УДК 004.056:519.8
DOI: https://doi.org/10.17721/ISTS.2025.9.18-25

Володимир АХРАМОВИЧ, д-р техн. наук, проф.
ORCID ID: 0000-0002-0086-9131
e-mail: 12z@ukr.net
Державний університет "Київський авіаційний інститут", Київ, Україна

Вадим АХРАМОВИЧ, завідувач комп'ютерним центром
ORCID ID: 0009-0003-2787-8745
e-mail: 12zstzi@gmail.com
Національна академія статистики, обліку та аудиту, Київ, Україна

Микола БРАІЛОВСЬКИЙ, канд. техн. наук, доц.
ORCID ID: 0000-0002-3148-1148
e-mail: brailovskyim@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Юрій ПЕПА, канд. техн. наук, доц.
ORCID ID: 0000-0003-2073-1364
e-mail: yurka14@gmail.com
Державний університет інформаційно-комунікаційних технологій, Київ, Україна

Тетяна ЛАПТЄВА, д-р філософії
ORCID ID: 0000-0002-5223-9078
e-mail: tetiana1986@ukr.net
Державний торговельно-економічний університет, Київ, Україна

КІЛЬКІСНЕ ДОСЛІДЖЕННЯ РИЗИКІВ МЕТОДОМ НЕЧІТКИХ МНОЖИН

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

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

Методи. *Для дослідження ризиків інформаційних систем застосовано метод нечітких множин. Цей метод дозволяє прогнозувати можливі економічні збитки. Запропонований підхід забезпечує можливість інтеграції різних факторів ризику в єдину модель, враховуючи як кількісні, так і якісні аспекти їхнього оцінювання.*

Результати. *У ході дослідження розроблено кількісний підхід до оцінювання ризиків інформаційних систем підприємств, що дозволяє комплексно аналізувати й оцінювати вплив різноманітних факторів ризику.*

Модель, яка враховує невизначеність, неточність і суб'єктивність даних, що особливо важливо в умовах нестабільного середовища. Це забезпечує високу адаптивність методу до різних сфер діяльності підприємства.

Запропоновано методику, яка дозволяє здійснювати кількісне оцінювання потенційних втрат, пов'язаних із ризиками в інформаційних системах, на основі статистичних та експертних даних.

На основі результатів оцінювання ризиків можуть бути розроблені рекомендації щодо вдосконалення заходів із захисту інформаційних активів підприємства. Це включає створення адаптивних стратегій захисту, орієнтованих на зменшення економічних втрат.

Висновки. *Використання методу нечітких множин для кількісного оцінювання ризиків інформаційних систем довело свою ефективність завдяки здатності враховувати невизначеність і суб'єктивність в оцінюванні даних. Розроблений підхід дозволяє не лише прогнозувати ризики, але й приймати обґрунтовані рішення щодо зменшення потенційних втрат, що є вагомим внеском у розвиток систем управління інформаційною безпекою підприємств.*

Ключові слова: *ризики, прогнозування, втрати, система захисту, кібербезпека, захист інформації.*

Вступ

У сучасному світі інформаційні системи відіграють ключову роль у діяльності підприємств різних галузей, забезпечуючи оброблення, зберігання та передачу даних. Водночас зростає складність і багатогранність ризиків, які можуть суттєво впливати на їхню ефективність та безпеку. Інформаційні ризики, пов'язані з втратами, витоками або пошкодженнями даних, стають усе критичнішими для бізнесу через постійно зростаючу залежність від інформаційних технологій.

Нині ефективне оцінювання ризиків інформаційних систем є складним завданням, оскільки вимагає врахування низки факторів: невизначеності даних, багатовимірності ризиків, економічних і технічних аспектів, а також впливу зовнішнього середовища. Традиційні методи оцінювання часто не здатні повністю враховувати ці аспекти, особливо у випадках, коли відсутні точні або повні дані.

У цьому контексті особливої актуальності набувають підходи, що дозволяють інтегрувати кількісні та якісні аспекти оцінювання, включаючи суб'єктивні думки експертів і статистичні дані. Використання методів нечітких множин є перспективним рішенням цієї проблеми, оскільки вони дозволяють працювати з невизначеністю, неточністю та суб'єктивністю у процесі прийняття рішень.

У цій роботі запропоновано метод кількісного дослідження ризиків, який дозволяє:

- враховувати широкий спектр параметрів, включаючи економічні, управлінські та технічні аспекти;
- здійснювати розрахунок ризиків на основі статистичних даних та експертних оцінок, особливо у слабкоформалізованому середовищі;
- представляти результати оцінювання як у числовій, так і в словесній формах, використовуючи лінгвістичні змінні для опису складних систем.

ISSN 2707-1758

Метод також забезпечує адаптивність до специфіки підприємств різних галузей і уможливлює врахування впливу часу, зовнішніх факторів і внутрішньої структури організації. Запропонований підхід відкриває нові можливості для аналізу ризиків, їхнього моделювання та прогнозування економічних наслідків.

Отже, у роботі розглянуто актуальну проблему аналізу ризиків інформаційних систем із використанням сучасних методів, які сприяють точнішому прогнозуванню та ефективнішому управлінню ризиками. Отримані результати можуть бути інтегровані в систему управління підприємств, сприяючи підвищенню їхньої конкурентоспроможності та стійкості до інформаційних загроз.

