ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

УДК 004.056:338 DOI: https://doi.org/10.30837/2522-9818.2025.3.166

А. Тімошин, Л. Калєніченко, Ю. Гнусов, І. Хавіна, М. Цуранов, І. Довгань

ІНТЕГРОВАНА МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ AHP ТА БАЙЄСОВИХ МЕРЕЖ

Предмет дослідження – управління ризиками інформаційної безпеки в умовах сучасного цифрового середовища, де необхідна інтеграція стратегічних та тактичних підходів для забезпечення адаптивного захисту. **Мета роботи** – розробка гібридної моделі управління кіберризиками шляхом поєднання методологічного аналізу, експертних оцінок, ймовірнісного моделювання та технічного моніторингу. **Завдання дослідження** полягають у: (1) аналізі взаємодоповнюваності методології CRAMM і систем SIEM; (2) побудові процедури кількісної пріоритезації загроз і вразливостей на основі аналітичного методу ієрархій (AHP); (3) інтеграції отриманих оцінок у байєсові мережі (BN) для ймовірнісного прогнозування ризиків; (4) реалізації запропонованого підходу за допомогою сучасних інструментів автоматизації. Методи, використані в роботі, включають: методологію CRAMM для ідентифікації активів, загроз і вразливостей; AHP Томаса Сааті для кількісної оцінки пріоритетів на основі експертних суджень із вимірюванням узгодженості за допомогою коефіцієнта конкордації Кендалла; математичне моделювання причинно-наслідкових зв'язків за допомогою байєсових мереж (BN); а також використання систем класу SIEM для оперативного моніторингу подій безпеки. Практична реалізація підходу здійснювалася за допомогою Python, зокрема бібліотек Numpy, SciPy, pgmpy, та веб-інтерфейсу Streamlit. **Результати.** Розроблено інтегрований підхід, що об'єднує CRAMM, AHP, BN та SIEM у єдину адаптивну систему управління ризиками. Показано, що AHP дозволяє перетворити суб'єктивні експертні оцінки в об'єктивні вагові коефіцієнти, що підвищує надійність аналізу. На основі цих даних побудовано байєсову мережу для оцінки ризику фінансових збитків, яка враховує наявність загрози, вразливості та можливий інцидент. Модель реалізовано програмно, продемонстровано процес факторизації спільного розподілу та маргіналізації прихованих змінних для отримання апостеріорних ймовірностей. Веб-інтерфейс на базі Streamlit забезпечує зручність використання інструменту непрофесійними користувачами. **Висновки.** Запропонований гібридний підхід дозволяє ефективно поєднати стратегічне планування (CRAMM), експертні оцінки (AHP), ймовірнісне моделювання (BN) та оперативний моніторинг (SIEM), формуючи проактивну, науково обґрунтовану систему управління ризиками. Така інтеграція забезпечує високий рівень адаптивності та точності в умовах динамічного загрозного ландшафту, що робить модель практично застосовною для організацій різного рівня.

Ключові слова: Методологія CRAMM, Системи SIEM, Аналітичний метод ієрархій (AHP), Байєсові мережі (BN), Експертні оцінки, Аналіз загроз та вразливостей.

Вступ

У сучасному цифровому середовищі кібербезпека набуває стратегічного значення, виходячи за межі технічних аспектів і стаючи невід'ємною складовою національної безпеки, економічної стійкості та захисту прав громадян. Хоча традиційно управління кіберризиками сприймається як прерогатива держави, реалії глобалізованого кіберпростору, постійне ускладнення атак та швидкий технологічний прогрес ставлять під сумнів ефективність виключно регульованого державного підходу. Державні структури часто відстають від темпів розвитку загроз, обмежені в ресурсах та експертній компетенції, тоді як самі загрози носять транснаціональний характер і вимагають оперативної, гнучкої та міжсекторної взаємодії. У цих умовах приватний сектор, який є лідером інновацій у сфері IT-безпеки, виступає ключовим партнером у забезпеченні комплексного захисту.

Ефективність сучасних систем управління ризиками інформаційної безпеки значною мірою базується на міжнародних стандартах, зокрема ISO/IEC 27005, який визнано одним із найповніших підходів до структурованого аналізу ризиків [6]. Однак, як показують дослідження, успішне впровадження таких стандартів вимагає інтеграції з гнучкими методологічними та технічними інструментами [19]. У контексті кібербезпеки велике значення має також аналітика великих даних, яка дозволяє поєднувати стратегічне планування з оперативним реагуванням [23].

Мета статті – розробити та обґрунтувати інтегрований гібридний підхід до управління

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33) ISSN 2524-2296 (online)

ризиками інформаційної безпеки, який поєднує переваги методологічного аналізу, експертних оцінок, ймовірнісного моделювання та реального часу моніторингу для формування адаптивної, проактивної системи захисту.

Завдання дослідження полягає у:

– аналізі ролі та взаємодоповнюваності методології CRAMM і систем SIEM у стратегічному та тактичному управлінні ризиками;

– розробці процедури кількісної пріоритезації загроз та вразливостей на основі аналітичного методу ієрархій (AHP) із вимірюванням узгодженості експертних думок;

– побудові ймовірнісної моделі управління ризиками за допомогою байєсових мереж (BN) з використанням даних, отриманих через AHP;

– демонстрації практичної реалізації запропонованого підходу з використанням сучасних інструментів автоматизації (Python, pgmpy, Streamlit).

1. Аналіз останніх досліджень і публікацій

На даний час розроблені потужні методології оцінки та управління ризиками інформаційної безпеки. Одна з таких методологій – це CRAMM, яка розроблена у Великій Британії. Вона фокусується на систематичному аналізі активів організації, ідентифікації загроз та вразливостей, а також оцінці потенційного впливу ризиків, що описується в детальних посібниках та документації. Ці матеріали надають покрокові інструкції щодо ідентифікації та оцінки активів, виявленні загроз та вразливостей, оцінки ризиків, вибору та впровадженні заходів безпеки на основі каталогів, моніторинг та перегляд. Програмний комплекс CRAMM версії 5.0 використовує кількісні та якісні методи оцінки ризиків. Ретельний аналіз методів CRAMM наведено в роботі [1].

В деяких роботах пропонуються методи і засоби оцінювання ризиків та управління ризиками інформаційної безпеки для конкретних сфер діяльності. Наприклад в роботі [2] проаналізовано шляхи зменшення рівня ризиків у сфері електронного бізнесу, де особливо вразливими є інформаційні та фінансові транзакції. Математична модель ризиків в цій роботі спирається на схеми незалежних випробувань Бернуллі та схему Пуассона. Тобто, здійснюється ймовірнісне прогнозування результатів. Ще одним прикладом окремого випадку щодо безпеки даних є робота [3], яка досліджує сучасні підходи та інструменти для забезпечення безпеки API у веб-застосунках, реалізованих за допомогою JavaScript. Дослідженню кібербезпеки інформаційних ресурсів підприємства в IT-галузі присвячена робота [4], в якій для мінімізації ризиків інформаційної безпеки використовується такий показник, як рівень витрат (в матеріальному або вартісному вираженні) на відновлення працездатності системи у разі її відмови за одним або декількома напрямками. Така модель зводиться до вирішення багатопараметричної задачі лінійного програмування. Взагалі, формула "*Ризик = Імовірність загрози × Потенційний збиток*" є однією з найпоширеніших у сфері управління ризиками. Вона використовується у різних стандартах і підходах до оцінки інформаційної безпеки, фінансового аналізу та управління ризиками. Наприклад, в роботі [5], розвинуто дискретну ймовірнісну модель багатокритеріального аналізу ушкодженості об’єкта захисту за припущення про незалежність атак та засобів захисту. Для випадкової величини кількості ушкоджень за фіксований проміжок часу отримано представлення у вигляді суми біноміально розподілених випадкових величин, які залежать від параметрів атак та захисту. Описано випадкові величини економічних втрат, часу відновлення та затрат на відновлення, для яких знайдено в аналітичному вигляді математичні сподівання та дисперсії.

