Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОД ВИБОРУ ПРОЄКТУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЕКСПЕРТНОГО ОЦІНЮВАННЯ»

Виконав: студент 2 курсу, групи 1БС-24м
спеціальності 125 Кібербезпека та захист інформації
_____Єгор ДМИТРИШИН
Керівник: к. т. н., професор кафедри ЗІ
_____Наталія КОНДРАТЕНКО
«19» грудня 2025 р.
Опонент: к. т. н., доцент кафедри ПЗ
_____Денис КАТЄЛЬНІКОВ
«19» грудня 2025 р.

Допущено до захисту
В.о. зав. кафедри ЗІ
д. т. н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«19» грудня 2025 р.

Вінниця ВНТУ – 2025 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 «Інформаційні технології»
Спеціальність – 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
В. о. зав. кафедри ЗІ, д. т. н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«24» 09 2025 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Дмитришину Єгору Тарасовичу

1. Тема роботи: «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» керівник роботи: Кондратенко Наталія Романівна, к.т.н. професор кафедри ЗІ, затверджені наказом ректора ВНТУ від 24 вересня 2025 року №313.
2. Строк подання студентом роботи 19 грудня 2025 року.
3. Вихідні дані до роботи:
   - множина альтернативних проєктів СЗІ варіанти складу й конфігурації засобів захисту, архітектурних рішень та організаційних заходів;
   - експертна інформація лінгвістичні оцінки та парні порівняння альтернатив/критеріїв, надані групою фахівців з інформаційної безпеки;
   - формат результатів інтегральні нечіткі та дефазифіковані оцінки альтернатив, ранжування проєктів системи захисту інформації.
4. Зміст текстової частини: Вступ. 1. Аналіз предметної області. 2. Організація багатокритеріального вибору системи захисту інформації на основі нечіткого аналізу альтернатив за допомогою експертного оцінювання. 3. Практична реалізація. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: схема алгоритму запропонованого підходу; блок-схема алгоритму розрахунку; графік перетинів профілів альтернатив.

6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Наталія КОНДРАТЕНКО, к.т.н. професор каф. ЗІ	25.09.25	03.10.25
2	Наталія КОНДРАТЕНКО, к.т.н. професор каф. ЗІ	25.09.25	03.11.25
3	Наталія КОНДРАТЕНКО, к.т.н. професор каф. ЗІ	25.09.25	17.11.25
4	Олександр ЛЕСЬКО, зав. каф. ЕПВМ, к. е. н., доц.	25.09.25	18.12.25

7. Дата видачі завдання 24 вересня 2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітки
1	Аналіз завдання. Вступ	24.09.2025 – 26.09.2025	
2	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	27.09.2025 – 07.10.2025	
3	Науково-технічне обґрунтування	11.10.2025 – 22.10.2025	
4	Побудова матриць попарних порівнянь критеріїв. Перевірка узгодженості (CI, CR)	23.10.2025 – 26.10.2025	
5	Оцінювання альтернатив за критеріями. Побудова функцій належності	27.10.2025 – 02.11.2025	
6	Агрегація оцінок (інтегральна оцінка), ранжування, дефазифікація	03.11.2025 – 10.11.2025	
7	Аналіз чутливості та інтерпретація результатів	11.11.2025 – 17.11.2025	
8	Розробка розділу економічного обґрунтування доцільності розробки	18.11.2025 – 22.11.2025	
9	Оформлення пояснювальної записки	23.11.2025 – 29.11.2025	
10	Попередній захист та доопрацювання МКР	29.11.2025 – 11.12.2025	
11	Перевірка на наявність текстових запозичень	12.12.2025 – 15.12.2025	
12	Представлення МКР до захисту, рецензування	16.12.2025 – 19.12.2025	
13	Захист МКР	19.12.2025 – 23.12.2025	

Студент _____ Єгор ДМИТРИ

Керівник роботи _____ Наталія КОНДРАТЕ

АНОТАЦІЯ

УДК 004.056.5

Дмитришин Є. Метод вибору проєкту системи захисту інформації на основі експертного оцінювання. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека та захист інформації, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2025. 87 с.

Укр. мовою. Бібліогр.: 30 назв; рис.: 7; табл.: 26.

Магістерська робота присвячена покращення ефективності методу вибору проєкту системи захисту інформації (СЗІ) на основі експертного оцінювання з використанням апарату теорії нечітких множин. Запропоновано процедуру багатокритеріального ранжування альтернатив, що включає попарні порівняння критеріїв і альтернатив, перевірку узгодженості експертних суджень (CI, CR), нормування та зважування (з урахуванням ваг експертів), обчислення інтегральної нечіткої оцінки та дефазифікацію для отримання підсумкового рейтингу. Підхід дає змогу працювати з лінгвістичними й неповними оцінками та підвищує відтворюваність результатів прийняття рішення.

Метод апробовано на прикладі ТОВ «ГРІН КУЛ»: оцінено 4 альтернативні варіанти побудови СЗІ за 6 групами критеріїв. Аналіз чутливості підтвердив стійкість лідера при зміні ваг критеріїв на ±20%. Метод може бути використаний для модернізації СЗІ, обґрунтування закупівель і підтримки інвестиційних рішень.

Ілюстративна частина складається з 6 плакатів.

Ключові слова: інформаційна безпека; система захисту інформації; багатокритеріальний вибір; нечіткі множини; експертне оцінювання; аналіз чутливості.

ABSTRACT

Dmytryshyn Y. Method for selecting an information security system project based on expert assessment. Master's thesis in the field of 125 – Cybersecurity and Information Protection, educational programme – Information and Communication Systems Security. Vinnytsia: VNTU, 2025. 87 p.

In Ukrainian. Bibliography: 30 titles; fig.: 7; tabl.: 26.

This master's thesis proposes a method for selecting an Information Security System (ISS) project based on expert judgement and fuzzy set theory. The method provides a multi-criteria ranking procedure that includes pairwise comparisons of criteria and alternatives, consistency checking of expert judgements (CI, CR), normalization and weighting (including expert weights), computation of an integrated fuzzy evaluation, and defuzzification to obtain a final ranking. The approach supports linguistic and incomplete assessments and improves the reproducibility of decision-making results.

The method was tested at LLC "GREEN COOL". Four ISS project alternatives were evaluated against six groups of criteria. Sensitivity analysis confirmed the leader's stability under ±20% changes in criteria weights. The method can be applied to ISS modernization, procurement justification, and investment decision support.

The illustrative part consists of 6 posters.

Keywords: information security; protection system; multi-criteria decision making; fuzzy sets; expert judgement; sensitivity analysis.

ЗМІСТ

ВСТУП

У сучасних умовах цифрової трансформації більшість критично важливих процесів від державного управління та банківської діяльності до промисловості й енергетики ґрунтуються на інтенсивному використанні інформаційних систем. Зростання обсягів оброблюваних даних, ускладнення IT- інфраструктури та постійна еволюція кіберзагроз призводять до того, що вимоги до систем захисту інформації (СЗІ) стають дедалі жорсткішими. При цьому помилковий або недостатньо обґрунтований вибір проєкту СЗІ може призвести до значних фінансових втрат, зупинки бізнес-процесів, витоку конфіденційної інформації та репутаційних ризиків.