Метою статті є розроблення й обґрунтування методу кількісного дослідження ризиків інформаційних систем підприємств, який враховує невизначеність, суб'єктивність і багатофакторність оцінок, а також забезпечує можливість прогнозування економічних наслідків ризиків і вдосконалення системи захисту інформаційних активів.

Огляд літератури. У статті (Korystin et al., 2024) Проведено соціальне опитування та дослідження експертної думки з метою реалізації загальної концепції стратегічного аналізу кібербезпеки в Україні. За допомогою методу, заснованого на визначенні середнього значення в певному наборі оцінок, а також методу, заснованого на теорії нечітких множин, було оцінено ризики поширення окремих кіберзагроз в Україні. Результати зведено для порівняння. Хоча використання різних методів вимірювання призвело до певних відмінностей у кількісних показниках ризику, порівняльний аналіз співвідношення рівнів різних кіберзагроз суттєво не змінився. Водночас метод нечітких наборів забезпечив гнучкішу інтерпретацію результатів для характеристики кіберзагроз із погляду їхнього висхідного або низхідного тренду.

У статті (Korchenko et al., 2021) відмічено, що один з актуальних напрямів, що розвиваються в області інформаційної безпеки, пов'язаний із використанням Honeypots (віртуальних приманок, онлайн-пасток), а вибір критеріїв для визначення найефективніших Honeypots і їхньої подальшої класифікації є актуальним завданням. Представлено основні продукти, в яких реалізовано технології віртуальної приманки. Вони часто використовуються для вивчення поведінки, підходів і методів, які застосовує стороння сторона для отримання несанкціонованого доступу до ресурсів інформаційної системи. Онлайн-хуки можуть імітувати будь-який ресурс, але частіше вони виглядають як справжні продакшн-сервери та робочі станції. Відомий ряд досить ефективних розробок, які використовують для розв'язання завдань виявлення атак на ресурси інформаційної системи (Barabash et al., 2025), в основі яких лежить апарат нечітких множин. Вони показали ефективність відповідного математичного апарату, використання якого, наприклад, для формалізації підходу до формування набору еталонних значень, дозволить поліпшити процес визначення найефективніших Honeypots. Для цього сформовано безліч характеристик (процес встановлення та налаштування, процес використання та підтримки, збір даних, рівень логування, рівень моделювання, рівень взаємодії), які визначають властивості онлайн-пасток. Ці характеристики стали основою для розроблення методу формування стандартів лінгвістичних змінних для подальшого відбору найбільш ефективних Honeypots.

У статті (Кочетков, Гаур, & Машін, 2019) розглянуто процес створення нечіткої продукційної моделі оцінювання ризику інформаційної безпеки підприємства. Показано, що традиційні методи недостатньо придатні для розв'язування подібних завдань саме тому, що вони не завжди можуть чітко описати умови і надати необхідні дані для прийняття відповідних рішень, зазвичай, виникає невизначеність. Показано, що існуючі методи врахування й оцінки ризиків не позбавлені суб'єктивізму й суттєвих умов, що призводять до неправильних оцінок ризиків проєктів. Суттєво, що якісно виконаний аналіз інформаційних ризиків дозволяє провести порівняльний аналіз "ефективність – вартість" різних варіантів захисту, обрати адекватні контрзаходи і засоби контролю, оцінити рівень залишкових ризиків. Крім того, інструментальні засоби аналізу ризиків (Собчук та ін., 2023), що ґрунтуються на сучасних базах знань (Yevseiev et al., 2022) і процедурах логічного висновку, дозволяють побудувати структурні й об'єктно-орієнтовані моделі інформаційних активів компанії, моделі загроз і моделі ризиків, пов'язаних з окремими інформаційними та бізнес-транзакціями і, отже, виявляти такі інформаційні активи компанії, ризик порушення захищеності яких є критичним, тобто неприйнятним. Запропоновано використання теорії нечіткої логіки для оцінювання ризиків (Barabash, Laptiev, & Grushina, 2023).

Для моделювання ризику інформаційної безпеки підприємства запропоновано нечіткі моделі надавати у вигляді нечітких мереж (Хорошко та ін., 2024). Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збиток організації. Взаємозв'язок між факторами (антецедентом) і показниками ризику (консеквентом) являє собою бінарне нечітке відношення на декартовому множенні відповідних нечітких множин. Нечітке причинно-наслідкове відношення між антецедентом і консеквентом задають у вигляді нечіткої продукції.

У статті (Yevseiev, Shmatko, & Romashchenko, 2019) вказано на те, що одним із нових і перспективних підходів до розв'язання проблеми оцінювання кібербезпеки на об'єктах критичної інфраструктури є використання теорії нечітких множин, наприклад, для оцінювання інформаційної безпеки. На практиці трапляються ситуації, коли на розрахунок кінцевих результатів істотно впливають невідповідності висновків або помилки експертів.

У статті (Varela, & Domingues, 2022) відмічено, що ризик є однією з найважливіших складових проєкту. Його правильне оцінювання та лікування збільшують шанси на успіх проєкту. У цій статті представлено ризики в проєктах з Data Science, оцінені за допомогою дослідження, проведеного за методикою Delphi, щоб відповісти на питання: "Які ризики проєктів з Data Science?". Дослідження дозволило виявити конкретні ризики, пов'язані з проєктами з Data Science, проте вдалося перевірити, що більше половини найбільш згадуваних ризиків схожі з іншими типами IT-проєктів.

