© Akhramovych V., Akhramovych V. Method for calculating information protection in social networks in the conditions of fuzzy sets // *Ukrainian Scientific Journal of Information Security, 2025, vol. 31, issue 1, pp. 15-22.* ©

DOI: 10.18372/2225-5036.31.20633

АНАЛІЗ БЕЗПЕКИ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ ТА ЛОКАЛЬНИХ МЕРЕЖАХ В УМОВАХ НЕЧІТКИХ МНОЖИН

Володимир Ахрамович[1], Вадим Ахрамович[2]

1. Державний університет «Київський авіаційний інститут»
2. Національна академія статистики, обліку та аудиту

АХРАМОВИЧ Володимир Миколайович, д.т.н., проф.
Рік та місце народження: 1951р., с. Луб'янка Поліського району, Київської обл.
Освіта: Київський політехнічний інститут 1980р.
Посада-професор кафедри кібербезпеки Державний університет: «Київський авіаційний інститут»,
Наукові інтереси: кібербезпека, інформаційна безпека, технічний захист інформації,- захист мереж, автоматизація захисту інформації.
Публікації: більше 220 наукових праць, серед них: монографії, наукові статті , підручники та навчально -методичні посібники.
E-mail: 12z@ukr.net
Orcid ID: 0000-0002-0086-9131

АХРАМОВИЧ Вадим Володимирович
Рік та місце народження 1980 р., м. Київ.
Освіта:, Київський політехнічний інститут 1993р.
Посада- завідувач ком'ютерним центром, Національної академії статистики, обліку та аудиту.
Наукові інтереси – кібербезпека, програмування, програмне та технічне забезпечення захисту інформації, мережі.
Публікації: більше 14 наукових праць, в тому числі - 3 Scopus,
E-mail: 12zstzi@ukr.net
ORCID ID: 0009-0003-2787-8745

Анотація*. У статті представлено підхід до аналізу безпеки інформації в корпоративних та локальних мережах в умовах невизначеності на основі теорії нечітких множин. Запропоновано методику, що поєднує математичне моделювання, експертні оцінки та інструменти нечіткої логіки для оцінювання ефективності системи захисту. Розглянуто вплив параметрів внутрішніх складових мережі та зовнішніх факторів, проведено оцінку їх значущості за допомогою методів PRCC та Sobol-аналізу. Наведено приклади обчислень, графічні ілюстрації та рекомендації щодо підвищення рівня захищеності інформації. Результати підтверджують доцільність застосування нечітких множин як інструменту для прийняття рішень у сфері кіберзахисту в умовах невизначеності.*

Ключові слова*: нечіткі множини, локальна та корпоративна мережі, моделювання, функція належності, система захисту, PRCC та Sobol-аналізи.*

Постановка проблеми

У сучасних корпоративних і локальних мережах неможливо точно визначити всі ризики та загрози (через їхню динамічність, різноманітність і прихований характер). Тому класичні методи оцінки часто не працюють, і потрібна модель, що враховує невизначеність та неповноту інформації. Пропонується інструментарій – нечіткі множини (fuzzy sets) дають змогу формалізувати невизначені параметри (наприклад, "високий рівень ризику", "середня надійність", "низький рівень атаки") через функції належності. Застосувати: фазифікацію – перетворення початкових числових або якісних даних у нечіткі; дефазифікацію – повернення результатів у зрозумілу кількісну форму (наприклад, інтегральний показник рівня захисту мережі).

Аналіз останніх досліджень і публікацій

Одним з нових та перспективних підходів до вирішення таких задач, заснованих на експертних оцінюваннях, є використання теорії нечітких множин [1- 4,7-10], наприклад, для оцінювання ризиків інформаційної безпеки [5,7,8]. Цей підхід дозволяє моделювати нечіткості та невизначеності в кібербезпековому контексті, надаючи можливість ефективно оцінювати загрози та їхні наслідки. При вирішенні задач експертного оцінювання, заснованого на використанні теорії нечітких множин виникає потреба в фазифікації початкових даних для подальшої їх обробки методами нечіткої логіки [6-10].

Мета та постановка завдання

Мета статті – розробити та обгрунтувати підхід до аналізу безпеки інформації в корпоративних і локальних мережах в умовах невизначеності на основі теорії нечітких множин.

Постановка завдання. Побудувати модель оцінки інформаційної безпеки корпоративних і локальних мереж у вигляді системи взаємодіючих параметрів та факторів (внутрішніх і зовнішніх).

Врахувати вплив кожної складової (наприклад: патч-менеджмент, політика доступу, резервування каналів, антивірусний захист, людський фактор, атаки ззовні).

Методи аналізу впливу параметрів. PRCC (Partial Rank Correlation Coefficient) – дозволяє визначити, які змінні найбільше впливають на

інтегральний показник безпеки. Sobol-аналіз – оцінює не тільки прямий, а й комбінований вплив параметрів (тобто взаємодію факторів ризику).

