

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

**Навчально-науковий інститут
«Інститут інформаційних технологій в економіці»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»

Галузь знань 12 «Інформаційні технології»

Спеціальність 124 «Системний аналіз»

Форма навчання: очно (денна)
очно (денна), заочна, дистанційна

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему «Розробка алгоритму ранжування та класифікації
кіберінцидентів шахрайства з використанням нечіткої логіки»
(назва теми)

здобувачки Стадник Мар'яни Василівни _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник к.е.н., доцент, Потапенко Сергій Дмитрович
(науковий ступінь, учене звання, ПІБ)

(niɒnuc)

**Робота допущена до захисту перед екзаменаційною комісією
з атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.ф.-м.н., проф., Джалладова І.А.

(niɔnuc)

Київ 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Навчально-науковий інститут «Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»
СПЕЦІАЛЬНІСТЬ 124 «СИСТЕМНИЙ АНАЛІЗ»

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми

_____ Джалладова І.А.
(підпис)

_____ 20__ р.

ЗАТВЕРДЖУЮ

Завідувач кафедри системного аналізу та
кібербезпеки

_____ Джалладова І.А.
(підпис)

_____ 20__ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти

_____ Стадник Мар'яні Василівні
(прізвище, ім'я, по батькові)

_____ очної (денної)

очної (денної), заочної, дистанційної

форми навчання

на підготовку кваліфікаційної бакалаврської роботи

**на тему «Розробка алгоритму ранжування та класифікації кіберінцидентів шахрайства з
використанням нечіткої логіки»**

Тему затверджено наказом ректора Університету від «26» квітня 2026 р. № 542-ст

Кваліфікаційна бакалаврська робота виконується на матеріалах

_____ Департаменту кіберполіції Національної поліції України

План кваліфікаційної бакалаврської роботи

Розділ 1	Особливості визначення кіберінцидентів та методів їх виявлення в задачах кібербезпеки (назва розділу)
Розділ 2	Методи подолання невизначеності в задачах кібербезпеки (назва розділу)
Розділ 3	Розроблення та застосування алгоритму ранжування та класифікації кіберінцидентів (назва розділу)

Об'єкт дослідження:	кіберінциденти шахрайства.
Предмет дослідження:	методи експертних оцінок та нечіткої логіки для ранжування та класифікації кіберінцидентів шахрайства.
Мета кваліфікаційної бакалаврської роботи:	огляд методів та створення алгоритму ранжування та класифікації кіберінцидентів шахрайства.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1	Визначити сутність кіберінцидентів шахрайства та особливості їхнього трактування сьогодні. Дослідити сутність проблеми невизначеності у сфері кіберінцидентів шахрайства та способів її усунення. Проаналізувати наукові дослідження щодо подолання зазначеної проблеми.
У розділі 2	Дослідити особливості застосування нечіткої логіки, нечітких множин, фазифікації, дефазифікації та функції належності для аналізу даних. Проаналізувати правила «якщо-то», математичні методи оцінювання й оброблення даних, експертні підходи, метод Дельфі, мінмакс нормалізацію, метод зваженої суми для класифікації кіберінцидентів шахрайства.
У розділі 3	Розробити алгоритм ранжування та класифікації кіберінцидентів шахрайства за визначеними рівнями ризику. Опис кроки розробленого алгоритму. Розробити сукупність правил «якщо-то» для перетворення критеріїв задачі, які описані лінгвістичними змінними, на чіткі значення. Класифікувати наявні інциденти у відповідності до алгоритму.

**Завдання підготував
науковий керівник**

(підпис)

С. Д. Потапенко
(ініціали, прізвище)

« ____ » _____ 20__ р.

**Завдання одержав
здобувач**

(підпис)

М. В. Стадник
(ініціали, прізвище)

« ____ » _____ 20__ р.

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 46 сторінок, 20 таблиць, 11 рисунків, список використаних джерел з 23 найменувань, додатки. **«Розробка алгоритму ранжування та класифікації кіберінцидентів шахрайства з використанням нечіткої логіки»**

Об'єктом дослідження є кіберінциденти шахрайства.

Предметом дослідження є методи експертних оцінок та нечіткої логіки для ранжування та класифікації кіберінцидентів шахрайства.

Мета кваліфікаційної бакалаврської роботи – це огляд методів для створення алгоритму ранжування та класифікації кіберінцидентів шахрайства.

Відповідно до поставленої мети були визначені такі завдання:

1. Розглянути проблему невизначеності щодо ранжування кіберінцидентів;
2. Розглянути теорію нечіткої логіки та методів експертних оцінок;
3. Розробити власний алгоритм ранжування та класифікації кіберінцидентів.

Практичне значення отриманих результатів:

Запропонований алгоритм може бути застосований для систем моніторингу кіберзагроз організацій та для аналізу кібершахрайства: оцінки критичності інцидентів, ранжування та класифікації їх за рівнем ризику.

Методи роботи: Для виконання поставлених завдань було використано метод Дельфі, мінмакс нормування, нечіткі правила виведення та функції належності.

Рік виконання кваліфікаційної бакалаврської роботи – 2026.

Рік захисту роботи – 2026.

Ключові слова: кіберінцидент, шахрайство, ранжування кіберінцидентів, класифікація інцидентів, нечітка логіка, нормалізація даних, метод Дельфі.

В і д г у к
про кваліфікаційну бакалаврську роботу
здобувача навчально-наукового інституту
«Інститут інформаційних технологій в економіці»
освітньо-професійної програми «Системний аналіз»

Стадник Мар'яни Василівни

(прізвище, ім'я, по батькові)

на тему «Розробка алгоритму ранжування та класифікації кіберінцидентів
шахрайства з використанням нечіткої логіки»

1. Актуальність теми: актуальність теми зумовлена зростанням кількості кіберінцидентів шахрайства та складністю їх своєчасного виявлення. Нечітка логіка дозволяє враховувати невизначеність даних під час ранжування та класифікації кіберінцидентів. Розробка відповідного алгоритму ранжування сприятиме підвищенню ефективності виявлення загроз і підтримки прийняття рішень.
2. Позитивні риси кваліфікаційної роботи: у роботі запропоновано алгоритм для ранжування та класифікації кіберінцидентів за рівнем ризику їх виникнення та за урахуванням природи оцінювання релевантних значень різноманітних факторів, що описують умови виникнення кіберінцидентів та визначено шляхи нормування зазначених факторів з метою їх подальшого оброблення та застосування.
3. Наявність самостійних розробок автора: автором запропоновано класифікацію інцидентів кібершахрайства, сформовано систему характеристик, що описують дані кіберінцидентів, сформовано систему правил «якщо-що» для подальшого оброблення кіберінцидентів, досліджено альтернативні шляхи отримання потрібних рішень через застосування методів експертного оцінювання та в умовах недостатньої повноти даних.
4. Цінність теоретичних висновків та практичних рекомендацій: сформовані у роботі пропозиції дозволяють визначити послідовність дій, що направлені на організацію ефективних процесів моніторингу та аналізу кіберзагроз, а також для формування додаткових напрямів подальшого аналізу можливостей виникнення кіберінцидентів у майбутньому.
5. Наявність недоліків: подана до захисту робота містила ряд недоліків редакційного характеру, які були усунуті в повному обсязі та суттєво не впливали на якість виконаної роботи.
6. Загальна оцінка кваліфікаційної бакалаврської роботи та її допущення до захисту перед ЕК: Теоретичні та практичні матеріали, що викладені у роботі, відповідають вимогам до робіт такого рівня, робота заслуговує на високу оцінку а її автор заслуговує на присвоєння освітньо-кваліфікаційного рівня бакалавр з освітньо-професійної програми «Системний аналіз». Робота може бути допущеною до захисту перед екзаменаційною комісією.

Науковий керівник

к.е.н., доцент

(посада, науковий ступінь, учене звання)

Потапенко С. Д.

(прізвище, ініціали)

(підпис)

“ ” _____ 20__ р.

Рецензія
на кваліфікаційну бакалаврську роботу
здобувача вищої освіти

Стадник Мар'яни Василівни

(прізвище, ім'я, по батькові)

Тема «Розробка алгоритму ранжування та класифікації кіберінцидентів
шахрайства з використанням нечіткої логіки»

Актуальність теми кваліфікаційної роботи і доцільність її розроблення. Тема роботи є актуальною в умовах збільшення кількості кіберінцидентів, в тому числі і шахрайства, які постійно змінюються та використовують нові схеми. Через це виникає необхідність у розробці методів автоматизації аналізу інцидентів та оцінки їх критичності. Використання методів нечіткої логіки дозволяє враховувати невизначеність, що є головною проблемою в кіберпросторі.

Якість проведеного дослідження. У роботі проведено аналіз предметної області та існуючих підходів до оцінювання ризиків, розглянуто методи нечіткої логіки та описано математичні методи необхідні для обробки даних. Автором запропоновано алгоритм, що дозволяє ранжувати та класифікувати інцидентів на основі сукупності характеристик.

Позитивні риси кваліфікаційної бакалаврської роботи. До переваг роботи слід віднести логічну структуру дослідження, орієнтація на практичний результат алгоритму та його адаптивність до змін характеристик кіберінцидентів. А також аналіз різних контекстів визначення інцидентів, як зарубіжного Europol, так і українського CERT-UA.

Зауваження. Доцільним було б розглянути питання перевірки точності та стійкості отриманих результатів при зміні експертних оцінок. Також підрозділ про класифікацію міг бути доповненим аналізом альтернативних методів класифікації та порівняння із запропонованим підходом. Проте названі недоліки на зміст роботи суттєво не впливають.

Практична значимість висновків і рекомендацій. Результати дослідження можуть бути використані для попереднього оцінювання ризиків кіберінцидентів, визначення пріоритетів реагування на загрози та підтримки процесів прийняття

рішень з кібербезпеки в підрозділах кіберполіції та організаціях. Запропонований алгоритм може бути інтегрований до вже існуючих систем управління інформаційною безпекою організацій або врахований при розробці нових програмних засобів моніторингу кіберзагроз.

Місце роботи та посада рецензента Департамент кіберполіції Національної поліції України, начальник управління полковник поліції

Куліш В. М.