У статті [6] розглядається структура оцінки ризиків інформаційної безпеки (ISRA), яка є основою для порівняння різних методів оцінки ризиків. Автори пропонують комплексну структуру, яка дозволяє порівнювати різні методи, додаючи нові завдання з кожного розглянутого методу. Якщо завдання було присутнє в дослідженому методі ISRA, але не в CURF, воно додавалося до моделі, що давало змогу виміряти повноту досліджуваних методів. За результатами дослідження, "ISO/IEC 27005 Information Security Risk Management" є найбільш повним підходом на даний момент.

Одним з показників, який відображає поточний стан кібербезпеки держави є Національний індекс кібербезпеки (National Cyber Security Index, NCSI). Це глобальний оперативний індекс, що оцінює готовність країн запобігати кіберзагрозам та керувати кіберінцидентами. NCSI також є базою даних із загальнодоступними доказовими матеріалами та інструментом для нарощування національного потенціалу кібербезпеки. В роботі [7] пропонується

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

комплекс формальних математичних моделей, які забезпечують опис завдання визначення національного рівня цифрового розвитку країн з урахуванням національного рівня кібербезпеки та кіберзахисту з позицій системного аналізу. Потрібно зауважити, що NSCI структуровано 46 індикаторами, з яких найбільш суттєвими є розробка політики кібербезпеки, аналіз кіберзагроз, професійний розвиток, захист цифрових послуг, електронна ідентифікація та довірчі послуги, захист персональних даних, боротьба з кіберзлочинністю, військові кібероперації. Зокрема, Україна посідає 15-те місце в цьому рейтингу з індексом 80.83. Це свідчить про відносно високий рівень кібербезпеки в країні.

З аналізу наявних підходів випливає, що більшість із них або надто загальні, або надто спеціалізовані, або засновані на статичних моделях, що не враховують динаміку кіберзагроз. Крім того, спостерігається розрив між стратегічними методологіями (наприклад, CRAMM) та тактичними системами (наприклад, SIEM), що призводить до фрагментарності в управлінні ризиками.

На основі виявлених прогалин, актуальною є задача розробки інтегрованого гібридного підходу до управління ризиками інформаційної безпеки, який:

– поєднує переваги методологічного аналізу (CRAMM) та оперативного моніторингу (SIEM);

– перетворює суб’єктивні експертні оцінки в об’єктивні кількісні показники за допомогою аналітичного методу ієрархій (AHP) із перевіркою узгодженості (коефіцієнт Кендалла);

– будує ймовірнісну модель причинно-наслідкових зв’язків між загрозами, вразливостями та інцидентами за допомогою байєсових мереж (BN);

– забезпечує автоматизовану реалізацію моделі з використанням сучасних інструментів (Python, pgmpy, Streamlit) для підвищення доступності та точності аналізу.

2. Матеріали та методи

2.1. CRAMM і SIEM як інструменти управління ризиками в інформаційній безпеці

Ефективне управління ризиками в інформаційній безпеці передбачає поєднання методологічних підходів до аналізу та оцінки загроз із практичними інструментами моніторингу й реагування. У цій площині важливу роль відіграють такі рішення, як програмний комплекс CRAMM та системи управління інформаційною безпекою класу SIEM.

CRAMM (CCTA Risk Analysis and Management Method) – це одна з перших стандартизованих методик аналізу та управління ризиками у сфері інформаційних технологій [1]. Вона була розроблена у Великій Британії Центральним агентством телекомунікацій (Central Computer and Telecommunications Agency, CCTA) ще у 1980-х роках та продовжує застосовуватись у сучасних версіях, зокрема у CRAMM 5.0. Її трьохетапний процес (ідентифікація активів, аналіз загроз, розрахунок ризиків) детально описаний у офіційному користувацькому посібнику [13]. Хоча CRAMM забезпечує комплексний підхід, його ефективність залежить від якості експертних суджень, що потребує доповнення формальними методами їхньої валідації [16].

Основна ідея CRAMM полягає у трьохетапному підході до управління ризиками:

1. Ідентифікація активів – визначення інформаційних ресурсів, технічних засобів та процесів, які підлягають захисту.

2. Аналіз загроз і вразливостей – оцінка можливих сценаріїв атаки чи випадкових інцидентів, що можуть вплинути на активи.

3. Розрахунок ризиків і вибір контрзаходів – визначення рівня ризику шляхом співставлення вартості активу, ймовірності реалізації загрози та потенційних наслідків.

CRAMM реалізує підхід, що поєднує формалізовані питання-анкети для експертів та базу знань із типовими загрозами та контрзаходами. Важливо, що методика орієнтована не лише на оцінку технічних аспектів безпеки, але й на управлінські та організаційні заходи. Таким чином, CRAMM забезпечує комплексний підхід до управління ризиками, хоча її головним недоліком залишається висока залежність від суб’єктивності експертних оцінок.

Системи управління інформаційною безпекою класу SIEM (Security Information and Event Management) з’явилися на початку 2000-х років як відповідь на потребу в централізованому зборі та аналізі подій безпеки. На відміну від CRAMM, що має аналітично-методологічний характер, SIEM орієнтовані на практичне виявлення та попередження інцидентів у режимі реального часу.

Системи SIEM є ключовим інструментом сучасного моніторингу безпеки, забезпечуючи збір, кореляцію подій і автоматизоване реагування [14].

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Згідно з останніми дослідженнями, їх еволюція включає інтеграцію з SOAR та використання машинного навчання для виявлення аномалій [23]. Особливо ефективні SIEM-системи при протидії складним атакам, таким як DDoS, де необхідна швидка кореляція подій [24].

Функціонал сучасних SIEM-систем зазвичай включає:

– збір та нормалізація даних з різних джерел: журнали подій ОС, мережеві пристрої, антивіруси, системи контролю доступу тощо.

– кореляція подій з метою виявлення складних атак, які неможливо розпізнати за допомогою окремих повідомлень.

– виявлення інцидентів і формування сповіщень для аналітиків безпеки.

– аналіз та звітність, що дає змогу формувати картину загроз і відповідати вимогам регуляторів.

– інтеграція з системами реагування, включно з автоматизацією дій (SOAR – Security Orchestration, Automation and Response).

Розвиток SIEM-систем останніх поколінь включає елементи машинного навчання та поведінкової аналітики, що дає можливість виявляти аномальні дії користувачів чи внутрішні загрози.

Попри відмінності у підходах, CRAMM і SIEM можна розглядати як взаємодоповнюючі інструменти в рамках загальної системи управління ризиками:

– CRAMM відповідає за методологічний рівень: виявлення цінних активів, аналіз можливих загроз і формування політики безпеки.

– SIEM реалізує практичний рівень: моніторинг середовища, збір доказів інцидентів і їх оперативне виявлення.

– об’єднавши результати CRAMM та SIEM, організація отримує як стратегічну, так і тактичну складову управління ризиками: від оцінки потенційних загроз – до їхнього реального підтвердження у вигляді подій.

Таким чином, CRAMM можна розглядати як інструмент планування та оцінки ризиків, тоді як SIEM – як інструмент оперативного контролю та моніторингу. У комплексі вони створюють основу для більш складних моделей аналізу, зокрема із залученням багатокритеріальних методів (AHP) та ймовірнісних підходів (Bayesian Networks), що розглядатимуться у наступних розділах статті.

