УДК 004.056.53 DOI: 10.31673/2412-4338.2025.019380

Шульга Володимир Петрович
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0003-4356-7288

Казмірчук Світлана Володимирівна
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0001-6083-251X

СИСТЕМА ОЦІНЮВАННЯ РІВНЯ РИЗИКІВ КІБЕРБЕЗПЕКИ

Анотація. *Розглянуто проблему оцінювання ризиків кібербезпеки в умовах збільшення кількості, різноманіття кіберзагроз та необхідність використання адаптивних методів для такого оцінювання. Проаналізовано існуючі систем оцінювання ризиків, такі як FAIR, OCTAVE і CRAMM та їхні обмеження у контексті сучасних загроз. Було обрано метод оцінювання ризиків гібридних загроз у сфері кібербезпеки, що базується на теорії нечітких множин, який дозволяє гнучко оцінювати рівень ризику в умовах невизначеності. Розроблено структурну модель, базовий алгоритм та програмну реалізацію системи оцінювання ризиків, які дозволили автоматизувати такий процес оцінювання при формуванні нових даних (результати експертного оцінювання, нові загрози тощо) та генерувати рекомендації щодо раціонального розподілу ресурсів. Структурна модель запропонованої системи складається з двох базових компонент, що відображаються підсистемами клієнтської обробки даних та серверної обробки даних. Підсистема клієнтської обробки даних забезпечує первинну обробку та збереження даних експертного оцінювання гібридних загроз. Вона складається з модуля авторизації експертів, експертного оцінювання та збереження даних. Підсистема серверної обробки даних виконує основні операції з обчислення значень ризику та формування звітів. Вона включає в себе модулі ідентифікації експертів та загроз, формування параметрів для подальшого оцінювання, фазифікації експертних оцінок, оцінювання рівня ризиків і генерації звіту. Проведено тестування та аналіз ефективності запропонованого підходу. Отримані результати можуть бути використані для підвищення рівня кібербезпеки організацій, подальшого прийняття рішення, щодо першочерговості обробки найактуальніших ризиків, раціонального розподілу наявних ресурсів необхідних для захисту та адаптації до нових загроз.*

***Ключові слова**: кібербезпека, гібридні загрози, кіберзагрози, оцінка ризиків, оцінювання ризиків, нечітка логіка, нечіткі множини, критична інфраструктура, лінгвістична змінна, рівень ризику, структурна модель, система оцінювання ризиків.*

Shulha Volodymyr
State university of information and communication technologies, Kyiv
ORCID 0000-0003-4356-7288

Kazmirchuk Svitlana
State university of information and communication technologies, Kyiv
ORCID 0000-0001-6083-251X

CYBERSECURITY RISK ASSESSMENT SYSTEM

Abstract. *This paper addresses the problem of cybersecurity risk assessment in the context of the growing number and diversity of cyber threats, emphasizing the need for adaptive evaluation methods. Existing risk assessment frameworks, such as FAIR, OCTAVE, and CRAMM, are analyzed, identifying their limitations in mitigating modern threats. A hybrid threat risk assessment method based on fuzzy set theory is selected, enabling flexible risk evaluation under uncertainty. A structural model, a core algorithm, and a software implementation of the risk assessment system are developed to automate the evaluation process as new data (expert assessments, emerging threats, etc.) become available, while also generating recommendations for optimal resource allocation. The proposed system's structural model consists of two primary components: the*

© Шульга В.П., Казмірчук С.В. 2025

client-side data processing subsystem and the server-side data processing subsystem. The client-side subsystem performs the initial processing and storage of expert assessments of hybrid threats, incorporating modules for expert authentication, risk assessment, and data storage. The server-side subsystem handles key risk computation tasks and report generation, comprising modules for expert and threat identification, parameter formation for further assessment, expert opinion fuzzification, risk level evaluation, and report generation. Comprehensive testing and performance analysis of the proposed approach were conducted. The obtained results demonstrate its applicability in enhancing organizational cybersecurity, prioritizing the mitigation of the most critical risks, optimizing resource allocation for protection, and adapting to evolving threats.

Keywords: *cybersecurity, hybrid threats, cyber threats, risk assessment, risk evaluation, fuzzy logic, fuzzy sets, critical infrastructure, linguistic variable, risk level, structural model, risk assessment system.*

1. Постановка проблеми

У сучасних умовах цифрової трансформації суспільства кібербезпека є одним із ключових чинників стабільного функціонування організацій, державних структур та країни в цілому. Збільшення кількості кіберзагроз, їх складність та адаптивність вимагають ефективних підходів до оцінювання рівня ризиків кібербезпеки. Існуючі методи часто базуються на суб'єктивних оцінках експертів або класичних математичних моделях, що можуть не враховувати динамічність сучасних кіберзагроз. Тому розробка ефективних систем оцінювання рівня ризиків кібербезпеки, які б дозволяли враховувати сучасні загрози, автоматизувати процеси аналізу та забезпечити прийняття своєчасних управлінських рішень є актуальним науковим завданням.

2. Аналіз останніх досліджень і публікацій

Вивчення наукових досліджень у сфері оцінювання ризиків кібербезпеки демонструє значний інтерес до методологій аналізу загроз та моделей управління ризиками.

Сьогодні існує широкий спектр засобів оцінювання ризиків, які представлені методичним [1, 2], програмним [3-5] та іншим забезпеченням [6-8]. Наприклад, у в розробках NIST (National Institute of Standards and Technology) представлено стандартизовані підходи до оцінювання ризиків, такі як NIST SP 800-30 [1], які пропонують методи ідентифікації, аналізу та управління ризиками. Однак, ці методи мають обмеження щодо адаптивності до новітніх загроз та швидкості реагування. Також існують дослідження, що базуються на використанні штучного інтелекту та машинного навчання для оцінювання ризиків. Наприклад, у роботі [6], присвячених застосуванню нейронних мереж та алгоритмів глибокого навчання, розглядаються підходи до автоматизованого аналізу аномалій у мережевому трафіку та виявлення потенційних загроз у режимі реального часу. Водночас виклики пов'язані з обґрунтуванням точності та ефективності таких методів досі залишаються актуальними, оскільки їх результати можуть залежати від якості вхідних даних, налаштувань алгоритмів та специфіки конкретних кіберзагроз.