(підпис, ПІБ)

Підпис затверджую: начальник управління полковник поліції

(посада, підпис)

Місце печатки організації, де працює рецензент

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ОСОБЛИВОСТІ ВИЗНАЧЕННЯ КІБЕРІНЦИДЕНТІВ ТА МЕТОДИ ЇХ ВИЯВЛЕННЯ В ЗАДАЧАХ КІБЕРБЕЗПКИ.....	5
1.1. Визначення кіберінцидентів шахрайства	5
1.2. Проблема невизначеності та її подолання.....	8
1.3. Огляд досліджень	10
РОЗДІЛ 2. МЕТОДИ ПОДОЛАННЯ НЕВИЗНАЧЕНОСТІ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ	12
2.1. Нечітка логіка	12
2.2. Математичні методи оцінювання та оброблення даних	18
2.3. Класифікація кіберінцидентів за рівнем небезпеки	25
РОЗДІЛ 3. РОЗРОБЛЕННЯ ТА ЗАСТОСУВАННЯ АЛГОРИТМУ РАНЖУВАННЯ ТА КЛАСИФІКАЦІЇ КІБЕРІНЦИДЕНТІВ	28
3.1. Розробка та опис структури алгоритму	28
3.2. Опис задачі та застосування алгоритму.....	31
3.3. Результати, переваги та недоліки використання алгоритму.....	41
ВИСНОВКИ.....	43
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	44
ДОДАТКИ.....	47

ВСТУП

Актуальність теми. Традиційні підходи до аналізу кіберінцидентів часто ґрунтуються на чітко визначених правилах і не враховують невизначеність, неповноту та нечіткість вхідних даних. Водночас характеристики кіберінцидентів, такі як складність реагування, рівень ризику або успішність усунення, часто мають лінгвістичний або експертний характер. У зв'язку з цим є доцільним застосування методів нечіткої логіки та системного аналізу, які дозволяють формалізувати невизначеність

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій показує проблему невизначеності в кіберінцидентах та доцільність використання методів експертних оцінок та нечіткої логіки для подолання проблеми.

Мета дослідження – огляд методів для створення алгоритму ранжування та класифікації кіберінцидентів шахрайства.

Завдання дослідження:

- Розглянути проблему невизначеності щодо ранжування кіберінцидентів;
- Розглянути теорію нечіткої логіки та методів експертних оцінок;
- Розробити власний алгоритм ранжування та класифікації кіберінцидентів.

Об'єкт дослідження – кіберінциденти шахрайства.

Предмет дослідження – методи експертних оцінок та нечіткої логіки для ранжування та класифікації кіберінцидентів шахрайства.

Методи дослідження – метод Дельфі, мінмакс нормування, функції належності, узагальнений критерій, правила ЯКЦО-ТО.

Теоретична, методична та практична значущість отриманих результатів. Результати дослідження можуть бути використані для аналізу кіберінцидентів шахрайства та їх ранжування за рівнем ризику.

Інформаційна база дослідження – наукові публікації в спеціалізованих журналах, початкові посібники, звіти.

РОЗДІЛ 1. ОСОБЛИВОСТІ ВИЗНАЧЕННЯ КІБЕРІНЦИДЕНТІВ ТА МЕТОДИ ЇХ ВИЯВЛЕННЯ В ЗАДАЧАХ КІБЕРБЕЗПКИ

1.1. Визначення кіберінцидентів шахрайства

Спочатку визначимо необхідні терміни – кіберінцидент та шахрайство.

Відповідно до статті 1 Закону України «Про основні засади забезпечення кібербезпеки України»:

- кіберінцидент – надзвичайна подія, пов’язана з реалізацією або можливістю реалізації кібератаки;

- кібератака – несанкціоновані дії, що здійснюються за допомогою інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційній (автоматизованій), телекомунікаційній, інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи.

ENISA – Агентство Європейського Союзу з питань кібербезпеки – має два визначення щодо кіберінциденту:

«Cyber incident – будь-яка подія, що впливає на будь-який з компонентів кіберпростору або на його функціонування, незалежно від того, чи є вона природною чи створеною людиною; зловмисною чи незловмисною; навмисною, випадковою або через некомпетентність; через розробку або через операційну взаємодію, називається кіберінцидентом. Також ми називаємо кіберінцидентом будь-який інцидент, спричинений будь-яким з компонентів кіберпростору, навіть якщо пошкодження/порушення, дисфункція спричинені поза кіберпростором.»

«Cyber accident. – визначають як будь-яку подію, пов’язану з кіберпростором, яка завдає значної шкоди кіберпростору або будь-якому іншому активу (має вплив на продуктивність, потребує ремонту, заміни) або спричиняє травми.»

Отже, кіберінцидент — це подія, яка порушує функціонування компонентам кіберпростору або загрожує конфіденційності, цілісності чи доступності інформаційних систем. Інцидент може впливати як на сам кіберпростір, так і за його межами.

Тепер розглянемо, що саме є шахрайством та які кіберінциденти класифікують як такі.

Europol — Агентство Європейського Союзу із співпраці у сфері правоохоронної діяльності — визначає шахрайство як «злочин, що здійснюється виключно або переважно в Інтернеті. Шахрайська схема здійснюється з метою виманити у жертв їхні активи, використовуючи неправдиві та обманливі приводи або за допомогою методів кібератак.»

До шахрайства відносять:

- 1) Фішинг — небажані повідомлення, що надходять з авторитетно джерела та як правило містять запити на платежі чи шкідливі посилання;
- 2) Смішинг — форма фішингу, що використовує текстові повідомлення в месенджерах;
- 3) Вішинг — форма фішингу, що використовує телефонні дзвінки або голосові повідомлення;
- 4) Соціальна інженерія — використання обману для маніпуляції людьми заради розголошення конфіденційної або особистої інформації;
- 5) Компрометація ділової електронної пошти (англ. BEC) — інцидент, де злочинці себе за довірених керівників, постачальників або партнерів, щоб обманом змусити співробітників виконати шахрайські банківські перекази або розкрити корпоративні дані;
- 6) Шахрайський сайт - будь-який шкідливий домен, який використовуються кіберзлочинцями для обману людей, крадіжки коштів або збору персональних даних.

ENISA використовує міжнародну класифікацію кіберінцидентів, яка зазначена в проєкті MISP (Malware Information Sharing Platform) – це безкоштовна платформа з відкритим вихідним кодом для збору, зберігання, аналізу та безпечного обміну інформацією про кіберзагрози. Основна ідея MISP полягає в тому, щоб створити середовище довіри, де організації можуть безпечно обмінюватися інформацією про загрози.

За цим проєктом ENISA поділяє кіберінциденти категорії Шахрайство (англ. Fraud) на 4 групи:

- 1) Несанкціоноване використання ресурсів (Unauthorized use of resources) – сюди також входять будь-які дії пов'язані з отриманням прибутку. Як приклад зазначають «використання електронної пошти для участі в незаконних ланцюгових листах з метою отримання прибутку або пірамідах»
- 2) Порухення авторських прав (Copyright) – наприклад, встановлення копій неліцензійного комерційного програмного забезпечення.
- 3) Маскарадинг (Masquerade) – використання копії ідентифікаторів суб'єкта або системи, в тому числі крадіжка особистості, для отримання вигоди.
- 4) Фішинг (Phishing) – маскуванню під іншу особу з метою переконання користувача виконати певну дію.

На основі цієї класифікації була розроблена українська версія. Державна команда реагування на комп'ютерні надзвичайні події України (CERT-UA), що діє при Держспецзв'язку, використовує MISP для обміну інформацією про кіберзагрози з міжнародними партнерами. Тут шахрайство не виділяють на окремі категорії, але визначено окремий тип шахрайства – шахрайський сайт (Fraudulent site) – це створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Натомість фішинг визначають як використання соціальної інженерії для збору інформації про користувача та класифікують під категорію Збір інформації зловмисником (Information Gathering).

Як бачимо, загального розбиття категорії шахрайство на різні типи не існує, оскільки кіберпростір постійно змінюється швидкими темпами та шахраї часто демонструють складні способи дії, які зазвичай є поєднанням різних видів шахрайства.

1.2. Проблема невизначеності та її подолання

Однією з ключових проблем аналізу кіберінцидентів є наявність невизначеності та нечіткості вхідних даних. Інформація про інциденти часто є неповною або представлена у вигляді лінгвістичних оцінок, що ускладнює застосування класичних математичних методів.

Основні джерела невизначеності:

- неповнота даних про інцидент;
- суперечливість інформації з різних джерел;
- відсутність статистики для оцінки ймовірностей;
- використання експертних суджень;
- постійна зміна тактик зловмисників;
- складність визначення меж між типами інцидентів.

За таких умов застосування лише класичних математичних моделей є недостатнім, оскільки вони потребують точних значень параметрів.

Одні із способів подолання невизначеності це використання методи системного аналізу та нечітку логіку.

Системний аналіз розглядає досліджуваний об'єкт як цілісну систему, елементи якої перебувають у взаємозв'язку. Суть системного аналізу полягає у створенні спрощеної моделі реального об'єкту або лише його окремої частини. Це

є необхідністю, оскільки інформації кількість інформації все дедалі збільшується та самі об'єкти стають складнішими, тому повний їх аналіз вимагає великої кількості ресурсів. Об'єкти як системи досліджують за допомогою особливих властивостей – системних параметрів, таких як: простота, складність, надійність. Основні принципи щодо інформації: неповнота, невизначеність, неоднозначність.

Кіберінцидент можна представити як систему, що містить:

- джерела атаки;
- ознаки компрометації;
- критичність активу;
- рівень достовірності інформації;
- можливі наслідки.

В даній роботі акцент зроблено на критичності активу.

Нечітка логіка, запропонована Л. Заде у 1965 році, дозволяє працювати з нечіткими множинами та лінгвістичними змінними, що забезпечує можливість формалізації експертних знань. Нечіткі алгоритми описують наближені міркування, тому є корисними для нечіткого прийняття рішень, де задачі є занадто складними для опису класичними бінарними моделями.

Крім того, як зазначає джерело [16], «використання нечіткої логіки в поєднанні із штучними нейронними мережами, еволюційними алгоритмами та іншими методами штучного інтелекту дозволяє покращити результати вибору рішень за рахунок настроювання параметрів моделі прийняття рішення.»

1.3. Огляд досліджень

Автори [9] прямо зазначають, що традиційні методи оцінювання кіберризиків вимагають точних ймовірностей та повних даних, що практично неможливо в реальних умовах. Запропонований ними підхід використовує нечітку логіку для врахування неоднозначності вхідних даних та експертних оцінок.

«Перетворюючи невизначені та неточні параметри (такі як впевненість у виявленні, серйозність вразливості та складність зловмисника) на нечіткі лінгвістичні змінні та застосовуючи комплексний механізм логічного висновку на основі правил (IF-THEN), ми продемонстрували, що модель ефективно відображає зміну ризику, плавно адаптуючись у міру розвитку атак від початкового проникнення до більш серйозних стадій... Вона краще обробляє невизначеність та неповні дані, ніж детерміновані методи, забезпечуючи надійні оцінки ризиків навіть за обмеженої інформації.»

