальну модель оцінювання ризиків на основі нечіткої логіки, адаптовану до специфіки IoT-середовищ.

3. Побудувати базу нечітких продукційних правил, що враховують експертні знання та контекст функціонування пристроїв.

4. Реалізувати модель на прикладі типового сценарію IoT-мережі та оцінити її ефективність порівняно з традиційними підходами.

Виклад основного матеріалу. Стрімке зростання кількості пристроїв Інтернету речей (IoT) супроводжується збільшенням поверхні атаки та підвищеним ризиком реалізації кіберзагроз. Уразливості, що виникають унаслідок слабкого шифрування, недостатньої автентифікації чи застарілого програмного забезпечення, створюють значні загрози як для індивідуальних користувачів, так і для критичної інфраструктури. Враховуючи обмеженість ресурсів IoT-пристроїв, динамічність середовища та високу невизначеність у поведінці компонентів мережі, традиційні методи оцінювання ризиків виявляються недостатньо ефективними. Зокрема, формалізовані числові моделі не здатні повною мірою врахувати неповноту, суб’єктивність і варіативність вхідної інформації, яка характерна для реального IoT-середовища.

У зв’язку з цим постає потреба в аналізі сучасних підходів до оцінювання ризиків безпеки IoT з метою виявлення їхніх сильних сторін та обмежень, особливо в контексті роботи в умовах невизначеності. Такий аналіз є необхідним кроком до обґрунтування доцільності використання альтернативних підходів – зокрема, методів нечіткої логіки, які забезпечують ефективну обробку нечітких, якісних та експертних даних.

Розглянемо основні наявні методи оцінювання ризиків інформаційної безпеки в IoT, а також охарактеризуємо їхні переваги й недоліки в контексті складної, динамічної та непередбачуваної природи середовища Інтернету речей.

1. Провести аналіз існуючих методів оцінювання ризиків безпеки в IoT та виявити їхні обмеження в умовах невизначеності.

Оцінювання ризиків інформаційної безпеки є критично важливим етапом управління кіберзахистом, зокрема в умовах зростання масштабів і складності IoT-середовищ. Протягом останніх років було розроблено низку методик для формалізованої оцінки ризиків, серед яких найпоширенішими є:

a) *CVSS (Common Vulnerability Scoring System)* – система, яка надає числову оцінку вразливостей за низкою показників: базових, тимчасових та контекстуальних;

b) *EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)* – методологія оцінювання ризиків, розроблена ANSSI (Франція), яка ґрунтується на моделюванні загроз і потреб у безпеці;

c) *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)* – метод, який орієнтований на визначення активів, вразливостей та загроз, із подальшим оцінюванням ризиків;

d) ISO/IEC 27005 – міжнародний стандарт, що регламентує процес оцінки інформаційних ризиків у межах систем управління інформаційною безпекою (ISMS).

Попри те, що ці методи добре зарекомендували себе в корпоративному IT-середовищі, вони мають суттєві обмеження при застосуванні в IoT-мережах, які характеризуються високим рівнем динамічності, розподіленості та технічної гетерогенності. Серед основних проблем можна виділити таке:

a) **Необхідність повних і точних даних.** Більшість методів вимагає наявності повної інформації про активи, типи вразливостей, шляхи реалізації атак, що у випадку IoT часто неможливо через обмежену спостережуваність пристроїв [11] (автори наголошують, що серед викликів у IoT – *«обмежена спостережуваність пристроїв», та що традиційні методи потерпають через ускладнену класифікацію активів і труднощі з отриманням точних даних*).

b) **Складність формалізації якісних чинників.** Наприклад, такі характеристики, як «критичність пристрою» чи «ймовірність компрометації» у контексті IoT, часто мають експертний або умовний характер і важко піддаються числовій оцінці [12]: *«Із зростанням складності, повсюдності та автоматизації технологічних систем, зокрема в контексті Інтернету речей (IoT), існує переконливий аргумент на користь того, що нам потрібні нові підходи до оцінювання ризиків і формування довіри до систем»*.

c) **Відсутність адаптивності.** Багато підходів засновані на фіксованих процедурах, які не враховують швидкі зміни в топології мережі чи поведінці пристроїв, що притаманні динамічним IoT-середовищам. Як підкреслюють автори [13], *«традиційні політики безпеки, розроблені для статичних середовищ, не здатні ефективно реагувати на динамічний, гетерогенний і ресурсно обмежений характер Інтернету речей (IoT)»*, що підкреслює необхідність розробки адаптивних та контекстно орієнтованих підходів до аналізу ризиків у таких системах.

d) **Ігнорування невизначеності та неповноти.** Традиційні системи оперують точними значеннями та не можуть працювати з розмитими або суперечливими вхідними даними, що часто спостерігається в IoT через фрагментованість джерел інформації [14].

e) **Складність масштабування.** У випадках, коли IoT-мережі охоплюють сотні або тисячі пристроїв, класичні методи стають громіздкими та трудомісткими у використанні. За словами [15], *«ці аналізи демонструють проблеми з масштабованістю, коли застосовуються до великої кількості IoT-додатків»*. Це підтверджує нагальну потребу в розробці легких, адаптивних та масштабованих моделей для IoT.

Таким чином, на тлі зростаючої складності, масштабності та гетерогенності IoT-середовищ застосування традиційних моделей оцінювання ризиків часто виявляється неефективним. Їхні обмеження – зокрема вимога повноти даних, низька адаптивність, складність формалізації якісних чинників, ігнорування невизначеності та труднощі з масштабуванням – призводять до зниження точності результатів, втрати актуальності або

надмірного спрощення складних сценаріїв загроз. У зв'язку з цим постає об'єктивна потреба у впровадженні інтелектуальних підходів, здатних працювати з нечіткими, частковими та суперечливими даними, а також враховувати специфіку та контекст функціонування IoT-систем.

Одним із перспективних напрямів є використання методів нечіткої логіки – інструменту, що дозволяє моделювати експертні знання у формі продукційних правил, працювати з лінгвістичними змінними та адаптуватися до динаміки кіберзагроз.

2. Сформулювати концептуальну модель оцінювання ризиків на основі нечіткої логіки, адаптовану до специфіки IoT-середовищ.

Враховуючи обмеження традиційних підходів до оцінювання ризиків у середовищах Інтернету речей, доцільно використати нечітку логіку як базову методологію для створення адаптивної, гнучкої та контекстно чутливої системи аналізу безпекових ризиків. Запропонована модель базується на поєднанні експертних знань та формалізованих правил нечіткого логічного виведення, що дозволяє враховувати невизначеність, неповноту та розмитість інформації. У межах цього дослідження запропоновано новий підхід до оцінювання ризиків безпеки в IoT-середовищах, який поєднує методи нечіткої логіки з контекстно залежним аналізом функціонування пристроїв. Цей підхід дозволяє враховувати як технічні характеристики, так і роль пристрою в мережі, тип взаємодії та середовище його використання.