На практиці організація часто має не один, а декілька можливих варіантів побудови системи захисту різні комбінації програмно-апаратних засобів, архітектурні рішення, варіанти інтеграції з наявною інфраструктурою, різні рівні автоматизації моніторингу та реагування на інциденти. Задача вибору проєкту системи захисту інформації є багатокритеріальною, де кожна альтернатива оцінюється за сукупністю технічних, організаційних, експлуатаційних та економічних показників, а також показників ризику. Значна частина цих характеристик має якісний, лінгвістичний характер і визначається на основі експертних суджень фахівців з інформаційної безпеки, адміністраторів IT-інфраструктури, економістів, представників керівництва. Такі оцінки є неповними, розмитими та суб’єктивними, що ускладнює їх безпосереднє використання в класичних кількісних методах.

В умовах підвищеної кіберзагрозливості, спричиненої, вибір адекватної системи захисту інформації набуває особливої важливості. Атаки на інформаційні ресурси органів влади, об’єктів критичної інфраструктури та бізнесу вимагають не стільки механічного нарощування окремих засобів захисту, скільки обґрунтованого проектування комплексних СЗІ з урахуванням реальних ризиків та ресурсних обмежень. Це посилює актуальність розробки методів підтримки прийняття рішень, здатних працювати з експертною інформацією та

невизначеними даними.

Саме тому тема магістерської кваліфікаційної роботи «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» є актуальною. Вона спрямована на формування формалізованого підходу до порівняння та ранжування альтернативних проєктів СЗІ на основі експертних лінгвістичних оцінок з використанням апарату теорії нечітких множин та методів багатокритеріального аналізу.

Метою роботи є покращення ефективності методу вибору системи захисту інформації на основі експертного оцінювання з використанням нечітких моделей, який забезпечує обґрунтований багатокритеріальний вибір альтернативи в умовах невизначеності вихідних даних.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– проаналізувати предметну область проєктування систем захисту інформації, основні характеристики безпеки, типові класи загроз, класифікацію засобів захисту та чинні стандарти інформаційної безпеки;

– сформулювати формальну постановку задачі багатокритеріального вибору проєкту СЗІ з урахуванням множини альтернатив, системи критеріїв та наявності невизначених (нечітких) експертних оцінок;

– опрацювати теоретичні основи теорії нечітких множин, лінгвістичних змінних, нечітких чисел і нечіткого багатокритеріального аналізу, релевантні задачі вибору в сфері кібербезпеки;

– розробити методологічний базис методу, побудувати лінгвістичні шкали для критеріїв оцінювання, визначити параметричні форми функцій належності, запропонувати підхід до отримання нечітких ваг критеріїв та нечітких локальних оцінок альтернатив на основі експертного оцінювання та парних порівнянь;

– сформувати математичну модель методу вибору проєкту СЗІ, що включає побудову нечітких матриць рішень, процедури агрегування експертних оцінок, обчислення інтегральних нечітких показників якості альтернатив та їх дефазифікацію;

– розробити алгоритм багатокритеріальної оцінки та ранжування альтернативних проєктів систем захисту інформації на основі отриманих нечітких оцінок та вагових коефіцієнтів;

– провести апробацію запропонованого методу на тестовому прикладі множини альтернативних проєктів СЗІ та проаналізувати вплив зміни ваг критеріїв і експертних оцінок на результуюче ранжування.

Об’єктом дослідження є процес вибору проєкту системи захисту інформації для інформаційної системи організації за наявності множини альтернативних рішень.

Предметом дослідження є методи та моделі багатокритеріального вибору проєкту системи захисту інформації на основі експертного оцінювання та теорії нечітких множин.

Наукова новизна роботи полягає у розробленні методу вибору проєкту системи захисту інформації, який поєднує експертне оцінювання з нечітким багатокритеріальним аналізом та дозволяє формально опрацьовувати лінгвістичні, неповні та розмиті оцінки. На відміну від класичних «жорстких» бальних схем, запропонований підхід використовує нечіткі ваги критеріїв та нечіткі локальні оцінки альтернатив, а також нечіткі матриці парних порівнянь для побудови інтегральних показників якості проєктів СЗІ.

Практичне значення одержаних результатів полягає в тому, що розроблений метод може бути використаний як основа для створення процедур та програмних засобів підтримки прийняття рішень при виборі проєктів систем захисту інформації в організаціях. Це дозволяє підвищити обґрунтованість та прозорість вибору, формалізувати роботу експертних комісій, зменшити вплив суб’єктивних чинників та врахувати одночасно технічні, організаційні й економічні аспекти безпеки.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд основних характеристик безпеки інформації

У сучасних умовах цифровізації практично всі види діяльності від державного управління та банківської справи до освіти і медицини спираються на інтенсивне використання інформаційних ресурсів. Інформація виступає ключовим активом, а її втрата чи спотворення можуть спричинити фінансові збитки, репутаційні втрати, порушення договірних зобов'язань і в окремих випадках становити загрозу національній безпеці. Відтак поняття безпеки інформації набуває ключового значення і є вихідною точкою для проєктування систем захисту. Метою системи захисту є забезпечення виконання визначених вимог до безпеки цих активів. Згідно з підходом, закладеним у стандартах серії ISO/IEC 27000 (у т.ч. ДСТУ ISO/IEC 27001:2023), головними цілями захисту є конфіденційність, цілісність і доступність (Confidentiality, Integrity, Availability – CIA), які утворюють базову тріаду безпеки та деталізуються низкою додаткових характеристик [2; 25].

Конфіденційність означає обмеження доступу до інформації для кола належним чином уповноважених суб'єктів, відтак конфіденційні дані не мають ставати відомими стороннім особам, що не є адресатами цієї інформації, а типовими проявами порушення виступають витоки, несанкціоноване копіювання чи ознайомлення зі службовими, фінансовими або персональними відомостями. У рамках системи захисту інформації конфіденційність забезпечується, зокрема, за рахунок розмежування прав доступу, застосування криптографічних засобів, організації режиму доступу до приміщень та носіїв інформації, впровадження політик поводження з конфіденційними даними.

Цілісність відображає вимогу до точності, повноти та незмінності інформації в процесі її зберігання, обробки та передачі. Дані мають залишатися такими, якими вони були сформовані, за винятком санкціонованих змін, внесених уповноваженими суб'єктами відповідно до встановлених процедур.

Порушення цілісності може мати місце як унаслідок навмисних дій порушника (модифікація записів у базі даних, підміна платіжних реквізитів, маніпуляція журналами подій), так і через випадкові помилки (збій програмного забезпечення, помилка оператора, відмова обладнання). Для забезпечення цілісності використовуються такі засоби, як контрольні суми, криптографічні хеш-функції, електронний підпис, контроль повноважень на зміну інформації.

Доступність характеризує здатність інформаційної системи надавати доступ до інформації та сервісів у необхідний момент часу уповноваженим користувачам із заданими показниками якості (затримками, швидкістю опрацювання запитів, пропускною здатністю). Порушення доступності виникає, коли інформація або сервіс недоступні в потрібний момент унаслідок відмови обладнання, помилок конфігурації, атак типу “відмова в обслуговуванні” (DoS/DDoS), аварій у мережевій інфраструктурі чи енергопостачанні. Забезпечення доступності базується на резервуванні критичних елементів системи, використанні відмовостійких рішень, організації резервного копіювання та планів аварійного відновлення, а також постійному моніторингу стану інфраструктури.