Окремий напрямок досліджень присвячений розробці методів кількісної оцінки ризиків кібербезпеки, зокрема, підходів, що базуються на теорії ігор та баєсових мережах [7]. Такі методи оцінювання вимагають точного визначення параметрів ризику, що може бути проблематичним при складних або нових загрозах.

Існуючі системи, наприклад, FAIR (Factor Analysis of Information Risk) [3] є популярним підходом до кількісного аналізу ризиків. Платформа OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [4] розроблена для оцінки загроз у корпоративних довкіллях. Також система CRAMM (CCTA Risk Analysis and Management Method) [5] застосовується для аналізу ризиків і управління ними у великих організаціях. При їх виборі і розробці перед фахівцями виникає низка питань пов'язаних з вибором вхідних величини для оцінювання ризиків, закладених в систему математичним апаратом, довкіллям, в якому здійснюється оцінювання, часовими межами для реалізації оцінювання, можливістю адаптації системи до вимог користувача тощо. В зазначених засобах, як правило, закладено

використання статистичних даних про інциденти, пов'язані з порушенням кібербезпеки. Але слід зауважити, що національна нормативно-правова база на державному рівні не сприяє підприємствам та установам забезпечувати ефективний процес збору таких даних. Це певним чином обмежує можливості використання відповідних існуючих засобів оцінювання ризиків.

Таким чином, аналіз останніх досліджень вказує на необхідність розробки нових систем які були більш гнучкими та придатними для сучасних динамічних довкіль кіберзагроз, тоді як традиційні системи більше підходять для регламентованого та бізнес-орієнтованого оцінювання ризиків.

3. Мета і задачі дослідження

Метою даного дослідження є розробка структурної моделі, базового алгоритму та програмної реалізації системи оцінювання ризиків кібербезпеки на основі теорії нечітких множин. Запропонована система має забезпечити врахування невизначеності вхідних даних, гнучкість в оцінюванні рівня ризику та адаптацію до нових загроз у кіберпросторі.

Для досягнення поставленої мети необхідно вирішити такі задачі:

1. Проаналізувати існуючі підходи до оцінювання ризиків кібербезпеки, включаючи класичні та сучасні методи;
2. Розробити структурну модель системи оцінювання ризиків, що базується на нечіткій логіці;
3. Розробити базовий алгоритм оцінювання ризиків із використанням нечітких множин;
4. Реалізувати програмний застосунок для автоматизації процесу оцінювання ризиків кібербезпеки;
5. Провести тестування та аналіз ефективності запропонованої системи в порівнянні з існуючими методами.

4. Результати дослідження

В роботі [8] був запропонований метод оцінювання ризиків гібридних загроз у сфері кібербезпеки на основі теорії нечітких множин. На підставі цього методу пропонується структурна модель системи та її програмна реалізація, яка дозволить автоматизувати такий процес оцінювання при формуванні нових даних (результати експертного оцінювання, нові загрози тощо) та генеруванні рекомендацій щодо раціонального розподілу ресурсів.

Структурна модель запропонованої системи (рис. 1) складається з двох базових компонент, що відображають підсистеми **клієнтської обробки даних** (ПКОД) та **підсистеми серверної обробки даних** (ПСОД). Опишемо склад кожної з них. Вони побудовані на підставі зазначеного методу у відповідності з етапами 1-9 [8].

Підсистема ПКОД забезпечує первинну обробку та збереження даних експертного оцінювання гібридних загроз. Вона складається з модуля авторизації експертів (МАЕ), експертного оцінювання (МЕО) та збереження даних (МЗД).

Підсистема ПСОД є базовою для роботи ризик-менеджера. Тут на підставі експертних оцінок, що надходять з ПКОД, після їх перетворення, формуються остаточні значення ризиків. Вона включає в себе модулі ідентифікації експертів (МІЕ) та загроз (МІЗ), формування параметрів для подальшого оцінювання (МФП), фазифікації експертних оцінок (МФЕО), оцінювання рівня ризиків (МОРР) і генерації звіту (МГЗ).

Розглянемо функціональне призначення кожного з зазначених модулів ПКОД і ПСОД. Підсистема ПКОД забезпечує взаємодію експерта із системою. Модуль МАЕ призначений для реалізації процедури ідентифікації та аутентифікації експерта в системі, який після успішної авторизації переходить до процесу оцінювання у МЕО. Так, відповідно до етапу 2 методу [8] реалізується оцінювання в МЕО гібридних загроз, які були попередньо ідентифіковані і збережені у базі даних. Тут на основі анкетування щодо значень «Ймовірності (Рівень оцінювання)» (***L***) та «Можливих наслідків (Вплив)» (***PC***) для кожної ідентифікованої загрози

за бальною шкалою для *L* (від 0 до10 балів) та для *PC* (від 0 до 15 балів) експерт проставляє свої оцінки. Користувачі вводять інформацію через інтерфейс, а саме клієнтської частини, після авторизації, що спрощує процес збору даних. Дані із МЕО надходять до МЗД для збереження отриманих оцінок у базі даних у вигляді відповідних таблиць. Інтерфейсна частина забезпечує зручний доступ для експертів до ідентифікованих загроз та введення їх оцінок.