2.1. Концептуальна модель оцінювання ризиків на основі нечіткої логіки.

Концептуально модель оцінювання ризиків IoT включає такі ключові компоненти:

А. *Вхідні лінгвістичні змінні:* характеристики ризику, які важко виміряти точно, але можуть бути описані мовою експертів (наприклад, імовірність атаки, критичність пристрою, рівень захисту).

Б. *Фазифікація:* перетворення чітких значень (наприклад, числових або категоріальних) у нечіткі множини для подальшої обробки.

В. *Нечітка база продукційних правил* типу IF–THEN, які моделюють експертну логіку оцінювання ризиків.

Г. *Механізм нечіткого логічного виведення* (наприклад, Mamdani або Sugeno), який визначає ступінь відповідності вхідних даних до встановлених правил.

Д. *Дефазифікація:* перетворення результату нечіткого логічного виведення в чітке числове значення ризику.

Е. *Модуль адаптації:* здатність моделі змінювати ваги змінних або оновлювати базу правил відповідно до змін середовища чи накопичення нових знань.

Описана вище структура моделі є універсальною для широкого кола задач нечіткого оцінювання ризиків. Проте для її ефективного застосування в середовищах Інтернету речей (IoT) вона потребує додаткової адаптації. Це зумовлено специфічними особливостями архітектури, динаміки та обмежень IoT-систем, які суттєво впливають як на природу ризиків, так і на методи їх оцінювання.

У зв'язку з цим при формуванні моделі були враховані такі унікальні властивості IoT-середовищ:

А. *Динамічність:* топологія, активність пристроїв та ризиковий профіль змінюються в реальному часі.

Б. *Гетерогенність:* різні типи пристроїв (сенсори, шлюзи, контролери) мають різний ступінь критичності та захищеності.

В. *Обмежені ресурси:* модель повинна бути легкою у розгортанні та не вимагати складних обчислень на периферійних пристроях.

Г. *Контекстна залежність:* оцінка ризику залежить не лише від технічних характеристик, а й від ролі пристрою у загальній бізнес-логіці системи.

Для кращого розуміння логіки функціонування запропонованої моделі нижче представлено її узагальнену структурну схему, що відображає основні етапи обробки даних, взаємодію компонентів та потік інформації від вхідних параметрів до остаточного результату оцінювання ризику.

На рис. 1 зображено структурну модель оцінювання ризиків інформаційної безпеки в IoT-середовищі на основі нечіткої логіки. Схема демонструє послідовність проходження даних: від надходження лінгвістично описаних вхідних характеристик (наприклад, ймовірність атаки, критичність пристрою) до формування інтегрованої числової оцінки ризику через механізми фазифікації, нечіткого логічного виведення та дефазифікації.

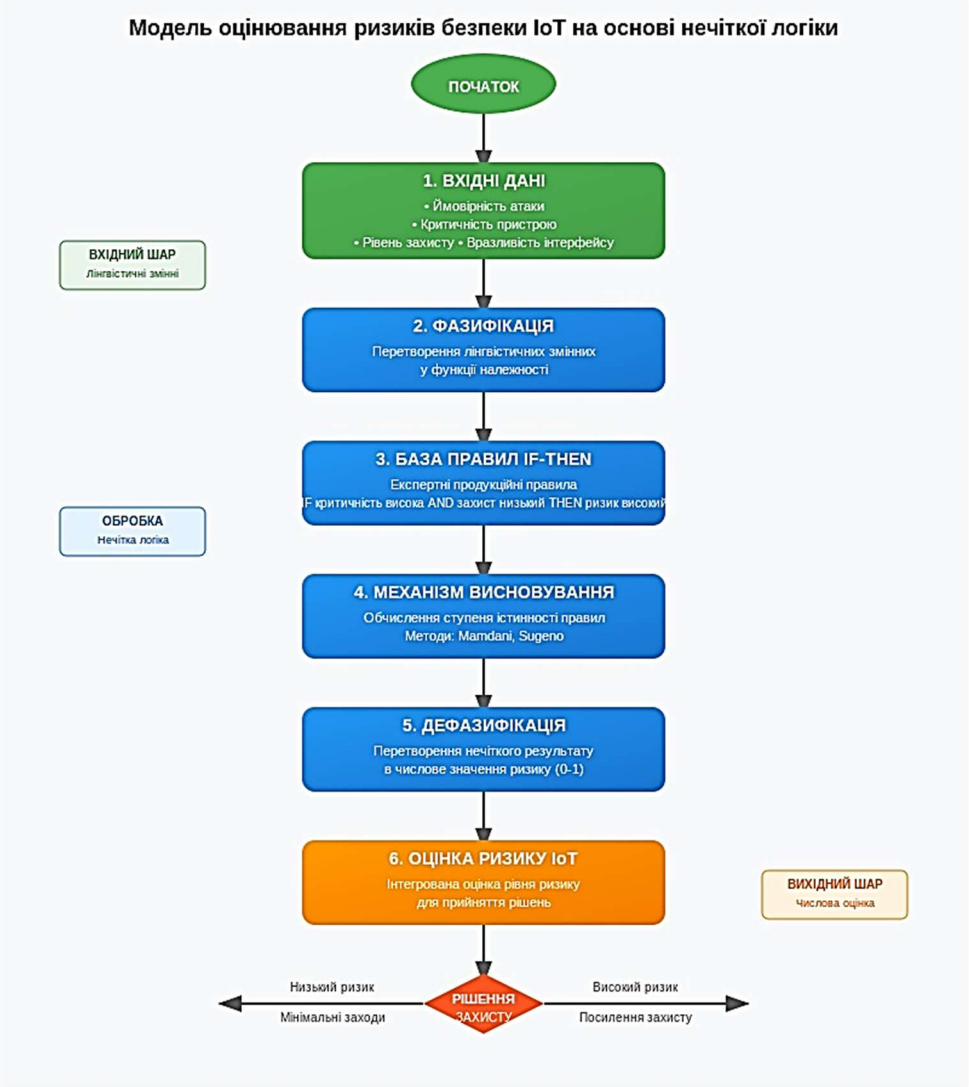

Рис. 1. Структурна модель оцінювання ризиків в IoT на основі нечіткої логіки
Джерело: розроблено автором.