У практиці проєктування систем захисту інформації базової тріади конфіденційність, цілісність і доступність недостатньо для повного окреслення вимог. Композиція цільових властивостей доповнюється автентичністю, підзвітністю, незаперечністю, надійністю та відмовостійкістю, а також захистом приватності. Так, автентичність забезпечує впевненість у справжності суб’єктів і об’єктів взаємодії та відсутності їх підміни; її досягають механізмами аутентифікації, зокрема перевіркою облікових даних, використанням одноразових кодів і криптографічних сертифікатів, оскільки брак автентичності підвищує ризик використання викрадених або підроблених записів доступу. Підзвітність формує можливість однозначно пов’язати виконані дії з конкретним суб’єктом і встановити його відповідальність; практична реалізація ґрунтується на повному та захищеному журналюванні подій, довготривалому зберіганні логів і регламентованих процедурах аудиту, без яких

розслідування інцидентів і правозастосування істотно ускладнюються. У свою чергу, незаперечність гарантує неспростовність факту ініціювання дії або накладення електронного підпису, що має вирішальне значення для електронного документообігу та платіжних систем.

Надійність і відмовостійкість відображають здатність системи підтримувати працездатність за умов збоїв, кібератак чи часткових відмов компонентів і оперативно відновлювати функціонування після інцидентів; попри близькість до доступності ці характеристики підкреслюють архітектурну та експлуатаційну стійкість інфраструктури і охоплюють резервування, дублювання критичних елементів, кластеризацію та перевірені процедури відновлення. Захист приватності визначає правомірність і пропорційність оброблення персональних даних, обмеження доступу до відомостей про особу, мінімізацію їх збирання і прозорість використання; зростаюча щільність регулювання у національних і міжнародних актах зумовлює інтеграцію цих вимог у політики та процеси організації.

Зазначені властивості перебувають у взаємозв’язку та можуть конфліктувати між собою. Надмірно жорсткі заходи із забезпечення конфіденційності (суцільне шифрування, багатоступеневі процедури аутентифікації) можуть негативно впливати на доступність і зручність користування системою. Навпаки, прагнення максимально спростити доступ до сервісів може послабити контроль і призвести до зростання ймовірності несанкціонованого доступу.

Отже, при проєктуванні системи захисту інформації необхідно знаходити збалансований компроміс між різними характеристиками безпеки з урахуванням контексту функціонування системи, критичності активів та вимог зацікавлених сторін.

Для формалізації вимог до безпеки інформації у практиці управління використовують систему показників та метрик, які відображають ступінь досягнення потрібних властивостей. Наприклад, рівень забезпечення конфіденційності може оцінюватися часткою зашифрованих каналів

передавання даних, відсотком облікових записів із багатофакторною аутентифікацією, наявністю сегментації мережі; стан цілісності – кількістю виявлених несанкціонованих змін у критичних базах даних, частотою контрольних перевірок; доступність – показниками середнього часу безвідмовної роботи, середнього часу відновлення сервісу після збою тощо. Ці метрики використовуються як для поточного моніторингу, так і для порівняння альтернативних рішень при виборі системи захисту.

Характеристики безпеки інформації не є абсолютними і сталими. Їхня актуальність залежить від архітектури інформаційної системи, застосованих технологій, організаційних процесів, рівня підготовки персоналу, а також від динаміки загрозового середовища. Поява нових видів атак, вразливостей програмного забезпечення або змін у нормативно-правовій базі може змінювати пріоритетність окремих властивостей безпеки для конкретної організації. Саме тому в сучасній практиці застосовується ризик-орієнтований підхід, за якого вимоги до конфіденційності, цілісності, доступності й інших характеристик формулюються з урахуванням оцінених ризиків та потенційних наслідків їх реалізації.

Таким чином, основні характеристики безпеки інформації формують концептуальну основу побудови системи захисту. Надалі, при покращення ефективності методу вибору проєкту системи захисту інформації, ці характеристики виступатимуть базою для формування критеріїв оцінювання альтернатив.

1.2 Загрози та підходи до їх класифікації

Побудова системи захисту інформації починається не з вибору конкретних технічних засобів, а з формалізованого опису загрозового середовища. Для математичної моделі багатокритеріального вибору це означає, що спочатку потрібно виділити типові класи загроз, а вже потім пов’язати їх з критеріями, за якими будуть порівнюватися альтернативні проєкти СЗІ. Самі по собі

характеристики ІБ задають лише цільовий стан. Щоб коректно формувати вимоги до системи захисту та обґрунтовувати вибір її проєкту, необхідно проаналізувати, за рахунок яких саме загроз цей цільовий рівень безпеки може бути порушений. Тому класифікація загроз виступає проміжною ланкою між концептуальними властивостями безпеки та критеріальною моделлю вибору системи захисту, яка далі використовується в математичній моделі та нечіткому аналізі [1; 21].

Аналіз загроз інформаційній безпеці є вихідною точкою для побудови системи захисту та подальшого багатокритеріального порівняння альтернатив. Під загрозою розумітимемо потенційно можливу подію, дію або сукупність умов, які за певних обставин здатні порушити конфіденційність, цілісність або доступність інформації та завдати шкоди інформаційній системі чи організації в цілому. Реалізація загрози завжди пов’язана з наявністю вразливостей та формує ризик, величина якого надалі відображається у вагомості критеріїв оцінювання альтернатив систем захисту. З позиції джерела походження доцільно розглядати природні, техногенні та антропогенні загрози, причому антропогенні загрози поділяються на зовнішні, що походять від сторонніх зловмисників, та внутрішні, пов’язані з діями співробітників, адміністраторів або підрядників. За наявністю умислу виділяють навмисні загрози, орієнтовані на досягнення шкідливої мети (злом, саботаж, шахрайство), та ненавмисні, які виникають унаслідок помилок, недбалості або недостатньої кваліфікації персоналу .

У критеріальній моделі це безпосередньо відображається через показники, що характеризують здатність системи захисту протидіяти зовнішнім атакам, контролювати внутрішні дії користувачів і знижувати наслідки людського фактора. З точки зору об’єкта впливу загрози класифікують за тим, яку базову властивість інформації вони порушують: конфіденційність (несанкціоноване розкриття або витік даних), цілісність (несанкціонована зміна чи знищення інформації) або доступність (блокування чи істотне ускладнення законного доступу до сервісів і ресурсів).

Багато сучасних атак мають комбінований характер, одночасно

впливаючи на декілька властивостей, що зумовлює необхідність комплексних інтегральних критеріїв рівня безпеки для подальшого нечіткого оцінювання альтернатив. Технічний аспект аналізу загроз доцільно доповнювати рівневим підходом, коли загрози розглядаються на фізичному, мережевому, системному, прикладному й організаційному рівнях. Такий поділ дозволяє пов’язати класи загроз із конкретними механізмами протидії та ввести до критеріальної моделі спеціалізовані під критерії, захист від фізичного доступу до обладнання, стійкість до мережевих атак, захист операційних систем і служб, безпеку прикладних компонентів, а також ефективність організаційних і процедурних заходів. Окреме значення для сучасних інформаційних систем мають загрози, пов’язані з людським фактором, насамперед соціальна інженерія та дії внутрішніх порушників. Вони важко формалізуються, мають виражений ймовірнісний характер і часто стають початковою ланкою складних комбінованих атак. Саме ці загрози обґрунтовують доцільність залучення експертних оцінок та використання нечіткої логіки при побудові моделі вибору системи захисту.