Результати (очікувані). Отримання інтегрального показника рівня захисту в умовах невизначеності.

Візуалізація результатів у вигляді графіків фазифікації/дефазифікації та діаграм чутливості (важливості факторів).

Визначення **"вузьких місць"** у системі захисту та формування рекомендацій (наприклад, підвищити NAC, оптимізувати політику доступу, посилити Zero Trust).

Вступ

Математична теорія нечітких множин (fuzzy sets) та нечітка логіка (fuzzy logic) розглядаються як ефективні інструменти моделювання невизначеності та неповноти інформації. Вони узагальнюють класичну теорію множин і формальну логіку, надаючи можливість працювати з неточними, розмитими та якісними даними. Основою нечіткої множини є функція належності, яка відображає ступінь належності елемента до певної множини у діапазоні від 0 до 1, що забезпечує більш гнучке представлення знань у порівнянні з традиційними бінарними підходами.

Застосування нечіткої логіки набуло значного поширення у сферах керування технологічними процесами, фінансового аналізу, прогнозування ризиків та інформаційної безпеки. В умовах постійного зростання кіберзагроз та ускладнення корпоративних і локальних мереж, зростає потреба у нових методах оцінювання стану їх захищеності. Класичні моделі оцінки часто не здатні адекватно відобразити багатофакторність і невизначеність сучасного інформаційного середовища, тоді як апарат нечітких множин дозволяє формалізувати експертні знання, врахувати невизначені параметри та оцінити вплив внутрішніх і зовнішніх факторів на систему захисту.

Суттєвою перевагою використання нечітких множин є можливість побудови інтегральних показників рівня безпеки, які враховують взаємодію великої кількості характеристичних параметрів мережі. Для визначення значимості окремих факторів та їхнього внеску у загальний рівень захисту доцільним є застосування методів аналізу чутливості, зокрема PRCC та Sobol-аналізу. Це дозволяє не лише оцінити поточний стан інформаційної безпеки корпоративних і локальних мереж, але й сформувати рекомендації щодо її підвищення.

Таким чином, актуальним завданням є розробка та застосування підходів до аналізу безпеки інформації, що базуються на теорії нечітких множин, з метою прийняття обґрунтованих управлінських рішень у сфері кіберзахисту.

Виклад основного матеріалу дослідження

І. Дослідження безпеки інформації в загальному вигляді для локальної мережі

1. Логіка підходу

Замість того, щоб оцінювати безпеку у чітких категоріях ("безпечна"/"небезпечна"), ми вводимо нечіткі змінні, які описують стан системи у вигляді ступенів належності до певних лінгвістичних термів:

низький рівень безпеки
середній рівень безпеки
високий рівень безпеки

Таким чином, одна і та ж система може бути на 0.6 "середньо безпечною" та на 0.3 "високо безпечною" одночасно.

2. Ключові етапи аналізу

2.1. Визначення вхідних параметрів

Параметри можуть залежати від специфіки системи. Для локальної мережі, наприклад:

Zp — рівень захисту периметру (0–100%)
Zk — рівень захисту каналів зв'язку
Cv — вразливість серверів
Ad — частота атак
Md — ефективність моніторингу

2.2. Фазифікація

Для кожного параметра визначаються функції належності. Наприклад, для Zp можна задати три лінгвістичні терми:

- "низький" (Low)
- "середній" (Medium)
- "високий" (High)

Типові форми функцій належності:

- трикутні
- трапецієподібні
- гаусові

2.3. База правил

На основі експертних знань будується нечітка база правил типу:

- IF ZpZ = High AND Cv = Low AND Md = High THEN Security Level = High
- IF ZpZ = Medium AND Cv= Medium THEN Security Level = Medium
- IF ZpZ = Low OR Cv= High THEN Security Level = Low

2.4. Агрегація та висновок

Застосовується один із методів нечіткого висновку:

- Mamdani (найбільш поширений)
- Sugeno (зручний для автоматичного керування)

2.5. Дефазифікація

Отриманий нечіткий результат переводимо у чітке число (наприклад, інтегральний індекс безпеки 0–100%). Методи дефазифікації:

- центр ваги (Centroid)
- середнє максимумів
- найбільш правдоподібне значення

3. Переваги підходу

- Можливість врахування неповних та суб'єктивних даних.
- Гнучке налаштування правил під конкретну систему.
- Інтуїтивно зрозуміле представлення для експертів.

4. Приклад

Якщо задати:

- Zp=70%Z = 70%Zp→ "Medium" (0.6), "High" (0.4)
- Cv=30%Cv = → "Low" (0.8), "Medium" (0.2)
- Md=90%Md = 90% → "High" (1.0)

За правилами ми можемо отримати нечітку оцінку:

Security = Low (0.1), Medium (0.5), High (0.7)

Після дефазифікації (метод центру ваги) → 77% рівня безпеки.