Як видно з рис. 1, модель складається з кількох послідовних етапів обробки, кожен з яких виконує специфічну функцію в процесі оцінювання ризику. Далі детально розглянемо зміст та призначення кожного з компонентів:

А. Вхідні дані.

На цьому етапі до системи надходять параметри, що характеризують поточний стан IoT-середовища. Це можуть бути як технічні показники (наприклад, кількість відкритих портів, наявність вразливостей, тип пристрою), так і експертні оцінки (наприклад, критичність функції пристрою або ймовірність атаки).

Б. Фазифікація.

Вхідні лінгвістичні змінні (наприклад, «високий ризик», «низька захищеність») перетворюються на функції належності, які дозволяють моделі працювати з розмитими, нечітко визначеними значеннями.

В. База нечітких правил IF–THEN.

Цей компонент містить формалізовані експертні знання у вигляді продукційних правил типу «Якщо – То». Наприклад: *«Якщо критичність пристрою висока і рівень захисту низький, то ризик високий»*. Кожне правило оцінюється відповідно до вхідних даних.

Г. Механізм нечіткого логічного виведення.

На цьому етапі виконується об'єднання результатів застосування усіх правил для формування узагальненої нечіткої оцінки ризику. Найчастіше використовується метод Мамдані або Сугено.

Д. Дефазифікація.

Нечітке значення, сформоване в попередньому блоці, перетворюється у конкретне числове або категоріальне значення (наприклад, 0,72 або «середній ризик»).

Е. Оцінка ризику.

Таким чином, концептуальна модель визначає основні етапи оцінювання ризику в IoT-середовищі. Для практичної реалізації цієї моделі необхідно задати параметри функцій належності вхідних та вихідної змінних, що й розглянуто у наступному підрозділі.

2.2. Параметри функцій належності

Для забезпечення відтворюваності результатів у роботі подано параметри функцій належності вхідних і вихідної лінгвістичних змінних. Усі змінні нормовано до діапазону [0; 10]. Для фазифікації використано трикутні (trimf) та трапецієподібні (trapmf) функції. Механізм нечіткого логічного виведення – Мамдані; оператори: AND = min, OR = max; імплікація = min; агрегування = max; дефазифікація – centroid.

Вхідні змінні:

a. Рівень вразливості пристрою (Low, Medium, High);
b. Критичність функцій (Low, Medium, High);
c. Захищеність каналу *зв'язку* (Low, Medium, High).

Вихідна змінна:

a. Рівень ризику (Low, Moderate, High, Critical).

Параметри функцій належності наведено у табл. 1.

Таблиця 1 – Параметри функцій належності

Змінна	**Терм**	**Форма**	**Параметри**
Вразливість	Low	trimf	[0, 0, 4]
	Medium	trimf	[2, 5, 8]
	High	trimf	[6, 10, 10]
Критичність	Low	trapmf	[0, 0, 2, 4]
	Medium	trimf	[3, 5, 7]
	High	trapmf	[6, 8, 10, 10]
Захищеність каналу	Low	trapmf	[0, 0, 2, 4]
	Medium	trimf	[3, 5, 7]
	High	trapmf	[6, 8, 10, 10]
Ризик	Low	trapmf	[0, 0, 1.5, 3.5]
	Moderate	trimf	[2.5, 5, 7.5]
	High	trimf	[6.5, 8, 9.5]
	Critical	trapmf	[8.5, 9.5, 10, 10]

Для наочності на рис. 2 подано графічне зображення функцій належності для вхідних та вихідної змінних. Видно, що терми мають плавні переходи та перекриття, що забезпечує адекватне відображення проміжних станів і контекстно залежне оцінювання ризику.

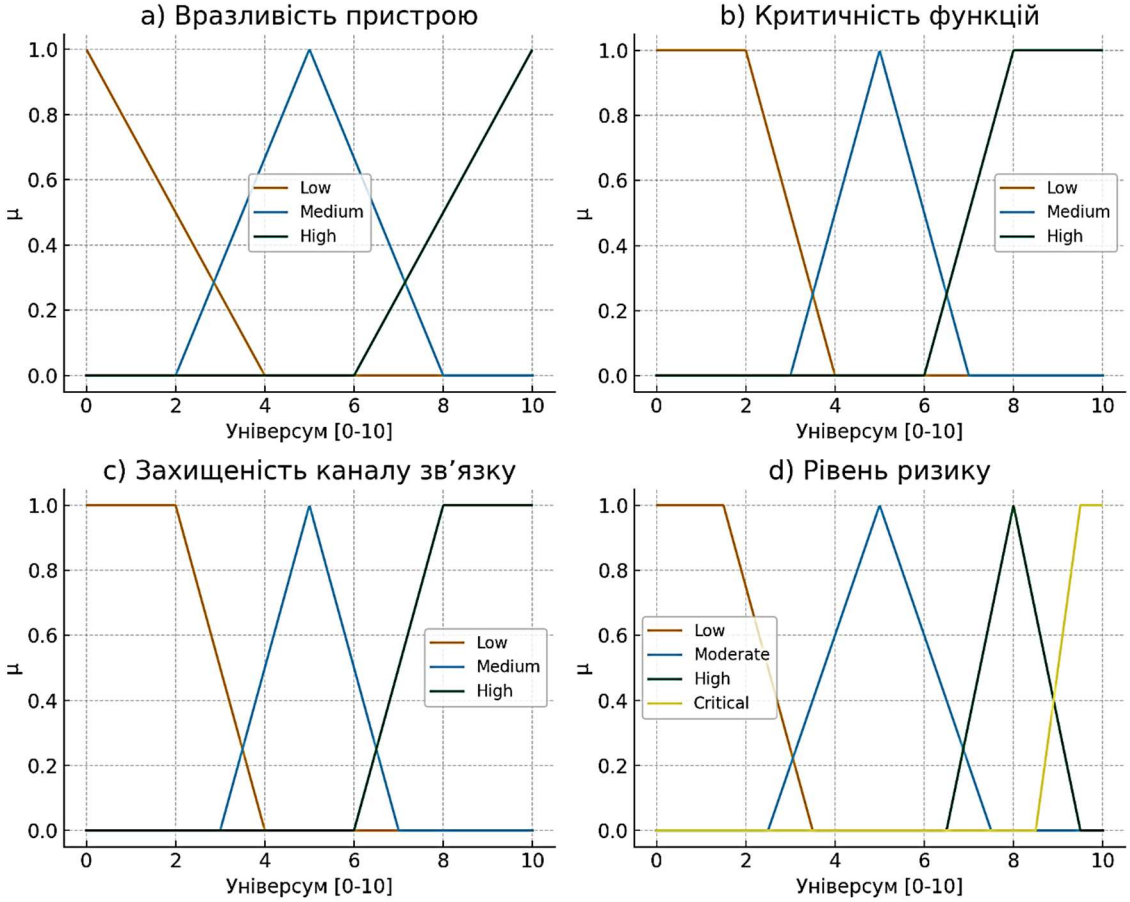

Рис. 2. Функції належності для вхідних і вихідної змінних
Джерело: розроблено автором.