Узагальнену класифікацію загроз інформаційній безпеці за основними ознаками наведено в таблиці 1.1.

Таблиця 1.1 – Класифікація загроз інформаційній безпеці

Ознака класифікації	**Клас загроз**	**Коротка характеристика**	**Приклади**
Джерело виникнення	Природні (стихійні)	Зумовлені дією сил природи	Пожежа, повінь, землетрус, гроза, екстремальні температури
Джерело виникнення	Техногенні	Відмови технічних та інженерних систем	Аварія електромережі, збій систем кондиціонування, поломка маршрутизатора
Джерело виникнення	Антропогенні зовнішні	Дії зовнішніх зловмисників	Хакерські атаки, кібершпигунство, конкурентна розвідка
Джерело виникнення	Антропогенні внутрішні	Дії внутрішніх користувачів	Несанкціонований доступ адміністратора, витік даних співробітником

Продовження табл. 1.1

Наявність умислу	Навмисні	Цілеспрямовані дії зі шкідливою метою	Віруси, трояни, цілеспрямована модифікація БД, саботаж
Наявність умислу	Ненавмисні	Помилки, недбалість, необізнаність	Випадкове видалення файлів, помилкове налаштування доступів
Об’єкт впливу	Конфіденційність	Несанкціоноване розкриття інформації	Перехоплення трафіку, витік баз даних, фішинг
Об’єкт впливу	Цілісність	Несанкціонована зміна або знищення даних	Підробка фінансових документів, модифікація записів у БД
Об’єкт впливу	Доступність	Порушення можливості законного доступу	DDoS-атака, відмова серверів, блокування ОС шкідливим ПЗ
Рівень реалізації	Фізичний	Вплив на обладнання та носії	Крадіжка сервера, несанкціонований вхід до серверної
Рівень реалізації	Мережевий	Вплив на мережеву інфраструктуру	Сканування портів, Man-in- the-Middle, DDoS
Рівень реалізації	Системний	Експлуатація вразливостей ОС та служб	Ескалація привілеїв, експлуатація сервісів
Рівень реалізації	Прикладний	Вразливості програм і веб-додатків	SQL-ін’єкції, XSS, обхід механізмів аутентифікації
Рівень реалізації	Організаційний	Обхід процедур, соціальна інженерія	Порушення політик, фішинг, інсайдерські дії

Таким чином, класифікація загроз у даній роботі має прикладний характер, на її основі виділяються цільові групи загроз, які мають бути покриті проєктом системи захисту, формуються узагальнені критерії та система підкритеріїв (наприклад, рівень протидії внутрішнім загрозам, ефективність захисту від DDoS-атак, стійкість до соціальної інженерії).

1.3 Підходи до класифікації засобів захисту

Після визначення базових властивостей інформаційної безпеки та аналізу загроз постає питання, якими саме засобами можна забезпечити належний рівень

захищеності. У практиці інформаційної безпеки використовується широкий спектр заходів від організаційних регламентів до складних програмно-апаратних комплексів. Щоб планувати, впроваджувати й оцінювати такі заходи, їх необхідно систематизувати. Саме для цього застосовуються різні підходи до класифікації засобів захисту інформації.

У практиці інформаційної безпеки доцільно виділити три ключові підходи до класифікації засобів захисту: за природою (способом реалізації), за функціональною роллю у життєвому циклі інциденту та за рівнем застосування в архітектурі інформаційної системи. Ці підходи не є взаємовиключними один і той самий засіб одночасно належить до певного класу за природою, виконує визначену функцію (превентивну, виявляючу, відновлювальну тощо) і діє на конкретному рівні (мережевому, системному, прикладному, організаційному). Саме ця багатовимірність надалі має бути формалізована в критеріальній моделі.

Перший підхід ґрунтується на природі засобів захисту, тобто на тому, яким чином вони реалізуються в організації. У цьому контексті виділяють організаційні, технічні, криптографічні, фізичні та інженерно-технічні засоби. Організаційні (адміністративні) засоби охоплюють політики інформаційної безпеки, регламенти доступу, інструкції, процедури реагування на інциденти, навчання й підвищення обізнаності персоналу; їх основна роль полягає у встановленні правил, розподілі відповідальності та формуванні культури безпеки [20; 23].

Технічні засоби включають програмні та апаратні рішення, що реалізують конкретні механізми протидії загрозам, системи контролю і розмежування доступу, міжмережеві екрани, системи виявлення й запобігання вторгненням, антивірусні комплекси, засоби резервного копіювання та моніторингу подій безпеки. Криптографічні засоби (алгоритми шифрування, протоколи захищеного обміну, електронний підпис, інфраструктура відкритих ключів) забезпечують конфіденційність, цілісність та автентичність даних при їх передаванні і зберіганні. Фізичні та інженерно-технічні засоби спрямовані на обмеження фізичного доступу до приміщень, обладнання та носіїв інформації, а також на

підтримання працездатності інфраструктури (системи контролю доступу до приміщень, відеоспостереження, сейфи, системи безперебійного живлення, резервні лінії зв’язку, кондиціонування, пожежогасіння).

Для математичної моделі цей підхід дозволяє сформувати групи критеріїв верхнього рівня, що відповідають основним напрямам: організаційний, технічний, криптографічний та фізично-інженерний захист, а оцінка альтернативного проєкту СЗІ включатиме ступінь повноти і якості реалізації кожного з цих напрямів.

Другий підхід до класифікації базується на функціональній ролі засобів захисту в життєвому циклі інциденту. У спрощеному вигляді йдеться про засоби, що запобігають реалізації загроз, засоби, що забезпечують своєчасне виявлення інцидентів, та засоби, орієнтовані на локалізацію наслідків і відновлення працездатності системи. Превентивні засоби знижують імовірність настання інциденту шляхом коректної конфігурації доступу, використання багатофакторної аутентифікації, сегментації мережі, своєчасного оновлення програмного забезпечення. Виявляючі засоби (системи виявлення вторгнень, платформи моніторингу подій безпеки, механізми контролю цілісності) забезпечують фіксацію підозрілої активності та інцидентів у прийнятні терміни.

Коригувальні та відновлювальні засоби реалізуються через процедурне й технічне відновлення після інциденту, включаючи відновлення даних із резервних копій, ізоляцію уражених сегментів, виконання планів аварійного відновлення. Окремо можна розглядати стримувальні та компенсуючі заходи, які підвищують ризик викриття порушника або тимчасово заміщають відсутні основні контролі.

Третій підхід пов’язаний із рівнем застосування засобів захисту в архітектурі інформаційної системи. Засоби можуть діяти на фізичному рівні (захист приміщень і обладнання), мережевому рівні (захист каналів зв’язку та мережевої інфраструктури), системному, або операційному, рівні (захист операційних систем та базових сервісів), прикладному рівні (захист бізнес-додатків та веб-сервісів), на рівні даних (безпосередній захист інформації), а

також на організаційно-управлінському рівні (процеси управління інформаційною безпекою, ризиками, інцидентами, доступом та змінами). Такий розподіл дозволяє оцінити глибину й багаторівневість захисту, а також виявити можливі «прогалини», коли окремі рівні системи залишаються недостатньо захищеними. Узагальнення основних класів засобів захисту, їх прикладів і призначення наведено в таблиці 1.2.