Автор [10] досліджує проблему оцінювання ризиків за відсутності достатньої статистичної інформації. Показано, що нечітка логіка є ефективним інструментом для роботи з неточними та неповними даними, а також для інтеграції експертних суджень у процес оцінювання ризиків.

«Для ризиків, які не мають відповідної моделі ймовірності, система нечіткої логіки може допомогти змодельовати причинно-наслідкові зв'язки, оцінити рівень ризику, послідовно ранжувати ключові ризики, а також врахувати наявні дані та думки експертів.»

Робота [11] показує систематичний огляд понад 400 робіт із кібербезпеки. Автори підкреслюють, що сучасні кіберзагрози мають багаторівневий, багатокроковий та динамічний характер, а існуючі моделі часто не враховують невизначеність та складність реальних атак. Невизначеності тут пов'язана з неповнотою інформації про атаки, складністю сценаріїв їх реалізації та відсутністю якісних даних, оскільки використовуються застарілі дані бо неповні.

Автори дослідження [12] використовують лінгвістичні зміни та експертні оцінки для оцінювання ризиків інформаційної безпеки. Автори також обґрунтовують використання нечітких множин саме для формалізації таких експертних оцінок та переходу від якісних суджень до кількісних оцінок ризику за 3 критеріями.

Автори дослідження [13] вказують, що класичні бінарні моделі прийняття рішень погано працюють у випадках, коли ознаки фішингових ресурсів є неповними або суперечливими. Для подолання цієї проблеми застосовується нечіткий логічний висновок.

Дослідження [14] присвячене онлайн-шахрайству в електронних аукціонах. Автори прямо зазначають, що розвиток електронної комерції створює умови невизначеності та появи шахрайських схем, які складно описати за допомогою жорстких правил класифікації. Проблема невизначеності полягає у декількох аспектах:

- шахраї створюють нові схеми, тому потрібна система, яка може еволюціонувати;
- для більшості характеристик відсутнє чітке розділення між шахрайською поведінкою та звичайними користувачами;
- людська інтерпретація результатів щодо репутації джерела про інцидент чи важливість активу, які важко описати чітко.

Для вирішення проблеми використовується нечітка нейромережева модель з базою правил ЯКЩО-ТО. Дана системи дозволяє перетворювати числові дані у лінгвістичні правила, зрозумілі експертам.

РОЗДІЛ 2. МЕТОДИ ПОДОЛАННЯ НЕВИЗНАЧЕНОСТІ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ

2.1. Нечітка логіка

2.1.1. Визначення нечітких множин

Чітка множина – це маржина, де значення деякого елемента може бути лише 0 – не належати даній множині, чи 1 – належати множині. Нечіткі множини ж розширюють можливі значення до відрізка $[0;1]$, замість бінарного значення $\{0; 1\}$.

Тобто, нечітка множина описує ступінь приналежності певного елемента до цієї множини. Це означає, що перехід від повної приналежності до повної неприналежності відбувається плавно на інтервалі $[0;1]$.

Математично нечітку множину можна записати наступним чином: нечіткою множиною A називають множину, що складається з сукупності впорядкованих пар:

$$A = \{(x; \mu_A(x)) | x \in X\},$$

де x – це елемент деякої множини X , $\mu_A(x)$ – функція належності нечіткої множини, яка приписує кожному елементу x його значення в множині.

Наприклад: візьмемо множину A – “людина, зі зростом більше за 180см – висока”. Позначимо x_1 – людину зростом 150 см, x_2 – 160см, x_3 – 170см, x_4 – 180см, x_5 – 190см.

Чіткий вигляд множини A «високих людей» мав би наступний вигляд:

$$A = \{(x_1; 0), (x_2; 0), (x_3; 0), (x_4; 1), (x_5; 1)\}.$$

Але нечітка множина B «високих людей» дозволяє записати елементи наступним чином:

$$B = \{(x_1; 0,5), (x_2; 0,7), (x_3; 0,9), (x_4; 1), (x_5; 1)\}.$$

Отримали, що кожній елемент множини X мають певний ступінь належності до множини B «людина з високим зростом».

2.1.2. Фазифікація та дефазифікація

Фазифікація – це процес перетворення чітких даних у нечіткі значення. На цьому етапі для кожного значення вхідної змінної визначається ступінь його належності до відповідних нечітких множин за допомогою функцій належності. Результатом фазифікації є набір значень функцій належності, які використовуються під час подальшого нечіткого логічного виведення.

Для опису нечітких множин також важливим терміном є лінгвістична змінна. Лінгвістична змінна – змінна, що за частую описується природною мовою: словами або словосполученнями. Данна змінна задається нечіткою множиною та відповідною функцією належності. Використання лінгвістичних змінних дозволяє описати якісні характеристики об'єктів і процесів. Наприклад, лінгвістична змінна «температура» може набувати значень «низька», «середня» або «висока».

Дефазифікація – перетворення нечітких вихідних даних у чітке числове значення. Метою дефазифікації є отримання результату у формі, придатній для подальших обчислень чи операцій.

2.1.3. Функції належності

Функція належності — це математична функція, що визначає ступінь належності елемента до нечіткої множини, приймаючи значення в інтервалі $[0;1]$.

Вона є основним елементом для графічного опису нечіткої множини на координатній площині. На практиці для побудови графіків найчастіше використовують функції, які можна задати аналітично, оскільки вони є зручними для обчислень і візуалізації.

Розглянемо деякі види функцій належності та зобразу їх графічно:

$$f(x; a, b) = \begin{cases} 1, & 0 \leq x < a \\ \frac{b-x}{b-a}, & a \leq x < b \\ 0, & b \leq x \end{cases} \quad (1)$$

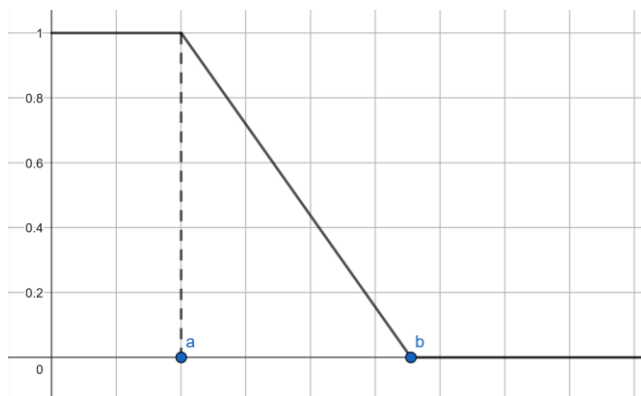


Рис.1. Функція належності (1)

де a, b – деякі дійсні числа, при чому $a \leq b$.

$$f(x; a, b) = \begin{cases} 0, & x < a \\ \frac{b-x}{b-a}, & a \leq x < b \\ 1, & b \leq x \end{cases} \quad (2)$$

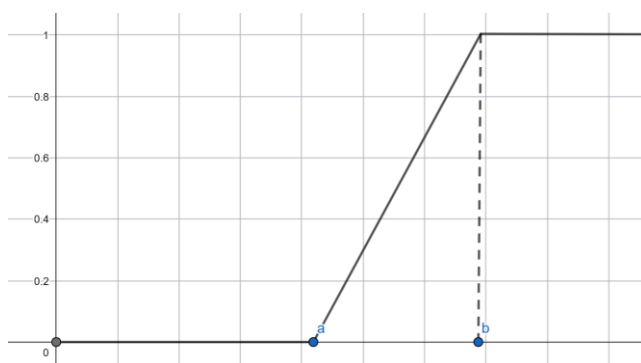


Рис.2. Функція належності (2)

де a, b – деякі дійсні числа, при чому $a \leq b$.

Трикутна функція належності записується наступною формулою:

$$f\Delta(x; a, b, c) = \begin{cases} 0, & x < a \\ \frac{x-a}{b-a}, & a \leq x < b \\ \frac{b-x}{c-b}, & b \leq x < c \\ 0, & c \leq x \end{cases} \quad (3)$$

де a, b, c – деякі дійсні числа, які стоять в такій послідовності: $a \leq b \leq c$.

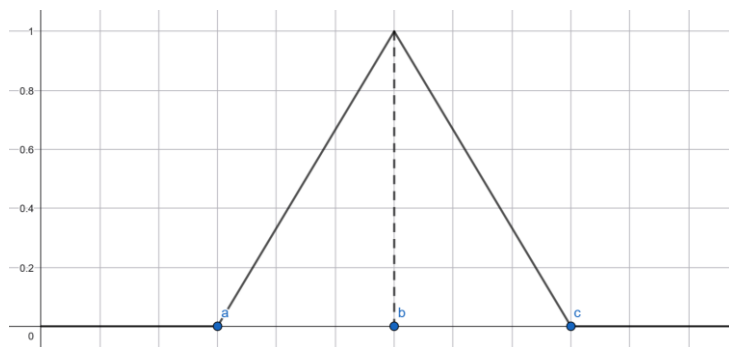


Рис.3. Функція належності (3)

Для зручності визначення рівня ризику – можна зобразити графіки функцій на одній координатній площині. Для прикладу використаю функції (1)-(3). Тоді функцію (1) можна записати як $f(x; a1, b1)$, функцію (3) - $f\Delta(x; a2, b2, c2)$, та функцію (2) - $f(x; a3, b3)$, де

$$0 < a1 < b1$$

$$0 < a2 < b2 < c2$$

$$0 < a3 < b3$$

$$0 < a1 < a2 < b1 < b2 < a3 < c2 < b3$$

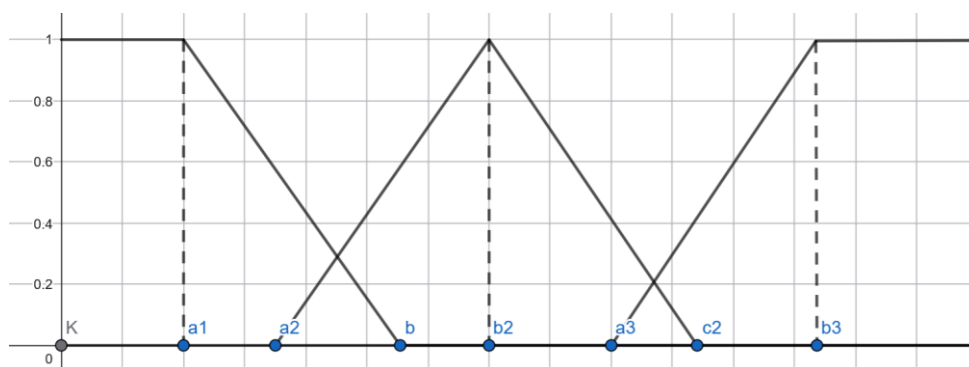


Рис.4. Об'єднаний графік функцій належності (1)-(3)

Тепер маємо спільний графік, який показує ступені належності певного об'єкту за трьома нечіткими визначеннями.