Отже, табл. 1 та рис. 2 забезпечують як формальну відтворюваність (через числові параметри), так і наочність моделі (через графічне подання функцій належності). Завдяки плавним переходам між термами й перекриттю областей визначення досягається можливість адекватного опису проміжних станів та обробки невизначеності у вхідних даних.

3. **Побудувати базу нечітких продукційних правил, що враховують експертні знання та контекст функціонування пристроїв.**

Оцінювання ризиків у середовищах Інтернету речей (IoT) вимагає гнучких методів, здатних працювати з неоднозначною, неповною та контекстно залежною інформацією. У зв'язку з цим у рамках запропонованої моделі особливу увагу приділено формуванню бази нечітких продукційних правил, яка відображає як технічні параметри пристроїв, так і експертні знання про їхню поведінку, призначення та ступінь критичності.

На відміну від традиційних моделей, що вимагають точних числових оцінок, нечітка база правил дозволяє описати взаємозв'язки між факторами ризику в лінгвістичній формі, наближеній до природної мови експертів. Це є особливо цінним в умовах IoT, де багато пристроїв не мають достатнього логування подій, а дані про вразливості або загрози – фрагментарні.

Кожне правило має загальний вигляд:

IF (умова 1) AND (умова 2) AND ... THEN (висновок).

Умови формуються на основі таких лінгвістичних змінних:

a. *Рівень вразливості пристрою:* (низький, середній, високий);

b. *Ступінь критичності функцій:* (некритичний, помірно критичний, критичний);

c. *Рівень безпеки каналу зв'язку:* (зашифрований, частково зашифрований, відкритий);
d. *Тип доступу до пристрою:* (локальний, віддалений, змішаний);
e. *Тип пристрою:* (сенсор, шлюз, контролер, вузол обробки).

Висновок формулюється як рівень ризику: (низький, помірний, високий, критичний).

Приклад нечіткого правила:

F `вразливість` = **висока** AND `критичність` = **критичний** AND `канал` = **відкритий** THEN `ризик` = **дуже високий.**

З метою ілюстрації логіки побудови бази нечітких продукційних правил на основі експертних оцінок та контекстних характеристик пристроїв на рис. 3 наведено відповідну блок-схему, яка демонструє основні етапи формування правил у запропонованій моделі.

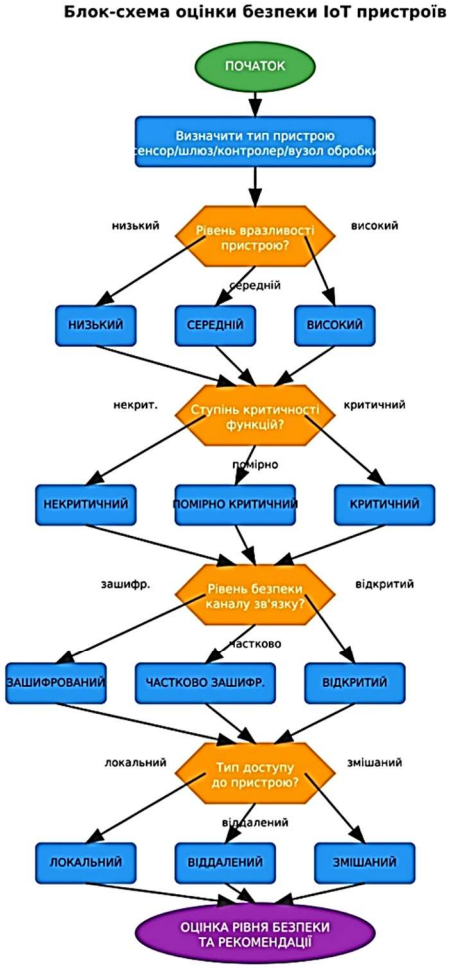

Рис. 3. Блок-схема оцінки безпеки IoT пристроїв

Джерело: розроблено автором.

Представлена на рис. 3 блок-схема демонструє загальні принципи побудови нечітких продукційних правил на основі лінгвістичних змінних, що застосовуються для формалізації експертних знань. Водночас для ефективного застосування цієї моделі в умовах реального IoT-середовища виникає необхідність у її контекстній адаптації – з урахуванням особливостей топології, ролі пристрою в мережі та специфіки взаємодії. Під контекстом розуміються такі характеристики, як місце в мережі (edge/core), тип взаємодії (M2M, user-device), а також характер середовища (медичне, промислове, побутове). Така контекстуалізація дозволяє:

а. адаптувати правила під специфіку сфери застосування IoT (наприклад, у промислових системах критичність шлюзів є вищою, ніж у побутових);

б. уточнювати терми в лінгвістичних змінних;

в. задавати динамічні ваги для різних умов (наприклад, у критичних зонах ризик зростає швидше).

Таким чином, контекстуалізація дозволяє значно підвищити точність та адаптивність системи оцінювання ризиків, формуючи правила, релевантні до конкретного середовища функціонування IoT-пристрою. З огляду на це, наступним ключовим кроком є безпосередня побудова бази продукційних правил, яка і реалізує логіку оцінювання ризику на основі поєднання технічних параметрів та контекстуальних ознак.

Методологія формування правил. Базу нечітких продукційних правил сформовано за допомогою поєднання трьох підходів:

a) *Аналіз стандартів і методик* (CVSS, ISO/IEC 27005, EBIOS) – для визначення базових факторів ризику.

b) *Аналіз наукових публікацій* [5-8, 11-15], де наведено типові сценарії атак і приклади нечітких систем для IoT.

c) *Експертне опитування* фахівців з кібербезпеки (метод Delphi у два раунди), які оцінювали комбінації вразливості, критичності та рівня захищеності каналів.

Побудова бази правил здійснюється у два етапи:

a) *Експертне визначення факторів ризику* та їхніх лінгвістичних термів.

b) *Формування нечітких правил на основі сценаріїв загроз*, типових для IoT-мереж (наприклад, несанкціонований доступ, атаки типу DoS, перехоплення трафіку, компрометація вузла керування тощо).