Таблиця 1.2 – Класифікація засобів захисту інформації

Клас засобів	**Приклади**	**Основне призначення**	**Рівень застосування**
Організаційні (адміністративні)	Політика ІБ; регламенти доступу; інструкції; навчання персоналу	Встановлення правил, розподіл відповідальності, формування культури безпеки	Організаційний, управлінський
Технічні програмні	Антивіруси; IDS/IPS; SIEM; системи контролю доступу; WAF	Виявлення та блокування атак, контроль доступу, моніторинг подій	Системний, мережевий, прикладний
Технічні апаратні	Міжмережеві екрани; апаратні криптомодулі; апаратні токени	Забезпечення високопродуктивних та захищених операцій	Мережевий, фізичний
Криптографічні	Алгоритми шифрування; протоколи TLS/IPsec; ЕЦП; PKI	Захист конфіденційності й цілісності даних, автентифікація	Рівень даних, мережевий
Фізичні	Замки, сейфи; системи відеоспостереження; СКУД	Обмеження фізичного доступу до приміщень, обладнання та носіїв	Фізичний
Інженерно-технічні	UPS; резервні лінії зв’язку; кондиціонування; пожежогасіння	Підтримка працездатності, захист від техногенних і природних впливів	Фізичний, інженерна інфраструктура
Превентивні	Сегментація мережі; “жорсткі” політики паролів; whitelisting	Зниження ймовірності реалізації загроз	Усі рівні
Виявляючі	IDS; SIEM; засоби контролю цілісності	Своєчасне виявлення інцидентів і аномалій	Мережевий, системний, прикладний

Розглянуті підходи до класифікації засобів захисту інформації мають безпосереднє значення для побудови багатокритеріальної моделі вибору проєкту системи захисту. Вони дозволяють системно охопити простір можливих заходів, структурувати характеристики альтернатив і ув’язати їх із класифікацією загроз, наведеною в попередньому підрозділі. З одного боку, це дає змогу виділити узагальнені групи критеріїв верхнього рівня (напрями захисту), з іншого – деталізувати їх через підкритерії, що відображають функціональну роль засобів та рівень їх застосування.

1.4 Стандарти інформаційної безпеки

Розвиток систем захисту інформації в сучасних організаціях відбувається в межах певних нормативних рамок. Ці рамки формуються міжнародними та національними стандартами, галузевими рекомендаціями та регуляторними вимогами. Стандарти інформаційної безпеки виконують кілька ключових функцій задають єдину термінологію та понятійний апарат, визначають модель побудови системи управління безпекою, формулюють набір вимог і контролів, а також встановлюють критерії оцінювання зрілості, відповідності та ефективності впроваджених заходів.

Одна з найбільш відомих груп стандартів у сфері інформаційної безпеки – сімейство ISO/IEC 27000, що описує підхід до побудови системи управління інформаційною безпекою (Information Security Management System, ISMS). Ці стандарти орієнтовані на організації будь-якого типу й задають структурований, циклічний підхід до управління безпекою.

Основні документи [23; 26; 27]:

– ISO/IEC 27000 містить загальний огляд сімейства стандартів, визначення термінів, базові принципи побудови ISMS. Встановлює єдину термінологічну основу для розуміння інших стандартів серії;

– ISO/IEC 27001 встановлює вимоги до системи управління інформаційною безпекою. Це сертифікаційний стандарт, що визначає, які

елементи має включати ISMS, аналіз контексту організації, визначення зацікавлених сторін, формування політики безпеки, оцінювання ризиків, планування й реалізація заходів, моніторинг, внутрішній аудит та постійне вдосконалення;

– ISO/IEC 27002 надає практичні рекомендації щодо застосування заходів безпеки (контролів), перелічених у додатку до ISO/IEC 27001. Містить каталог контролів, політики безпеки, організація інформаційної безпеки, управління активами, контроль доступу, криптографічний захист, фізична безпека, безпека експлуатації, безпека мереж, безпека розроблення й супроводу, управління інцидентами, безперервність бізнесу;

– ISO/IEC 27005 присвячений управлінню ризиками інформаційної безпеки. Містить модель процесу ідентифікації активів, загроз, вразливостей, аналізу наслідків та ймовірностей, оцінки ризиків і вибору варіантів оброблення ризиків;

– ISO/IEC 27035 описує управління інцидентами інформаційної безпеки від виявлення та реєстрації до аналізу, реагування, ліквідації наслідків і накопичення знань.

Сімейство ISO/IEC 27000 є важливим орієнтиром при розробленні проєктів систем захисту, оскільки визначає, які процеси та компоненти мають бути реалізовані. Для задачі вибору проєкту система критеріїв може будуватися на основі вимог ISO/IEC 27001 та переліку контролів ISO/IEC 27002.

Для оцінки окремих програмних і апаратних продуктів використовуються стандарти ISO/IEC 15408 (Common Criteria). Вони задають формальну схему опису та оцінювання функціональних і гарантійних вимог до безпеки IT-продуктів, операційних систем, мережевих пристроїв, міжмережевих екранів, криптографічних модулів.

Наявність сертифіката відповідності Common Criteria для засобів захисту інформації, рівень EAL, відповідність певному профілю захисту є важливими показниками при виборі технічних засобів, особливо для об’єктів критичної інфраструктури.

Значний вплив на практику ІБ мають також рекомендаційні документи Національного інституту стандартів і технологій США (NIST). До найбільш відомих належать:

– NIST SP 800-53 каталог заходів безпеки для інформаційних систем, згрупованих за сімействами (контроль доступу, аудит, конфігураційна безпека, реагування на інциденти, фізична безпека тощо);

– NIST SP 800-30 та 800-37 рекомендації щодо оцінювання та управління ризиками;

– NIST Cybersecurity Framework (CSF) рамкова модель, що групує активності з кібербезпеки за п’ятьма функціями: Identify, Protect, Detect, Respond, Recover.

Паралельно застосовуються фреймворки управління ІТ та ІБ, такі як COBIT та ITIL, які допомагають інтегрувати вимоги безпеки в загальну систему управління ІТ та бізнес-процесами.

На національному рівні діють закони та підзаконні акти, що регламентують захист інформації в інформаційно-телекомунікаційних системах, захист персональних даних, порядок застосування засобів технічного та криптографічного захисту, створення комплексних систем захисту інформації. Частина міжнародних стандартів гармонізована у вигляді національних стандартів. Для окремих секторів (фінансового, енергетичного, телекомунікаційного) додатково встановлюються галузеві регуляторні вимоги щодо мінімального рівня безпеки, обов’язковості аудиту, резервування, застосування криптографічних засобів. Порівняльну характеристику ключових стандартів та фреймворків інформаційної безпеки наведено в таблиці 1.3

Стандарти інформаційної безпеки задають структуру предметної області й формують природну основу для побудови багатокритеріальної моделі оцінки альтернатив. Більшість вимог і контролів можуть бути відображені у вигляді критеріїв або показників, які оцінюються експертами, ступінь відповідності ISO/IEC 27001, покриття контролів ISO/IEC 27002, наявність сертифікацій за Common Criteria, відповідність національним і галузевим регуляторним вимогам.