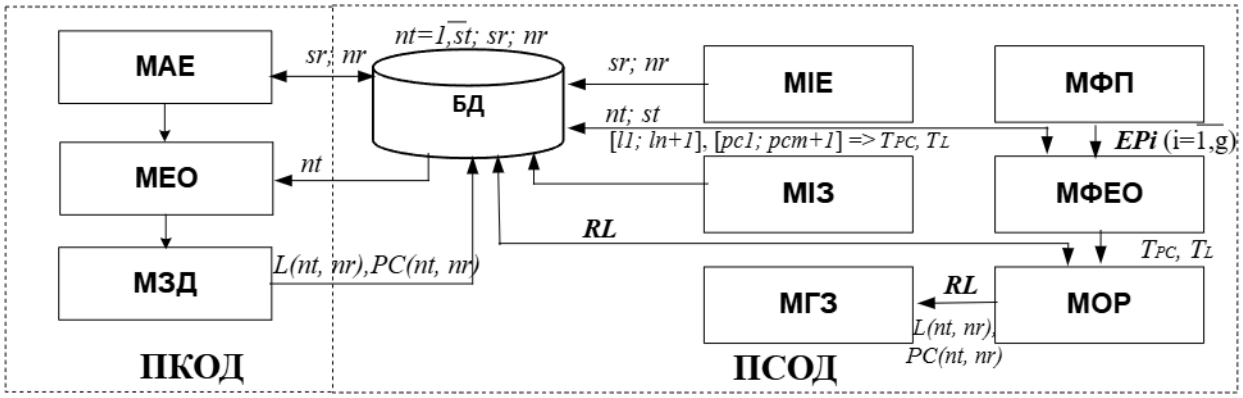


Рис. 1. Структурне модель системи ОР

Підсистема ПСОД виконує основні операції з обчислення значень ризику та формування звітів. Після проходження реєстрації ризик-менеджер за допомогою МІЕ вносить в базу даних інформацію про експертів, а також з допомогою МІЗ додає до відповідної таблиці, всі ідентифіковані гібридні загрози у відповідності етапу 1 методу [8], у першому стовбці зазначений поточний номер $nt=\overline{1,st}$ ідентифікованої гібридної загрози (st – кількість загроз), а другому – її ідентифікатор. Далі, дані підготовлені для передачі до ПКОД. Після отримання усіх необхідних оцінок від респондентів, в МФП у відповідності до етапів 3 та 6 в [8] реалізується фазифікація інтервалів $[l_1; l_2[$, $[l_2; l_3[$, $[l_3; l_4] = [0; 3[$, $[3; 7{,}5[$, $[7{,}5; 10]$ та $[c_1; c_2[$, $[c_2; c_3[$, $[c_3; c_4[$, $[c_4; c_5] = [0; 3[$, $[3; 7{,}5[$, $[7{,}5; 12{,}5[$, $[12{,}5; 15]$ для ***L*** і ***PC*** у результаті чого отримуємо нечіткі числа (НЧ) з $\underset{\sim}{T}_{L}(nt,nr)_j$, $\underset{\sim}{T}_{PC}(nt,nr)_i$ – терм-множининами ($j=\overline{1,3}, i=\overline{1,4}$). Також, тут формується еталони для оцінювання ризиків з використанням лінгвістичної змінної "RISK LEVEL" (***RL***). Далі, в МФЕП з бази даних надходять результати оцінювання експертів для фазифікації їх суджень (етап 4 в [8]). Модуль МОР (етап 5, 7, 8 в [8]) обчислює середні значення результатів опитування для *nt*-ї загрози за допомогою метода лінійної апроксимації за локальними максимумами [9] на основі формули $\underset{\sim}{RL}(nt)=\underset{\sim}{AV}_{\boldsymbol{L}}(nt)\,\tilde{\odot}\,\underset{\sim}{AV}_{\boldsymbol{PC}}(nt)$ (де $nt=\overline{1,st}$, $\tilde{\odot}$ – знак операції нечіткого множення, а $\underset{\sim}{AV}_{\boldsymbol{L}}(nt)$ та $\underset{\sim}{AV}_{\boldsymbol{PC}}(nt)$ – середні значення НЧ для ***L*** та ***PC*** *nt*-ї загрози) обчислюється ризик. Далі, для порівняння отриманих НЧ скористаємось множиною узагальненої відстані Хеммінга:

$$\left\{\bigcup_{nt=1}^{st}\left\{\bigcup_{i=1}^{n}\{H(nt,i)\}\right\}\right\}=\left\{\bigcup_{nt=1}^{st}\left\{\bigcup_{i=1}^{n}h\left(\underset{\sim}{RL}(nt),\underset{\sim}{T}_{RL}(nt)_i\right)\right\}\right\}=$$

$$\left\{\bigcup_{nt=1}^{st}\left\{\bigcup_{i=1}^{n}\sum_{k=1}^{4}\left|\underset{\sim}{RL}(nt)_k-\underset{\sim}{T}_{RL}(nt)_{ik}\right|\right\}\right\},$$

де для *nt*-ї загрози мінімальне значення $H_{min}(nt)$ із всіх

$$\bigcup_{i=1}^{n}\{H(nt,i)\}$$

буде свідчити про найбільшу наближеність НЧ до еталонного [9] ($nt = \overline{1, st}$, де st – кількість загроз, а $i = \overline{1, n}$, де n – кількість терм-множин), отримані результати зберігається у відповідних таблицях в базі даних. Для інтерпретації результатів в МГЗ (етап 9 в [8]) за сформованими асоціативними правилами визначається поточне значення ризику і формується звіт у .xlsx форматі для зручності подальшого опрацювання отриманих даних. Звіт містить графічну і текстову інтерпретацію оцінених ризиків.