Для ілюстрації логіки формування правил нижче наведено приклад таблиці (матриці), у якій представлено взаємозв'язок між вразливістю, критичністю, типом доступу та іншими факторами ризику в контексті IoT.

Таблиця 2 – Нечіткі правила оцінювання ризику в IoT

Вразливість	**Критичність функцій**	**Захист каналу**	**Тип доступу**	**Тип пристрою**	**Середовище**	**Ризик**
Висока	Критична	Відкритий	Віддалений	Шлюз	Промислове	Дуже високий
Висока	Критична	Частково захищений	Віддалений	Контролер	Медичне	Дуже високий
Середня	Помірно критична	Частково захищений	Змішаний	Сенсор	Побутове	Помірний
Низька	Некритична	Зашифрований	Локальний	Сенсор	Побутове	Низький
Середня	Критична	Відкритий	Віддалений	Вузол обробки	Критична інфраструктура	Високий
Висока	Помірно критична	Зашифрований	Віддалений	Контролер	Промислове	Високий
Середня	Некритична	Зашифрований	Локальний	Сенсор	Побутове	Низький
Висока	Критична	Зашифрований	Віддалений	Вузол обробки	Медичне	Високий

Джерело: розроблено автором.

Представлена табл. 2 демонструє приклади нечітких правил, сформованих на основі комбінації технічних та контекстуальних факторів. Вона ілюструє, як система може визначати рівень ризику залежно від поєднання таких змінних, як критичність функцій пристрою, тип доступу, рівень захисту каналу та середовище експлуатації.

Завдяки використанню лінгвістичних термів і контекстної інформації система здатна адаптивно реагувати на зміну умов, забезпечуючи більш точне та інтерпретоване оцінювання ризику. Такий підхід підвищує гнучкість та ефективність кіберзахисту в умовах гетерогенних та динамічних IoT-мереж.

4. Реалізувати модель на прикладі типового сценарію IoT-мережі та оцінити її ефективність порівняно з традиційними підходами.

Для демонстрації практичної реалізації запропонованої моделі було змодельовано типовий фрагмент IoT-мережі, що включає гетерогенні пристрої з різними рівнями критичності, типами доступу, каналами зв'язку та контекстами функціонування (побутовий, промисловий). Такий підхід дозволяє перевірити адаптивність і точність запропонованої системи оцінювання ризиків у різних умовах. Описана мережа містить ключові компоненти сучасного IoT-середовища – сенсори, контролери, шлюзи, вузли обробки та хмарну інфраструктуру – і відображає характерні зв'язки між ними, включаючи локальні та віддалені з'єднання, а також різний рівень захисту каналів передачі даних. У моделі враховано як технічні, так і контекстуальні характеристики пристроїв, що дозволяє оцінити ризики з урахуванням їхнього функціонального призначення, місця в мережі та середовища експлуатації.

На рис. 4 представлено узагальнену схему змодельованого фрагмента IoT-мережі, яка візуалізує структурні компоненти, рівні ризику та типи комунікаційних каналів. Схема ілюструє взаємозв'язки між пристроями в контексті запропонованої моделі оцінювання ризиків, що ґрунтується на лінгвістичних змінних та контекстно орієнтованих правилах.

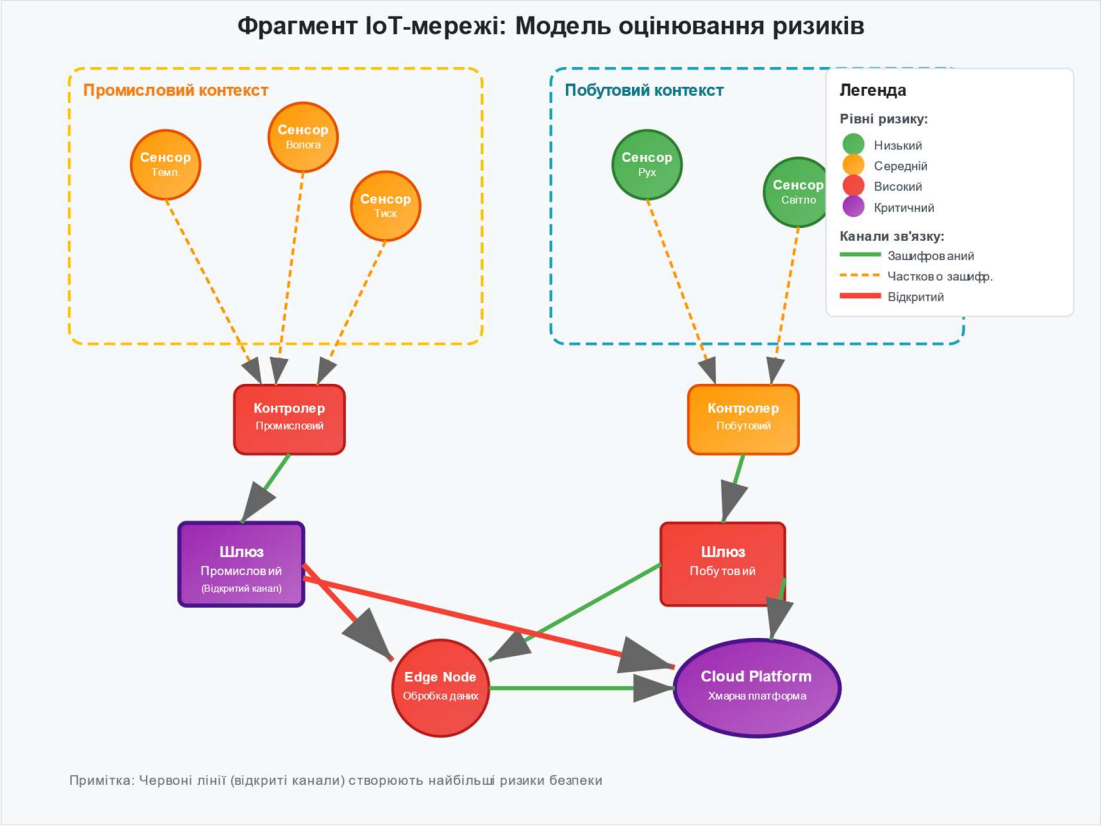

Рис. 4. Узагальнена схема IoT-мережі

Джерело: розроблено автором.

Для реалізації моделі оцінювання ризиків було використане середовище MATLAB із використанням Fuzzy Logic Toolbox. Було створено нечітку логічну систему типу Mamdani [16] з трьома вхідними змінними: рівень вразливості, критичність функцій пристрою та рівень захищеності каналу зв'язку та однією вихідною змінною – рівнем ризику.