Методи

Для дослідження ризиків інформаційних систем застосовано метод нечітких множин. Цей метод дозволяє:

- прогнозувати можливі економічні збитки;
- розробляти стратегії покращення й оптимізації системи захисту інформації (Лаптєв та ін., 2024).

Запропонований підхід забезпечує можливість інтеграції різних факторів ризику в єдину модель, враховуючи як кількісні, так і якісні аспекти їхнього оцінювання.

ISSN 2707-1758

Результати

Основні аспекти опису:

1. Нечіткість ризиків.

Ризики досить зрідка мають чіткі межі, а їхні наслідки залежать від багатьох факторів, часто недостатньо визначених.

Наприклад, ризик втрати даних можна описати нечіткою множиною: "високий ризик", "середній ризик", "низький ризик", що базується на експертних оцінках або історичних даних.

2. Лінгвістичні змінні.

Для моделювання ризиків використовують лінгвістичні змінні (Лукова-Чуйко, & Лаптєва, 2024), такі як:

- імовірність ризику (низька, середня, висока);
- вплив ризику (незначний, помірний, критичний).

Ці змінні перетворюються на нечіткі множини, які визначаються функціями належності.

3. Функції належності.

Функції належності відображають, наскільки певний ризик належить до кожної категорії. Наприклад, для "високого ризику":

$$\mu(x) = \begin{cases} 0; & x \le a; \\ \dfrac{x-a}{b-a}; & a \lhd x \le b; \\ 1; & x \rhd b. \end{cases}$$

де x – оцінка ризику; a і b – межі категорій.

4. Композиція ризиків.

Використовують правила нечіткої логіки для аналізу взаємозв'язків між ризиками. Наприклад, якщо ймовірність ризику висока і вплив критичний, то загроза є серйозною.

5. Ранжування та прийняття рішень.

На основі інтегральних показників (напр., методу центра ваги) здійснюють ранжування ризиків. Прийняття рішень враховує нечіткість оцінок, що дозволяє вибрати найкращі стратегії для їхньої мінімізації.

Наприклад, ризик кібератаки можна описати як

- імовірність: середня (0.5), висока (0.7);
- вплив: критичний (0.8).

Висновок – ризик розміщено в зоні високої небезпеки (за нечіткими правилами).

Нечіткі множини дозволяють ефективно працювати з недостатньо структурованими даними, враховуючи складність і багатофакторність ризиків інформаційних систем.

Методи трапеції та трикутника широко використовують у теорії нечітких множин для визначення функцій належності ризиків. Наприклад:

1. Метод трикутника.

Функція належності у формі трикутника визначається трьома параметрами: (a, b, c), тут a – ліва межа (мінімальне значення, де належність = 0); b – пік трикутника (максимальна належність = 1); c – права межа (значення, де належність знову = 0):

$$\mu(x) = \begin{cases} 0, & x \le a \quad \text{або} \quad x; \\ \dfrac{x-a}{b-a}, & a < x \le b; \\ \dfrac{c-x}{c-b}, & b < x < c. \end{cases}$$

Розглянемо приклад.

Нехай імовірність ризику втрати даних оцінюють за шкалою 0–10. Тоді "середній ризик" має трикутну форму з параметрами (3, 5, 7):

$$\mu(4) = \frac{4-3}{5-3} = 0.5 \text{ при } x = 4;$$

$$\mu(6) = \frac{7-6}{7-5} = 0.5 \text{ при } x = 6.$$

Отже, коли $x \equiv 4x$ і $x \equiv 6x$, то вони належать до "середнього ризику" на 50 %, а коли $x \equiv 5x$, то це відповідає 100 % "середнього ризику", бо це пікове значення.

2. Метод трапеції.

Функцію належності у формі трапеції визначають чотирма параметрами: (a, b, c, d), де a – ліва межа (належність = 0); b – початок плато (належність починає = 1); c – кінець плато (належність = 1); d – права межа (належність знову = 0):

$$\mu(x) = \begin{cases} 0, & x \le a \quad \text{або} \quad x; \\ \dfrac{x-a}{b-a}, & a < x \le b; \\ 1, & b < x \le c; \\ \dfrac{d-x}{d-c}, & b < x < c. \end{cases}$$

Розглянемо приклад.

Оцінимо рівень кібератаки на інформаційну систему. "Критичний вплив" описуємо трапецією з параметрами (6, 8, 10, 12):

$$\mu(7) = \frac{7-6}{8-6} = 0.5 \text{ при } x = 7;$$

$$\mu(9) = 1, \text{ оскільки } 8 < x \le 10;$$

$$\mu(11) = \frac{12-11}{12-10} = 0.5 \text{ при } x = 11.$$

Отже, коли $x \equiv 7x$, то вони належать до "критичного впливу" на 50 %, а при $x \equiv 9x$ виходить "критичний вплив" зі 100 %.

3. Комбінація методів.

Аналізуючи ризики часто комбінують трикутні та трапецієподібні функції. Причому, зазвичай імовірність ризику моделюється трикутником, бо вона має пікову оцінку, а вплив ризику моделюється трапецією, бо він стабільно високий у певному діапазоні.

4. Візуалізація.

Трикутник використовують, коли потрібно акцентувати на єдиному піковому значенні. Трапеція підходить для опису стабільного рівня ризику в межах певного інтервалу.

