ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ: СТВОРЕННЯ, ВИКОРИСТАННЯ, ДОСТУП ТА УПРАВЛІННЯ

ЗБІРНИК МАТЕРІАЛІВ

Міжнародної науково-практичної Інтернет-конференції

20-21 листопада 2024 р.

Міністерство освіти і науки України
Вінницький національний технічний університет
Національна академія Державної прикордонної служби України ім. Богдана Хмельницького
Одеський національний технологічний університет
Вінницький національний медичний університет ім. М.І. Пирогова
КЗВО "Вінницька академія безперервної освіти"
Сумський обласний інститут післядипломної педагогічної освіти
Університет Бельсько-Бяльський (Польща)

«ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ: СТВОРЕННЯ, ВИКОРИСТАННЯ, ДОСТУП ТА УПРАВЛІННЯ»

ЗБІРНИК МАТЕРІАЛІВ

Міжнародної науково-практичної Інтернет-конференції
20-21 листопада 2024 р.

Суми/Вінниця
НІКО/КЗВО «Вінницька академія безперервної освіти»
2024

УДК 004
ББК 32.97
Е50

Рекомендовано до видання Вченою радою КЗВО «Вінницька академія безперервної освіти» (протокол № 8 від 20.11.2024 р.)

Електронні інформаційні ресурси: створення, використання, доступ та управління. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції 20-21 листопада 2024 р. – Суми/Вінниця: НІКО / КЗВО «Вінницька академія безперервної освіти», 2024. – 220 с.

ISBN 978-617-7422-24-1

Збірник містить матеріали Міжнародної науково-практичної Інтернет конференції «Електронні інформаційні ресурси: створення, використання, доступ та управління. Матеріали збірника подано у авторській редакції. Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, статистичних даних, власних імен та інших відомостей, Матеріали відтворюються зі збереженням змісту, орфографії та синтаксису текстів, наданих авторами.

УДК 004
ISBN 978-617-7422-24-1

ПОЗНЯК В.А, КАТЄЛЬНІКОВ Д.І,
Вінницький національний технічний університет

РОЗРОБКА ЕКСПЕРТНОЇ СИСТЕМИ ДЛЯ ЗАХИСТУ ДАНИХ

Анотація: Досліджено концепцію експертної системи захисту даних, що використовує нечітку логіку для аналізу та оцінки рівня безпеки в умовах динамічних кіберзагроз. Застосовано складні параметри, включаючи поведінку користувача, рівень фізичної безпеки, метрики доступу, аналітику мережевого трафіку а також зовнішні загрози. Проведено аналіз системи, що демонструє її ефективність у виявленні загроз та прийнятті рішень на основі нечіткої логіки.

Ключові слова: експертна система, захист даних, нечітка логіка, поведінка користувача, кібербезпека.

Вступ. В умовах сучасних кіберзагроз компаніям важливо забезпечити надійний захист даних, що стає дедалі складнішим через зростання кількості та складності атак [1]. Експертні системи, засновані на нечіткій логіці, дозволяють створювати гнучкі методи захисту, які адаптуються до рівня загрози й оперативно реагують на нові ризики. Особливо актуальними стають системи, що можуть працювати з неповною або нечіткою інформацією, зокрема при оцінці поведінки користувачів та наявних технічних факторів.

Мета. Розробка систему захисту даних на основі нечіткої логіки, яка дозволить оцінювати рівень безпеки даних у режимі реального часу й адаптувати політику доступу та контролю залежно від наявних параметрів загрози.

Експертна система для захисту даних є важливим елементом у сучасних інформаційних системах, адже вона дозволяє ефективно оцінювати та виявляти

загрози на основі аналізу поведінки користувачів, фізичної безпеки, доступу до даних та інших параметрів. Для реалізації такої системи було використано нечітку логіку, яка дозволяє враховувати невизначеність і неповноту даних.

В якості нечіткої логіки в системі оцінки загрози використовується метод Мамдані. Цей метод застосовується для оцінки складних процесів. Ключовими етапами в методі Мамдані є нечітке виведення, агрегування та дефазифікація [2].

Експертна система захисту даних базується на кількох основних параметрах:

1. Поведінка користувача (ПК) – аналізує активність користувачів у системі [3].