Для кожної із вхідних змінних визначено по три терми (низький, середній, високий), а для вихідної – чотири (низький, помірний, високий, критичний), що дозволяє точніше моделювати перехідні стани.

Базу нечітких продукційних правил було сформовано програмно, враховуючи взаємозв'язок вхідних факторів. Загалом реалізовано 27 правил, які описують комбінації умов і відповідних рівнів ризику. Такий підхід дозволяє автоматизувати процес прийняття рішень, що особливо важливо в умовах швидкозмінного середовища IoT.

Результати моделювання подано у вигляді поверхні нечіткої логічної інтерпретації (рис. 5), яка демонструє залежність рівня ризику від рівня вразливості та критичності при фіксованому рівні захищеності каналу. Видно, що найвищі ризики виникають у ситуаціях, коли пристрій є водночас критичним і вразливим, а канал передачі даних – незахищеним.

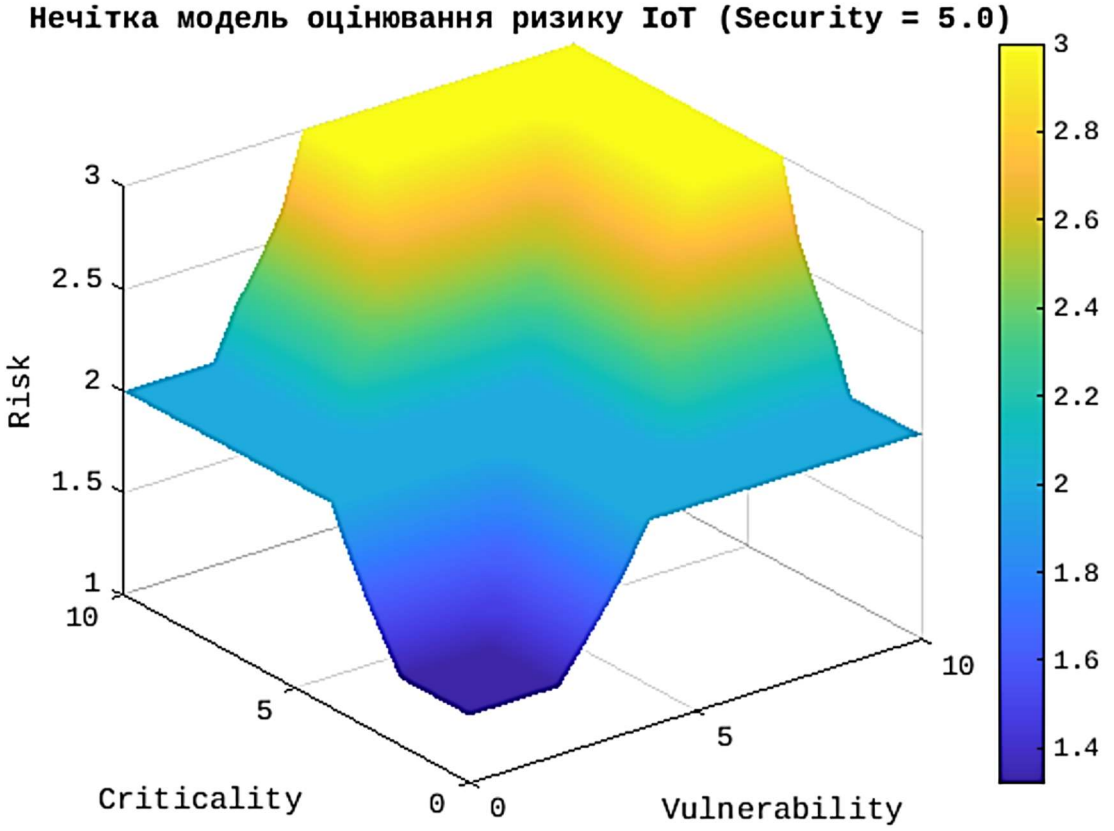

Рис. 5. Тривимірна візуалізація оцінювання ризику в IoT на основі нечіткої логіки
Джерело: розроблено автором.

Процедура оцінювання за методологією EBIOS. Для проведення порівняльного аналізу використано методологію *EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)*, яка включає такі основні етапи:

1. *Ідентифікація контексту* – визначено пристрої (сенсори, контролери, шлюзи, вузли обробки), їх функції та середовище експлуатації (промислове, медичне, побутове).
2. *Моделювання загроз* – враховано потенційні атаки (DoS, MITM, несанкціонований доступ, компрометація вузлів керування).
3. *Оцінка ймовірності реалізації загроз* – виконувалась за якісною шкалою (низька, середня, висока) залежно від типу доступу, рівня захищеності каналів та відомих вразливостей.
4. *Оцінка впливу на бізнес-процеси* – визначено три рівні: низький, високий, критичний.
5. *Визначення рівня ризику* – поєднання ймовірності та впливу згідно з матрицею EBIOS.

Наприклад, вузол обробки у промисловому контексті отримав категорію *Критичний*, оскільки навіть при середній ймовірності атаки наслідки призводять до порушення критичних бізнес-процесів. Натомість побутовий сенсор із низькою вразливістю та захищеним каналом класифіковано як *Низький ризик*, адже вплив на систему у випадку компрометації є мінімальним.

З метою об'єктивного порівняння запропонованої моделі на основі нечіткої логіки з усталеною методологією EBIOS було проведено оцінювання ризиків для однакових умов у типовому фрагменті IoT-мережі. В обох випадках враховувалися ключові фактори: рівень вразливості пристрою, критичність його функцій та рівень захисту каналу зв'язку. У той час як EBIOS базується на дискретній класифікації ризиків за заздалегідь визначеними пороговими значеннями, модель Mamdani забезпечує континуальне (плавне) оцінювання з використанням нечітких лінгвістичних правил.

У табл. 3 наведено результати оцінювання ризиків для вибірки з 8 типових пристроїв у мережі**,** які функціонують у різних контекстах (промисловому, медичному, побутовому). Для кожного пристрою вказано значення трьох вхідних параметрів, а також результати оцінки ризику за обома підходами.

Таблиця 3 – Порівняння результатів оцінювання ризику: нечітка логіка і EBIOS

Пристрій	**Вразливість**	**Критичність**	**Захист каналу**	**Ризик (Fuzzy)**	**Ризик (EBIOS)**
Шлюз промисловий	Висока	Критична	Низький	9.1 (Критичний)	Критичний
Контролер медичний	Висока	Критична	Середній	7.8 (Високий)	Високий
Сенсор побутовий	Середня	Помірна	Середній	5.1 (Помірний)	Середній
Сенсор побутовий	Низька	Низька	Високий	2.4 (Низький)	Низький
Вузол обробки	Середня	Критична	Низький	7.3 (Високий)	Критичний
Контролер промисловий	Висока	Помірна	Високий	6.4 (Високий)	Середній/Високий
Сенсор побутовий	Середня	Низька	Високий	3.1 (Низький)	Низький
Вузол обробки	Висока	Критична	Високий	7.0 (Високий)	Високий

Джерело: розроблено автором.