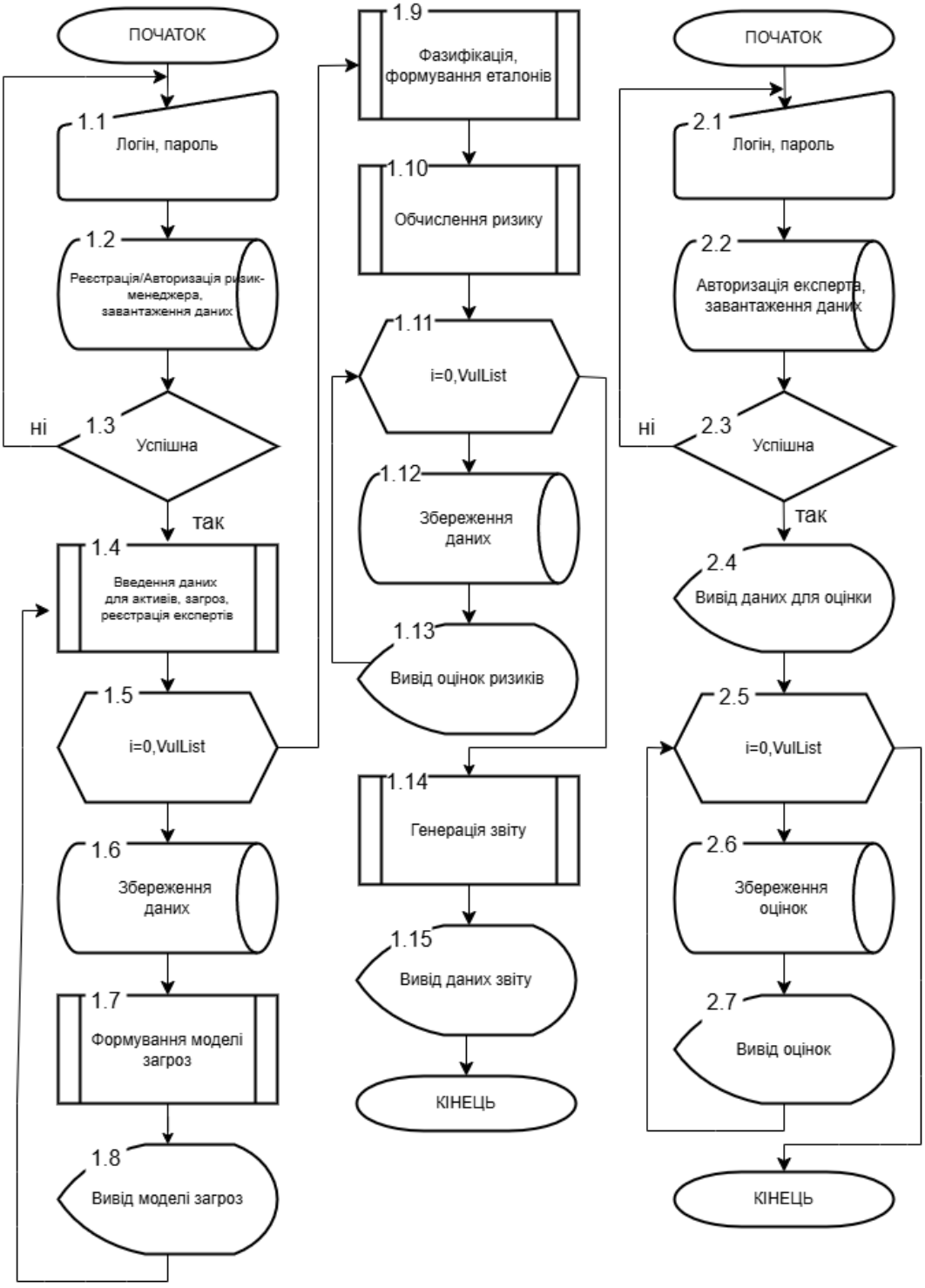


Рис. 2. Базовий алгоритм роботи системи оцінювання рівня ризику кібербезпеки: серверна та клієнтська частина

Опишемо процес функціонування системи:

1. **Введення даних експертами**. За допомогою клієнтської частини експерти ідентифікують загрози та вводять бали для їх оцінки (ймовірність і наслідки). Дані зберігаються у базі даних через модуль збереження.

2. **Обробка даних на сервері**. Дані передаються до ПСОД, де виконуються розрахунки рівня ризику для кожної загрози.

3. **Формування звіту**. На основі результатів обчислень генерується звіт, який відображає кількісні значення ризиків, графічні діаграми та текстову інтерпретацію.

Запропонована система оцінки ризиків кібербезпеки, наприклад, може бути реалізована програмно і працювати на основі запропонованого базового алгоритму (рис. 2).

Відповідно до цього алгоритму, робота системи починається з авторизації (при першому запуску ініціалізується процедура «Реєстрація» (див. рис. 3)) ризик-менеджера (на рис. 2 вершина 1.1 і 1.2) за допомогою введення логіну та паролю (рис. 4).

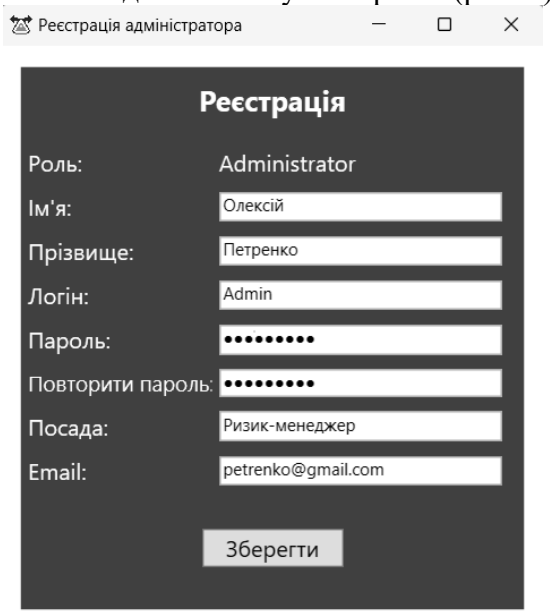


Рис. 3. Вікно реєстрації ризик-менеджера

Пароль в базі даних зберігається у хешованому вигляді, для цього використовується SHA256 (рис. 5).