   Низький ризик: 0–5 взаємодій за секунду.

   Середній ризик: 5–10 взаємодій за секунду.

   Високий ризик: 10–15 взаємодій за секунду.

2. Фізична безпека (ФБ) – оцінює захищеність апаратних ресурсів.

   Низький ризик: понад 80% захищених ресурсів.

   Середній ризик: 50–80% захищених ресурсів.

   Високий ризик: менше 50% захищених ресурсів.

3. Метрики доступу (МД) – аналізує рівень доступу користувачів до чутливих даних [4].

   Низький ризик: менше 20% користувачів мають повний доступ.

   Середній ризик: 20–50% користувачів мають повний доступ.

   Високий ризик: понад 50% користувачів мають повний доступ.

4. Аналіз мережевого трафіку (АМТ) – виявляє підозрілу активність у мережі [5].

   Низький ризик: трафік до 100 Мбіт/с.

   Середній ризик: трафік від 100 до 500 Мбіт/с.

   Високий ризик: трафік понад 500 Мбіт/с.

5. Зовнішні загрози (ЗЗ) – оцінює ризики від зовнішніх атак за годину.

   Низький ризик: менше 5 атак на годину.

   Середній ризик: 5–20 атак на годину.

   Високий ризик: понад 20 атак на годину.

   База правил нечіткого логічного виведення:

R1: Якщо ПК є середнього ризику, ФБ є низького ризику, МД є середнього ризику, АМТ є високого ризику, і ЗЗ є низького ризику, тоді рівень загрози низький.

R2: Якщо ПК є середнього ризику, ФБ є середнього ризику, МД є середнього ризику, АМТ є середнього ризику, і ЗЗ є середнього ризику, тоді рівень загрози середній.

R3: Якщо ПК є низького ризику, ФБ є високого ризику, МД є низького ризику, АМТ є високого ризику, і ЗЗ є високого ризику, тоді рівень загрози високий.

Лінгвістичні терми входів описуються такими нечіткими множинами:

Поведінка користувача (ПК):

Рисунок 1 – Нечіткі терми-оцінки Поведінки користувача

Фізична безпека (ФБ):

Рисунок 2 – Нечіткі терми-оцінки Фізичної безпеки

Метрики доступу (МД):

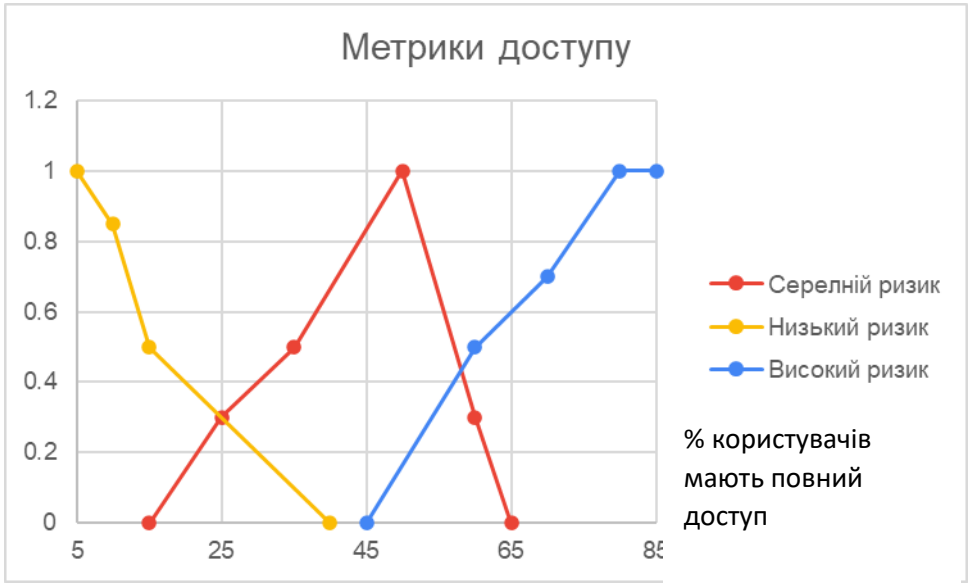

Рисунок 3 – Нечіткі терми-оцінки Метрики доступу

Аналіз мережевого трафіку (АМТ):