Таблиця 1.3 – Порівняння основних стандартів та фреймворків інформаційної безпеки

Стандарт / фреймворк	**Основна мета**	**Об'єкт регулювання**	**Тип документа**
ISO/IEC 27001	Вимоги до ISMS	Процеси управління ІБ в організації	Сертифікаційний стандарт
ISO/IEC 27002	Рекомендовані контролі	Конкретні заходи та практики безпеки	Практичний кодекс
ISO/IEC 27005	Управління ризиками ІБ	Процес оцінювання та оброблення ризиків	Методичний стандарт
ISO/IEC 15408 (Common Criteria)	Оцінювання безпеки IT-продуктів	Функціональні та гарантійні вимоги до засобів захисту	Стандарт оцінювання
NIST CSF	Рамка кібербезпеки	Функції та категорії дій з кібербезпеки	Рекомендаційний фреймворк
Національні стандарти та НПА	Регулювання ІБ на рівні держави	Вимоги до захисту інформації, персональних даних, КСЗІ	Закони, підзаконні акти, ДСТУ
Превентивні	Сегментація мережі; "жорсткі" політики паролів; whitelisting	Зниження ймовірності реалізації загроз	Усі рівні
Виявляючі	IDS; SIEM; засоби контролю цілісності	Своєчасне виявлення інцидентів і аномалій	Мережевий, системний

Оскільки значна частина цих вимог має якісний, лінгвістичний характер, їх оцінювання здійснюється за участю експертів. Це зумовлює потребу в методах, здатних працювати з нечіткими, суб'єктивними оцінками, – зокрема, у нечітких моделях багатокритеріального вибору, які будуть використані у подальших розділах.

1.5. Сучасні методи та засоби оцінювання стану безпеки

Оцінювання стану інформаційної безпеки є невід'ємним елементом системи управління захистом інформації в сучасних організаціях. Результати такого оцінювання дають змогу визначити, наскільки ефективними є впроваджені заходи, які ризики залишаються неприйнятними, які напрями

потребують підсилення та додаткових ресурсів. При цьому оцінка рівня безпеки використовується не лише як засіб контролю поточного стану, а й як підґрунтя для обґрунтування управлінських рішень, у тому числі для багатокритеріального вибору проєктів систем захисту інформації [16].

Специфіка предметної області інформаційної безпеки полягає у високому рівні невизначеності вихідних даних. Частина показників може бути зафіксована кількісно, наприклад, кількість виявлених вразливостей, час відгуку системи, частота інцидентів. Водночас суттєва частина інформації має якісний, лінгвістичний або експертний характер – це оцінки рівня ризику, ймовірності реалізації загроз, адекватності організаційних заходів, зрілості процесів тощо. Такі оцінки ґрунтуються на неповній інформації про загрози й вразливості, наближених прогнозах поведінки порушника та суб'єктивному досвіді експертів [3].

У практиці оцінювання стану інформаційної безпеки застосовується низка усталених підходів. Аудити та перевірки відповідності орієнтовані на встановлення факту дотримання вимог стандартів, законодавчих і внутрішніх нормативних документів. Вони базуються на аналізі документації, політик, процедур, а також на опитуваннях і інтерв'ю з персоналом. Однак отримані результати часто мають переважно формальний характер і не завжди повною мірою відображають фактичний технічний стан безпеки. Класичний аналіз ризиків передбачає ідентифікацію активів, загроз і вразливостей, оцінювання можливих наслідків та ймовірностей реалізації загроз, а також розрахунок інтегральної оцінки ризику. Цей підхід забезпечує зв'язок із бізнес-цілями організації, але стикається з труднощами при кількісному визначенні ймовірностей та збитків, унаслідок чого ключові параметри ризику часто задаються вербальними категоріями, а не точними числовими значеннями. Широко застосовуються системи метрик та індикаторів інформаційної безпеки, які включають ключові показники ефективності та показники ризику. Вони дають змогу відслідковувати динаміку стану захисту й наочно представляти інформацію керівництву. Водночас такі показники зазвичай охоплюють

переважно кількісні аспекти і не завжди адекватно відображають складні якісні характеристики, зокрема організаційні або поведінкові фактори [18; 19].

Тестування на проникнення й аналіз вразливостей забезпечують виявлення конкретних технічних слабких місць, помилок конфігурації, небезпечних версій програмного забезпечення. Вони дають детальну технічну картину, проте не охоплюють організаційні аспекти, людський фактор і не формують безпосередньо інтегральної оцінки стану безпеки. Оцінювання зрілості процесів інформаційної безпеки спрямоване на визначення рівня системності підходу до захисту, класифікуючи процеси за рівнями від несформованих до оптимізованих і керованих. Однак отримувані оцінки значною мірою залежать від суб'єктивних суджень учасників оцінювання.

Паралельно із цими підходами в сучасних інформаційних системах масово впроваджуються автоматизовані засоби моніторингу та оцінювання стану безпеки. До них належать сканери вразливостей, які аналізують мережеві сервіси, операційні системи та веб-додатки; системи виявлення та запобігання вторгненням; системи моніторингу подій безпеки та кореляції журналів; платформи управління вразливостями й ризиками; панелі моніторингу, які агрегують ключові показники. Ці засоби істотно підвищують оперативність, масштабованість та деталізацію оцінювання технічного стану безпеки, але не усувають проблеми інтерпретації результатів і визначення їх практичної важливості.

Незважаючи на значні обсяги технічних даних, що генеруються автоматизованими засобами, загальна картина стану безпеки залишається неповною та неоднозначною. Не всі виявлені вразливості є однаково критичними, не кожна аномалія свідчить про реальний інцидент, а сукупність формально позитивних індикаторів не гарантує відсутності одиничних, але дуже небезпечних ризиків [4].

Унаслідок цього ключовими проблемами оцінювання залишаються неповнота даних, невизначеність ймовірностей і наслідків, лінгвістичний характер значної частини оцінок, а також динамічність загрозового середовища,

що постійно змінюється. В описаних умовах центральну роль в оцінюванні стану безпеки відіграють експерти – фахівці з інформаційної безпеки, інформаційних технологій, бізнес-підрозділів, представники керівництва. Саме вони інтерпретують технічні результати в термінах реальних бізнес-ризиків, визначають пріоритетність загроз і заходів захисту, обґрунтовують вибір між альтернативними проєктами систем захисту. Водночас експертні судження характеризуються суб'єктивністю, можуть бути частково непослідовними, суперечливими та відрізнятися залежно від досвіду та ролі окремих експертів. Це обумовлює необхідність застосування формалізованих методів обробки експертних оцінок, які структурують процес оцінювання, дають змогу виявляти і зменшувати вплив суб'єктивних викривлень, забезпечують узгодження й агрегування думок групи експертів, а також підвищують прозорість і відтворюваність результатів. У цьому контексті особливу роль відіграють методи, здатні працювати з нечіткими, наближеними, частково суперечливими даними.

Задача вибору проєкту системи захисту інформації має багатокритеріальний характер необхідно одночасно враховувати технічні, організаційні, економічні, нормативні та ризик-орієнтовані показники. Більшість цих критеріїв не може бути оцінена абсолютно точно й однозначно, а їхні значення доцільно задавати у вигляді інтервалів, вербальних шкал або лінгвістичних термів. Класичні методи багатокритеріального вибору, які вимагають подання оцінок у формі чітких чисел, у такій ситуації часто не відображають реальної розмитості й невизначеності вхідних даних. На цьому тлі методи нечіткого багатокритеріального аналізу є природним та обґрунтованим інструментом підтримки прийняття рішень. Вони дають змогу задавати експертні оцінки у вигляді нечітких чисел, що відображають діапазон можливих значень та ступінь упевненості; працювати безпосередньо з лінгвістичними шкалами типу «низький», «середній», «високий рівень ризику»; агрегувати суперечливі судження кількох експертів з урахуванням їхньої компетентності; формально порівнювати альтернативи в умовах невизначеності.