Розглянемо приклад використання даного графіку. Візьмемо довільні значення елементів множини $X=\{x_1, x_2, x_3\}$:

$$a_2 < x_1 < b_1$$

$$b_2 < x_2 < a_3$$

$$a_3 < x_3 < c_2$$

Позначу їх на графіку.

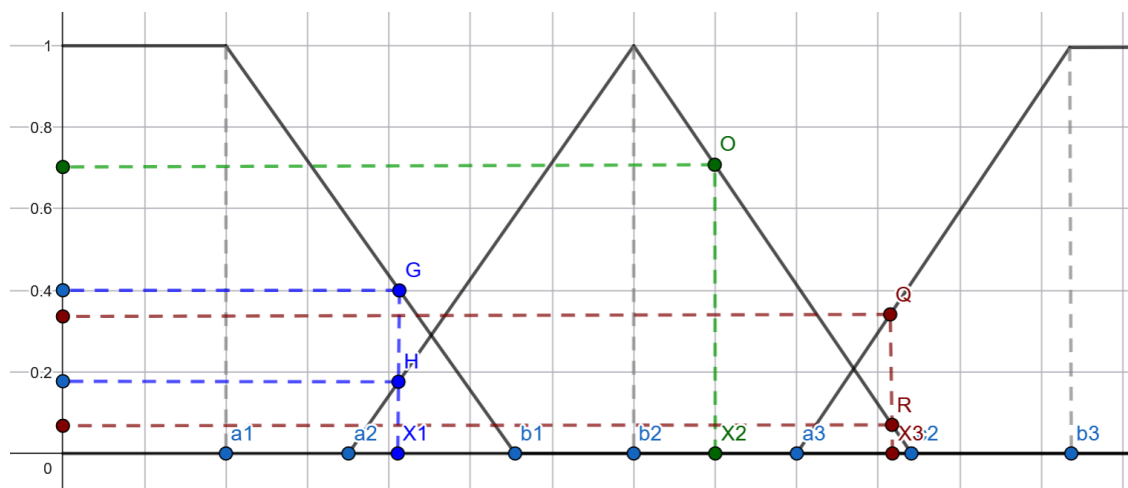


Рис.5. Приклад застосування об'єднаного графіка функцій належності (1)-(3)

Маємо, що

- X_1 – перетинає лінії f_1 в точці $G(x_1; 0.4)$, f_2 в точці $H(x_1; 0.18)$, та не перетинає f_3
- X_2 – перетинає лише f_2 в т. $O(x_2; 0.7)$
- X_3 – перетинає f_2 в т. $R(x_3; 0.06)$ та f_3 в т. $Q(x_3; 0.35)$

Тоді можна записати значення належності для елементів множини X як:

$$B = \{(x; (\mu_1(x), \mu_2(x), \mu_3(x))) | x \in X\}$$

Маємо:

$$B = \{(x_1; (0.4; 0.18; 0)), \\ (x_2; (0; 0.7; 0)), \\ (x_3; (0; 0.06; 0.35))\}$$

2.1.4. Правила «Якщо-то»

Основу нечітких експертних систем становить база знань, яка містить набір продукційних правил типу IF–THEN («ЯКЩО–ТО»). Такі правила описують причинно-наслідкові зв'язки між вхідними та вихідними змінними та дозволяють формалізувати експертні знання. Загальний вигляд правила має форму:

$$\text{IF } x \in A \text{ THEN } y \in B,$$

де x – вхідна лінгвістична змінна, A – нечітка множина, що описує її значення, y – вихідна змінна, а B – множина, яка визначає результат. Множина B може бути як нечіткою, так і чіткою, залежно від проблеми.

Перша частина «ЯКЩО» називається антецедентом, решта частини «ТО» називається наслідком. У антецеденті частина IF спрямована на визначення належності вхідної змінної x , що відповідає нечіткій множині A . У наслідку частини THEN знаходиться значення вихідної змінної y .

Наприклад, для системи керування температурою можна сформулювати правило:

$$\text{IF температура є високою THEN швидкість вентилятора є великою.}$$

У цьому випадку поняття «висока температура» та «велика швидкість» задаються нечіткими множинами з відповідними функціями належності.

Для опису складніших залежностей використовуються правила з кількома умовами, поєднаних логічними операторами AND (ТА) або OR (АБО):

IF температура є високою AND вологість є великою THEN швидкість вентилятора є дуже великою.

Тут логічний оператор AND реалізується через операцію перетину нечітких множин, найчастіше за допомогою мінімуму або добутку значень функцій належності.

У ході нечіткого логічного виведення визначається ступінь активації кожного правила бази знань, після чого результати їх застосування агрегуються для отримання остаточного рішення системи.

2.2. Математичні методи оцінювання та оброблення даних

2.2.1. Методи експертних оцінок

Методи системного аналізу використовують для подолання невизначеності, яка може бути обумовлена неповнотою даних чи нестачею інформації для знаходження результату.

Одна група методів – це експертні методи. Експертний аналіз ґрунтується на використанні знань і досвіду фахівців для оцінювання складних ситуацій та прогнозування розвитку стану системи чи певного об'єкту. Він застосовується у випадках, коли недостатньо достовірних статистичних даних або проблема не піддається повній математичній формалізації. Результатом роботи експертів є експертна оцінка – судження щодо поставленої задачі, яке після узагальнення використовується для формування висновків і рекомендацій.

Залежно від форми роботи та кількості залучених експертів поділяють дві експертні оцінки – індивідуальні та колективні. Індивідуальні методи базуються на думці одного експерта і дозволяють максимально використати його професійні знання, однак обмежуються суб'єктивністю та вузькістю досвіду одного спеціаліста.

Колективні методи спираються на думки групи експертів і забезпечують більш об'єктивні результати. Ці методи поділяють на дві групи:

- методи групової експертизи – коли експертів збирають разом, спільно обговорюють питання та приходять до консенсусу, наприклад: експертні комісії, «мозковий штурм»;
- методи опитування – коли експерти надають оцінки окремо один від одного, наприклад: метод Дельфі, метод попарних порівнянь.

Процес експертного оцінювання включає:

- формулювання мети та завдань дослідження,
- підбір експертів,
- вибір способу збору інформації,
- опрацювання отриманих даних та
- інтерпретацію результатів.

Одним із головних недоліків експертних оцінок підлягає питання про саму проблему, яку хочемо вирішити. Джерело [18] зазначає, що головне припущення щодо експертних оцінок є те, що «значення досліджуваної характеристики знаходиться усередині діапазону оцінок, одержуваних від групи експертів, і що узагальнена колективна думка є достовірним. Однак це припущення не завжди є правильним.» Тому автор пропонує розділити питання, до яких застосовується методи експертних оцінок на два класи:

- 1) більш загальні проблеми, які містять достатньо інформації, де вважають одного експерта «зберігачем великого обсягу інформації, а групову думку експертів – близькою до істини»;
- 2) вузькоспеціалізовані проблеми певної області, де думка одного експерта, який глибоко досліджує наявну проблему, може бути більш значимою за групову оцінку та може бути загубленою при опрацюванні результатів.

Тепер розглянемо метод анкетування.

Анкетування передбачає письмове опитування експертів за допомогою анкет, що можуть містити відкриті, закриті або альтернативні питання.

Відкриті питання – питання на які експерти дають довільну відповідь. Дозволяє охопити всі можливі варіанти думок щодо події, проте ускладнює обробку результатів та знаходження узагальненої думки. Закриті питання – застосовують, коли порівнюють чітко визначені дві альтернативи та необхідно визначити до якої схиляються більшість експертів. Альтернативні питання – коли є чіткі дані щодо декількох альтернатив, які слід впорядкувати або оцінити за бальною шкалою.

За необхідності процедура анкетування проводиться у кілька турів для уточнення оцінки чи перевірки узгодженості думок експертів. Якщо анкетування з самого початку заплановано на декілька турів, то на першому турі використати питання відкритого типу щодо проблеми, після – закриті або питання з варіантами відповідей.

Разом з анкетою експертам надається пояснювальна записка, що містить мету та завдання експертизи, необхідну інформацію щодо проблеми та інструкції щодо заповнення анкети.

Кроки проведення анкетування:

- 1) Надати інформацію щодо проблеми у вигляді мети та завдання анкети
- 2) Заповнення експертами анкети
- 3) Статистична обробка результатів
- 4) Формування висновків щодо наданих думок
- 5) Пояснити експертам причини незгоди їх думок з колективними та за згодою перегляд власних суджень

- 6) Повторне проведення турів починаючи з кроку 2 з метою зменшення мінливості між оцінками експертів

Проведення турів продовжується допоки оцінки не надійдуть до певного рівня стабільності, що обчислюється за певним показником.

2.2.2. Метод Дельфі

Метод Дельфі – це різновид методу експертних оцінок, що базується на багатоетапному анонімному анкетуванні групи експертів. Його метою є досягнення узгодженої думки щодо досліджуваної проблеми шляхом послідовного уточнення оцінок та надання зворотного зв'язку.

На першому етапі експерти незалежно один від одного відповідають на запитання анкети. Отримані результати статистично обробляються: визначаються середнє значення або медіана, а також виявляються крайні оцінки. Після цього експертам повідомляються узагальнені результати без розкриття авторства відповідей. Якщо оцінка окремого експерта суттєво відрізняється від загальної тенденції, йому пропонується обґрунтувати свою позицію або переглянути оцінку.

У наступних турах експерти можуть змінювати свої відповіді з урахуванням отриманої інформації та аргументувати причини прийнятого рішення. Після кожного туру результати знову обробляються та надсилаються учасникам.

Процедура повторюється до досягнення прийнятного рівня узгодженості оцінок або стабільності суджень експертів. Остаточний результат зазвичай визначається на основі середнього значення або медіани отриманих оцінок.

Анонімність під час використання методу Дельфі дозволяє зменшити вплив, науковий чи авторитарний, на думку експертів.

Під час обробки результатів знаходять:

- рівень узгодженості думок, який надає підтвердження достовірності суджень експертів;
- визначають узагальнену оцінку певного об'єкту або сукупності об'єктів;
- та, за необхідності, визначення залежності між думками двох окремих експертів.