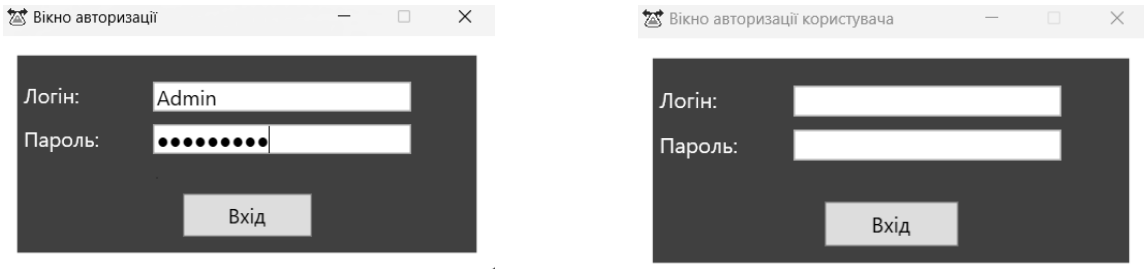
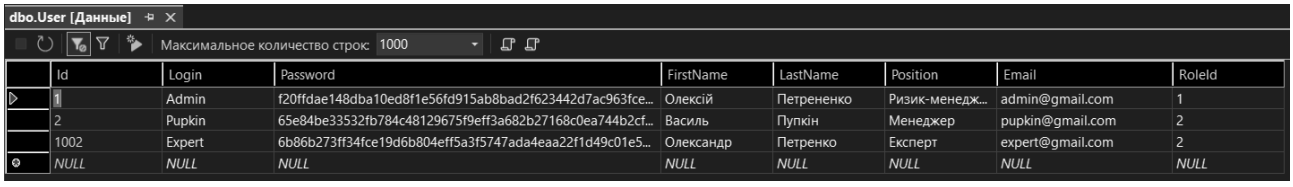


Рис. 4. Вікно авторизації Ризик-менеджера та експерта


dbo.User [Данные]

Максимальное количество строк: 1000

Id	Login	Password	FirstName	LastName	Position	Email	RoleId
1	Admin	f20ffdae148dba10ed8f1e56fd915ab8bad2f623442d7ac963fce...	Олексій	Петрененко	Ризик-менедж...	admin@gmail.com	1
2	Pupkin	65e84be33532fb784c48129675f9eff3a682b27168c0ea744b2cf...	Василь	Пупкін	Менеджер	pupkin@gmail.com	2
1002	Expert	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e5...	Олександр	Петренко	Експерт	expert@gmail.com	2
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Рис. 5. Таблиця із зареєстрованими користувачами

Після успішної авторизації (див. рис. 2 вершина 1.3) проводиться налаштування системи ризик-менеджером, яка пов’язана із внесенням необхідних даних для подальшого оцінювання рівнів ризику. На цьому етапі відбувається реєстрація експертів (рис. 6), введення даних щодо існуючих активів (рис. 7) та відповідних загроз (рис. 8) (реалізація вершини 1.4 на рис. 2).

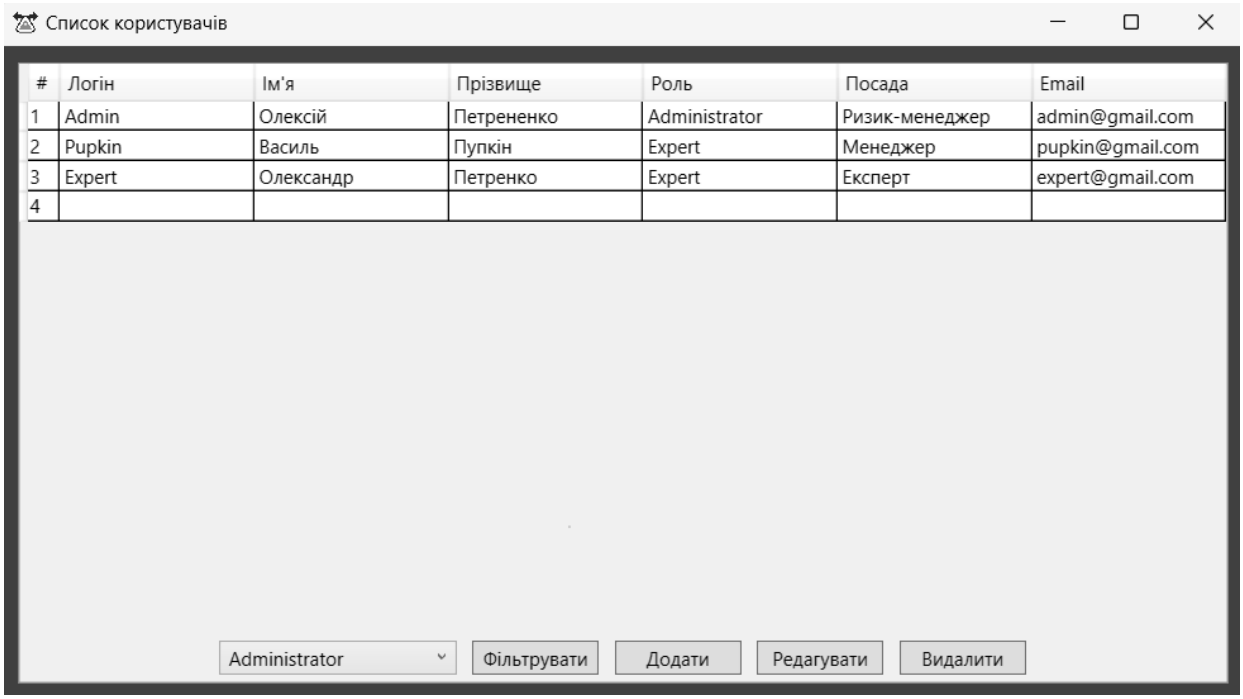


Рис. 6. Вікно реєстрації експертів в системі

Усі введені дані зберігаються у базі даних у відповідних таблицях (див. рис. 2, вершини 1.5-1.6). Також, відповідно до вершини 1.7 (рис. 2) ризик-менеджер формує модель загроз (рис. 9) для подальшої їх ідентифікації та оцінювання експертами, відповідно до визначених активів.