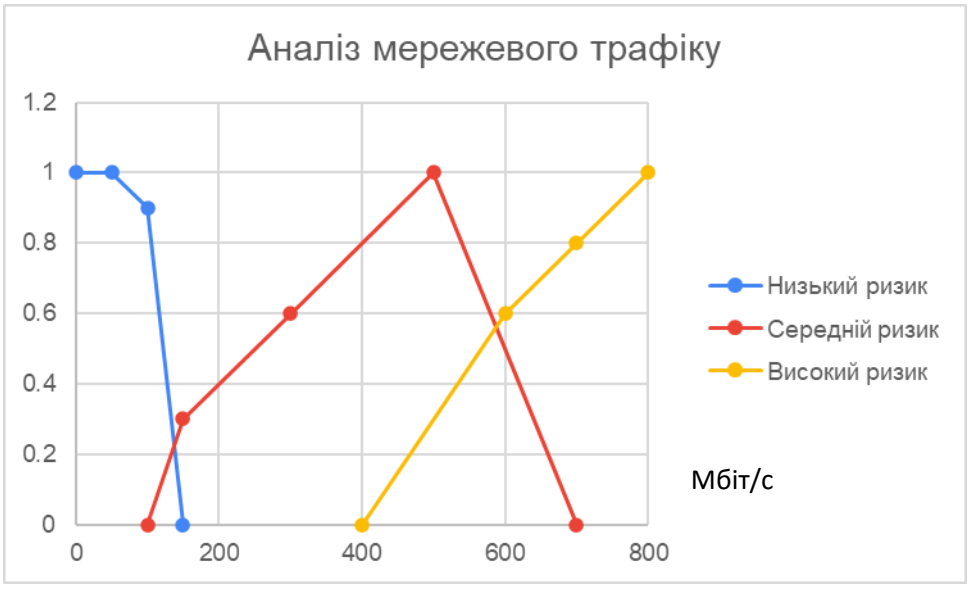

Рисунок 4 – Нечіткі терми-оцінки Аналізу мережевого трафіка

Зовнішні загрози (ЗЗ):

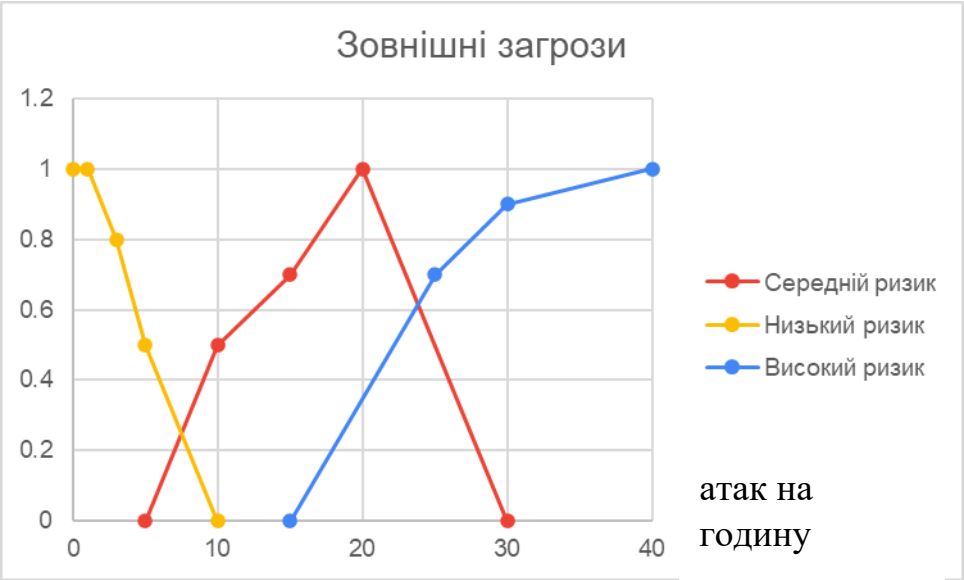

Рисунок 5 – Нечіткі терми-оцінки Зовнішніх загроз

Розглянуто сценарій: Організація «А» функціонує при наступних параметрах.