2.2. Метод попарних порівнянь

Аналітичний метод ієрархій (AHP), запропонований Т. Сааті [16], є одним із найпоширеніших багатокритеріальних методів прийняття рішень у сфері інформаційної безпеки. Важливим елементом є оцінка узгодженості експертних думок, для чого використовується коефіцієнт конкордації Кендалла [8]. Як показано в [10], цей підхід дозволяє кількісно оцінювати ризики, зменшуючи суб’єктивність. Для покращення узгодженості матриць попарних порівнянь можуть застосовуватися алгоритми оптимізації [11]. Останні дослідження демонструють, що комбінація AHP із байєсовими мережами дозволяє проводити кількісну оцінку ризиків навіть за умов неповних даних [25].

2.2.1. Класична модель метода Сааті. Припустимо, що перелік загроз T сформовано $\left(|T|=n\right)$, тоді їх ранжування для інформаційної системи може бути виконано різними способами. Якщо експерти досягли спільної згоди щодо класифікації попарним порівнянням загроз за рівнем ризику, то складається квадратна матриця попарних порівнянь A розміром $\left(n\times n\right)$. Елементи матриці $A=\left(a_{ij}\right)$ – це експертні оцінки важливості одного елемента щодо іншого. Чим більше значення $a_{ij}>1$ (як правило, це цілі числа), тим елемент (загроза) T_i важливіший за T_j. При цьому, $a_{ji}=1/a_{ij}$, $a_{ii}=1$. Часто використовується 9-бальна шкала Сааті: 1 – однакове значення; 3 – слабка перевага; 5 – сильна перевага; 7 – дуже сильна перевага; 9 – абсолютна перевага. Проміжні значення 2, 4, 6, 8 використовуються для уточнень. Побудована таким чином матриця попарних порівнянь називається класичною матрицею Сааті. Для отримання ваги відносної важливості кожної із загроз (вектора ваг), достатньо нормалізувати класичну матрицю (кожен елемент поділити на суму відповідного стовпця) і обчислити середнє значення по рядках.

2.2.2. Реалізація метода Сааті на основі матриці ранжувань. Інший підхід щодо реалізації метода попарних порівнянь починається з побудови *матриці ранжування* загроз $R=\left(r_{ij}\right)$ (іншими словами, таблиці експертних оцінок). Рядкам матриці ранжування відповідають об’єкти (загрози), а стовпцям – експерти (надалі, E). Припустимо, що

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

кількість загроз $|T| = n$, а кількість експертів $|E| = m$. Тоді маємо матрицю $R(n \times m)$. Чисельність групи експертів, як правило, становить 7–8 осіб. Кожний експерт заповнює свій стовпець, оцінюючи загрози шляхом надання їм рангів. Ранжування працює так, що 1 – це ранг для найбільш небезпечної загрози; n – ранг для найменш небезпечної загрози; іншим загрозам надаються якісь проміжні (цілі) значення на розсуд експерта. Більшість методик AHP припускають, що вищий пріоритет загрози має нижчий ранг. Це відповідає стандартам оцінки ризиків.

Для визначення ступеня згоди між експертами щодо ранжування загроз, використовують коефіцієнт конкордації Кендалла [8].

Наступним кроком обчислюють матриці попарних порівнянь A^r $\left(r = \overline{1,m}\right)$ по кожному експерту. Порівнюються між собою ранги матриці ранжування, окремо по кожному стовпцю, і формується квадратна матриця розміром $(n \times n)$. Тобто, кожному стовпцю відповідає матриця. Якщо загроза T_i більш небезпечна ніж T_j, то приймають $a_{ij} = 1$, $a_{ji} = 0$, $a_{ii} = 0,5$, $i, j = \overline{1,n}$. Щоб дістати групову оцінку ступеня впливу кожної з загроз на результат, будується матриця математичних сподівань X_r оцінок кожної з пар чинників. Якщо матриці попарних порівнянь A_r пораховані, то матриця математичних сподівань є сума цих матриць помножена на $1/m$. Завдання оцінювання коефіцієнтів відносної важливості зводиться до визначення максимального власного значення матриці X_r та відповідного йому власного вектора k з використанням ступеневого (ітераційного) алгоритму [9, 10].

Подальша процедура виявлення найбільш критичної загрози полягає в оцінки вразливостей. Спочатку формується перелік вразливостей і далі експерти, кожний окремо, оцінюють вразливості по тому ж самому принципу, як це було у випадку загроз. Далі також визначають ступень згоди між експертами, і, остаточно, обчислюють вектор коефіцієнтів відносної важливості вразливостей.

На підставі векторів коефіцієнтів відносної важливості загроз та коефіцієнтів відносної важливості вразливостей будують порівняльну матрицю (таблицю) загроз та вразливостей. Рядки таблиці відповідають вразливостям, стовпці – загрозам. Якщо елемент вектора загроз T є більшим за відповідний елемент вектора вразливостей W, то в таблиці на перетині стовпця загроз з рядком вразливостей ставиться знак "+", у протилежному випадку – "0". Та загроза, яка має найбільше число поєднань з вразливостями (стовпець з найбільшою кількістю знаку "+") є самою пріоритетною [10].

Отже, загальна схема оцінки ризиків методом попарних порівнянь представлена на рис. 1.

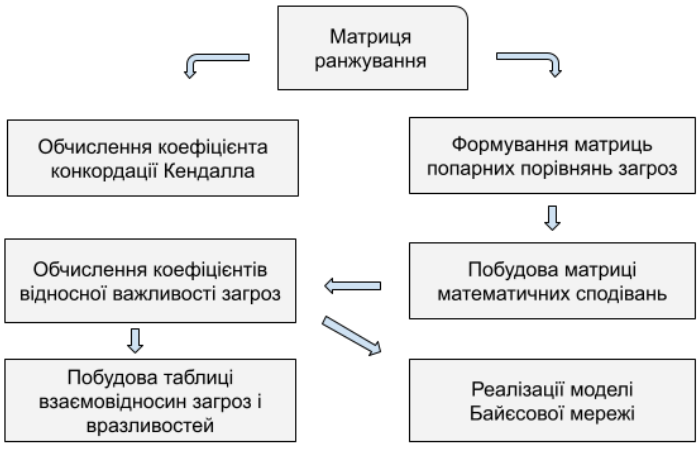

Рис. 1. Загальна схема оцінки ризиків методом попарних порівнянь

2.3. Математична модель BN

Байєсові мережі (BN) є потужним інструментом моделювання причинно-наслідкових зв'язків у системах управління ризиками [17]. Вони дозволяють враховувати невизначеність і динаміку загрозного середовища, що робить їх особливо придатними для аналізу кіберризиків [18]. Як показано в [20],

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

гібридні моделі, що поєднують AHP і BN, забезпечують високу точність прогнозування. Посилання на референсну модель управління ризиками [21] підтверджує, що BN можуть бути частиною повноцінної системи ISRM. Нещодавні дослідження також підтверджують їхню ефективність у випадках неповних даних [25].

Нехай маємо множину випадкових змінних (вузлів) $X = X_1,\ldots,X_n$. Байєсова мережа (BN) – це орієнтовний ациклічний граф $G=(X,E)$, де E – множина дуг.

Кожен вузол X_i має умовний розподіл

$$P(X_i \mid Pa(X_i)), \tag{8}$$

де $Pa(X_i)$ – множина "батьків" вузла X_i у G (вузли з яких у графі виходять стрілки в X_i).

Повна факторизація для спільного розподілу така:

$$P(X_i,\ldots,X_n)=\prod_{i=1}^{n}P(X_i)\mid Pa(X_i)) \tag{9}$$

На практиці явно побудувати цей розподіл досить складно, так як кількість комбінацій зростає експоненційно з числом вузлів у мережі. Це робить прямий обчислювальний підхід практично неможливим навіть для відносно невеликих моделей. Щоб уникнути цієї проблеми, у байєсових мережах застосовують спеціальні алгоритми *інференсу*, які дозволяють отримати потрібні апостеріорні ймовірності без явного формування всього розподілу. Серед таких алгоритмів можна виділити:

– точні методи: Variable Elimination, Junction Tree;

– наближені методи: Sampling (Gibbs Sampling, Likelihood Weighting), Belief Propagation.