Таким чином, невизначеність вхідних даних і ключова роль експертного оцінювання є фундаментальними характеристиками задачі вибору системи захисту інформації й визначають доцільність застосування нечітких багатокритеріальних методів, на основі яких у подальших розділах формується відповідна математична модель.

Висновки до розділу 1

У розділі визначено концептуальну основу інформаційної безпеки як системи взаємопов’язаних властивостей. Показано, що тріада конфіденційність-цілісність-доступність (CIA) є базовою, однак для практичного проєктування СЗІ її необхідно доповнювати характеристиками автентичності, підзвітності, незаперечності, надійності/відмовостійкості та захисту приватності. Обґрунтовано, що ці властивості можуть конфліктувати, тому в реальних умовах потрібне компромісне, ризик-орієнтоване формування вимог із використанням метрик та показників для подальшого порівняння альтернатив.

Систематизовано підходи до аналізу та класифікації загроз як проміжної ланки між цільовими властивостями безпеки й критеріальною моделлю вибору. Узагальнено класи загроз за джерелом виникнення, наявністю умислу, об’єктом впливу (C/I/A) та рівнем реалізації (фізичний, мережевий, системний, прикладний, організаційний). Підкреслено комбінований характер сучасних атак і значущість людського фактора (соціальна інженерія, внутрішні порушники), що зумовлює необхідність інтегральних критеріїв та залучення експертних оцінок.

Розглянуто класифікацію засобів захисту за трьома взаємодоповнювальними вимірами: за природою (організаційні, технічні, криптографічні, фізичні, інженерні), за функціональною роллю (превентивні, виявляючі, коригувальні/відновлювальні) та за рівнем застосування в архітектурі системи. Показано, що така багатовимірна систематизація дозволяє формувати структуру критеріїв верхнього рівня та деталізувати її підкритеріями для

оцінювання повноти й глибини захисту.

Проаналізовано роль стандартів і фреймворків у формуванні вимог до СЗІ. Встановлено, що сімейство ISO/IEC 27000 задає модель побудови ISMS, ISO/IEC 27001/27002 можуть виступати основою для критеріального опису контролів, ISO/IEC 27005 – для ризик-орієнтованого підходу, а ISO/IEC 15408 (Common Criteria) – для оцінювання безпеки окремих IT-продуктів. Додатково зазначено значення рекомендацій NIST і національних регуляторних вимог як джерел критеріїв відповідності та зрілості.

Узагальнено сучасні методи оцінювання стану безпеки (аудити, аналіз ризиків, метрики, тестування на проникнення, оцінювання зрілості, автоматизований моніторинг) і виокремлено їх обмеження, пов’язані з невизначеністю даних, лінгвістичним характером частини показників та складністю інтегральної інтерпретації результатів. Обґрунтовано ключову роль експертів у прийнятті рішень і зроблено висновок про доцільність використання формалізованих методів обробки експертних суджень та нечітких багатокритеріальних моделей для вибору проєкту СЗІ.

Отримані результати формують методичне підґрунтя для наступних розділів: визначені властивості безпеки, класи загроз, підходи до класифікації засобів, стандарти та особливості оцінювання безпеки дозволяють побудувати систему критеріїв і підкритеріїв, а також обґрунтувати застосування експертного оцінювання та нечіткої логіки в задачі вибору оптимальної архітектури СЗІ.

2 ОРГАНІЗАЦІЯ БАГАТОКРИТЕРІАЛЬНОГО ВИБОРУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ НЕЧІТКОГО АНАЛІЗУ АЛЬТЕРНАТИВ ЗА ДОПОМОГОЮ ЕКСПЕРТНОГО ОЦІНЮВАННЯ

2.1 Моделі багатокритеріального вибору системи захисту інформації на основі нечітких множин з врахуванням експертного оцінювання

Вибір системи захисту інформації (СЗІ) для конкретної організації належить до класу багатокритеріальних задач прийняття рішень. На практиці це означає, що особа, яка приймає рішення, повинна обрати один варіант СЗІ з кількох конкуруючих, причому кожен з них характеризується різними групами показників. У такій ситуації застосування лише класичних методів оптимізації, що потребують точних числових даних, є недостатнім. Реальні оцінки експертів часто мають розпливчастий або неповний характер і природно описуються лінгвістичними термінами. Тому для формалізації таких оцінок доцільно застосовувати апарат нечітких множин у поєднанні з експертним оцінюванням.

Нехай задано множину альтернативних проєктів СЗІ $P = \{P_1, P_2, ..., P_m\}$, де P_j – j-та альтернативна архітектура СЗІ, що описує конкретну комбінацію програмно-апаратних засобів захисту, політик доступу, організаційних заходів та процедур супроводу; m – кількість альтернатив. Для оцінювання цих альтернатив використовується множина узагальнених критеріїв $G = \{G_1, G_2, ..., G_6\}$, де G_i – і-та група критеріїв, що відображає ключовий аспект якості СЗІ; n – кількість критеріїв (у роботі прийнято n = 6).Такий підхід дозволяє структурувати вимоги до СЗІ, групуючи численні показники у декілька логічних блоків [3; 4; 5].

Спираючись на загальну структуру вимог до інформаційної безпеки, запропонуємо ввести такі узагальнені критерії:

G_1 – забезпечення конфіденційності та цілісності інформації (протидія несанкціонованому доступу, несанкціонованим змінам, витокам даних). До цієї

групи можуть входити підкритерії, що описують керування доступом, криптографічний захист даних “у спокої” та “в каналі”, сегментацію мережі, журналювання та контроль цілісності [14].

G_2 – забезпечення доступності та відмовостійкості (стійкість до збоїв, наявність засобів резервування та відновлення). Цей критерій характеризує здатність СЗІ забезпечувати функціонування захищеної системи за наявності відмов окремих компонентів, збоїв мережі, аварійних ситуацій.

G_3 – відповідність нормативно-правовим вимогам та стандартам. Це включає відповідність національним і міжнародним стандартам у сфері захисту інформації, галузевим рекомендаціям, внутрішнім регламентам організації, а також вимогам регуляторних органів.

G_4 – інтегрованість та сумісність із наявною IT-інфраструктурою. Сюди відносяться можливості взаємодії СЗІ з існуючими інформаційними системами, базами даних, мережевою інфраструктурою, програмними продуктами, протоколами та сервісами.

G_5 – експлуатаційні характеристики (зручність адміністрування, керованість, можливість масштабування). Цей критерій описує складність налаштування, наявність засобів моніторингу та звітності, гнучкість зміни політик безпеки, а також здатність системи адаптуватися до росту навантаження та розширення інфраструктури.

G_6 – економічна доцільність / сукупна вартість володіння (TCO) (витрати на придбання, впровадження, супровід і розвиток). У межах цього критерію враховуються як початкові капітальні витрати, так і операційні витрати, пов’язані з технічною підтримкою, оновленням, навчанням персоналу тощо.