- Zp (периметровий захист) = 72%
- Cv (вразливість серверів) = 35%
- Md (ефективність моніторингу) = 88%
- Інтегральний показник безпеки (після дефазифікації, центроїд) ≈ **65.91**
- Графіки членства для Zp, Cv, Md та агрегований вихід з показаним центроїдом.

Нечіткий аналіз вхідних даних інформаційної безпеки: - Безпека периметра Zp = 72 (рис. 1) - Вразливість сервера Cv = 35 (рис.2) - Ефективність моніторингу Md = 88 (рис.3) Метод: Мамдані (I=мін, або=макс), дефазифікація: центроїд. Індекс дефазифікованої безпеки: 65,91 (рис. 4).

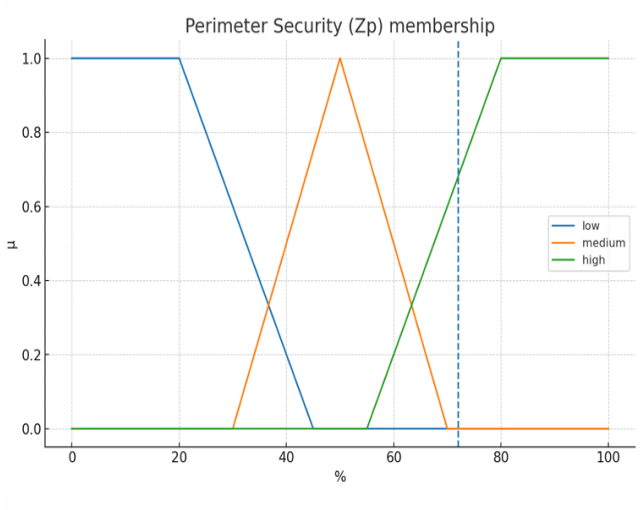

Рис. 1. Функція належності від параметрів безпеки периметра

Ускладнимо модель додавши ще три складові безпеки захисту (рис. 5,6) та введемо два види аналізу для наглядності.

PRCC (Partial Rank Correlation Coefficient)

- Метод базується на ранговій кореляції (Спірмена).
- Дозволяє оцінити монотонний зв'язок між кожною вхідною змінною і вихідним показником.
- Дає інформацію: «Як сильно змінюється результат при зміні однієї змінної, якщо зафіксувати інші».
- Дуже зручний для моделей із невеликою кількістю параметрів і коли очікується, що вплив змінних на результат є приблизно монотонним.

Рис. 2. Функція належності від параметрів вразливості серверів

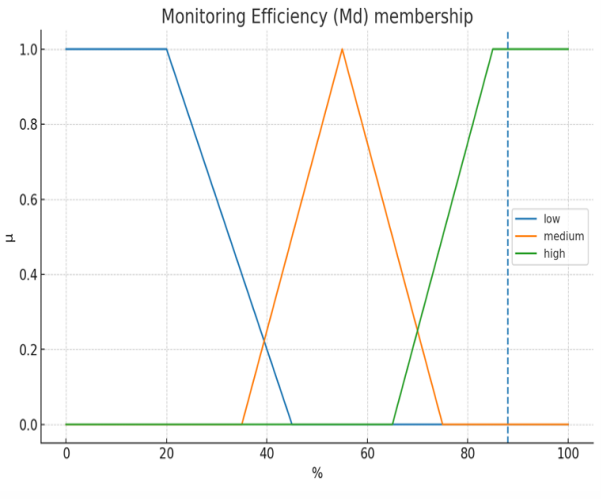

Рис. 3. Функція належності від параметрів ефективності моніторінгу

Агрегований вихід і центроїд

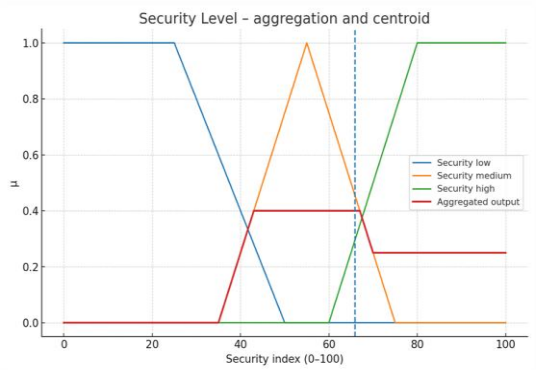

Рис. 4. Функція належності від параметрів показника безпеки

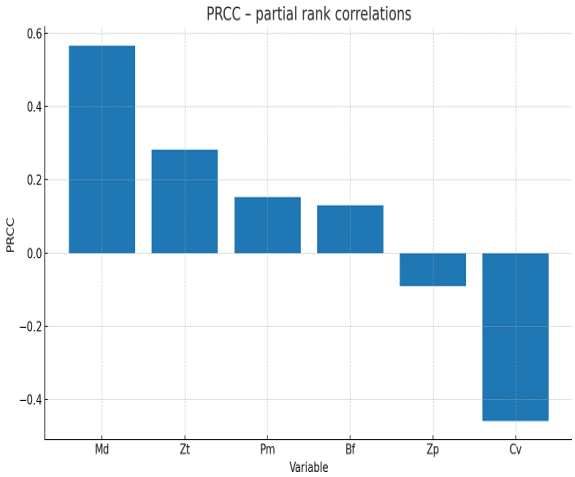

Рис. 5. PRCC (часткові рангові кореляції): показує монотонний вплив кожної змінної з урахуванням взаємовпливу інших

Sobol-аналіз

- Метод на основі розкладу дисперсії.
- Розглядає всю варіацію виходу моделі і розкладає її на частки, які пояснюються різними змінними та їх взаємодіями.
- Дає глобальний аналіз чутливості (не лише прямий ефект змінної, але й комбіновані ефекти).