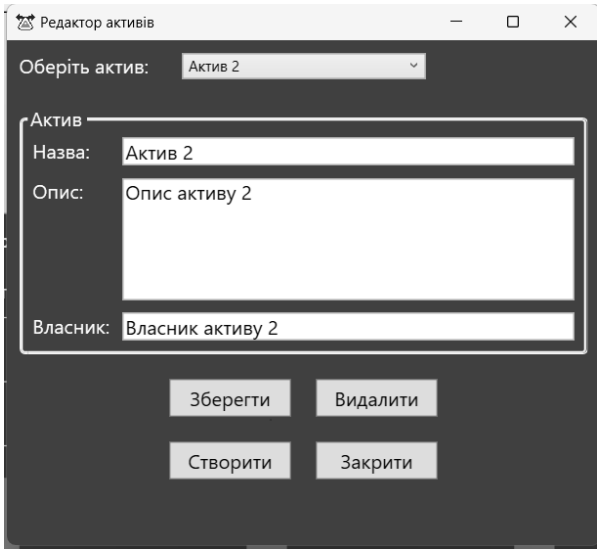


Рис. 7. Вікно редактора активів

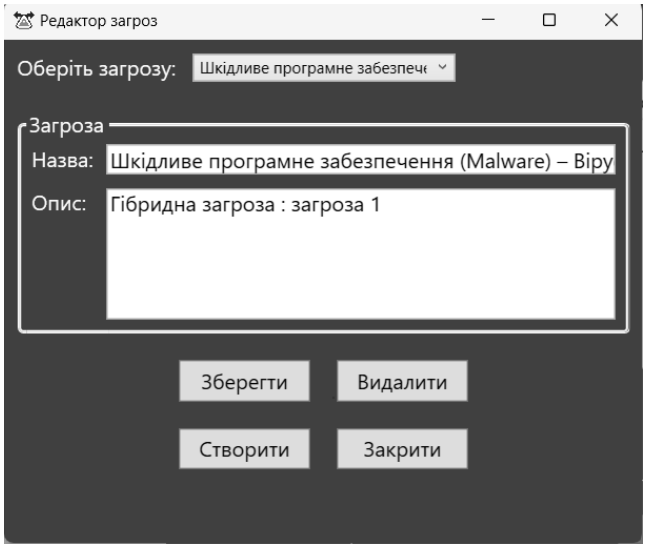


Рис. 8. Вікно редактора загроз

Процес ідентифікації і оцінювання загроз пов'язаний з роботою кожного експерта на своєму робочому місці, де здійснюється авторизація в системі (див. рис. 4 та рис. 2, вершини 2.1-2.2). При успішній авторизації (вершина 2.3, рис. 2) відбувається ініціалізація списку активів та загроз (див. рис. 2, вершина 2.4).

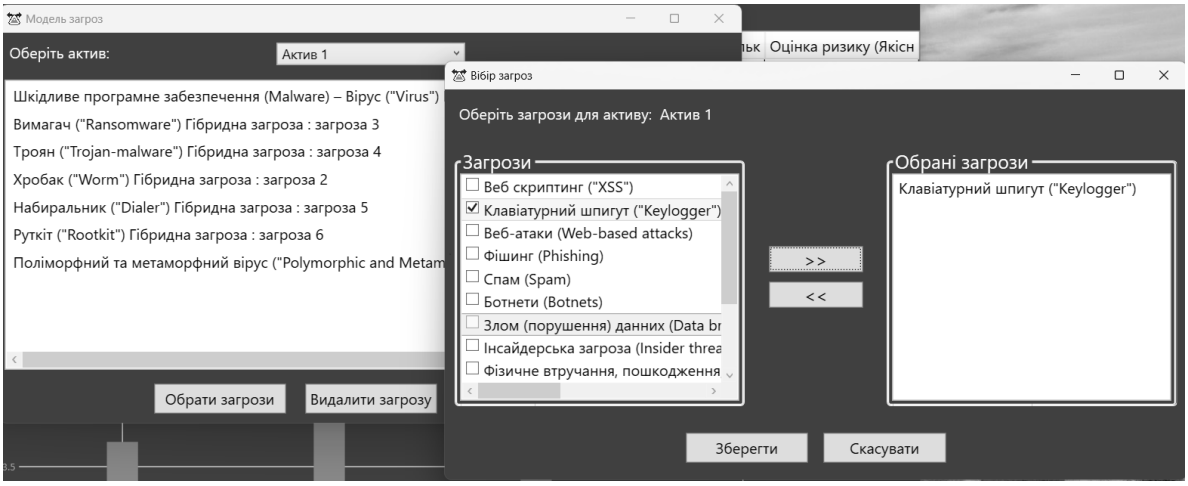


Рис. 9. Вікно формування моделі загроз

Для здійснення оцінювання відповідної гібридної загрози по кожному експерту (респонденту) ініціалізуються бали оцінок (див. рис. 10 та рис. 2, вершини 2.5-2.7). Всі внесені дані зберігаються у базі даних у відповідних таблицях.

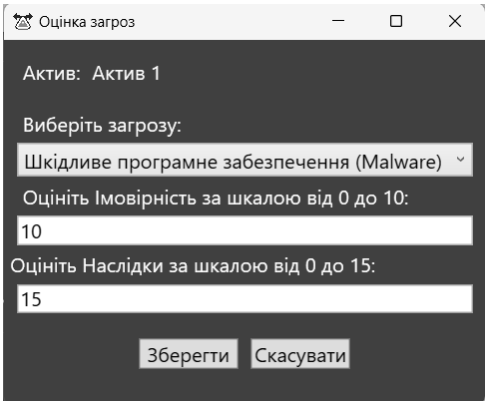


Рис. 10 Вікно оцінювання загрози Шкідливе програмне забезпечення (Malware) – Вірус ("Virus") для Активу 1