Як видно з табл. 3, модель Mamdani дозволяє більш гнучко враховувати комбінації факторів, забезпечуючи детальніший спектр ризиків. Наприклад, для вузла обробки з критичними функціями та середнім рівнем захисту EBIOS присвоює найвищу категорію («Критичний»), тоді як нечітка модель дає значення *7.3*, що відповідає високому, але не максимальному рівню. Така точність може бути критично важливою при автоматичному розгортанні заходів реагування в умовах обмежених ресурсів.

Адаптивність моделі. У представлених експериментах розглянуто переважно статичні сценарії, проте важливою особливістю запропонованої моделі є здатність до адаптації. Це забезпечується такими механізмами:

1. *Динамічне оновлення правил.* База нечітких правил може бути автоматично доповнена або змінена залежно від нових подій у мережі. Наприклад, при виявленні нового типу атаки (перехоплення трафіку, підробка сенсора) формується додаткове правило IF–THEN, яке відображає змінені умови.

2. *Актуалізація ваг факторів ризику.* В умовах змін у середовищі (наприклад, підвищення критичності шлюзу у промисловому контексті) модель дозволяє оперативно скоригувати ваги лінгвістичних змінних без повного переналаштування системи.

3. *Інтеграція з потоковим моніторингом.* Використання MATLAB/Simulink дає можливість реалізувати обробку даних у реальному часі, що дозволяє змінювати параметри функцій належності або додавати нові правила на основі поточного стану мережі.

Таким чином, запропонована модель може працювати не лише у статичних сценаріях, але й у динамічних умовах, коли топологія мережі та характер загроз постійно змінюються. Це підтверджує її потенціал для практичного застосування у системах моніторингу та реагування на інциденти в IoT.

Висновки. У ході дослідження було запропоновано та реалізовано контекстно орієнтовану модель оцінювання ризиків в IoT-середовищі на основі нечіткої логіки. Модель враховує не лише технічні характеристики пристроїв, а і їхню критичність, тип каналів зв'язку та контекст експлуатації. Завдяки використанню лінгвістичних змінних і нечіткого виведення типу Mamdani вдалося побудувати систему, здатну адаптивно оцінювати рівень ризику в умовах високої динамічності, гетерогенності та неповноти даних, що притаманні IoT-мережам.

Проведено моделювання типового фрагмента IoT-мережі в MATLAB з візуалізацією поверхні оцінювання ризику, а також виконано порівняльний аналіз результатів із традиційною методологією EBIOS. Отримані результати демонструють перевагу запропонованого підходу у точності, гнучкості й здатності до пояснюваності рішень.

Наукова новизна отриманих результатів:

1. Запропоновано контекстно орієнтовану модель оцінювання ризиків в IoT-мережах з урахуванням критичності, вразливості та типу захищеності каналів зв'язку.

2. Розроблено методику формування бази нечітких продукційних правил, яка поєднує аналіз стандартів (CVSS, ISO/IEC 27005, EBIOS), наукових публікацій та експертних оцінок (метод Delphi). Це забезпечує відтворюваність та обґрунтованість логіки правил, що відрізняє підхід від існуючих статичних моделей. Реалізовано нечітке виведення типу Mamdani з лінгвістичними змінними, що забезпечує більш природне і адаптивне оцінювання ризику порівняно з класичними методами.

3. Проведено порівняльний аналіз з методологією EBIOS, що дозволило емпірично обґрунтувати переваги запропонованої моделі в умовах реальних IoT-сценаріїв.

Практична значимість результатів:

1. Розроблена модель може бути застосована в системах моніторингу кібербезпеки IoT для автоматичного визначення рівня ризику і пріоритезації заходів реагування.

2. Результати можуть бути використані в процесі проєктування безпечних IoT-інфраструктур, зокрема у промислових, побутових та критичних середовищах.

3. Інструментарій реалізовано у MATLAB, що дозволяє легко адаптувати його для практичних впроваджень, тестування та навчання.

4. Підхід забезпечує можливість швидкої адаптації до нових загроз шляхом зміни або доповнення правил, що критично важливо для гнучкого реагування у реальному часі.

Отже, результати дослідження підтверджують доцільність використання нечітких моделей для оцінювання ризиків у гетерогенному середовищі IoT. Запропонований підхід дозволяє підвищити точність і гнучкість рішень, а також слугує основою для побудови більш стійких і адаптивних систем інформаційної безпеки.

Список використаних джерел

1. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. Computer, *44*(9), 51-58. https://doi.org/10.1109/mc.2011.291.

2. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008.

3. Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (e-health) systems. Journal of Medical Systems, *40*(12). https://doi.org/10.1007/s10916-016-0597-z.

4. Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019). AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. У *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)*. IEEE. https://doi.org/10.1109/ccwc.2019.8666450.

5. Atlam, H. F., Walters, R. J., Wills, G. B., & Daniel, J. (2019). Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT. *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-019-01214-w.

6. Al-Kasassbeh, M., Almseidin, M., Alrfou, K., & Kovacs, S. (2020). Detection of IoT-botnet attacks using fuzzy rule interpolation. *Journal of Intelligent & Fuzzy Systems*, *39*(1), 421-431. https://doi.org/10.3233/jifs-191432.

7. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221. https://doi.org/10.1016/j.comnet.2018.03.012.

8. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial internet of things. *Symmetry*, *15*(10), 1958. https://doi.org/10.3390/sym15101958.

9. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018.

10. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023b). Fuzzy logic and its application in the assessment of information security risk of industrial internet of things. *Symmetry*, *15*(10), 1958. https://doi.org/10.3390/sym15101958.

11. Al-Khafajiy, A., Hussain, A., Baker, T., Aslam, N., & Alazab, M. (2025). A hybrid deep learning-based risk assessment model for securing the Internet of Things. *Computers & Security, 140,* Article 103419. https://www.sciencedirect.com/science/article/pii/S0167404825001452.

12. Nurse, J. R. C., Radanliev, P., Creese, S., & De Roure, D. (2018b). If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems. У *Living in the internet of things: Cybersecurity of the* IoT - *2018*. Institution of Engineering and Technology. https://doi.org/10.1049/cp.2018.0001.

13. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002.