Підходить для складних, нелінійних моделей і багатьох параметрів.

Нові вхідні змінні (всі у шкалі 0–1):

- Pm — patch-менеджмент (вище = краще)
- Bf — інтенсивність багфіксів/ремедіації (вище = краще)
- Zt — індекс Zero Trust (нульова довіра). (вище = краще).

Логіка нечіткого висновку: Mamdani (AND=min, OR=max), дефазифікація — центроїд. Додамо правила, що підсилюють "High Security" при високих Pm/Bf/Zt і знижують безпеку при їх низьких значеннях, а також взаємокомпенсаційні сценарії.

Демонстраційний приклад (новий)

- Zp=72, Cv=35, Md=88, Pm=76, Bf=69, Zt=81
- Показник безпеки ≈ 78.61

Аналіз чутливості

- PRCC (часткові рангові кореляції): показує монотонний вплив кожної змінної з урахуванням взаємовпливу інших.
- Sobol (first/total): варіаційна важливість (першого порядку та загальна) оцінена за схемою Saltelli (pick-freeze) без зовнішніх бібліотек.

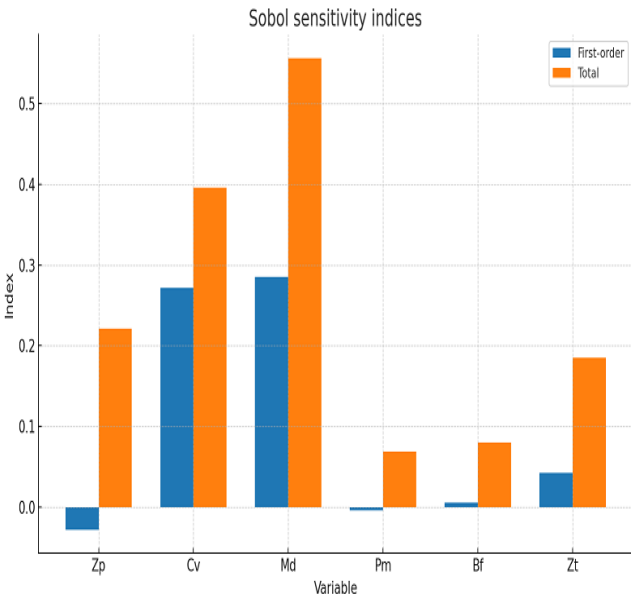

Рис. 6. Sobol (first/total): варіаційна важливість (першого порядку та загальна) оцінена за схемою Saltelli (pick-freeze).

II. Дослідження безпеки інформації в загальному вигляді для корпоративної мережі.

Відображення змінних.

- Seg (раніше Zp): сегментація мережі — VLAN/мікросегментація/NAC
- Vuln_internal (раніше Cv): внутрішня вразливість хостів і сервісів (вище = гірше)
- Mon_ew (раніше Md): моніторинг east-west (IDS/NetFlow)
- Patch_endpoints (Pm): патч-менеджмент робочих станцій/серверів
- Bugfix_cadence (Bf): темп ремедіації/закриття CVE
- ZeroTrust_score (Zt): стан Zero Trust (ідентифікація, PoLP, сегментація доступу)

Демонстраційний сценарій (LAN)

- Seg=68, Vuln_internal=42, Mon_ew=74, Patch_endpoints=82, Bugfix_cadence=63, ZeroTrust_score=77
- Показник безпеки LAN ≈ 71.10
- Оцінка нечіткої безпеки корпоративної мережі (Mamdani, centroid)

Змінне зіставлення: Seg (Zp) VLAN/мікросегментація/NAC Vulne_internal (Cv) внутрішня вразливість хоста/сервісу (вище=гірше). Mon_ew (Md) Моніторинг East-West (IDS/NetFlow). Patch_endpoints (Pm) виправлення кінцевої точки/сервера. Bugfix_cadence (Bf) каденція виправлення ZeroTrust_score (Zt). Позиція Zero Trust Приклади значень: {'Seg': 68, 'Vuln_internal': 42, 'Mon_ew': 74, 'Patch_endpoints': 'Bugfix_cadence': 63, 'ZeroTrust_score': 77} Індекс безпеки з дефаззифікацією: 71.10 (рис. 7).