1. Поведінка користувача: 11 взаємодій за секунду (високий ризик)

2. Фізична безпека: 80% захищених ресурсів (середній ризик)

3. Метрики доступу: 30% користувачів мають повний доступ (низький ризик)

4. Аналіз мережевого трафіку: 600 Мбіт/с (середній ризик)

5. Зовнішні загрози: 5 атак на годину (високий ризик)

Таблиця 1 – Значення функцій належності нечітких термів

	Низький ризик	Середній ризик	Високий ризик
ПК	0.0	0.5	0.45
ФБ	0.4	1.0	0.0
МД	0.2	0.4	0.0
АМТ	0.0	0.5	0.6
ЗЗ	0.5	0.19	0.0

Обчислення рівнів істинності правил:

R1:

ПК (середній ризик) має належність 0.5.

ФБ (низький ризик) має належність 0.4.

МД (середній ризик) має належність 0.4.

АМТ (високий ризик) має належність 0.6.

ЗЗ (низький ризик) має належність 0.5.

Рівень істинності: $a1 = min(0.5, 0.4, 0.4, 0.6, 0.5) = 0.4$.

R2:

Всі значення відповідають умовам середнього ризику.

Рівень істинності: $a2 = min(0.5, 1.0, 0.4, 0.5, 0.19) = 0.19$.

R3:

ПК (низький ризик) активується частково з належністю 0.0.

ФБ (високий ризик) має належність 0.0.

МД (низький ризик) має належність 0.2.

АМТ (високий ризик) має належність 0.6.

ЗЗ (високий ризик) має належність 0.0.

Рівень істинності: $a3 = min(0.0, 0.0, 0.2, 0.6, 0.0) = 0.0$.

Агрегування виходів - дозволяє сформувати узагальнений набір значень для нечіткої множини, що описує кінцевий рівень загрози для організації [6].

Агреговано результати для кожного правила:

B1: Високий рівень загрози з належністю 0.4.

B2: Середній рівень загрози з належністю 0.19.

B3: Високий рівень загрози з належністю 0.0.

Об'єднання результату: $B = B1 \cup B2 \cup B3 = \{0/1, 0.5/1, 1/1\}$.

Дефазифікація виходу - перетворення нечіткої множини у чітке значення [7].

$$y = \frac{(0 \times 0.4) + (0.5 \times 0.19) + (1 \times 0)}{1 + 1 + 1} = \frac{0 + 0.2 + 0}{3} = 0.095$$

Таким чином, рівень загрози для заданих умов є низьким і становить 9.5% - це означає, що рівень безпеки функціонування достатній.

Висновок. Запропонована система дозволяє розширити можливості аналізу й захисту даних, автоматизуючи процеси прийняття рішень. Використання нечітких множин дає змогу швидко адаптуватися до нових умов і реагувати на зміни в поведінці користувачів, зменшуючи ризики.

Список використаних джерел

1. Why training is the best defence against cybersecurity and data threats. URL: https://thomasmurray.com/training-employees-cyber-security (Last accessed: 10.11.2024).

2. Mamdani, Ebrahim H . "Application of fuzzy algorithms for control of simple dynamic plant". Proceedings of the Institution of Electrical Engineers. 121 (12): 1585–1588. doi:10.1049/piee.1974.0328.

3. User Behavior Analysis for Detecting Compromised User Accounts. URL: https://www.researchgate.net/publication/374277004 (Last accessed: 10.11.2024).

4. 14 Cybersecurity Metrics + KPIs You Must Track in 2024. URL: https://www.upguard.com/blog/cybersecurity-metrics (Last accessed: 10.11.2024).

5. Survey on Network Security Traffic Analysis and Anomaly Detection Techniques. URL: https://www.researchgate.net/publication/380903277 (Last accessed: 10.11.2024).

6. Fuzzy Inference Process URL: https://la.mathworks.com/help/fuzzy/fuzzy-inference-process.html (Last accessed: 10.11.2024).

7. Defuzzification Methods. URL: https://la.mathworks.com/help/fuzzy/defuzzification-methods.html (Last accessed: 10.11.2024).