Для перевірки рівня узгодженості думок використовують декілька показників, які наведено на рисунку нижче:

Вид показника	Формула	Позначення
Статистичні	$\overline{\varphi(i)} = \frac{\sum_{j=1}^m \varphi(i)_j}{m}$	$\overline{\varphi(i)}$ - середнє арифметичне значення вагомості i -го показника; $\varphi(i)_j$ - вагомість, зазначена j -м експертом по i -му показнику; m - число експертів
	$\overline{\sigma} = \sqrt{\frac{\sum_{j=1}^m [\varphi(i)_j - \overline{\varphi(i)}]^2}{m}}$	$\overline{\sigma}$ - середньо-квадратове відхилення для i -го показника;
	$V = \frac{\overline{\sigma}}{\overline{\varphi(i)}} \cdot 100$	V - коефіцієнт варіації (коефіцієнт мінливості думок експертів) по i -му показнику
Евристичні	$s = \sum_{l=1}^m \rho_l$	ρ_l - ранг оцінки вагомості i -го показника (ціле або дробове число);
	$\overline{s} = \frac{s}{n}$	$\overline{s}$ - середнє арифметичне значення суми рангів по всім n показникам
	$d_i = s - \overline{s}$	d_i - відхилення суми рангів від середнього арифметичного значення
	$T_i = \sum_{l=1}^L (t_l^3 - t_l)$	T_i - показник зв'язаності рангів; L - кількість груп зв'язаних рангів; t_l - кількість зв'язаних рангів в l -й групі;
	$W = \frac{12 \cdot \sum_{l=1}^n d_l^2}{m^2 \cdot (n^3 - n) - m \cdot \sum_{l=1}^n T_l}$	W - коефіцієнт конкордації. Основний показник, що характеризує погодженість думок експертів по усіх n показниках
	$\chi_R^2 = \frac{12 \cdot \sum_{l=1}^n d_l^2}{m \cdot n \cdot (n+1) - \frac{1}{n-1} \cdot \sum_{l=1}^n T_l}$	Фактичне значення критеріальної статистики χ_R^2 , яка розподілена по χ^2 при $\mathcal{Q} = n - 1$

Рис. 6. Статистичні та евристичні показники математичної статистики. Джерело: [20, с.158].

Середньо-квадратичне відхилення використовується, коли надається кількісна оцінка за допомогою певної шкали.

$$\sigma = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n}}$$

Де x_i – окреме значення в наборі даних, $\bar{x}$ – середнє значення всіх даних, n – обсяг сукупності. Чим менше значення середнього квадратичного відхилення, тим більш узгодженими вважаються думки експертів. Зазвичай, оцінки вважаються узгодженими при $\sigma < 0.1$, але припускається межа < 0.3 .

Коефіцієнти конкордації – Кендалла або Спірмена – використовуються, коли необхідно визначити зв'язок двома експертами. Коефіцієнти використовуються при питаннях впорядкування об'єктів.

2.2.3. Мінмакс нормалізація даних

Мін-макс нормування даних – дозволяє перетворити значення даних в діапазон $[0;1]$. Нормування застосовують, коли характеристики чи критерії певного об'єкта вимірюються в різних величинах (кг, км, години тощо) або мають сильні числові розбіжності (10 вимірюваних одиниць та 1000). Нормалізація дозволяє зберегти форму розподілу даних.

Формула нормування значень елемента наступна:

$$f_i^* = \frac{f_i - f_{\min}}{f_{\max} - f_{\min}}, \quad \text{якщо } f_i \text{ максимізуємо;} \quad (4)$$

$$f_i^* = \frac{f_{\max} - f_i}{f_{\max} - f_{\min}}, \quad \text{якщо } f_i \text{ мінімізуємо.} \quad (5)$$

Де: f_i – значення критерію певного елемента, f_{max} , f_{min} – мінімальне та максимальне значення критерію серед усіх елементів. Після отримуємо нормалізовані значення f_i^* в межах $[0;1]$.

Наприклад, маємо таблицю з певними об'єктами та критеріями, які обчислюються в різних одиницях виміру:

Таблиця 2.2.3.1. Приклад застосування нормування.

Об'єкт	Ресурси (кг)	Час виготовлення (год)	Витрати (тис. грн)	Якість (оцінка 1-10)
O1	20	4	100	6
O2	16	2	130	7
O3	17	6	120	8
O4	12	4	134	8
O5	23	2	129	9

Нехай, критерії 'Ресурси', 'Час виготовлення', 'Витрати' – до мінімуму, а 'Якість' – до максимуму.

Після використання мін-макс нормування отримаємо:

Таблиця 2.2.3.2. Приклад нормалізованих даних.

Об'єкт	Ресурси	Час виготовлення	Витрати	Якість
O1	0,273	0,500	1	0
O2	0,636	1	0,118	0,333
O3	0,545	0	0,412	0,667
O4	1	0,500	0	0,667
O5	0	1	0,147	1

2.2.4. Метод зваженої суми

Зважена сума – узагальнений критерій для певного об'єкту.

Формула узагальненого критерію обчислюється як сума добутків значення критерію та його відповідної ваги:

$$F(x) = \sum w_i f_i \quad (6)$$

Де f_i – значення критерію, w_i – вага критерію. При цьому сума ваг w_i повинна дорівнювати 1.

Наприклад, використаємо попередній приклад даних для об'єкту №1 з таблиці 2.2.3.2.

Нехай, відомо ваги для кожного критерію:

- Ресурси $w_1 = 0.2$
- Час виготовлення $w_2 = 0.1$
- Витрати $w_3 = 0.35$
- Якість $w_4 = 0.35$

Тоді перемножуємо ваги на нормалізовані значення критеріїв та сумуємо.

$$F(O1) = 0,273 * 0.2 + 0.5 * 0.1 + 1 * 0.35 + 0 * 0.35 = 0,4546$$

Отримаємо в результаті один критерій – узагальнена оцінка щодо об'єкту O1:

$$F(O1) = 0,4546.$$

2.3. Класифікація кіберінцидентів за рівнем небезпеки

Розглянемо декілька прикладів класифікації кіберінцидентів за рівнем небезпеки (або ще називають рівнем критичності).

США виділяють 5 рівнів: Надзвичайно-критичний, Критичний, Високий, Середній, Низький. Але більшість інцидентів підпадають під 4 рівні без надзвичайно-критичного.

	General Definition	Observed Actions	Intended Consequence ¹
Level 5 <i>Emergency</i> (Black)	<i>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.</i>	Effect	Cause physical consequence
Level 4 <i>Severe</i> (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</i>	Presence	Damage computer and networking hardware
Level 3 <i>High</i> (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Engagement	Corrupt or destroy data Deny availability to a key system or service
Level 2 <i>Medium</i> (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Preparation	Steal sensitive information Commit a financial crime
Level 1 <i>Low</i> (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>		Nuisance DoS or defacement
Level 0 <i>Baseline</i> (White)	Unsubstantiated or inconsequential event.		

Рис. 7. Класифікація кіберінцидентів США. Джерело: [23, с. 26]

Французька система виділяє 6 рівнів: Надзвичайно-критичний, Критичний, Важливий інцидент, Середній інцидент, Інцидент, Важлива подія.

GRAVITY SCALE	EQUIVALENCE WITH THE US CISS	IMPACTS	CHARACTERIZATION AS ARMED AGGRESSION WITHIN THE MEANING OF ARTICLE 51 OF THE UNITED NATIONS
LEVEL 5 - EXTREME EMERGENCY	Level 5 Emergency (Black)	Extreme Impact	Probably possible: to be considered on a case by case basis.
LEVEL 4 - MAJOR CRISIS	Level 4 Severe (Red)	Major Impact	
LEVEL 3 - CRISIS	Level 3 High (Orange)	Strong and Extensive Impact	Probably not possible: actions corresponding to these levels could nonetheless constitute other internationally wrongful acts (intervention, violation of sovereignty, use of force, etc.).
LEVEL 2 - SERIOUS INCIDENT	Level 2 Medium (Yellow)	Strong and circumscribed impact	
LEVEL 1B - INCIDENT	Level 1 Low (Green)	Medium and circumscribed impact	
LEVEL 1A - SIGNIFICANT EVENT		Low impact	
LEVEL 0 - EVENT	Level 0 Baseline (White)	Negligible Impact	

Рис. 8. Класифікація кіберінцидентів Франції. Джерело: [23, с.27]

CERT-UA в 2022 році виділяла 3 категорії критичності: Висока, Середня, Низька. З 2023 року – виділяє 4 категорії: Критичний, Високий, Середній, Низький.

Рівень критичності	H1 2025	H2 2025	Зміна за період
Критичний	1	0	-100%
Високий	6	5	-17%
Середній	2 944	2895	-2%
Низький	67	9	-87%
Загалом	3 018	2 909	-4%

Рис. 9. Порівняння кількості кіберінцидентів в 1-ому та 2-ому півріччі 2025 р. Джерело: [21, с.9]

РОЗДІЛ 3. РОЗРОБЛЕННЯ ТА ЗАСТОСУВАННЯ АЛГОРИТМУ РАНЖУВАННЯ ТА КЛАСИФІКАЦІЇ КІБЕРІНЦИДЕНТІВ

3.1. Розробка та опис структури алгоритму

Запропоную наступний алгоритм для ранжування та класифікації кіберінцидентів за рівнем ризику для задачі:

Нехай дано кіберінциденти $A_1, A_2, \dots, A_n$ та їх характеристики $A = \{a_{11}, a_{21}, \dots, a_{nm}\}$ за критеріями X_1, X_2, X_m . Для зручності запишу у табличній формі:

Таблиця 3.1.1. Початкові дані кіберінцидентів та їх характеристик.

Інцидент	X_1	X_2	...	X_k	...	X_m
A_1	a_{11}	a_{12}		L_1		a_{1m}
A_2	a_{21}	a_{22}		L_1		a_{2m}
...						
A_n	a_{n1}	a_{n1}		L_d		a_{nm}

Нехай критерій X_k – нечіткий критерій, який описується лінгвістичною змінною $L = \{L_1, L_2, \dots, L_d\}$.

Кроки алгоритму:

- 1) Перетворення значення нечіткого критерію X_k в чітке числове значення за допомогою бази правил ЯКЩО-ТО.

Правила можуть бути записані у вигляді:

ЯКЩО Рівень складності = ... , ТО X_k = ...

ЯКЩО Тип інциденту = ... ТА Рівень складності = ... , ТО X_k = ...

Або використовувати інші логічні оператори та умови.