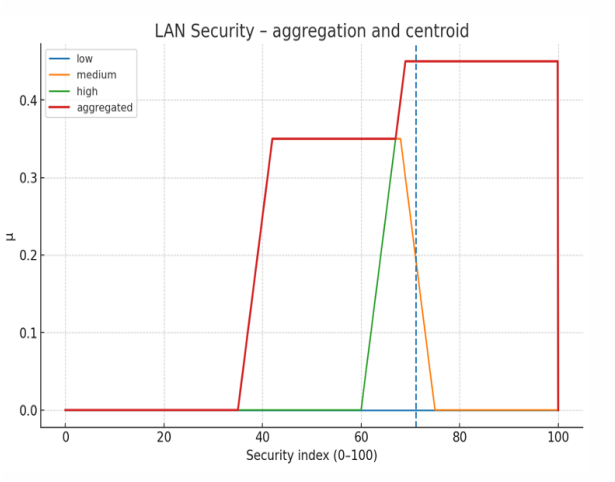

Рис. 7. Функція належності від параметрів захисту мережі (графік агрегованого виходу).

Додамо ще змінні: NAC як окрему змінну, врахувати AD-групи/PoLP, резервне копіювання (RPO/RTO) і зробити порівняння "поточний стан → цільовий" із таблицею зміни індексу та рекомендаціями. Ітак додано змінні NAC, AD_PoLP, Backup_score, і виконано порівняння *поточного* та *цільового* станів (табл. 1).

Коротко:

- Поточний індекс безпеки ≈ 55.00
- Цільовий індекс (після покращень) ≈ 81.38
- Очікуване зростання ≈ +26.38 пунктів
- Оцінка безпеки корпоративної мережі

Поточний показник у порівнянні з цільовим показником Поточний індекс безпеки: 55,00 Цільовий індекс безпеки: 81,38 Прогнозоване покращення: 26,38 балів . Дані наведені в табл. 1. Результати розрахунків – рис. 8.

Таблиця 1

Значення показників корпоративної мережі

Метрика	Поточне значення	Значення для досягнення мети
Сегментація	68.0	80.0
Внутрішня вразливість	42.0	25.0
Щотижневий моніторинг кінцевих точок	74.0	82.0
Оновлення кінцевих точок	82.0	92.0
Регулярність виправлення помилок	63.0	85.0
Нульовий бал довіри	77.0	88.0
Контроль доступу до мережі	55.0	85.0
Відстеження життєвого циклу політик Active Directory.	50.0	85.0
Резервна_оцінка	60.0	90.0
Показник захисту	55.0	81.38

За результатами аналізу можливо зробити короткі рекомендації:

- Підсилити NAC: впровадити централізований контроль доступу, 802.1X, профілі пристроїв, інтеграцію з CMDB/AD.
- AD / PoLP: провести аудит груп, прибрати надмірні привілеї, запровадити JIT/тимчасові привілеї.
- Політика патч-менеджменту: автоматизувати патчі, тестування та швидке розгортання критичних оновлень.
- Резервування: перевірити RPO/RTO, тестувати відновлення, шифрувати бекапи та зберігати їх відокремлено.
- Hardening: внутрішній скан, прибрати невикористовувані сервіси, налаштувати EDR і хост-фаєрволи.

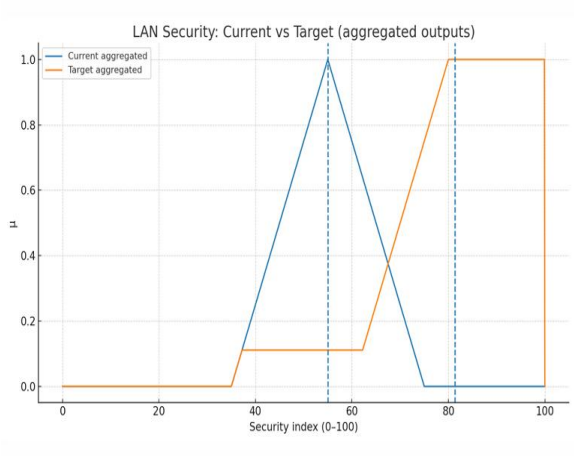

Рис. 8. Функція належності від параметрів показника захисту

Детальний аналіз чутливості для дев'яти змінних (рис. 9,10), пріоритетний план дій з оцінкою очікуваного внеску в показник безпеки.

План дій та аналіз чутливості

Поточний індекс: 55.00

Цільовий індекс: 81.38

Очікуване покращення: 26.38 пунктів

Пріоритетні дії (на основі сумарних індексів Соболя):

NAC (Контроль доступу до мережі): поточне=55, цільове=85, очікуваний внесок ≈ 7.68 пунктів; Sobol_total=0.256.

AD_PoLP (Принцип найменших привілеїв у Active Directory): поточне=50, цільове=85, очікуваний внесок ≈ 3.21 пунктів; Sobol_total=0.092.

Mon_ew (Щотижневий моніторинг кінцевих точок): поточне=74, цільове=82, очікуваний внесок ≈ 1.27 пунктів; Sobol_total=0.158.