Байєсові мережі забезпечують ефективне обчислення умовних ймовірностей, використовуючи локальні залежності між змінними та *факторизацію* глобального розподілу, або іншими словами – "структурну формулу" моделі.

У байєсовій мережі ми розділимо вузли графу так: $X = Q\cup H\cup E$, де Q – запитувані (цільові) вузли, H – приховані вузли, E – спостережені вузли (evidence). Приховані вузли (hidden variables) – це ті змінні X_i, для яких ми не маємо фактичних даних, але вони впливають на залежності між запитуваними і спостереженими змінними.

І тепер, основна задача – знайти маргінальний (умовний) розподіл цільових вузлів при наявності спостережень e:

$$P(Q\mid e)=\frac{\sum_H P(Q,H,e)}{\sum_{Q,H}P(Q,H,e)} \tag{10}$$

Тобто, інференс зводиться до *маргіналізації* – сумування по всіх можливих комбінаціях прихованих змінних H. Зробимо уточнення чисельнику формули (10):

$$\sum_H P(Q,H,e)=\sum_H\prod_{i=1}^{n}P(X_i|Pa(X_i)) \tag{11}$$

Знаменник формули (10) є просто нормалізаційною константою.

Нагадаємо, що марковським покриттям (MB – Markov blanket) вузла X_i вважається мінімальна множина вузлів, яка робить X_i умовно незалежним від усіх інших у мережі. Воно складається з "батьків" вузла X_i (тобто, це $Pa(X_i)$), "дітей" вузла X_i (це $Ch(X_i)$) і "батьків дітей" вузла X_i. Таким чином,

$$MB(X_i)=Pa(X_i)\cup Ch(X_i)\cup\bigcup_{Y\in Ch(X_i)}Pa(Y) \tag{12}$$

Тим самим ми підкреслюємо те, що нам важливі значення вузлів із $MB(X_i)$, і інші вузли мережі G не несуть додаткової інформації про вузол X_i. Це є ключовим моментом в інференсі, тобто обчисленні апостеріорних ймовірностей P(гіпотеза | спостереження), коли знання про вузли оновлюються при отриманні нових даних.

Серед ключових моментів побудови байєсової мережі є матриця умовних ймовірностей (CPT – Conditional Probability Table), рядки якої відповідають можливим комбінаціям значень "батьків" $Pa(X_i)$, а стовпці – можливим значенням самого вузла X_i. Отже,

$$\Theta_i=\begin{bmatrix} P(X_i=x_{i1}\mid Pa(X_i)=p_{i1} & \cdots & P(X_i=x_{im}\mid Pa(X_i)=p_{i1}\\ \vdots & \ddots & \vdots \\ P(X_i=x_{i1}\mid Pa(X_i)=p_{ik} & \cdots & P(X_i=x_{im}\mid Pa(X_i)=p_{ik}\end{bmatrix}. \tag{13}$$

При цьому,

$$\sum_{j=1}^{m}P(X_i=x_{ij}|Pa(X_i)=p_{ir})=1,\forall r\in\{1,\ldots,k\}. \tag{14}$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

CPT задає локальні правила ймовірності для кожного вузла, в той час коли маргінальні розподіли дозволяють об'єднати всі локальні ймовірності у глобальний розподіл мережі, щоб відповісти на питання "яка ймовірність певної події/стану вузла Q, якщо ми знаємо деякі спостереження e ".

3. Результати дослідження та експерименти

3.1. Практична реалізація методу попарних порівнянь

Обчислення коефіцієнтів відносної важливості на основі матриці ранжування можна здійснити з використанням бібліотек Python, і, веб-інтерфейсу Streamlit для зручності роботи експертів [11, 15].

Будемо вважати, що ми отримали оцінки загроз від експертів і маємо матрицю ранжувань $R = (r_{ij})$. Приклад матриці ранжувань в табличному виді представлено в табл. 1.

Таблиця 1. *Формування матриці експертних оцінок*

	E1	E2	E3	E4	E5	E6
T1	1	3	2	3	3	3
T2	2	2	4	2	4	2
T3	3	1	5	1	2	1
T4	4	6	6	5	6	4
T5	5	5	1	4	1	5

де T – загрози, E – експерти. Нагадаємо, що 1 – це ранг для найбільш *небезпечної* загрози. Треба зауважити, що при *класичному* ранжуванні кожній загрозі надається унікальний ранг. У випадку *рангування з повторами* експерт може вказати однаковий ранг для загроз, якщо на його думку ці загрози мають однакову важливість. У цьому випадку, при розрахунку коефіцієнта Кендалла або створенні матриць попарних порівнянь це допустимо. При однакових рангах, в матриці попарних порівнянь, пара оцінюється як 0.5 (часткова перевага).

Програма на Python обчислення коефіцієнтів відносної важливості (SAAT-ваг) буде складатися з декілька модулів (функцій). Перша функція, kendall_concordance(expert_ratings), рахує коефіцієнт конкордації Кендалла (Kendall's W) для визначення ступеня згоди між експертами. Параметром функції є матриця ранжувань. Формула для обчислення Kendall's W:

$$K_{con} = S / S_{\max} \ , \qquad (1)$$

де S – дисперсія сум ранжувань (по кількості експертів), $S_{\max} = \frac{n^3 - n}{12}$ – максимально можлива сума квадратів відхилень (n – кількість загроз). Обчислення середніх рангів для кожної загрози (по рядкам транспонованої матриці R) реалізовано в бібліотеки Numpy (Python) так → mean_ranks = np.mean(matrix.T, axis=0). Сума квадратів відхилень середніх рангів від середнього значення рангу → S = np.sum((mean_ranks – np.mean(mean_ranks))**2).

Для перевірки значущості коефіцієнта використовується критерій χ-квадрат, який обчислюється так:

$$\chi^2 = m \cdot (n-1) \cdot K_{con} \, . \qquad (2)$$

Значення χ^2 порівнюється з критичним значенням χ^2_{crit} при рівні значущості α і ступенях свободи $n-1$. Якщо $\chi^2 > \chi^2_{crit}$, то узгодженість оцінок експертів вважається статистично значущою. Як правило, рівень значущості α вибирають 0.05, тобто 95% довірчий рівень. Для визначення χ^2_{crit} скористаємось кодом Python, який формує таблицю критичних значень для зазначених рівнів значущості і ступенів свободи. Для цього використовується модуль chi2 бібліотеки scipy.stats. Остаточно, функція kendall_concordance залишає повідомлення зі значеннями χ^2, χ^2_{crit} та висновком про узгодженість оцінок експертів.

Наступна функція,
create_pairwise_comparison_matrix(expert_ratings),
формує матриці попарних порівнянь загроз. Елементи матриці визначаються визначаються за формулою (1).

$$A_r = (a^r_{ij}) = \begin{cases} 1, & \text{якщо } T^r_i < T^r_j \\ 0.5, & \text{якщо } T^r_i \approx T^r_j \\ 0, & \text{якщо } T^r_i > T^r_j \end{cases} \qquad (3)$$

де r – номер експерта,

T^r_i – ранг T_i-ої загрози E_r-го експерта.

Функція create_pairwise_comparison_matrix реалізована за рахунок звичайних операторів циклу та умовного оператора.

Матриця математичних сподівань X обчислюється функцією
Python build_expectation_matrix(pairwise_matrices).
Її параметром є список квадратних матриць попарних порівнянь, pairwise_matrices. Фактично,

$$X_T = \frac{1}{m} \sum A_r \, , \qquad (4)$$

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

і тому ця функція містить звичайний цикл для додавання всіх матриць A_r.

Формування вектора відносної важливості $\vec{k} = [k_1, k_2, \ldots, k_n]^T$ зводиться до визначення максимального власного значення матриці X_T та відповідного йому власного вектора $\vec{k}$ з використанням ступеневого (ітераційного) алгоритму.