Ці методи дозволяють адаптивно моделювати ризики з урахуванням нечітких меж і полегшують їхню інтерпретацію.

Фазифікація та дефазифікація на основі оцінювання ризиків інформаційної системи.

1. Постановка задачі.

Оцінимо ризик кібератаки на основі двох змінних: імовірність атаки (P) у відсотках (0–100 %); вплив атаки (I) за шкалою 0–10. Вихідна змінна – рівень ризику (R) за шкалою 0–10.

Використаємо три лінгвістичні змінні для кожного з параметрів: 1) імовірність атаки: низька (Low), середня (Medium), висока (High); 2) вплив атаки: незначний (Low), помірний (Medium), критичний (High); 3) рівень ризику: низький (Low), середній (Medium), високий (High).

2. Фазифікація.

Під фазифікацією розумітимемо процес перетворення числових даних на нечіткі множини.

Візьмемо, наприклад такі дані: P = 65 %; $I = 7$ та оцінимо функції належності.

ISSN 2707-1758

Для ймовірності P:

$$\text{Low: трикутник } (0,20,40) \to \mu_{\text{Low}}(65) = 0;$$

$$\text{Medium: трапеція } (30,50,70,90) \to \mu_{\text{Medium}}(65) = \frac{90-65}{90-70} = 0.25;$$

$$\text{High: трикутник } (60,80,100) \to \mu_{\text{High}}(65) = \frac{65-60}{80-60} = 0.25.$$

Для впливу I:

$$\text{Low: трикутник } (0,2,4) \to \mu_{\text{Low}}(7) = 0;$$

$$\text{Medium: трапеція } (3,5,7,9) \to \mu_{\text{Medium}}(7) = 0.5;$$

$$\text{High: трикутник } (6,8,10) \to \mu_{\text{High}}(7) = 0.5.$$

Фазифіковані значення:
для P: Medium = 0.25; High = 0.25;
для I: Medium = 0.5; High = 0.5.

3. Правила нечіткої логіки.

На основі фазифікованих правил використовуємо таку базу правил:

1) якщо P_{Low} і $I_{\text{Low}} \to R_{\text{Low}}$;

2) якщо P_{Medium} і $I_{\text{Medium}} \to R_{\text{Medium}}$;

3) якщо P_{High} і $I_{\text{High}} \to R_{\text{High}}$;

4) якщо P_{High} і $I_{\text{Medium}} \to R_{\text{High}}$,

а також інші два правила (з урахуванням ступенів належності):

5) для правила 2): min(0.25, 0.5) = 0.25;

6) для правила 4): min(0.25, 0.5) = 0.25.

4. Агрегація.

Агрегація об'єднує вихідні ступені належності для різних правил у нечітку множину вихідної змінної R. В результаті:

$R_{\text{Medium}} = 0.25$;

$R_{\text{High}} = 0.25.$

5. Дефазифікація.

Дефазифікація перетворює нечітку множину R на конкретне числове значення. Використаємо метод центра ваги (centroid):

$$R = \frac{\int x\mu_R(x)dx}{\int \mu_R(x)dx}.$$

Проведемо розрахунки.

Припустимо, що R_{Medium} задано трапецією (4, 5, 6, 7); а R_{High} – трикутником (6, 8, 10), тоді ваги:

$\mu_{\text{Medium}}(x) = 0.25;$

$\mu_{\text{High}}(x) = 0.25.$

Обчислення центра ваги дає

$$R = \frac{5.5 \cdot 0.25 + 8 \cdot 0.25}{0.25 + 0.25} = 6.75.$$

Висновок. Рівень ризику становить 6.75 за шкалою 0–10. Це вказує на помірно високий рівень ризику.

Розглянемо два приклади.

Приклад 1.

Необхідно підрахувати збиток за рік банку у разі прогнозованих показників, спираючись на попередні статистичні дані підприємства, а саме: ймовірність 24 атак; вплив атаки – критичний; рівень ризику – низький (Low); імовірність 250 атак; вплив атаки – середній; рівень ризику – середній (Medium); імовірність 3250 атак; вплив атаки – низький.

Критичний рівень – збитки від однієї атаки від 1 млн дол. до 500 млн дол. США.

Середній рівень – збитки від однієї атаки від 50 тис. дол. до 500 тис. дол. США.

Низький рівень – збитки від однієї атаки від 200 дол. до 10 тис. дол. США.

Відсоток нейтралізації атак за рахунок системи захисту (99–99,9) %.

Імовірність атаки (P) у відсотках (0–100 %).

Вплив атаки (I) за шкалою 0–10.

Для розрахунку можливого збитку за рік роботи банку необхідно виконати такі кроки:

1) Визначення параметрів і нечітких множин:

- Імовірність атак (кількість атак на рік);
- вплив атаки (розмір збитків від однієї атаки);
- рівень ризику (Low, Medium, High);
- відсоток нейтралізації атак.

2) Формування нечітких множин для оцінювання збитків.

Для кожного рівня ризику (Low, Medium, High) задаємо діапазони. Для критичного рівня (High Risk):

- збитки за одну атаку (1 млн дол., 500 млн дол. США);
- кількість атак (1, 24);
- загальні збитки

(1 10^6 дол. США, 24500 10^6 дол. США);

- середній збиток 250 500 000 дол. США;
- успішно реалізується 1 % атак.