- 2) Оскільки дані часто мають різні вимірювання, то необхідно нормалізувати дані - привести їх до діапазону $[0;1]$ за мін-макс нормуванням:

Нехай критерії $X_1 - X_{k-1}$ – хочемо мінімізувати, та $X_k - X_m$ – максимізувати.
Тоді використовуємо формули (4), (5)

Маємо результат:

Таблиця 3.1.2. Нормалізовані результати.

Інцидент	X_1	X_2	...	X_m
A1	a_{*11}	a_{*12}		a_{*1m}
A2	a_{*21}	a_{*22}		a_{*2m}
...				
A_n	a_{*n1}	a_{*n2}		a_{*nm}

2) Отримання ваг критеріїв. Використовуємо метод Делфі для опитування експертів.

Нехай була набрана група експертів $E = \{E_1, E_2, \dots, E_g\}$, яким була надата анкета для заповнювання.

Питанням анкети може бути: надайте оцінку критеріям за їх важливістю для визначення рівня ризику кіберінциденту . Шкала від 1 (не важливий) до 10 (дуже важливий).

Після заповнення отримаємо таблицю оцінок:

Таблиця 3.1.3. Запис оцінки експертів щодо важливості критеріїв.

Експерт	X_1	X_2	...	X_m
E1	e_{11}	e_{12}		e_{1m}
E2	e_{21}	e_{22}		e_{2m}
...				
E_g	e_{g1}	e_{g2}		e_{gm}

Наступним кроком слід перевірити узгодженість та за необхідності проведення декількох додаткових турів опитування.

Ваги для критеріїв отримуємо за як відношення середньої оцінки критерію до суми середніх оцінок всіх критеріїв:

$$W_i = \frac{Avg(X_i)}{\sum Avg(X_i)}$$

Таблиця 3.1.4. Обчислення ваг для кожного критерію.

	X1	X2	...	Xm	Sum
Avg e	Avg X1	Avg X2		Avg Xm	Sum (avg X)
W	W1	W2		Wm	

4) Використання узагальненого критерію за формулою (6).

Отримуємо тоді рівень ризику як суму добутків значень критеріїв та їх відповідні ваги.

Отримуємо числове значення рівня ризику для кожного інциденту.

Таблиця 3.1.5. Результат обчислення ризику.

Інцидент	Ризик
A1	R1
A2	R2
...	
Am	Rm

5) Ранжування – поставлення кіберінцидентів в порядку спадання залежно від ризику.

Таблиця 3.1.6. Ранжування кіберінцидентів.

№	Інцидент	Ризик
---	----------	-------

1	A*1	R*1
2	A*2	R*2
	...	
m	A*m	R*m

6) Класифікація кіберінцидентів за лангвістичними змінами, що словесно описують рівень ризику.

Для цього необхідно визначити необхідну кількість рівнів для класифікації, та потім визначити межі кожного рівня за допомогою функцій належності. Тоді для кожного кіберінциденту буде нечітка змінна рівня ризику:

$$A^* = \{ (\text{Рівень } 1; \mu_1), (\text{Рівень } 2; \mu_2), \dots, (\text{Рівень } n; \mu_n) \}$$

Після вибираємо максимум із значень належностей – це і буде рівень ризику записаний лінгвістично.

Отримаємо кінцевий результат у вигляді:

Таблиця 3.1.7. Остаточний вигляд результату.

№	Інцидент	Ризик	Рівень
1	A*1	R*1	Рівень *1
2	A*2	R*2	Рівень *2
	...		
m	A*m	R*m	Рівень *m

3.2. Опис задачі та застосування алгоритму

Нехай відомо наступні інциденти шахрайства:

- А – SMS-фішинг (смішинг) нібито від банку про запит на підтвердження даних. Повідомлення містить посилання на вебсторінку, що імітує офіційну

сторінку банку, де користувач повинен вести реквізити картки та код підтвердження;

- В – Фішинг через електронну пошту від державного органу, де просять терміново ознайомитися з документом або перейти за посиланням. Після відкриття вкладення чи перехід за посиланням встановлюється шкідливе програмне забезпечення;
- С – Шахрайство в соц-мережі про збір коштів для хворої дитини, використовуються фото- та відео-матеріали, після отримання коштів сторінка видаляються, банківські реквізити змінюються. Відомо посилання на сторінку в соц-мережі;
- D – Шахрайство через зламану сторінку знайомого, вимагання терміново позичити гроші;
- Е – Шахрайський інтернет-магазин, пропонуються товари за низькими цінами, часткова або повна передплата, але товар не надсилається, викрадаються платіжні дані покупців;

Та їх характеристики за критеріями:

- X1 – час виявлення, год
- X2 – час усунення, год
- X3 – успішність усунення, %
- X4 – складність реагування – нечітка змінна, лінгвістичні терміни
- X5 – витрати, людино-години

Дані про інциденти записано в таблиці:

Таблиця 3.2.1. Початкові дані.

№	Інцидент	X1	X2	X3	X4	X5
1	А	3,5	6,4	40,3	Середнє	14,0
2	В	4,0	12,1	75,5	Легко	12,6
3	С	2,3	17,4	23,4	Легко	16,0

4	D	8,0	16,0	45,0	Середнє	14,9
5	E	7,7	48,0	68,1	Складно	24,2

Необхідно – ранжувати інциденти за рівнем ризику від найбільшого ризику до найменшого та класифікувати залежно від рівня ризику.

За алгоритмом описаним в п.п. 3.1:

- 1) Спочатку за правилами «ЯКЩО-ТО» - перетворити критерії, які описані лінгвістичною зміною, на чіткі значення.

Визначимо лінгвістичні зміни:

$$L = \{\text{Легко, Середнє, Складно}\}$$

Нехай, нечіткі правила записані за схемою:

ЯКЩО Тип інциденту = ... ТА Рівень складності = ... , ТО $X_4 = \dots$

База правил може набувати вигляду:

- 1) ЯКЩО Тип інциденту = SMS-фішинг ТА Складність = Легко, ТО $X_4 = 0.2$
- 2) ЯКЩО Тип інциденту = SMS-фішинг ТА Складність = Середня, ТО $X_4 = 0.4$
- 3) ЯКЩО Тип інциденту = Фішинговий e-mail ТА Складність = Легко, ТО $X_4 = 0.3$
- 4) ЯКЩО Тип інциденту = Зламаний акаунт ТА Складність = Середня, ТО $X_4 = 0.5$
- 5) ЯКЩО Тип інциденту = Шахрайський збір коштів у соцмережі ТА Складність = Легко, ТО $X_4 = 0.35$
- 6) ЯКЩО Тип інциденту = Шахрайський збір коштів у соцмережі ТА Складність = Середня, ТО $X_4 = 0.6$

- 7) ЯКЩО Тип інциденту = Шахрайство через маркетплейс ТА Складність = Середня, ТО $X_4 = 0.45$
- 8) ЯКЩО Тип інциденту = Шахрайство через маркетплейс ТА Складність = Складно, ТО $X_4 = 0.65$

Тепер перетворюємо нечітку множину «Складність реагування» в чітку.

Таблиця 3.2.2. Дані без лінгвістичної змінної.

№	Інцидент	X1	X2	X3	X4	X5
6	A	3,5	6,4	40,3	0,4	14,0
7	B	4,0	12,1	75,5	0,3	12,6
8	C	2,3	17,4	23,4	0,35	16,0
9	D	8,0	16,0	45,0	0,5	14,9
10	E	7,7	48,0	68,1	0,65	24,2

2) Нормалізація даних – перетворюємо дані за мін-макс нормуванням

Нехай критерій X_3 – необхідно максимізувати, а всі інші – мінімізувати. Тоді за формулами (4), (5) отримаємо нормалізовані дані:

Таблиця 3.2.3. Нормалізовані дані.

№	Інцидент	X1	X2	X3	X4	X5
11	A	0,79	1,00	0,32	0,71	0,88
12	B	0,70	0,86	1,00	1,00	1,00
13	C	1,00	0,74	0,00	0,86	0,71
14	D	0,00	0,77	0,41	0,43	0,80
15	E	0,05	0,00	0,86	0,00	0,00

3) Отримання ваг критеріїв за допомогою методу Дельфі.

Нехай група експертів складається з 4 осіб, які дають свої оцінки незалежно один від одного в анкеті.

Анкета містить наступну інформацію:

- Питання анкети: надайте оцінку критеріям X1-X5 за їх важливістю для визначення рівня ризику кіберінцидентів шахрайства.

Далі надано самі критерії.

- Мета анкети: для визначення ваг для кожного критерію.
- Метод заповнення: за 10-ти бальною шкалою, де 1 – не важливий до 10 – дуже важливий.

Питання анкети є питанням 1-го класу, оскільки питання не є вузькоспеціалізованим, та альтернативного типу, оскільки містить бальну шкалу як варіант відповідей.

Після заповнення отримаємо наступну таблицю:

Таблиця 3.2.4. Оцінка експертів щодо важливості критеріїв.

№	X1	X2	X3	X4	X5
1	7	8	9	6	7
2	6	7	8	7	8
3	7	8	9	5	9
4	8	6	8	7	8

Перевірка узгодженості думок за допомогою середнього квадратичного відхилення. Отримаємо:

Таблиця 3.2.5. Оцінка експертів та перевірка узгодженості.

№	X1	X2	X3	X4	X5
1	7	8	9	6	7
2	6	7	8	7	8
3	7	8	9	5	9
4	8	6	8	7	8
Avrg	7	7,25	8,5	6,25	8
σ	0,707	0,829	0,5	0,829	0,707

Оцінки вважаються узгодженими при $\sigma < 0.1 - 0.3$. Оскільки оцінки не узгодженні, то використаємо середні оцінки як підказку для проведення наступних турів опитування до задовільного рівня середньоквадратичного відхилення σ (Додаток А).

Після виконання турів та перевірки узгодженості отримаємо остаточні оцінки:

Таблиця 3.2.6. Оцінки останнього туру.

№	X1	X2	X3	X4	X5
1	7	7	8,6	6	7,3
2	6,8	7	8,3	6,7	7,6
3	7	7,5	8,5	6,4	8
4	7,2	7,2	8,3	6,5	7,8

Далі необхідно визначити ваги кожного критерія. Знаходимо ваги як ділення середньої оцінки на суму середніх оцінок:

$$W_i = \frac{Avrg(X_i)}{\sum Avrg(X_i)}$$

Маємо:

Таблиця 3.2.6. Ваги кожної характеристики.