Схема ітераційного алгоритму наступна:

1. Початкова умова $t = 0$, $k^{[0]} = (1,1,\ldots,1)^T$.

2. Рекурентні співвідношення задані формулами (2):

$$\lambda^{[t]} = (1,1,\ldots,1) \cdot Y^{[t]}, \quad k^{[t]} = \frac{1}{\lambda^{[t]}} \cdot Y^{[t]}, \qquad (5)$$

де $\lambda^{[t]} = X \cdot k^{[t-1]}$, $t = \overline{1,m}$.

3. Ознакою закінчення алгоритму є умова:

$$\max \left| k^{[t]} - k^{[t-1]} \right| < E, \qquad (6)$$

де E – задана точність (наприклад, 0.001).

Функція iterative_algorithm(X, epsilon=1e-3) обчислює вектор $\vec{k}$ відповідно до алгоритму.

Варіант веб-сторінки в Streamlit з розрахунками представлено на рисунку 2.

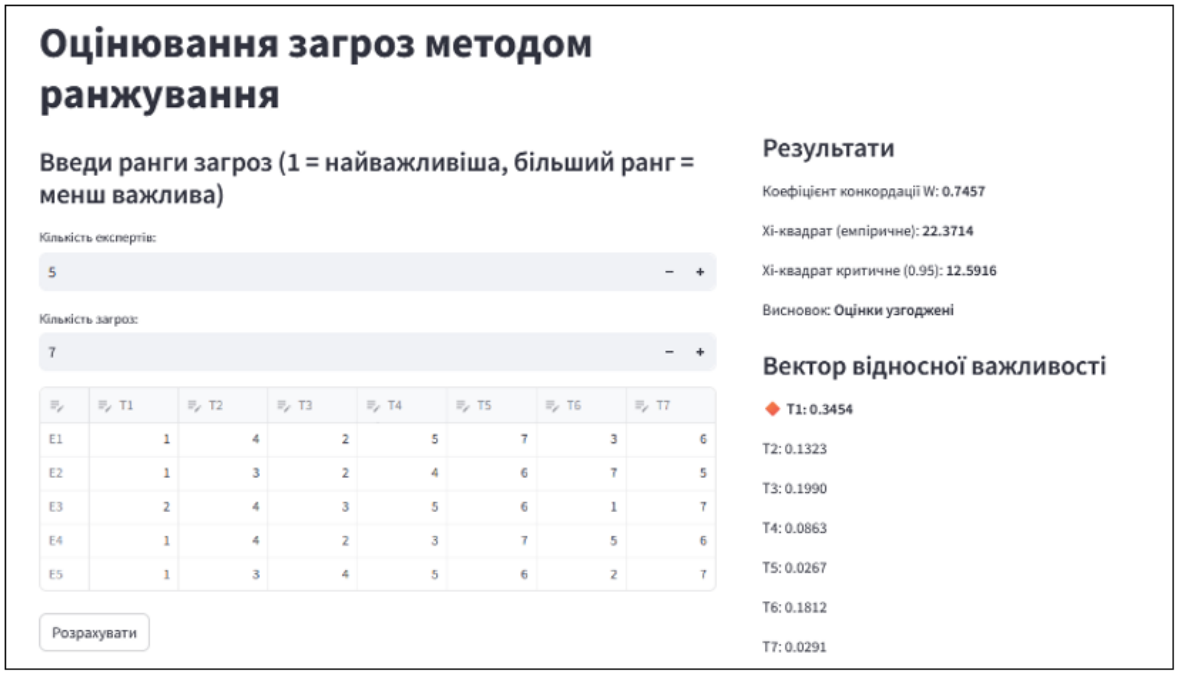

Рис. 2. Веб-інтерфейс застосунку в Streamlit для оцінювання загроз

Застосунок було протестовано на багатьох прикладах, зокрема на прикладі з 7 загрозами і 5 експертами. В результаті отримано коефіцієнт узгодженості $W = 0.7457$, який був статистично значущим при

$$\chi^2 = 22.3714 > \chi^2_{crit} = 12.5916. \qquad (7)$$

Найбільший коефіцієнт важливості мала загроза T1, що відображено у веб-інтерфейсі.

3.2. Приклад побудови баєсової мережі

Розглянемо 4 бінарні змінні (вузли):

T – загроза атаки $(\{\text{yes, no}\})$.

V – вразливість в системі $(\{\text{yes, no}\})$.

I – інцидент (проникнення/витік даних) $(\{\text{yes, no}\})$.

L – значні фінансові втрати $(\{\text{yes, no}\})$.

Нехай маємо наступний граф G (мережа ризику кіберінциденту):

$$T \to I \to L, \quad V \to I \qquad (15)$$

Поставимо задачу оцінки ризику збитків L. Тоді граф G поділиться наступним чином:

$$Q = \{L\}, \quad E = \{T, V\}, \quad H = \{I\} \qquad (16)$$

Інформація про загрози T та вразливості V може бути отримана методом AHP, який розглянуто у розділі 2.

Спільна ймовірність для всіх вузлів факторизується як:

$$P(T,V,I,L) = P(T)P(V)P(I|\ T,V)P(L|\ I) \qquad (17)$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Будуємо CPT для вузла I. Інцидент залежить від T і V, тому маємо таку таблицю:

$P(I|T,V) =$

	$V=0$	$V=1$
$T=0$	$P(I=1\|0,0)$	$P(I=1\|0,1)$
$T=1$	$P(I=1\|1,0)$	$P(I=1\|1,1)$

При цьому, $P(I=0|\ T,V)=1-P(I=1|\ T,V))$.

Збитки залежать тільки від I:

$P(L|I) =$

I	$P(L=1\|I)$
0	α
1	β

Основна задача полягає в обчисленні ймовірності:

$$P(L|\ T,V)=\sum_I P(L,I|\ T,V). \qquad (18)$$

Але, згідно попереднім міркуванням, виконаємо факторизацію:

$$P(L|\ T,V)=\sum_I P(L\,|\,I)P(I|\ T,V). \qquad (19)$$

Якщо перейти до числових значень, то нехай $\alpha=0.1,\ \beta=0.8$.

Припустимо, що

$$P(I=1|\ T=1,V=1)=0.9$$
$$P(I=1|\ T=1,V=0)=0.6$$
$$P(I=1|\ T=0,V=1)=0.5$$
$$P(I=1|\ T=0,V=0)=0.1$$

Імовірності для збитків:

$$P(L=1|\ I=1)=0.8$$
$$P(L=1|\ I=0)=0.1$$

Тоді,

$$P(L=1|\ T=1,V=1)=(0.8\cdot 0.9)+(0.1\cdot 0.1)=0.72+0.01=0.73.$$
$$P(L=1|\ T=1,V=0)=(0.8\cdot 0.6)+(0.1\cdot 0.4)=0.48+0.04=0.52.$$
$$P(L=1|\ T=0,V=1)=(0.8\cdot 0.5)+(0.1\cdot 0.5)=0.4+0.05=0.45.$$
$$P(L=1|\ T=0,V=0)=(0.8\cdot 0.1)+(0.1\cdot 0.9)=0.08+0.09=0.17.$$

Тепер можемо записати вже CPT для L після маргіналізації прихованого вузла I:

$P(L=1|T,V) =$

	$V=0$	$V=1$
$T=0$	0.17	0.45
$T=1$	0.52	0.73

Ми отримали готову таблиця умовних імовірностей, яку можна використовувати для оцінки ризику збитків L.

Наведений приклад побудови BN "T → I → L ←V" відповідає сучасним практикам моделювання кіберризиків [17]. Подібні структури використовуються в гібридних фреймворках для оцінки фінансових наслідків інцидентів [20]. Використання даних AHP для заповнення CPT підтверджується дослідженнями, що демонструють можливість інтеграції експертних оцінок у ймовірнісні моделі [25].