Для середнього рівня (Medium Risk):

- збитки за одну атаку
- (50 тис. дол., 500 тис. дол. США);
- кількість атак (10, 250);
- загальні збитки

(10 10^5 дол. США, 250500 10^5 дол. США);

- середній збиток 275 000 дол. США;
- успішно реалізується 1 % атак.

Для низького рівня (Low Risk):

- збитки за одну атаку (200 дол., 10 тис. дол. США).
- кількість атак (300, 3250);
- загальні збитки

(300200 дол. США, 3250 10 10^5 дол. США);

- середній збиток 5 100 дол. США;
- успішно реалізується 0,1 % атак.

3) Розрахункова формула для кожного рівня ризику:

$$\text{Збиток} = \text{Середня кількість атак} \times \text{Середній збиток} \times \frac{1 - \text{Відсоток нейтралізації}}{100}.$$

Середня кількість атак обчислюється як середнє значення діапазону атак.

4) Розрахунок можливого збитку.

Для критичного рівня (High Risk):
P = 24; I = 10; середній збиток 250 500 000 дол. США; нейтралізація загроз 99 %.

ISSN 2707-1758

Збиток критичний = 24×1×10×250500000×0,01=601 200 000 дол. США.

Для середнього рівня (Medium Risk):

$P = 250$; $I = 10$; середній збиток 275 000 дол. США; нейтралізація загроз 99 %.

Збиток середній = 250×1×5×275000×0,01=3 437 500 дол. США.

Для низького рівня (Low Risk):

$P = 3250$; $I = 1$; середній збиток 5 100 дол. США; нейтралізація загроз 99,9 %.

Збиток низький = 3250×1×5100×0,001=16 575 дол. США.

Загальний можливий збиток оцінимо за формулою

Загальний збиток = Збиток критичний + Збиток середній + Збиток низький;

Загальний збиток = 601 200 000 + 3 437 500 + 16 575 = 604 654 075 дол. США.

Приклад розробленої програми для обчислення збитків мовою програмування Python

```
# ------------------------------------------------------------------
# Параметри завдання
# Збитки за одну атаку (у доларах США)
loss_per_attack = {
    "High": (1e6, 500e6),      # Критичний рівень
    "Medium": (50e3, 500e3),   # Середній рівень
    "Low": (200, 10e3)         # Низький рівень
}

# Програма на Python, яка використовується для розрахунків

# Кількість атак
attacks_range = {
    "High": (1, 24),           # Критичний рівень
    "Medium": (10, 250),       # Середній рівень
    "Low": (300, 3250)         # Низький рівень
}

# Процент нейтралізації атак (у частках)
protection_efficiency = (0.99, 0.999)  # Від 99% до 99.9%

# Розрахунок загальних збитків
def calculate_losses(loss_range, attack_range, protection_range):

    # Розрахунок кількості пропущених атак
    min_attacks = attack_range[0] * (1 - protection_range[1])  # Мінімум атак, які
                                                               # прорвались
    max_attacks = attack_range[1] * (1 - protection_range[0])  # Максимум атак, які
                                                               # прорвались

    # Розрахунок збитків
    min_loss = min_attacks * loss_range[0]  # Мінімальний збиток
    max_loss = max_attacks * loss_range[1]  # Максимальний збиток

    return (min_loss, max_loss)

# Розрахунок для кожного рівня ризику
total_losses = {}
for risk_level in loss_per_attack.keys():
    total_losses[risk_level] = calculate_losses
    (
        loss_range=loss_per_attack[risk_level],
        attack_range=attacks_range[risk_level],
        protection_range=protection_efficiency
    )

# Загальні збитки по всіх рівнях
overall_min_loss = sum(loss[0] for loss in total_losses.values())
overall_max_loss = sum(loss[1] for loss in total_losses.values())

# Вивід результатів
total_losses, (overall_min_loss, overall_max_loss)
# ------------------------------------------------------------------
```


ISSN 2707-1758

Ця програма спочатку задає діапазони кількості атак і збитків для кожного рівня ризику. Потім вона обчислює кількість пропущених атак, враховуючи ефективність захисту, і підраховує загальні збитки для кожного рівня ризику, а також суму всіх рівнів.

Приклад 2.

Оцінювання збитків банку за допомогою нечітких множин.

Опишемо початкові умови.

Банк стикається з кібератаками протягом року. Статистичні дані свідчать, що загальний прогнозований збиток за максимальної кількості атак становить 5 млн дол. США. Кількість атак оцінюється в діапазоні від 0 до 5000. Необхідно оцінити збитки для конкретного випадку, наприклад, коли очікувана кількість атак за рік становить 3000.

Розв'язання.

1. Визначення нечітких множин.

1) Кількість атак (x):

"Мала" (L): $x \le 2000$;

"Середня" (M): $2000 < x \le 4000$;

"Велика" (H): $x > 4000$.

2) Збиток (S):

"Низький" (L): $S \le 2$ млн дол. США;

"Середній" (M): $2 < S \le 4$ млн дол. США;

"Високий" (H): $S > 4$ млн дол. США.

2. Функції належності.

Розглянемо функції належності для різних кількостей атак.