Bugfix_cadence (Регулярність виправлення помилок): поточне=63, цільове=85, очікуваний внесок ≈ 0.63 пунктів; Sobol_total=0.029.

Backup (Резервне копіювання): поточне=60, цільове=90, очікуваний внесок ≈ 0.63 пунктів; Sobol_total=0.021.

Patch_endpoints (Патчинг кінцевих точок): поточне=82, цільове=92, очікуваний внесок ≈ 0.27 пунктів; Sobol_total=0.027.

ZeroTrust (Модель нульової довіри): поточне=77, цільове=88, очікуваний внесок ≈ 0.04 пунктів; Sobol_total=0.003.

Seg (Сегментація мережі): поточне=68, цільове=80, очікуваний внесок ≈ 0.04 пунктів; Sobol_total=0.003.

Vuln_internal (Внутрішні вразливості): поточне=42, цільове=25, очікуваний внесок ≈ -11.53 пунктів; Sobol_total=0.678.

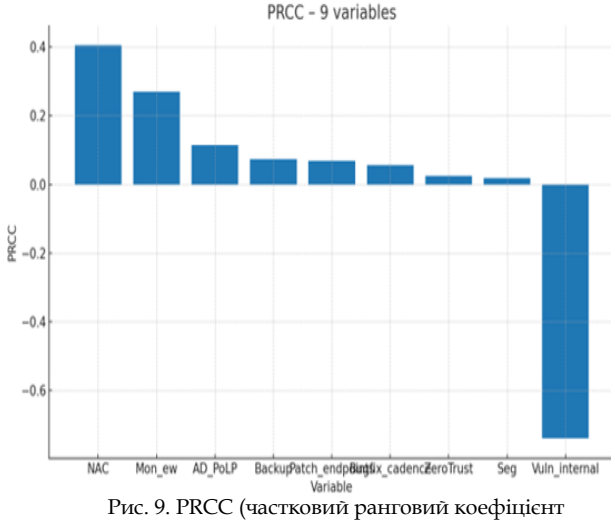

Рис. 9. PRCC (частковий ранговий коефіцієнт кореляції): варіаційна важливість (першого порядку та загальна) оцінена за схемою Saltelli (pick-freeze).

За результатами аналізу можна навести наступні рекомендації

- Підсилити NAC: централізований контроль доступу, 802.1X, профілі пристроїв, інтеграція з AD/CMDB.
- AD/PoLP: аудит привілеїв, JIT/тимчасові права, MFA для адміністративних облікових записів.
- Патч-менеджмент: автоматизація, тестування, приоритизація критичних патчів.
- Бекапи: перевірка RPO/RTO, тестування відновлення, шифрування та офсайт-зберігання.

1) Підсилення NAC / контролю доступу (Високий пріоритет) Нижче — план, впорядкований за пріоритетністю (враховано взаємодії та можливий вплив на індекс). Кожен пункт містить: мету → техзавдання → інструменти/практики → KPI/метрика вимірювання → оцінка складності/зусиль (низький/середній/високий).

Мета: забезпечити централізоване відсічення небажаних пристроїв/сегментацію на рівні портів/802.1X/ контекстного доступу. Техзавдання:

– Аудит існуючої інфраструктури комутаторів і точок доступу, інвентар пристроїв.

– Розгорнути 802.1X аутентифікацію для провідних VLAN; інтегрувати зі списками AP (RADIUS + AD).

– Впровадити профілі пристроїв (BYOD vs managed) + політики карантину (quarantine) для невідомих хостів.

– Налаштувати NAC-політики на сегментування East–West (мікросегментація) для критичних VLAN. Інструменти / практики: Cisco ISE, Aruba ClearPass, FreeRADIUS + NAC-агенти; інтеграція з CMDB/AD.

KPI:

– % пристроїв під контролем NAC (ціль: >90%)

– % невідомих пристроїв, направлених у карантин

– Зниження кількості неблокованих внутрішніх підключень/інцидентів (часом). Складність: середня–висока.

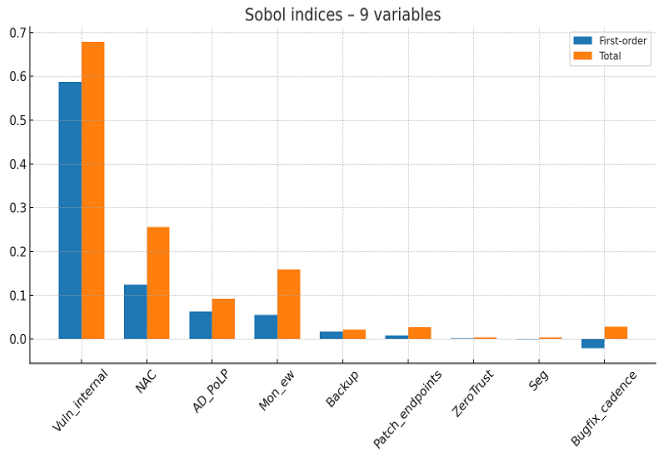

Рис. 10. . Sobol (first/total): варіаційна важливість (першого порядку та загальна) оцінена за схемою Saltelli (pick-freeze).