3.3 Реалізація побудови баєсової мережі на Python

Для реалізації BN використана бібліотека pgmpy – одна з найпоширеніших у науковому співтоваристві для роботи з ймовірнісними графічними моделями [15]. Її функціонал дозволяє будувати мережі, визначати CPT та виконувати інференс за допомогою алгоритмів, таких як Variable Elimination [17]. Подібні підходи успішно застосовуються в задачах оцінки ризиків [20].

Загальна структура коду виглядає так:

1. Створення моделі: model = BayesianNetwork([('T', 'I'), ('V', 'I'), ('I', 'L')]);
2. Вказуємо значення CPT для вузлів I та L, використовуючи клас TabularCPD;
3. Додаємо CPT до моделі: model.add_cpds(cpd_T, cpd_V, cpd_I, cpd_L);
4. Перевіряємо модель: ok = model.check_model();
5. Готуємо ймовірнісний висновок: infer = VariableElimination(model);
6. Виводимо результати:

```
q1 = infer.query(variables=['L'], evidence={'T': 1, 'V': 1})
print("\nP(L | T=1, V=1):\n", q1)
q2 = infer.query(variables=['L'], evidence={'T': 0, 'V': 1})
print("\nP(L | T=0, V=1):\n", q2)
```

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Висновки й перспективи подальшого дослідження

У статті розглянуто комплексний підхід до управління ризиками інформаційної безпеки, заснований на інтеграції методологічного планування, експертних оцінок, кількісного моделювання та технічного моніторингу. Показано, що ефективна система кібербезпеки повинна поєднувати стратегічні та тактичні інструменти, забезпечуючи як довгострокове планування, так і оперативне реагування на загрози.

Методологія CRAMM виявилася ефективним інструментом для структурованого аналізу активів, загроз і вразливостей, а також для формування політики безпеки. Однак її суб'єктивність потребує доповнення об'єктивними кількісними методами. Системи класу SIEM, навпаки, забезпечують реальний час моніторингу, кореляцію подій і швидке виявлення інцидентів, але не вирішують завдання пріоритезації ризиків на стратегічному рівні. Саме тому їх слід розглядати не як конкурентні, а як взаємодоповнюючі компоненти єдиної системи управління ризиками.

Для усунення суб'єктивності експертних оцінок запропоновано використання аналітичного методу ієрархій (AHP) за Т. Сааті, реалізованого на основі матриці ранжувань. Цей підхід дозволяє отримати вектор ваг (SAAT-ваг), що кількісно відображає пріоритетність загроз і вразливостей. Особливу увагу приділено вимірюванню узгодженості експертних думок за допомогою коефіцієнта конкордації Кендалла, що підвищує надійність результатів. Реалізація методу на Python із використанням бібліотек Numpy, SciPy та веб-інтерфейсу Streamlit робить його доступним і практично застосовним для організацій будь-якого рівня.

Найбільш інноваційним елементом дослідження є інтеграція отриманих кількісних оцінок у байєсові мережі (BN). Байєсові мережі дозволяють моделювати причинно-наслідкові зв'язки між загрозами, вразливостями, інцидентами та фінансовими збитками, забезпечуючи гнучкий імовірнісний інференс. На прикладі побудови мережі "T → I → L ← V" показано, як на основі даних AHP можуть бути сформовані таблиці умовних ймовірностей (CPT) і отримані точні оцінки ризику через маргіналізацію прихованих змінних. Використання бібліотеки pgmpy для Python дозволяє автоматизувати процес моделювання та ймовірнісного висновування.

Запропонований гібридний підхід відповідає сучасним тенденціям інтеграції стратегічних та тактичних інструментів управління ризиками [19]. Поєднання CRAMM, AHP, BN та SIEM дозволяє створити адаптивну систему, яка враховує як організаційні, так і технічні аспекти безпеки [23]. Перспективним напрямом є подальше розширення моделі шляхом інтеграції з SOAR-системами та використанням методів машинного навчання для динамічного оновлення параметрів BN [20].

Список літератури

1. Сидоркін П. Г., Горліченко С. О., Некоз В. С., Шилан М. В. Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 FOR RISK. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 2 (47). С. 41 – 47. DOI: https://doi.org/10.33099/2311-7249/2023-47-2-41-47
2. Берко А. Ю., Висоцька В. А., Рішняк І. В. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції. Інформаційні системи та мережі: [збірник наукових праць]: Видавництво Львівської політехніки. 2008. № 610 (1). С. 20 – 33. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16336/vis610inform-syst-20-33.pdf
3. Залива В. В. Методики захисту API за допомогою JavaScript: математичні моделі для підвищення безпеки. *Телекомунікаційні та інформаційні технології.* 2024. № 3 (84). С. 4 – 11. DOI: 10.31673/2412-4338.2024.030411
4. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. *Вчені записки ТНУ імені В.І. Вернадського.* 2020. Том 31 (70) № 5 С. 9–74. DOI https://doi.org/10.32838/2663-5941/2020.5/12
5. A multicriterial analysis of the efficiency of conservative information security systems / Dudykevych V., Prokopyshyn I., Chekurin V., Opirskyy I., Lakh Yu., Kret T., Ivanchenko Ye., Ivanchenko I., *Eastern-European Journal of Enterprise Technologies.* 2019.Vol. 3, Issue 9 (99). P. 6–13. DOI: https://doi.org/10.15587/1729-4061.2019.166349
6. Gaute Wangen, Christoffer Hallstensen, Einar Snekkenes. A framework for estimating information security risk assessment method completeness. *Int. J. Inf. Secur.* 2018. Vol. 17. P. 681 – 699. DOI: https://doi.org/10.1007/s10207-017-0382-0
7. Барченко Н. Л., Любчак В. О., Лаврик Т. В. Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. *КІБЕРБЕЗПЕКА: освіта, наука, техніка.* 2022. № 2(18). С. 73 – 85.