"Мала" кількість атак:

$$\mu L(x) = \begin{cases} 1, & x \ge 1000; \\ \dfrac{2000 - x}{1000}, & 1000 < x \le 2000; \\ 0, & x > 2000. \end{cases}$$

"Середня" кількість атак:

$$\mu M(x) = \begin{cases} 0, & x \ge 2000; \\ \dfrac{x - 2000}{1000}, & 2000 < x \le 3000; \\ \dfrac{4000 - x}{1000}, & 3000 < x \le 4000; \\ 0, & x > 4000. \end{cases}$$

"Велика" кількість атак:

$$\mu H(x) = \begin{cases} 0, & x \le 3000; \\ \dfrac{2000 - x}{1000}, & 1000 < x \le 2000; \\ 0, & x > 2000. \end{cases}$$

Розрахунки для збитків.

"Низький" рівень:

$$\mu L(S) = \begin{cases} 1, & S \le 2; \\ \dfrac{4 - S}{2}, & 2 < S \le 4; \\ 0, & S > 4. \end{cases}$$

"Середній" рівень:

$$\mu M(S) = \begin{cases} 0, & S \le 2; \\ \dfrac{S - 2}{2}, & 2 < S \le 4; \\ \dfrac{6 - S}{1000}, & 4 < S \le 6; \\ 0, & S > 6. \end{cases} \quad (1)$$

"Високий" рівень:

$$\mu H(S) = \begin{cases} 0, & S \le 4; \\ \dfrac{S - 4}{2}, & 4 < S \le 6; \\ 1, & S > 6. \end{cases}$$

3. База правил:

- якщо кількість атак "Мала", то збиток "Низький";
- якщо кількість атак "Середня", то збиток "Середній";
- якщо кількість атак "Велика", то збиток "Високий".

4. Розрахунок збитків.

Для x = 3000 ::

- "Мала" кількість: $\mu L(3000) = 0$ (поза межами);
- "Середня" кількість: $\mu M(3000) = 1$;
- "Велика" кількість: $\mu H(3000) = 0$.

Отже, активується правило: "якщо атак "Середня" кількість, то збиток "Середній"", тоді для збитків середній рівень S знаходять із формули (1).

Використаємо дефазифікацію методом центрування ваги:

$$S = \frac{\int_2^6 S\mu M(S)dS}{\int_2^6 \mu M(S)dS} = \frac{14}{4} = 3.5 \text{ млн дол. США.}$$

Відповідь. Прогнозований збиток банку для 3000 атак становить 3.5 млн дол. США.

Дискусія і висновки

У роботі представлено метод кількісного дослідження ризиків, що базується на аналізі й оцінюванні ризиків інформаційних систем. Запропонований підхід дозволяє використовувати широкий спектр параметрів, які забезпечують створення гнучких засобів оцінювання. Цей метод дає можливість розраховувати ризики як на основі статистичних даних, так і на основі експертних оцінок, зроблених в умовах невизначеності та слабкоформалізованого середовища (Лукова-Чуйко, & Лаптєва, 2024).

Особливістю підходу є врахування таких факторів:

- період часу;
- галузь діяльності;
- економічна й управлінська специфіки підприємства.

ISSN 2707-1758

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

У ході дослідження розроблено кількісний підхід до оцінювання ризиків інформаційних систем підприємств, що дозволяє комплексно аналізувати й оцінювати вплив різноманітних факторів ризику. Основні результати роботи включають таке.

Розроблення моделі оцінювання ризиків на основі нечітких множин:

1. Модель враховує невизначеність, неточність і суб'єктивність даних, що особливо важливо в умовах нестабільного середовища. Це забезпечує високу адаптивність методу до різних сфер діяльності підприємства.
2. Прогнозування економічних збитків.
3. Запропонована методика дозволяє здійснювати кількісне оцінювання потенційних втрат, пов'язаних із ризиками в інформаційних системах, на основі статистичних та експертних даних. Це сприяє кращому розумінню масштабів можливих наслідків інформаційних інцидентів.
4. На основі результатів оцінювання ризиків можуть бути розроблені рекомендації щодо вдосконалення заходів із захисту інформаційних активів підприємства. Це включає створення адаптивних стратегій захисту, орієнтованих на зменшення економічних втрат.
5. Розроблена система відображення результатів дозволяє представляти дані в числовому і словесному виглядах, що підвищує зрозумілість і зручність для різних категорій користувачів, включаючи управлінців і технічних фахівців.
6. Методика адаптується до специфіки різних підприємств і галузей, забезпечуючи гнучкість у застосуванні для компаній із різною структурою та масштабом діяльності.

За результатами роботи можна зробити такі висновки:

1. Ефективність запропонованого методу.

Використання методу нечітких множин для кількісного оцінювання ризиків інформаційних систем довело свою ефективність завдяки здатності враховувати невизначеність і суб'єктивність в оцінці даних.

2. Практична цінність дослідження.

Розроблений підхід дозволяє не лише прогнозувати ризики, але й приймати обґрунтовані рішення щодо зменшення потенційних втрат, що є вагомим внеском у розвиток систем управління інформаційною безпекою підприємств.

3. Інтеграція результатів у практику.

Отримані результати можуть бути інтегровані у процеси управління підприємством, сприяючи підвищенню їхньої стійкості до ризиків, пов'язаних з інформаційними системами. Запропоновані висновки демонструють значущість і потенціал подальшого розвитку методів оцінювання ризиків для підвищення ефективності управління інформаційною безпекою.

Напрями подальших досліджень і подальші роботи можуть бути спрямовані на розроблення автоматизованих інструментів для оцінювання ризиків на основі запропонованого методу, а також на поглиблене дослідження галузевих особливостей ризиків в інформаційних системах.