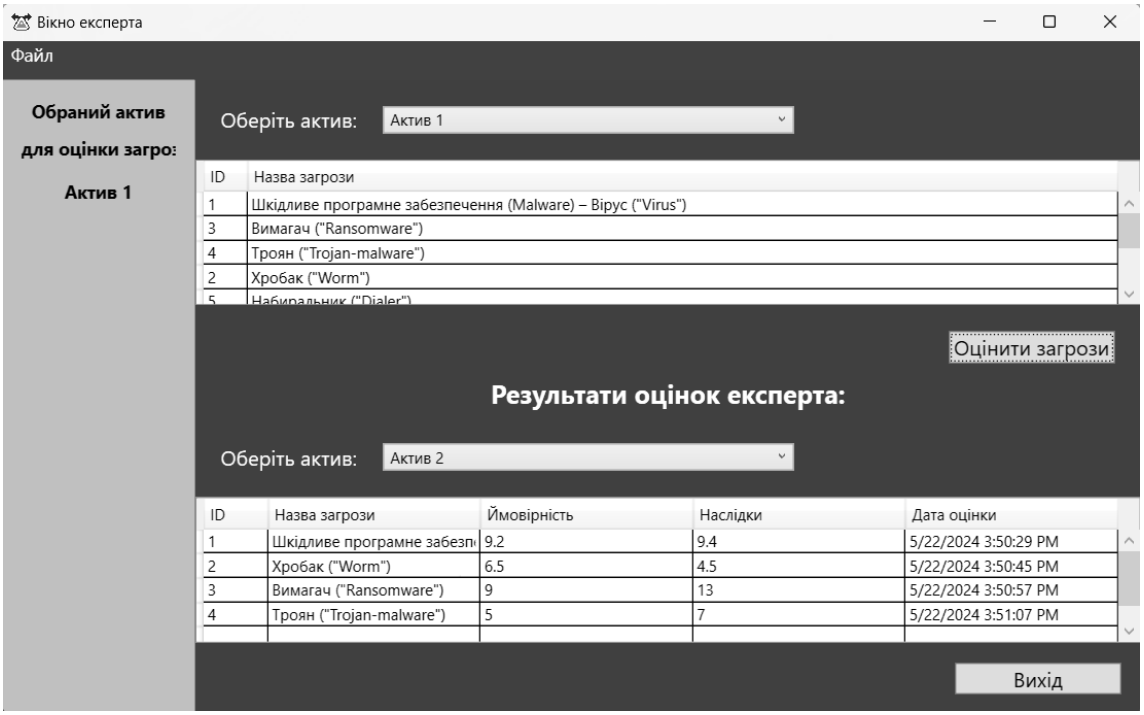


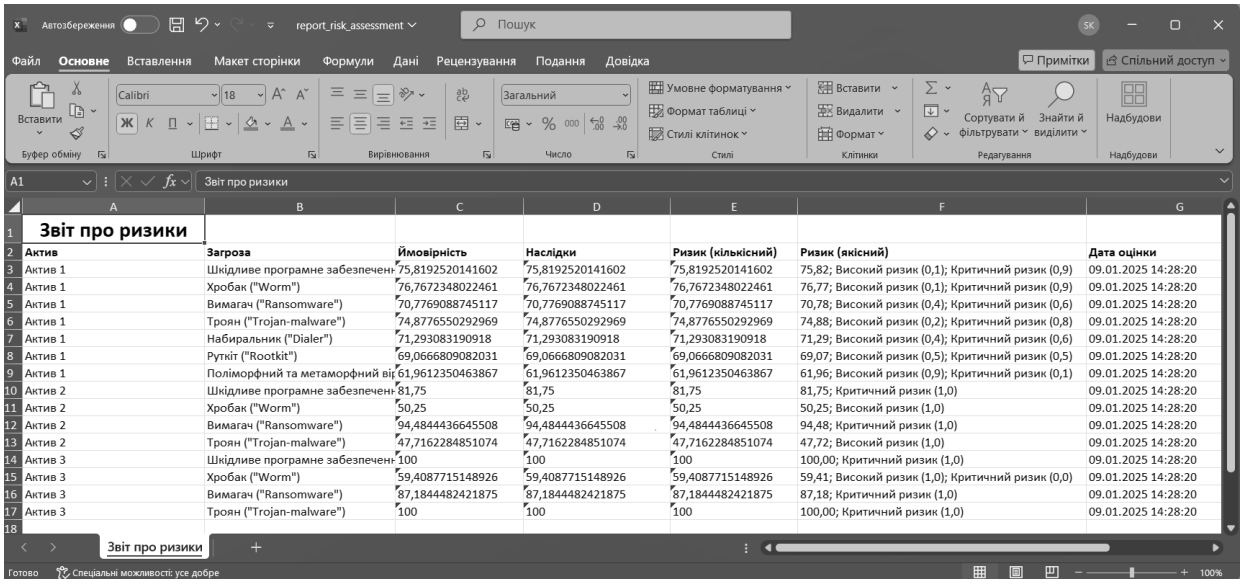
Рис. 11. Головне вікно робочого столу експерта

Результат оцінювання та поточний стан, експерт може ідентифікувати у своєму робочому вікні, при цьому для кожного респондента виводяться виключно його результати оцінювання (рис. 11).

Після отримання усіх оцінок від експертів ризик-менеджер переходить до етапу визначення рівня ризику (див. рис. 2, вершини 1.9-1.10 та рис. 12). Для цього необхідно активувати кнопку «Оцінити ризик».

Рис. 12. Головне вікно робочого столу ризик-менеджера

Далі, при активуванні кнопки «Зберегти» дані записуються у базу даних (див. рис. 2, вершини 1.11-1.13). Також, для генерації звіту та його завантаження (див. рис. 2, вершини 1.14-1.15) ризик-менеджеру необхідно застосувати відповідну кнопку. Звіт генерується та записується у файл формату .xlsx.