8. Amanda Gearharta, D. Terrance Booth, Kevin Sedivec and Christopher Schauer. Use of Kendall's coefficient of concordance to assess agreement among observers of very high resolution imagery. Geocarto International 2013. Vol. 28, No. 6, P. 517–526. DOI: 10.1080/10106049.2012.725775
9. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ. 2015. 288 с.
10. Дзюба Л. Ф., Чмир О. Ю. Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики. Львівський державний університет безпеки життєдіяльності. Вісник ЛДУБЖД. 2022. №26. С. 47–54. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vldubzh_2022_26_8
11. Олецький О. В. Підвищення узгодженості матриць попарних порівнянь у методі аналізу ієрархій на основі розв'язків систем лінійних алгебраїчних рівнянь. Наукові записки НаУКМА. Комп'ютерні науки. 2022. Том 5. 2022. С. 85–91. DOI: 10.18523/2617-3808.2022.5.85-91
12. Wilson, Simon and De Persis, Cristina and Bosque, José Luis and Huertas, Irene and Sillero Denamiel, Maria Remedios, Quantitative System Risk Assessment from Incomplete Data with Belief Networks and Pairwise Comparison Elicitation. URL: https://ssrn.com/abstract=4577878 (дата звернення 01.07.2025)
13. CRAMM Version 5.1 User Guide. URL: https://pdfcoffee.com/cramm-version-51-user-guide-pdf-free.html (дата звернення 01.07.2025
14. Смірнова Т. В., Константинова Л. В., Конопліцька-Слободенюк О. К., Козлов Я. О., Кравчук О. В., Козірова Н. Л., Смірнов О. А. Дослідження сучасного стану SIEM-систем. "Кібербезпека: освіта, наука, техніка" No 1(25), P. 6–18. 2024 DOI: https://doi.org/10.28925/2663-4023.2024.25.618
15. Ankur Ankan, Abinash Panda. pgmpy: Probabilistic Graphical Models using Python. 2015. URL: https://www.researchgate.net/publication/328778465_pgmpy_Probabilistic_Graphical_Models_using_Python (дата звернення 01.07.2025)
16. Saaty T. L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. *McGraw-Hill*. 1980. URL: https://www.scirp.org/reference/ReferencesPapers?ReferenceID=1895817
17. Fenton N., Neil M. Risk Assessment and Decision Analysis with Bayesian Networks. *CRC Press*. 2012. 4 p. DOI: https://doi.org/10.1080/15598608.2014.847770
18. Khakzad N., Khan F., Amyotte P. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering & System Safety*, №111, 2013. P. 81–92. DOI: https://doi.org/10.1016/j.ress.2012.10.015
19. Borg A., Feldt R., Hansson K. Cyber security risk assessments: Systematic development of a risk assessment process using the ISO. *IEC 27005 standard. Computers & Security*, № 47, P. 128–143. 2014. DOI: https://doi.org/10.1016/j.cose.2014.07.003
20. Sharma S., Singh S., Sharma A. A hybrid framework for cyber risk assessment using fuzzy AHP and Bayesian networks. *Journal of Information Security and Applications*, № 52, 102492 p. 2020. DOI: https://doi.org/10.1016/j.jisa.2020.102492
21. Cherdantseva Y., Hilton J. A reference model of information security risk management. *Proceedings of the 2013 9th International Conference on Availability, Reliability and Security (ARES)*, P. 546–555. 2013. DOI: https://doi.org/10.1109/ARES.2013.72
22. Onwuegbuzie A. J., Collins K. M. T., Jiao, Q. G. The role of theory in advanced mixed research designs. *International Journal of Multiple Research Approaches*, № 4(1), P. 8–22. 2010. DOI: https://doi.org/10.5172/mra.4.1.8
23. Akhgar B., Chalkidis G., Hessami A. G. Cybersecurity Big Data Analytics: Governance and strategic decision making in cyberspace. *Springer*. 2020. DOI: https://doi.org/10.1007/978-3-030-43541-7
24. Zargar S. T., Joshi J., Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*, 15(4), P. 2046–2069. 2013. DOI: https://doi.org/10.1109/SURV.2013.031413.00127
25. Wilson S. P., De Persis C. Quantitative system risk assessment from incomplete data with belief networks and pairwise comparison elicitation. *Risk Analysis*, 42(8), P. 1683–1702. 2022. DOI: https://doi.org/10.1111/risa.13878

References

1. Sydorkin, P. H., Horlichenko, S. O., Nekoz, V. S., Shylan, M. V. (2023), "Methods of information security risk management CRAMM and COBIT 5 FOR RISK". ["Metody upravlinnia ryzykamy informatsiinoi bezpeky CRAMM ta COBIT 5 FOR RISK"]. *Modern Information Technologies in the Sphere of Security and Defense*, № 2(47), P. 41–47. DOI: https://doi.org/10.33099/2311-7249/2023-47-2-41-47

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

2. Berko, A. Yu., Vysotska, V. A., Rishniak, I. V. (2008), "Methods and means of assessing information security risks in e-commerce systems". [Metody ta zasoby otsiniuvannia ryzykiv bezpeky informatsii v systemakh elektronnoi komertsii]. *Information Systems and Networks: [collection of scientific papers]: Lviv Polytechnic Publishing House*, 610(1), P. 20–33. available at: https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16336/vis610inform-syst-20-33.pdf
3. Zalyva, V. V. (2024), "API protection methods using JavaScript: mathematical models for enhancing security". ["Metodyky zakhystu API za dopomohoiu JavaScript: matematychni modeli dlia pidvyshchennia bezpeky"], *Telecommunication and Information Technologies*, № 3(84), P. 4–11. DOI: 10.31673/2412-4338.2024.030411
4. Karpovych, I. M., Hladka, O. M., Nakonechna, Yu. A. (2020), "Analysis of information system security risks of an IT enterprise". ["Analiz ryzykiv bezpeky informatsiinoi systemy IT-pidpryiemstva"]. *Scientific Notes of V.I. Vernadsky TNU*, № 31(70)(5), P. 9–74. DOI https://doi.org/10.32838/2663-5941/2020.5/12
5. Dudykevych, V., Prokopyshyn, I., Chekurin, V., Opirskyy, I., Lakh, Yu., Kret, T., Ivanchenko, Ye., Ivanchenko, I. (2019), "A multicriterial analysis of the efficiency of conservative information security systems". *Eastern-European Journal of Enterprise Technologies*, № 3(9)(99), P. 6–13. DOI: https://doi.org/10.15587/1729-4061.2019.166349
6. Wangen, G., Hallstensen, C., Snekkenes, E. (2018), "A framework for estimating information security risk assessment method completeness". *International Journal of Information Security*, № 17, P. 681–699. DOI: https://doi.org/10.1007/s10207-017-0382-0
7. Barchenko, N. L., Liubchak, V. O., Lavryk, T. V. (2022), "Model of indicators for assessing the national level of digitalization and cybersecurity of world states". ["Model indykatoriv otsinky natsionalnoho rivnia tsyfrovizatsii ta kiberbezpeky derzhav svitu"] *Cybersecurity: education, science, technology*, 2(18), P. 73–85.
8. Gearharta, A., Booth, D. T., Sedivec, K., Schauer, C. (2013), "Use of Kendall's coefficient of concordance to assess agreement among observers of very high resolution imagery". *Geocarto International*, № 28(6), P. 517–526. DOI: 10.1080/10106049.2012.725775
9. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V. (2015), "Information and cybersecurity: sociotechnical aspect". [Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt]. *Kyiv: DUT*. 288 p.
10. Dziuba, L. F., Chmyr, O. Yu. (2022), "Assessment of information security risks using methods of mathematical statistics". ["Otsiniuvannia ryzykiv informatsiinoi bezpeky z vykorystanniam metodiv matematychnoi statystyky"]. *Bulletin of Lviv State University of Life Safety*, № 26, P. 47–54. available at: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vldubzh_2022_26_8
11. Olietskyi, O. V. (2022), "Improving the Consistency of Pairwise Comparison Matrices in the Analytic Hierarchy Process Based on Solutions of Systems of Linear Algebraic Equations". *Scientific Notes of NaUKMA. Computer Sciences*. Vol. 5. P. 85–91. DOI: 10.18523/2617-3808.2022.5.85-91
12. Wilson, Simon, De Persis, Cristina, Bosque, José Luis, Huertas, Irene, Sillero, Denamiel, Maria, Remedios "Quantitative System Risk Assessment from Incomplete Data with Belief Networks and Pairwise Comparison Elicitation". available at: https://ssrn.com/abstract=4577878 (last accessed 01.07.2025)
13. "CRAMM Version 5.1 User Guide". available at: https://pdfcoffee.com/cramm-version-51-user-guide-pdf-free.html (last accessed 01.07.2025
14. Smirnova, T. V., Konstantinova, L. V., Konoplitska-Slobodeniuk, O. K., Kozlov, Y. O., Kravchuk, O. V., Kozirova, N. L., Smirnov, O. A. (2024), "Research on the Current State of SIEM Systems". *Cybersecurity: Education, Science, Technology*, *1*(25). P. 6–18. DOI: https://doi.org/10.28925/2663-4023.2024.25.618
15. "Ankur Ankan, Abinash Panda. pgmpy: Probabilistic Graphical Models using Python". 2015. available at: https://www.researchgate.net/publication/328778465_pgmpy_Probabilistic_Graphical_Models_using_Python (last accessed 01.07.2025)
16. Saaty, T. L. (1980), "The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation". *McGraw-Hill*. available at: https://www.scirp.org/reference/ReferencesPapers?ReferenceID=1895817
17. Fenton, N., Neil, M. (2012), "Risk Assessment and Decision Analysis with Bayesian Networks". *CRC Press*. 4 p. DOI: https://doi.org/10.1080/15598608.2014.847770
18. Khakzad, N., Khan, F., Amyotte, P. (2013), "Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches". *Reliability Engineering & System Safety*, № 111, P. 81–92. DOI: https://doi.org/10.1016/j.ress.2012.10.015
19. Borg, A., Feldt, R., & Hansson, K. (2014), "Cyber security risk assessments: Systematic development of a risk assessment process using the ISO". *IEC 27005 standard. Computers & Security*, № 47, P. 128–143. DOI: https://doi.org/10.1016/j.cose.2014.07.003