2) AD / PoLP (Privilege management) — аудит та мінімізація привілеїв (Високий)

Мета: зменшити ризик lateral movement та привілейованих атак. Техзавдання:

– Провести аудит AD: ідентифікувати акаунти з надлишковими правами, перевірити членства в групах Domain Admins, локальні адміни.

– Запустити застосування PoLP: створити ролі, мінімізувати постійні адміністративні обліки.

– Впровадити MFA для адміністративних облікових записів і JIT/JEA для привілеїв. Інструменти: Microsoft LAPS, Privileged Access Management (PAM) рішення (CyberArk/HashiCorp/Vault/Azure PIM), Defender for Identity / ATA.

KPI:

– % адміністративних обліків з MFA

– % надлишкових прав зменшено (до цільового)

– Число облікових записів з постійними високими привілеями (повинен падати). Складність: середня.

3) Політика патч-менеджменту (Patch endpoints) (Високий → середній)

Мета: зменшити вік уразливостей; підвищити швидкість ремедіації. Техзавдання:

– Централізувати патчинг (SCCM/Intune/WSUS, для Linux — Ansible/JAMF для macOS).

– Встановити SLA для критичних/високих CVE (наприклад: розгортання/тестування → пріоритет). (Примітка: не вказую часові оцінки тут — лише SLA-показник.)

– Впровадити автоматичний pipeline: тестування → staging → продакшн. Інструменти: Microsoft Endpoint Configuration Manager, Microsoft Intune, WSUS, Ansible, RedHat Satellite, vulnerability scanner integration (Qualys, Tenable, Nessus).

KPI:

– % пристроїв, патчені протягом SLA для критичних CVE

– Середній час до патча (MTTP) — метрична, але без точного числового таргету тут. Складність: середня.

4) **Hardening, внутрішній скан і EDR (Vuln_internal** → дуже високий вплив)

Мета: знизити внутрішні вразливості та виявлення ворога в ранній фазі. Техзавдання:

– Повний внутрішній скан (credentialed scans) → класифікація вразливостей.

– Розгортання/налаштування EDR (endpoint detection & response) на всіх критичних/корпоративних вузлах.

– Впровадити HIPS/Host firewall та жорсткі політики конфігу. Інструменти: EDR (CrowdStrike, Microsoft Defender for Endpoint, SentinelOne), Nessus/Qualys/Tenable.

KPI:

– Зниження числа High/Critical внутрішніх уразливостей

– % endpoint з EDR agent встановлено та online

– Число виявлених/зупинених спроб lateral movement. Складність: висока.

5) **Резервне копіювання та відновлення (Backup)** (середній)

Мета: гарантувати RPO/RTO, запобігти втраті даних у атаці (ransomware). Техзавдання:

– Огляд існуючих бек-ап-процесів; впровадити регулярне тестування відновлення.

– Шифрування бекапів, зберігання оффсайт, політика версіонування. Інструменти: Veeam, Commvault, Rubrik, cloud-backups (S3 with MFA-delete).

KPI:

– % успішно протестованих відновлень

– Швидкість відновлення (RTO) та допустимий RPO відповідно до бізнес-потреб. Складність: середня.

6) **Моніторинг East–West та SIEM/Detection (Mon_ew)** (середній)

Мета: покращити видимість внутрішнього трафіку і скоротити mean time to detect. Техзавдання:

– Впровадити NetFlow/PCAP/IDS у critical east–west точках; лог-агрегація в SIEM.

– Налаштувати детекшн-правила та threat hunting.

– Інструменти: Zeek/Bro, Suricata, Elastic/ELK, Splunk, Microsoft Sentinel.

KPI:

– Mean time to detect (MTTD) і mean time to respond (MTTR) — моніторити прогрес

– % критичних подій з ескалацією/автоматичною реакцією. Складність: середня.

7) Zero Trust (Zt): політики доступу та мікросегментація (середній)

Мета: рухатися від «периметру» до моделі least privilege в кожному доступі. Техзавдання:

– OIDC/MFA everywhere, контекстний доступ (device posture), політики PoLP у шлюзах.

– Мікросервісна/апп-сегментація, застосування мережевих політик (K8s NetworkPolicy якщо є).Інструменти: Proxy/Identity gateway, ZTNA (Zscaler, Cloudflare Access), kube network policy.

KPI:

– % критичних додатків під ZTNA/контекстним доступом

– % доступів, що вимагають MFA/контекстної авторизації

– Складність: середня–висока.

8) Bugfix cadence & DevSecOps (середній)

Мета: пришвидшити реагування на знайдені вразливості, інтегрувати безпеку в CI/CD.

Техзавдання:

– Впровадити процес triage → assign → fix → verify.