14. Pal, S., Khalifa, S., Miller, D., Dedeoglu, V., Dorri, A., Ramachandran, G., Moghadam, P., Kusy, B., & Jurdak, R. (2024). Uncertainty propagation in the internet of things. *Discover Internet of Things*, *4*(1). https://doi.org/10.1007/s43926-024-00085-2.

15. Ibrahim Abdul Abdulrahman, Gabriel Tosin Ayodele, Grace Efahn Egbedion, Jacob Alebiosu, Ezeagba Jetta Somtochukwu & Omotolani Eniola Akinbolajo. (2025). Securing Internet of Things (IoT) ecosystems: Addressing scalability, authentication, and privacy challenges. *World Journal of Advanced Research and Reviews*, *26*(1), 523-534. https://doi.org/ 10.30574/wjarr.2025.26.1.0999.

16. Mamdani, E. H., & Assilian, S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller. *International Journal of Man-Machine Studies*, *7*(1), 1-13. https://doi.org/10.1016/ s0020-7373(75)80002-2.

References

1. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. Computer, *44*(9), 51-58. https://doi.org/10.1109/mc.2011.291.

2. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008.

3. Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (e-health) systems. Journal of Medical Systems, *40*(12). https://doi.org/10.1007/s10916-016-0597-z.

4. Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019). AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. У *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)*. IEEE. https://doi.org/10.1109/ccwc.2019.8666450.

5. Atlam, H. F., Walters, R. J., Wills, G. B., & Daniel, J. (2019). Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT. *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-019-01214-w.

6. Al-Kasassbeh, M., Almseidin, M., Alrfou, K., & Kovacs, S. (2020). Detection of IoT-botnet attacks using fuzzy rule interpolation. *Journal of Intelligent & Fuzzy Systems*, *39*(1), 421-431. https://doi.org/10.3233/jifs-191432.

7. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221. https://doi.org/10.1016/j.comnet.2018.03.012.

8. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial internet of things. *Symmetry*, *15*(10), 1958. https://doi.org/10.3390/sym15101958.

9. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018.

10. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023b). Fuzzy logic and its application in the assessment of information security risk of industrial internet of things. *Symmetry*, *15*(10), 1958. https://doi.org/10.3390/sym15101958.

11. Al-Khafajiy, A., Hussain, A., Baker, T., Aslam, N., & Alazab, M. (2025). A hybrid deep learning-based risk assessment model for securing the Internet of Things. *Computers & Security, 140,* Article 103419. https://www.sciencedirect.com/science/article/pii/S0167404825001452.

12. Nurse, J. R. C., Radanliev, P., Creese, S., & De Roure, D. (2018b). If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems. У *Living in the internet of things: Cybersecurity of the* IoT - *2018*. Institution of Engineering and Technology. https://doi.org/10.1049/cp.2018.0001.

13. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002.

14. Pal, S., Khalifa, S., Miller, D., Dedeoglu, V., Dorri, A., Ramachandran, G., Moghadam, P., Kusy, B., & Jurdak, R. (2024). Uncertainty propagation in the internet of things. *Discover Internet of Things*, *4*(1). https://doi.org/10.1007/s43926-024-00085-2.

15. Ibrahim Abdul Abdulrahman, Gabriel Tosin Ayodele, Grace Efahn Egbedion, Jacob Alebiosu, Ezeagba Jetta Somtochukwu & Omotolani Eniola Akinbolajo. (2025). Securing Internet of Things (IoT) ecosystems: Addressing scalability, authentication, and privacy challenges. *World Journal of Advanced Research and Reviews*, *26*(1), 523-534. https://doi.org/ 10.30574/wjarr.2025.26.1.0999.

16. Mamdani, E. H., & Assilian, S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller. *International Journal of Man-Machine Studies*, *7*(1), 1-13. https://doi.org/10.1016/ s0020-7373(75)80002-2.

Отримано 03.07.2025

TECHNICAL SCIENCES AND TECHNOLOGIES

UDC 004.2

Yuriy Pidlisnyi

Postgraduate student of the Department of Cybersecurity and Mathematical Modeling
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: ypodlesny@ukr.net. **ORCID:** https://orcid.org/0009-0001-9783-3898. **ResearcherID:** LSL-1170-2024

FUZZY LOGIC IN IOT SECURITY RISK ASSESSMENT: RULE CONSTRUCTION AND IMPLEMENTATION

This paper presents a context-aware model for information-security risk assessment in Internet-of-Things (IoT) environments, built on Mamdani-type fuzzy logic. Unlike traditional deterministic schemes, the model couples device-level attributes with operational context, enabling robust reasoning over incomplete, vague, and conflicting evidence typical of dynamic IoT networks. The input space comprises device vulnerability, function criticality, and protection of the communication channel; additionally, the device's role in the topology, access type, and deployment environment (household, industrial, medical) are considered during rule design. Expert knowledge is formalized as a coherent base of 27 fuzzy IF–THEN rules. Inference follows the Mamdani pipeline with AND = min, OR = max, implication = min, aggregation = max, and centroid defuzzification. The implementation in MATLAB (Fuzzy Logic Toolbox) normalizes linguistic variables to [0, 10] and uses triangular and trapezoidal membership functions to ensure smooth term transitions.

Validation was performed on a simulated fragment of a heterogeneous IoT network (sensors, controllers, gateways, processing nodes) with varied access patterns and channel protection levels. The results exhibit continuous risk surfaces and smooth transitions between risk levels, avoiding the staircase effects inherent to discrete matrices. A representative case shows that a processing node with critical functions and a partly protected channel is rated High (~7.3) by the fuzzy model, whereas EBIOS categorizes it as Critical, yielding finer prioritization for resource-aware response while remaining consistent in clearly low/high scenarios. The approach preserves explainability via linguistic rules, tolerates missing or imprecise inputs, and is suitable for integration with edge/gateway monitoring to support automated, real-time risk analysis.

The proposed model can serve as a foundation for adaptive risk-assessment systems in dynamic and safety-critical IoT settings. Future work includes enriching the input features with threat-intelligence signals, modeling temporal decay of evidence, and federated aggregation of local risk estimates for large-scale deployments.

Keywords: *Internet of Things (IoT); risk assessment; fuzzy logic; Fuzzy Logic Toolbox; Mamdani; information security; EBIOS.*

Fig.: 5. Table: 3. References: 16.

Підлісний Ю. І. Нечітка логіка в оцінюванні ризиків безпеки IoT: побудова правил і реалізація. *Технічні науки та технології,* 2025. № 3(41). С. 237-253. DOI: https://doi.org/10.25140/2411-5363-2025-3(41)-237-253.