№	X1	X2	X3	X4	X5	
1	7	7	8,6	6	7,3	
2	6,8	7	8,3	6,7	7,6	
3	7	7,5	8,5	6,4	8	
4	7,2	7,2	8,3	6,5	7,8	SUM
Avrg	7	7,175	8,425	6,4	7,675	36,675
W	0,191	0,196	0,230	0,175	0,209	

4) Використовуємо узагальнений критерій за формулою (6).

Таблиця 3.2.7. Узагальнений критерій інцидентів.

Інцидент	F
A	0,73
B	0,92
C	0,63
D	0,49
E	0,21

Отримали значення узагальненого критерію.

5) Ранжування за рівнем ризику.

Маємо значення одного критерію F , проте, це не означає, що він показує рівень ризику. Якщо розглянути на нормалізовані дані, то можна побачити, що інцидент E має багато нулів, а інцидент B – одиниць. Це показує, що інцидент E має багато максимальних значень, тобто він один з важких інцидентів, а B – мінімальних, тобто він один із найлегших.

В такому випадку не є доцільним розглядати критерій F як рівень ризику, оскільки тоді він показує, що інцидент E має найменший ризик, а B – найбільший.

Пропоную тоді розглянути рівень ризику як одиниця відняти узагальнений критерій F:

$$R = 1 - F$$

Отримаємо рівень ризику:

Таблиця 3.2.8. Значення ризику інцидентів.

Інцидент	R
A	0,27
B	0,08
C	0,37
D	0,51
E	0,79

Тоді ранжування від найбільшого до найменшого ризику:

Таблиця 3.2.9. Ранжування інцидентів за рівнем ризику.

№	Інцидент	R
1	E	0,79
2	D	0,51
3	C	0,37
4	A	0,27
5	B	0,08

6) Класифікація за рівнем ризику.

Оскільки українська практика поділяє інциденти на 4 категорії залежно від ризику, то використаємо їх також. Нехай тоді функції належності для рівнів набувають вигляду:

Для «Низького рівня» визначу межі від 0 до 0.3.

$$f(x; a, b) = \begin{cases} 1, & 0 < x \leq 0.2 \\ \frac{0.3 - x}{0.1}, & 0.2 < x \leq 0.3 \\ 0, & 0.3 < x \end{cases}$$

Для «Середнього рівня» - від 0.2 до 0.6.

$$f\Delta(x; a, b, c) = \begin{cases} 0, & x \leq 0.2 \\ \frac{x - 0.2}{0.2}, & 0.2 \leq x \leq 0.4 \\ \frac{0.6 - x}{0.2}, & 0.4 \leq x \leq 0.6 \\ 0, & 0.6 \leq x \end{cases}$$

Для «Високого рівня» - від 0.5 до 0.9.

$$f\Delta(x; a, b, c) = \begin{cases} 0, & x \leq 0.5 \\ \frac{x - 0.5}{0.2}, & 0.5 \leq x \leq 0.7 \\ \frac{0.7 - x}{0.2}, & 0.7 \leq x \leq 0.9 \\ 0, & 0.9 \leq x \end{cases}$$

Для «Критичного рівня» - від 0.8 до 1.

$$f(x; a, b) = \begin{cases} 0, & x \leq 0.8 \\ \frac{0.9 - x}{0.1}, & 0.8 \leq x \leq 0.9 \\ 1, & 0.9 \leq x < 1 \end{cases}$$

Де значення рівня ризику описується в межах $x \in [0;1]$

Зображення всіх ризиків на одному графіку, де вісь ординат позначає рівень ризику, а абсцис – належність:

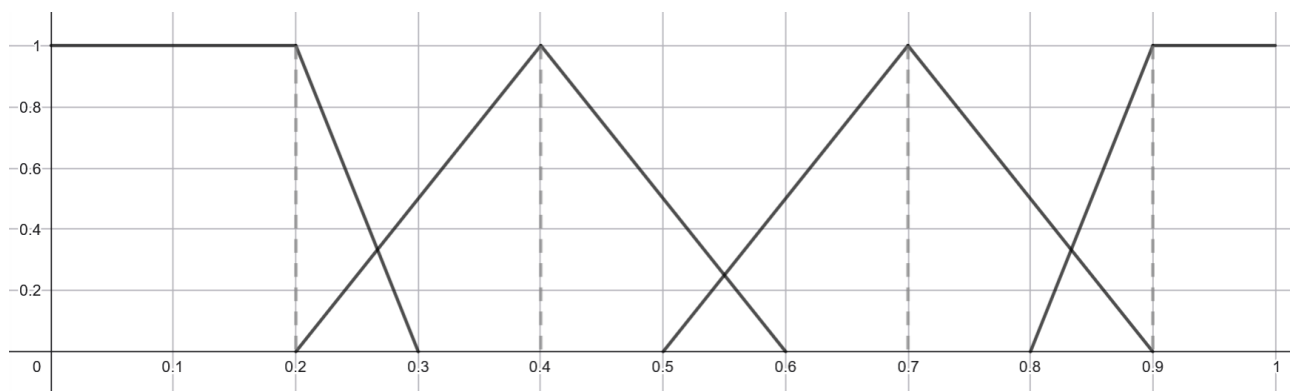


Рис. 10. Зображення всіх рівнів.

Тепер можна записати нечіткі значення рівня ризику для кожного інциденту як:

$$A_p = \{ (\text{Низький}; \mu 1), (\text{Середній}; \mu 2), (\text{Високий}; \mu 3), (\text{Критичний}; \mu 4) \}$$

Маємо для інциденту А:

$$A = \{ (\text{Низький}; 0,3), (\text{Середній}; 0,35), (\text{Високий}; 0), (\text{Критичний}; 0) \}$$

На графіку для інциденту А:

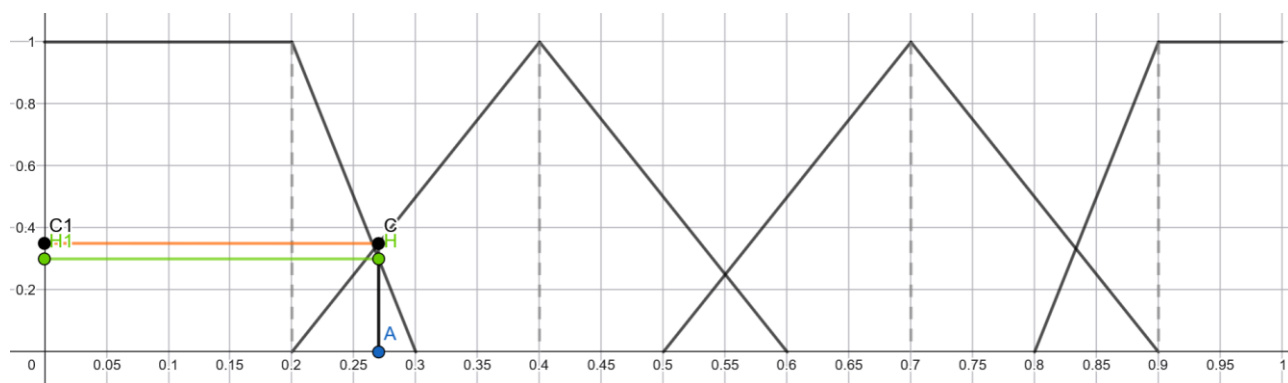


Рис. 11. Зображення рівня приналежності інциденту А.

Та вибравши найбільше значення функції належності отримаємо лінгвістичне позначення рівня ризику. Для інциденту А – найбільша належність відповідає середньому рівню. Роблю так для всіх інших інцидентів.

$$E = \{ (\text{Низький}; 0), (\text{Середній}; 0), (\text{Високий}; 0,55), (\text{Критичний}; 0) \}$$

$$D = \{ (\text{Низький}; 0), (\text{Середній}; 0,45), (\text{Високий}; 0,05), (\text{Критичний}; 0) \}$$

$$C = \{ (\text{Низький}; 0), (\text{Середній}; 0,85), (\text{Високий}; 0), (\text{Критичний}; 0) \}$$

$$B = \{(\text{Низький}; 1), (\text{Середній}; 0), (\text{Високий}; 0), (\text{Критичний}; 0)\}$$

Можемо записати результат у вигляді таблиці:

Таблиця 3.2.10. Остаточний результат алгоритму.

№	Інцидент	Ризик	Рівень
1	Е	0,79	Високий
2	Д	0,51	Середній
3	С	0,37	Середній
4	А	0,27	Середній
5	В	0,08	Низький

Отримали кінцевий результат.

3.3. Результати, переваги та недоліки використання алгоритму

Найбільший ризик має інцидент Е – шахрайський інтернет-магазин, після слідує Д – шахрайство через зламаної сторінку знайомого, далі інцидент С – шахрайство в соціальній мережі про збір коштів, А – SMS-фішинг від банку, В – Фішинг через електронну пошту, інцидент з найменшим ризиком.

Результати обчислень, а саме: значення ризику, приналежність кіберінциденту до певного рівня ризику – можуть бути використані як вхідні дані для наступних обчислень.

Розроблений алгоритм має як переваги, так і недоліки. До переваг можна віднести:

- перетворення лінгвістичних оцінок щодо характеристик в чіткі значення для обчислень;

- використовує експертні знання для визначення важливості кожної характеристики, таким чином долає певну невизначеність;
- отримання в результаті чітке значення ризику, ранжування інцидентів шахрайства та нечітке значення ризику представлене у зрозумілій людині формі.

Алгоритм є адаптивним, оскільки експертні оцінки та межі функцій належності легко переглянути та змінити в разі необхідності.

Недоліком даного алгоритму є залежність від експертних оцінок щодо важливості характеристик та меж функцій належності для рівня ризику, а також визначення умов та чітких значень щодо характеристик, які описані лінгвістичними змінами.

ВИСНОВКИ

Метою даної роботи була розробка алгоритму ранжування та класифікації кібернцидентів шахрайства в умовах невизначеності інформації. Аналіз наукових джерел показав, що традиційні підходи не завжди забезпечують достатню ефективність під час роботи з лінгвістичними оцінками та експертними знаннями. Для досягнення поставленої мети було проаналізовано особливості кіберінцидентів шахрайства, досліджено сучасні підходи до оцінювання ризиків та обґрунтовано використання методів системного аналізу і нечіткої логіки.

Результатом роботи став алгоритм, який складається з шести кроків, та забезпечує оцінку ризику кіберінцидентів на основі експертних знань і нечітких правил виведення. Запропонований підхід дозволяє формалізувати суб'єктивні експертні оцінки, враховувати невизначеність вхідних даних та отримувати узагальнену оцінку рівня ризику інциденту.