Внесок авторів: Володимир Ахрамович – концептуалізація; методологія; аналіз джерел; Вадим Ахрамович – збір емпіричних даних і валідація; емпіричне дослідження, підготування огляду літератури; Микола Браіловський – проєктування комп'ютерних програм; реалізація комп'ютерного коду та допоміжних алгоритмів; Юрій Пепа – тестування компонентів коду; Тетяна Лаптєва – написання початкового варіанта (чернетки) статті.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

Кочетков, О. В., Гаур, Т. О., & Машін, В. М. (2019). Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. *Наукові праці ОНАЗ ім. О. С. Попова,* 1, 97–104. https://doi.org/10.33243/2518-7139-2019-1-1-97-104

Лаптєв, О. А., Колесник, В. В., Ровда, В. В. & Половінкін, М. І. (2024). Метод підвищення захисту особистих даних за рахунок синтезу резильєнтних віртуальних спільнот. *Сучасний захист інформації,* 4(60), 141–146. https://doi.org/10.31673/2409-7292.2024.040015

Лукова-Чуйко, Н., & Лаптєва, Т. (2024). Метод виявлення неправдивої інформації на основі експертної оцінки. *Захист інформації,* 26(1), 29–35. https://doi.org/10.18372/2410-7840./26.18822

Собчук, В. В., Циганівська, І. М., Лаптєв, О. А., & Журавльов, В. М. (2023). Планування технологічних ланцюжків засобами скінченно частково впорядкованих множин. *Наукоємні технології,* 60(4), 372–385. https://doi.org/10.18372/2310-5461.60.18266

Хорошко, В. О., Лаптєв, О. А., Хохлачева, Ю. Є., Аблуллах, Аль-Далваш Ф., & Пепа, Ю. В. (2024). Особливості проектування захищених інформаційних мереж. *Наукоємні технології,* 62(2), 154–163. https://doi.org/10.18372/2310-5461.62.18709

Barabash, O., Laptiev, O., & Grushina, O. (2023). The Conceptual Model of the Intelligent Network. *Сучасний захист інформації,* 4(56), 1–9. https://doi.org/10.1016/j.procs.2021.12.100 та https://doi.org/10.31673/2409-7292.2023.030202

Barabash, O., Sobchuk, V., Sobchuk, A., Musienko, A., & Laptiev, O. (2025). Algorithms for Synthesis of Functionally Stable Wireless Sensor Network. *Advanced Information Systems*, 9(1), 70–79. https://doi.org/10.20998/2522-9052.2025.1.08

Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S., Kurchenko, O., Laptiev, O., Sievierinov, O., & Tkachuk, S. (2021). Development of a Method for Constructing Linguistic Standards for Multi-criteria assessment of Honeypot Efficiency. *Eastern European Journal of Enterprise Technologies,* 111(3/9), 63–83. https://doi.org/10.15587/1729-4061.2021.225346

Korystin, O., Korchenko, O., Kazmirchuk, S., Demediuk, S., & Korystin, O. (2024). Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Set Theory. *International Journal of Computer Network and Information,* 16(1), 24–34. https://doi.org/10.5815/ijcnis.2024.01.02

Varela, C., & Domingues, L. (2022). Risks of Data Science Projects – A Delphi Study. *Procedia Computer Science,* 196, 982–989.

Yevseiev, S., Rzayev, K., Laptiev, O., Hasanov, R., Milov, O., Asgarova, B., Camalova, J., & Pohasii, S. (2022). Development of a Hardware Cryptosystem Based on a Random Number Generator with Two Types of Entropy Sources. *Eastern-European Journal of Enterprise Technologies,* Vol. 5, 9(119), 6–16. https://doi.org/10.15587/1729-4061./2022.265774

Yevseiev, S., Shmatko, O., & Romashchenko, N. (2019). Algorithm of Information Security Risk Assessment Based on Fuzzy-multiple Approach. *Сучасні інформаційні системи,* 3(2), 73–79. https://doi.org/10.20998/2522-9052.2019.2.13

References

Barabash, O., Laptiev, O., & Grushina, O. (2023). The Conceptual Model of the Intelligent Network. *Modern Information Security,* 4(56), 1–9 [in Ukrainian]. https://doi.org/10.31673/2409-7292.2023.030202

Barabash, O., Sobchuk, V., Sobchuk, A., Musienko, A., & Laptiev, O. (2025). Algorithms for Synthesis of Functionally Stable Wireless Sensor Network. *Advanced Information Systems,* 9(1), 70–79. https://doi.org/10.20998/2522-9052.2025.1.08

Khoroshko, V. O., Laptiev, O. A., Khokhlacheva, Y. E., Fouad Al-Dalvash A., & Pepa, Y. V. (2024). Features of Designing Secure Information Networks.*Scientific Technologies,* 62(2), 154–163 [in Ukrainian]. https://doi.org/10.18372/2310-5461.62.18709

Kochetkov, O. V., Gaur, T. O., & Mashin, V. M. (2019). Enterprise Information Security Risk Assessment System Based on Fuzzy Logic. *Scientific Works of O.S. Popov ONAT,* 1, 97–104 [in Ukrainian]. https://doi.org/10.33243/2518-7139-2019-1-1-97-104

Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S., Kurchenko, O., Laptiev, O., Sievierinov, O., & Tkachuk, S. (2021). Development of a Method for Constructing Linguistic Standards for Multi-criteria assessment of Honeypot