– Інтегрувати SAST/DAST в пайплайни, автозавдання для критичних findings.

– Інструменти: GitHub Actions/GitLab CI + Snyk/Dependabot/OWASP ZAP.

KPI:

– Середній час від виявлення уразливості до релізу виправлення (MTTR_vuln)

– % PR з пройденими SAST-перевірками

– Складність: середня.

Висновки.

Проведений аналіз показав, що показники складових мережі безпосередньо впливають на інтегральний рівень захисту інформації: із зростанням їх значень рівень захисту підвищується, тоді як зовнішні фактори (наприклад, вразливості серверів) мають зворотний негативний ефект.

Використання методів PRCC та Sobol-аналізу дало змогу кількісно оцінити значимість впливу внутрішніх параметрів мережі та зовнішніх загроз на загальний показник безпеки. Встановлено, що їхній вплив є суттєвим та визначає кінцевий результат кіберзахисту.

Наведений приклад зміни показників захисту інформації підтвердив, що за рахунок корекції параметрів мережі та мінімізації зовнішніх ризиків можливе як суттєве підвищення, так і зниження рівня захищеності. Це демонструється побудованими графіками та таблицями, що відображають динаміку зміни інтегрального показника.

Запропонований підхід дозволяє візуалізувати ступінь впевненості експертів у належності параметрів до прийнятного рівня захисту. Використання трикутних і трапецієподібних функцій належності забезпечує більш точне представлення впливу окремих факторів на загальний показник безпеки.

Розроблений метод розрахунку інтегрального показника захисту інформації на основі теорії нечітких множин може бути ефективно застосований у практичних завданнях кібербезпекового оцінювання корпоративних та локальних мереж, а також слугувати інструментом для прийняття управлінських рішень у сфері інформаційної безпеки.

Список літератури

[1]. A. Korchenko, V. Breslavskyi, S. Yevseiev, N. Zhumangalieva, A. Zvarych, S. Kazmirchuk, O. Kurchenko, O. Laptiev, O. Sievierinov, S. Tkachuk, Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency, EasternEuropean Journal of Enterprise Technologies, 2021. Vol.111. №.3/9. pp. 63-83.

[2]. С. П. Євсеєв, О. В. Шматко, Н. В. Ромащенко, Алгоритм оцінювання ступеня ризику інформаційної безпеки, що базується на нечіткомножинному підході, Сучасні інформаційні системи, 2019. Т. 3, № 2. С. 73-79.

[3]. О. В. Кочетков, Т. О. Гаур, В. М. Машін, Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки, Наукові праці ОНАЗ ім. О.С. Попова. 2019., № 1. С. 97-104.

[4]. А.О. Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень, Монографія, Київ, ЦП «Компринт», 2019, 361 с.

[5]. О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017, 435 с.

[6]. А.Г. Корченко Построение систем защиты информации на нечетких множествах. Теория и практические решения, Киев. «МК-Пресс», 2006, 320 с.

[7] . О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017 – 435 с.

[8] А. Корченко, А. Архипов, С. Казмирчук, Анализ и оценивание рисков информационной безопасности. Монография, Киев: ООО «Лазурит-Полиграф», 2013, с. 275.

[9] Вадим Ахрамович, Володимир Ахрамович. Метод розрахунку показника захисту інформації ком'ютера в умовах невизначеності. Information Technology and Security.January-June2025. Vol. 13. Iss. 1(24) pp. 55-68. DOI 10.20535/2411-1031.2025.13.1.328898.

[10] Володимир Ахрамович, Олександр Лаптєв, Анна Ільєнко, Вадим Ахрамович. Метод розрахунку захисту інформації у соціальних мережах в умовах нечітких множин. Безпека інформації, Том 30 № 3 (2024): с. 358-364.

УДК 004.738.5

Akhramovych V., Akhramovych V. Information security analysis in corporate and local networks under fuzzy sets.
Abstract. This paper presents an approach to information security analysis in corporate and local networks under uncertainty based on fuzzy set theory. The proposed methodology integrates mathematical modeling, expert evaluations, and fuzzy logic tools to assess the effectiveness of protection systems. The influence of internal network components and external factors is examined, and their significance is evaluated using PRCC and Sobol sensitivity analyses. Examples of calculations, graphical illustrations, and practical recommendations for improving information protection are provided. The results confirm the effectiveness of applying fuzzy sets as a decision-support tool for cybersecurity assessment under uncertainty.
Keywords: fuzzy sets, local and corporate networks, modeling, membership function, security system, PRCC and Sobol analyses.

Ахрамович Володимир Миколайович, д.т.н, проф., професор кафедри кібербезпеки Державний університет: «Київський авіаційний інститут».
Akhramovych Volodymyr, Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity State University «Kyiv Aviation Institute».

Ахрамович Вадим Володимирович, завідувач комп'ютерним центром Національної академії статистики, обліку та аудиту.
Akhramovych Vadym, Head of the Computer Center of the National Academy of Statistics, Accounting and Audit.