Практична цінність роботи полягає у можливості використання отриманих результатів для підтримки процесів моніторингу та аналізу кіберзагроз, а також для формування додаткових показників для подальшого аналізу інцидентів. Алгоритм забезпечує гнучке налаштування параметрів моделі та може адаптуватися до швидких змін в кіберпросторі.

Недоліками запропонованого алгоритму є залежність від якості експертних оцінок і відсутність механізмів роботи з відсутніми даними.

Перспективами подальших досліджень є інтеграція методів машинного навчання та розширення алгоритму для обробки більшої кількості типів кіберінцидентів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1) Стаття 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. <https://zakon.rada.gov.ua/laws/show/2163-19>
- 2) ENISA Reports Reference Incident Classification Taxonomy 2018. Електронний ресурс. URL: <https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy>
- 3) MISP. Електронний ресурс. URL: <https://www.misp-project.org/>
- 4) CERT-UA. Перелік категорій кіберінцидентів від 28.10.2021. Електронний ресурс. URL: <https://cert.gov.ua/recommendation/16904>
- 5) EUROPOL. Online fraud schemes definition. <https://www.europol.europa.eu/crime-areas/online-fraud-schemes>
- 6) EUROPOL SPOTLIGHT - ONLINE FRAUD SCHEMES: A WEB OF DECEIT 2023. <https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report-Online-fraud-schemes.pdf>
- 7) Zadeh L. A. Fuzzy sets / L. A. Zadeh // Information and Control. – 1965. – Т. 8, № 3. – Р. 338-353.
- 8) Прокопенко Т. О. Теорія систем і системний аналіз : навч. посіб. [Електронний ресурс] / Т. О. Прокопенко ; М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2019. – 139 с
- 9) Yuliia Nakonechna, Savchuk B., Kovalova A. Fuzzy logic in risk assessment of multi-stage cyber attacks on critical infrastructure networks, 2024. Електронний ресурс. URL: <https://tacs.ipt.kpi.ua/article/view/318023>
- 10) Fakhravar H. Quantifying Uncertainty in Risk Assessment using Fuzzy Theory, 2020. Електронний ресурс. URL: <https://arxiv.org/abs/2009.09334>
- 11) Huang S., Poskitt C., Shar L. Security Modelling for Cyber-Physical Systems: A Systematic Literature Review, 2024. <https://arxiv.org/abs/2404.07527v3>
- 12) Kerimkhulle, S.; Dildebayeva, Z.; Tokhmetov, A.; Amirova, A.; Tussupov, J.; Makhazhanova, U.; Adalbek, A.; Taberkhan, R.; Zakirova, A.; Salykbayeva, A. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. Symmetry 2023, 15, 1958. <https://doi.org/10.3390/sym15101958>

- 13) Almseidin, M.; Alkasassbeh, M.; Alzubi, M.; Al-Sawwa, J. Cyber-Phishing Website Detection Using Fuzzy Rule Interpolation. *Cryptography* 2022, 6, 24. <https://doi.org/10.3390/cryptography6020024>
- 14) de Campos Souza, P.V.; Lughofer, E.; Batista, H.R.; Guimaraes, A.J. An Evolving Fuzzy Neural Network Based on Or-Type Logic Neurons for Identifying and Extracting Knowledge in Auction Fraud. *Mathematics* 2022, 10, 3872. <https://doi.org/10.3390/math10203872>
- 15) Волошин, О. Ф. Моделі та методи прийняття рішень : навч. посіб. для студ. вищ. навч. закл. / О. Ф. Волошин, С. О. Мащенко. – 2-ге вид., перероб. та допов. – К. : Видавничо-поліграфічний центр "Київський університет", 2010. – 336 с
- 16) Міца О.В., Лавер В.О. Системний аналіз : навч.-метод. посіб. / О.В. Міца, В.О. Лавер. – Ужгород : вид-во ПП «АУТДОР - ШАРК», 2021. – 63 с.
- 17) Системний аналіз [Електронний ресурс] : навч. посіб. / А.В. Малієнко, О.Б. Владико, Т.В. Хом'як, С.В. Козир; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2026. – 250 с.
- 18) Дивак, М. П. Системний аналіз : метод. посіб / М. П. Дивак". – Тернопіль : Економічна думка, 2004. – 136 с.
- 19) М.О. Ніколов. «Основи теорії систем». ДУІКТ, 2015 – 188с.
- 20) Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
- 21) CERT-UA. Кіберзагрози: Україна. Аналітика за II півріччя 2025. Електронний ресурс. URL: <https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku>
- 22) CERT-UA. Аналітика хакерських атак проти України за 2 півріччя 2023 року. Електронний ресурс. URL: <https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64621&embedded=true&a=bi>

- 23) OSCE. CYBER INCIDENT CLASSIFICATION. A Report on Emerging Practices within the OSCE region 2022. Электронный ресурс. URL: <https://tntd.osce.org/secretariat/530293>

ДОДАТКИ

Додаток А

Таблиця А.1 Перший тур опитування експертів.

№	X1	X2	X3	X4	X5
1	7	8	9	6	7
2	6	7	8	7	8
3	7	8	9	5	9
4	8	6	8	7	8
Avrg	7	7,25	8,5	6,25	8
σ	0,707	0,829	0,500	0,829	0,707

Таблиця А.2 Другий тур опитування експертів, зміна оцінки всіх критеріїв.

№	X1	X2	X3	X4	X5
1	7	7	9	6	7,3
2	6,5	7	8,3	7	7,6
3	7	7,5	8,5	6	8
4	7,6	7,2	8	6,5	8
Avrg	7,025	7,175	8,45	6,375	7,725
σ	0,390	0,205	0,364	0,415	0,295

Таблиця А.3 Третій тур опитування, зміна оцінок всіх критеріїв, окрім X2 та X5.

№	X1	X2	X3	X4	X5
1	7	7	8,6	6	7,3
2	6,8	7	8,3	6,7	7,6

3	7	7,5	8,5	6,4	8
4	7,2	7,2	8,3	6,5	7,8
Avrg	7	7,175	8,425	6,4	7,625
σ	0,141	0,205	0,130	0,255	0,259

Метадані

ДОКУМЕНТ

Заголовок

БКР_Стадник_М_В

Автор

Стадник М В

Науковий керівник / Експерт

Потапенко С.Д.

ІД документу

334365816

ОРГАНІЗАЦІЯ

Назва організації

**Kyiv National Economic University named after Vadym Hetman
KNEU**

підрозділ

кафедра системного аналізу та кібербезпеки

ЗВІТ

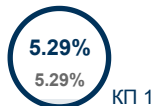
Дата звіту

2026-06-19

Дата редагування

Обсяг знайдених подібностей

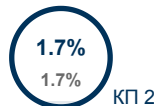
Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1

25

Довжина фрази для коефіцієнта подібності 2



КП 2

5838

Кількість слів



КЦ

41642

Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про **МОЖЛИВІ** маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		0
Інтервали		0
Мікропробіли		0
Білі знаки		1
Парафрази (SmartMarks)		16

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз			Колір тексту
#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)	
1	http://elibrary.knu.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf	45 0 (0 77 %)	

2	https://zavantag.com/docs/374/index-208283-1.html?page=2	28 0 (0.48 %)
3	https://studopedia.su/11_108931_metod-delfi.html	26 0 (0.45 %)
4	Педагогічні умови самореалізації особистості в процесі навчання фундаментальних дисциплін у технічному ЗВО (на прикладі курсу фізики в НТУ «ХПІ») 12/12/2024 V. N. Karazin Kharkiv National University (KGNU) (УІПА - Педагогіки, методики та менеджменту освіти)	22 0 (0.38 %)
5	https://studopedia.su/11_108931_metod-delfi.html	12 0 (0.21 %)
6	PENGUNAAN HEC-RAS DAN HIDROGRAF SATUAN SINTETIK UNTUK ANALISIS DEBIT BANJIR Dwi Ariyani,Ernas Fadly Ahmad, Fadli Kurnia;	12 0 (0.21 %)
7	http://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf	12 0 (0.21 %)
8	https://zavantag.com/docs/374/index-208283-1.html?page=2	12 0 (0.21 %)
9	https://zavantag.com/docs/374/index-208283-1.html?page=2	11 0 (0.19 %)
10	http://dspace.wunu.edu.ua/bitstream/316497/40460/1/dis_barna.pdf	11 0 (0.19 %)

База даних RefBooks (0.86 %)



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
джерело: Paperity		
1	PENGUNAAN HEC-RAS DAN HIDROGRAF SATUAN SINTETIK UNTUK ANALISIS DEBIT BANJIR Dwi Ariyani,Ernas Fadly Ahmad, Fadli Kurnia;	27 (3) (0.46 %)
2	Flesh flies (Diptera: Sarcophagidae) colonising large carcasses in Central Europe P. Chabanet;	13 (2) (0.22 %)
3	Дослідження профілів користувачів соціальних мереж Ткаченко В.В., Чередніченко О.Ю., Масихнович О.О., Вовк М.А.;	10 (2) (0.17 %)

Домашня база даних



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
Програма обміну базами даних (0.63 %)		
4	Педагогічні умови самореалізації особистості в процесі навчання фундаментальних дисциплін у технічному ЗВО (на прикладі курсу фізики в НТУ «ХПІ») 12/12/2024 V. N. Karazin Kharkiv National University (KGNU) (УІПА - Педагогіки, методики та менеджменту освіти)	22 (1) (0.38 %)
5	Посередництво у системі технологій торгівлі 4/9/2025 Lviv Professional College of Food Technology and Business, National University of Food Technoloaies (Lviv Professional College of Food Technoloav and Business. National University of	10 (1) (0.17 %)

6	КІБЕРБЕЗПЕКА МОРЕПЛАВСТВА: ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ 12/5/2024 National university "Odessa maritime academy" (Дипломна робота магістра)	5 (1) (0.09 %)
---	---	----------------

Інтернет (3.8 %)



#	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
7	https://zavantag.com/docs/374/index-208283-1.html?page=2	84 (6) (1.44 %)
8	http://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf	57 (2) (0.98 %)
9	https://studopedia.su/11_108931_metod-delfi.html	38 (2) (0.65 %)
10	http://dspace.wunu.edu.ua/bitstream/316497/40460/1/dis_barna.pdf	22 (2) (0.38 %)
11	https://cybersec.net.ua/normatyvni-dokumenty/524-yak-povidomliaty-pro-kiberintsydent-perelik-katehorii-kiberintsydentiv.html	11 (1) (0.19 %)
12	https://infopedia.su/16xd7d9.html	10 (1) (0.17 %)



Список прийнятих фрагментів

#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)
---	-------	---------------------------------------