ISSN 2707-1758

Efficiency. *Eastern European Journal of Enterprise Technologies,* 111(3/9), 63–83. https://doi.org/10.15587/1729-4061.2021.225346

Korystin, O., Korchenko, O., Kazmirchuk, S., Demediuk, S., & Korystin, O. (2024). Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Set Theory. *International Journal of Computer Network and Information,* 16(1), 24–34. https://doi.org/10.5815/ijcnis.2024.01.02

Laptiev, O. A., Kolesnyk, V. V., Rovda, V. V., & Polovinkin, M. I. (2024). A Method for Increasing Personal Data Protection Through the Synthesis of Resilient Virtual Communities. *Modern Information Security,* 4(60), 141–146 [in Ukrainian]. https://doi.org/10.31673/2409-7292.2024.040015

Lukova-Chuyko, N., & Laptieva, T. (2024). Method of Detecting False Information Based on Expert Assessment. *Information Protection,* 26(1), 29–35 [in Ukrainian]. https://doi.org/10.18372/2410-7840.26.18822

Sobchuk, V. V., Tsyganivska, I. M., Laptev, O. A., & Zhuravlev, V. M. (2023). Planning of Technological Chains by Means of Finitely Partially Ordered Sets. *Science-intensive Technologies,* 60(4), 372–385 [in Ukrainian]. https://doi.org/10.18372/2310-5461.60.18266

Varela, C., & Domingues, L. (2022). Risks of Data Science Projects – A Delphi Study. *Procedia Computer Science,* 196, 982–989.

Yevseiev, S., Rzayev, K., Laptiev, O., Hasanov, R., Milov, O., Asgarova, B., Camalova, J., & Pohasii, S. (2022). Development of a Hardware Cryptosystem Based on a Random Number Generator with Two Types of Entropy Sources. *Eastern-European Journal of Enterprise Technologies,* Vol. 5, 9(119), 6–16. https://doi.org/10.15587/1729-4061.2022.265774

Yevseiev, S., Shmatko, O., & Romashchenko, N. (2019). Algorithm of Information Security Risk Assessment Based on Fuzzy-multiple Approach. *Сучасні інформаційні системи,* 3(2), 73–79. https://doi.org/10.20998/2522-9052.2019.2.13

Отримано редакцією журналу / Received: 17.05.25
Прорецензовано / Revised: 27.05.25
Схвалено до друку / Accepted: 13.06.25

Volodymyr AKHRAMOVYCH, DSc (Engin.), Prof.
ORCID ID:0000-0002-0086-9131
e-mail: 12z@ukr.net
State University "Kiev Aviation Institute", Kyiv, Ukraine

Vadym AKHRAMOVYCH, Head of the Computing Center
ORCID ID: 0009-0003-2787-8745
e-mail: 12zstzi@gmail.com
National Academy of Statistics, Accounting and Auditing, Kyiv, Ukraine

Mykola BRAILOVSKYI, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-3148-1148
e-mail: brailovskyim@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Yuriy PEPA, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0003-2073-1364
e-mail: yurka14@gmail.com
State University of Information and Communication Technologies, Kyiv, Ukraine

Tetiana LAPTIEVA, PhD
ORCID ID: 0000-0002-5223-9078
e-mail: tetiana1986@ukr.net
State University of Trade and Economics, Kyiv, Ukraine

QUANTITATIVE RISK ASSESSMENT USING THE FUZZY SETS METHOD

Background. ***This paper presents a quantitative risk assessment method based on the analysis and evaluation of risks in information systems. The proposed approach enables the use of a wide range of parameters, providing the creation of flexible assessment tools. This method allows calculating risks based on both statistical data and expert evaluations conducted under conditions of uncertainty and poorly formalized environments.***

Additionally, the developed methods provide the representation of results in both numerical and verbal forms. For example, linguistic variables, which are often used to describe complex systems characterized by both quantitative and qualitative parameters, can be utilized. The risks of information systems can be described through a conceptual fuzzy set model that accounts for uncertainty, imprecision, and subjectivity in their evaluation.

Methods. ***The fuzzy sets method was applied to study the risks of information systems. This method facilitates the prediction of potential economic losses. The proposed approach allows the integration of various risk factors into a unified model, considering both quantitative and qualitative aspects of their assessment.***

Result. ***During the study, a quantitative approach to assessing the risks of enterprise information systems was developed, enabling a comprehensive analysis and evaluation of the impact of various risk factors. The main results of the work include:***

The model accounts for uncertainty, imprecision, and subjectivity of data, which is especially important in unstable environments. This ensures high adaptability of the method to different areas of enterprise activity.

The proposed methodology enables the quantitative assessment of potential losses associated with risks in information systems based on statistical and expert data.

Based on the risk assessment results, recommendations can be developed to improve measures for protecting the enterprise's information assets. This includes the creation of adaptive protection strategies aimed at reducing economic losses.

Conclusions. ***The use of the fuzzy sets method for quantitative risk assessment of information systems has proven its effectiveness due to its ability to account for uncertainty and subjectivity in data evaluation. The developed approach not only predicts risks but also supports informed decision-making to reduce potential losses, contributing significantly to the development of enterprise information security management systems.***

Keywords: ***risks, forecasting, losses, protection system, cybersecurity, information protection.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ISSN 2707-1758