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

20. Sharma, S., Singh, S., & Sharma, A. (2020), "A hybrid framework for cyber risk assessment using fuzzy AHP and Bayesian networks". *Journal of Information Security and Applications*, № 52, 102492 p. DOI: https://doi.org/10.1016/j.jisa.2020.102492
21. Cherdantseva, Y., Hilton, J. (2013), "A reference model of information security risk management". *Proceedings of the 2013 9th International Conference on Availability, Reliability and Security (ARES)*, P. 546–555. DOI: https://doi.org/10.1109/ARES.2013.72
22. Onwuegbuzie, A. J., Collins, K. M. T., Jiao, Q. G. (2010), "The role of theory in advanced mixed research designs". *International Journal of Multiple Research Approaches*, № 4(1), P. 8–22. DOI: https://doi.org/10.5172/mra.4.1.8
23. Akhgar, B., Chalkidis, G., Hessami, A. G. (2020), "Cybersecurity Big Data Analytics: Governance and strategic decision making in cyberspace". *Springer*. DOI: https://doi.org/10.1007/978-3-030-43541-7
24. Zargar, S. T., Joshi, J., & Tipper, D. (2013), A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*, № 15(4), P. 2046–2069. DOI: https://doi.org/10.1109/SURV.2013.031413.00127
25. Wilson, S. P., De Persis, C. (2022), "Quantitative system risk assessment from incomplete data with belief networks and pairwise comparison elicitation". *Risk Analysis*, № 42(8), P. 1683–1702. DOI: https://doi.org/10.1111/risa.13878

Надійшла (Received) 05.04.2025

Відомості про авторів / About the Authors

Тімошин Анатолій Сергійович – кандидат фізико-математичних наук, доцент, Харківський національний університет внутрішніх справ, доцент кафедри інформаційних систем та технологій, e-mail: timxxvii@gmail.com, ORCID ID: https://orcid.org/0009-0005-6916-8252

Калєніченко Лідія Іванівна – доктор юридичних наук, професор, Харківський національний університет внутрішніх справ, завідувач кафедри інформаційних систем та технологій ННІ №4, e-mail: Kalenichenkolida@gmail.com, ORCID ID: https://orcid.org/0000-0003-4068-4729

Гнусов Юрій Валерійович – кандидат технічних наук, доцент, Харківський національний університет внутрішніх справ, завідувач кафедри кібербезпеки та DATA-технологій, e-mail: duke6969@i.ua, ORCID ID: https://orcid.org/0000-0002-9017-9635

Хавіна Інна Петрівна – кандидат технічних наук, доцент, Харківський національний університет внутрішніх справ, доцент кафедри кібербезпеки та DATA-технологій, e-mail: inna.khavina25@gmail.com, ORCID ID: https://orcid.org/0000-0002-1856-1186

Цуранов Михайло Віталійович –Харківський національний університет внутрішніх справ, старший викладач кафедри кібербезпеки та DATA-технологій, e-mail: ukrbear2006@gmail.com, ORCID ID: https://orcid.org/0000-0002-2115-7029

Довгань Ірина Артурівна – Харківський національний університет внутрішніх справ, викладач кафедри інформаційних систем та технологій, e-mail: dovganirisha@gmail.com, ORCID ID: https://orcid.org/0009-0001-0440-9810

Timoshyn Anatolii – Associate Professor, Kharkiv National University of Internal Affairs, Associate Professor of the Department of Information Systems and Technologies.

Kalienichenko Lidia – Doctor of Law, Professor, Kharkiv National University of Internal Affairs, Department of Information Systems and Technologies (Head of Department).

Gnusov Yurii – Candidate of technical science, Associate Professor, Kharkiv National University of Internal Affairs, Head of the Department of Cybersecurity and DATA Technologies

Khavina Inna – Candidate of technical science, Associate Professor, Kharkiv National University of Internal Affairs, Associate Professor of the Department of Cybersecurity and DATA Technologies

Tsuranov Mykhailo – Kharkiv National University of Internal Affairs, Senior Lecturer, Department of Cybersecurity and DATA Technologies

Dovhan Iryna – Kharkiv National University of Internal Affairs, Teacher of the Department of Information Systems and Technologies.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

INTEGRATED INFORMATION SECURITY RISK MANAGEMENT MODEL BASED ON AHP AND BAYESIAN NETWORKS

The **subject** of the study is information security risk management in a modern digital environment, where the integration of strategic and tactical approaches is necessary to ensure adaptive protection. The **purpose** of the work is to develop a hybrid model of cyber risk management by combining methodological analysis, expert assessments, probabilistic modeling and technical monitoring. The **objectives** of the study are: (1) analysis of the complementarity of the CRAMM methodology and SIEM systems; (2) construction of a procedure for quantitative prioritization of threats and vulnerabilities based on the analytical hierarchy process (AHP); (3) integration of the obtained estimates into Bayesian networks (BN) for probabilistic risk forecasting; (4) implementation of the proposed approach using modern automation tools. The **methods** used in the work include: CRAMM methodology for identifying assets, threats and vulnerabilities; Thomas Saati's AHP for quantitative assessment of priorities based on expert judgments with measurement of consistency using the Kendall concordance coefficient; mathematical modeling of causal relationships using Bayesian networks (BN); and the use of SIEM-class systems for operational monitoring of security events. The practical implementation of the approach was carried out using Python, in particular the Numpy, SciPy, pgmpy libraries, and the Streamlit web interface. **Results**. An integrated approach was developed that combines CRAMM, AHP, BN, and SIEM into a single adaptive risk management system. It is shown that AHP allows you to transform subjective expert assessments into objective weighting factors, which increases the reliability of the analysis. Based on these data, a Bayesian network was built to assess the risk of financial losses, which takes into account the presence of a threat, vulnerability, and a possible incident. The model is implemented programmatically, demonstrating the process of factoring the joint distribution and marginalizing latent variables to obtain posterior probabilities. The web interface based on Streamlit ensures the ease of use of the tool by non-professional users. **Conclusions**. The proposed hybrid approach allows for the effective combination of strategic planning (CRAMM), expert assessments (AHP), probabilistic modeling (BN) and operational monitoring (SIEM), forming a proactive, scientifically sound risk management system. Such integration provides a high level of adaptability and accuracy in a dynamic threat landscape, which makes the model practically applicable for organizations of various levels.

Keywords: CRAMM methodology; SIEM systems; Analytic Hierarchy Process (AHP); Bayesian Networks (BN), Expert evaluation; Threat and vulnerability analysis.

Бібліографічні описи / Bibliographic descriptions

Тімошин А.С., Калєніченко Л.І., Гнусов Ю.В., Хавіна І.П., Цуранов М.В., Довгань І.А. Інтегрована модель управління ризиками інформаційної безпеки на основі AHP та байєсових мереж. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 3 (33). С. 166–179. DOI: https://doi.org/10.30837/2522-9818.2025.3.166

Timoshyn, A., Kalienichenko, L., Gnusov, Y., Khavina, I., Tsuranov, M., Dovhan, I. (2025), "Integrated information security risk management model based on AHP and bayesian networks", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (33), P. 166–179. DOI: https://doi.org/10.30837/2522-9818.2025.3.166