Звіт про ризики

Актив	Загроза	Ймовірність	Наслідки	Ризик (кількісний)	Ризик (якісний)	Дата оцінки
Актив 1	Шкідливе програмне забезпечення	75,8192520141602	75,8192520141602	75,8192520141602	75,82; Високий ризик (0,1); Критичний ризик (0,9)	09.01.2025 14:28:20
Актив 1	Хробак ("Worm")	76,7672348022461	76,7672348022461	76,7672348022461	76,77; Високий ризик (0,1); Критичний ризик (0,9)	09.01.2025 14:28:20
Актив 1	Вимагач ("Ransomware")	70,7769088745117	70,7769088745117	70,7769088745117	70,78; Високий ризик (0,4); Критичний ризик (0,6)	09.01.2025 14:28:20
Актив 1	Троян ("Trojan-malware")	74,8776550292969	74,8776550292969	74,8776550292969	74,88; Високий ризик (0,2); Критичний ризик (0,8)	09.01.2025 14:28:20
Актив 1	Набиральник ("Dialer")	71,293083190918	71,293083190918	71,293083190918	71,29; Високий ризик (0,4); Критичний ризик (0,6)	09.01.2025 14:28:20
Актив 1	Руткіт ("Rootkit")	69,0666809082031	69,0666809082031	69,0666809082031	69,07; Високий ризик (0,5); Критичний ризик (0,5)	09.01.2025 14:28:20
Актив 1	Поліморфний та метаморфний ві	61,9612350463867	61,9612350463867	61,9612350463867	61,96; Високий ризик (0,9); Критичний ризик (0,1)	09.01.2025 14:28:20
Актив 2	Шкідливе програмне забезпечення	81,75	81,75	81,75	81,75; Критичний ризик (1,0)	09.01.2025 14:28:20
Актив 2	Хробак ("Worm")	50,25	50,25	50,25	50,25; Високий ризик (1,0)	09.01.2025 14:28:20
Актив 2	Вимагач ("Ransomware")	94,4844436645508	94,4844436645508	94,4844436645508	94,48; Критичний ризик (1,0)	09.01.2025 14:28:20
Актив 2	Троян ("Trojan-malware")	47,7162284851074	47,7162284851074	47,7162284851074	47,72; Високий ризик (1,0)	09.01.2025 14:28:20
Актив 3	Шкідливе програмне забезпечення	100	100	100	100,00; Критичний ризик (1,0)	09.01.2025 14:28:20
Актив 3	Хробак ("Worm")	59,4087715148926	59,4087715148926	59,4087715148926	59,41; Високий ризик (1,0); Критичний ризик (0,0)	09.01.2025 14:28:20
Актив 3	Вимагач ("Ransomware")	87,1844482421875	87,1844482421875	87,1844482421875	87,18; Критичний ризик (1,0)	09.01.2025 14:28:20
Актив 3	Троян ("Trojan-malware")	100	100	100	100,00; Критичний ризик (1,0)	09.01.2025 14:28:20

Рис. 13. Звіт з оцінок рівня ризику

5. Висновки і перспективи подальших досліджень

Таким чином, розроблено структурну модель системи оцінювання ризиків, яка за рахунок структурних компонент підсистем клієнтської та серверної обробки даних, а також складових їх модулів авторизації експертів, експертного оцінювання, збереження даних, ідентифікації експертів та загроз, формування параметрів для подальшого оцінювання, фазифікації експертних оцінок, оцінювання рівня ризиків і генерації звіту, в яких реалізовано запропоновані методи [8, 10], дозволила розробити алгоритм та відповідний програмний застосунок для автоматизації процесу оцінювання рівня ризику і на підставі отриманих даних раціонально розподілити наявні ресурси необхідні для захисту.

Також на основі запропонованої моделі розроблено базовий алгоритм і відповідне програмне забезпечення оцінювання у вигляді прикладної програмної системи – «СИСТЕМА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ», яка безпосередньо дозволяє реалізовувати процес оцінювання рівня ризику і надавати звіти для подальшого прийняття рішення, щодо першочерговості обробки тих ризиків, які є найактуальнішими.

Список використаної літератури

1. «Guide for Conducting Risk Assessments. Recommendations of the National Institute of Standards and Technology [Joint Task Force Transformation Initiative]». National Institute of Standards and Technology Special Publication 800-30 Rev. 1, Falls Church: Natl. Inst. Stand. Technol, 2012, p. 95. https://doi.org/10.6028/NIST.SP.800-30r1

2. Risk management - Principles and guidelines. AS/NZS ISO 31000:2009. Nundah : ISO working group – risk management Terminology. 2009. p. 35. https://www.standards.govt.nz/shop/ASNZS-ISO-310002009

3. FAIR Institute. Factor Analysis of Information Risk (FAIR) Framework. Available at: https://www.fairinstitute.org/

4. Alberts, C.; Dorofee, A. OCTAVE Threat Profiles. Software Engineering Institute, Carnegie Mellon University. Available online: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/AlbertsDorofee_OCTAVEThreatProfiles.pdf.

5. CCTA. "CRAMM User Guide." Central Computer and Telecommunications Agency, UK, 1996. Pp. 997–1018.

6. Buczak, A.L. and Guven, E. A. Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials. 2016. №18. Pp. 1153-1176. https://doi.org/10.1109/COMST.2015.2494502.

7. Jiali Wang, Martin Neil, Norman Fenton. Bayesian Network Approach for Cyber Risk Assessment. Computers & Security. Vol. 89, 2020. https://doi.org/10.1016/j.cose.2019.101659

8. Oleksandr Evgeniyovych, Korystin, Oleksandr, Korchenko, Svitlana, Kazmirchuk, Serhii, Demediuk, & Oleksandr Oleksandrovych, Korystin. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory, International Journal of Computer Network and Information Security (IJCNIS). 2024. №16 (1). Pp. 24-34. https://doi.org/10.5815/ijcnis.2024.01.02.

9. Korchenko, A.G. Construction of information protection systems on fuzzy sets. Theory and practical solutions, Kiev: «MK-Press». 2006. p. 320.

10. Morklyanik, B., Korchenko, O., Kubiv, S., Kazmirchuk, S., & Teliushchenko, V. (2023). The method of phasification of intervals for solving cybersecurity assessment tasks at critical infrastructure facilities. Ukrainian Scientific Journal of Information Security. 2023. №29 (3). Pp. 103-110.