Оцінювання здійснює група експертів: $E = \{e_1, e_2, ..., e_k\}$, де k – кількість експертів. До складу групи доцільно включати фахівців з інформаційної безпеки, адміністраторів IT-інфраструктури, представників замовника/керівництва та (за потреби) економістів. Такий склад дозволяє врахувати різні точки зору на одну й ту саму альтернативу: технічну реалізовність, відповідність вимогам, експлуатацію та витрати.

Для того щоб зменшити суб’єктивність та отримати відтворювані результати, експертні судження формуються у вигляді попарних порівнянь [14]:

– попарне порівняння критеріїв Gi для визначення їх відносної важливості;

– попарне порівняння альтернатив Pj за кожним критерієм Gi.

Інтенсивність переваги задається впорядкованою лінгвістичною шкалою з подальшим переведенням у числа (зручно застосовувати дев’ятибальну шкалу 1-9). Отримані матриці порівнянь підлягають перевірці узгодженості суджень. Для цього обчислюють індекс узгодженості CI та відношення узгодженості CR; якщо CR перевищує припустиме значення (як правило, 0,1), відповідні порівняння переглядаються та уточнюються.

За наявності кількох експертів попарні порівняння агрегуються в групове рішення. Практично доцільно використовувати геометричне середнє елементів матриць (як стандартний підхід для групового AHP), а за потреби враховувати ваги компетентності експертів. Це дозволяє отримати узагальнені матриці, на основі яких далі визначаються: відносні ваги критеріїв; локальні оцінки альтернатив за кожним критерієм.

Нечітка модель використовується для того, щоб кожну альтернативу Pj представити не одним “жорстким” числом, а ступенем виконання вимог за критеріями та інтегральною оцінкою прийнятності з урахуванням: лінгвістичних і неповних оцінок (невизначеність); важливості критеріїв (пріоритезація); консервативної логіки вибору, коли слабке значення за критичним критерієм не повинно “перекриватися” лише одним сильним показником.

У підсумку загальна логіка запропонованого підходу наведена на рисунку 2.1. Подана схема відображає послідовність переходу від формування множини альтернатив і системи критеріїв до експертних попарних порівнянь, отримання узгоджених локальних оцінок та їх подальшої агрегації в інтегральний показник для ранжування та вибору проєкту СЗІ. Ключовими контрольними точками є агрегування групових суджень та контроль узгодженості, що запобігає випадковим і суперечливим рішенням.

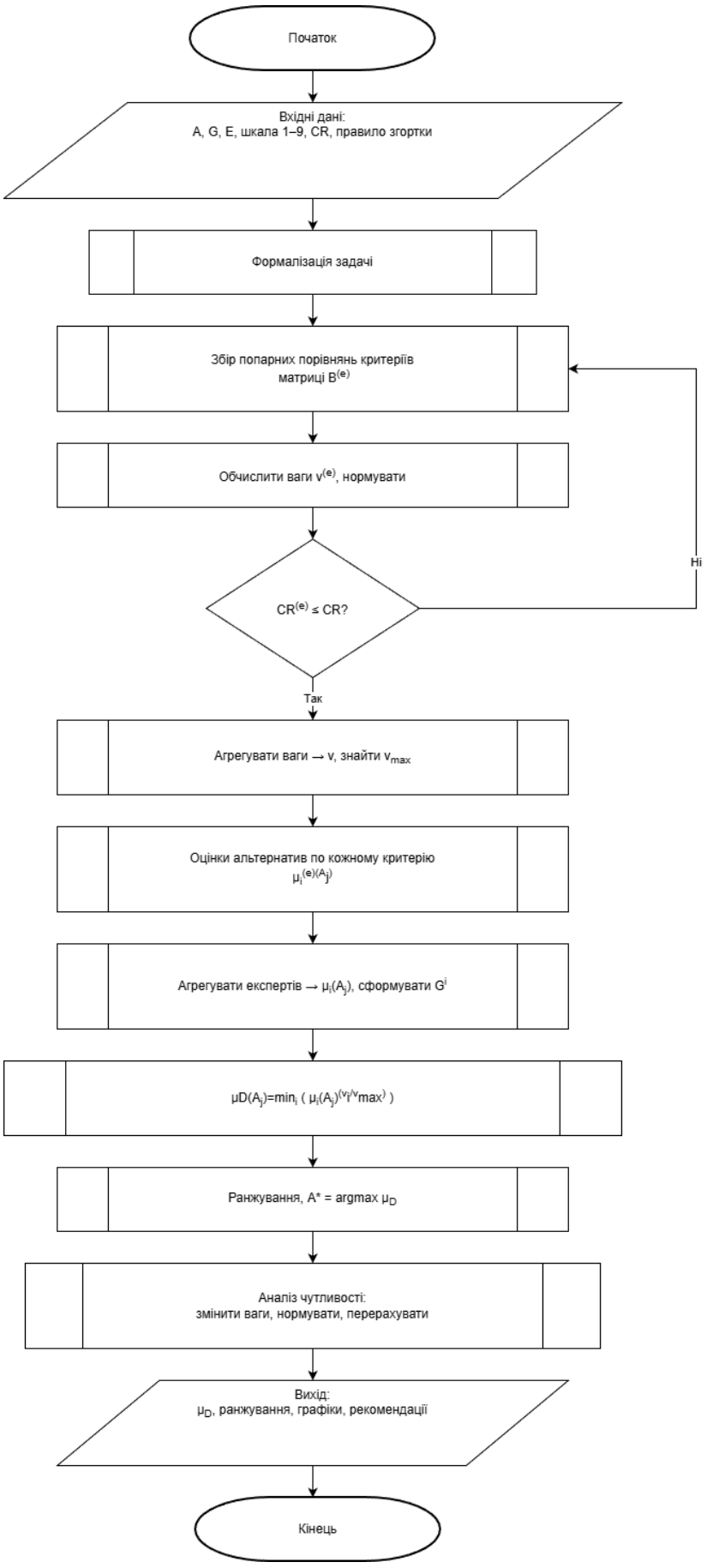


Рисунок 2.1 – Схема алгоритму запропонованого підходу

Таким чином, сформовано постановку задачі багатокритеріального вибору проєкту СЗІ через множину альтернатив P та систему критеріїв G, визначено зміст критеріїв G_1-G_6 і принципи організації експертного оцінювання. Це створює методичну основу для подальшої формалізації нечітких оцінок, побудови локальних показників за критеріями та процедур інтегральної агрегації.

2.2 Методологічний базис нечітких множин для організації нечіткого аналізу альтернатив

Задача вибору системи захисту інформації має багатокритеріальний характер і спирається на лінгвістичні експертні оцінки. Для формалізації таких оцінок доцільно використовувати апарат нечітких множин і нечітких чисел, який дозволяє відобразити невизначеність та суб'єктивність суджень без примусової "жорсткої" кількісної інтерпретації на початковому етапі.

Відповідно до теорії нечітких множин, для кожного критерію G_i на множині альтернатив P задаємо нечітку множину:

$$C_i = \{\mu_{Gi}(P_1)/P_1, \mu_{Gi}(P_2)/P_2, \dots, \mu_{Gi}(P_m)/P_m\}, \quad (2.1)$$

де C_i – нечітка множина альтернатив, прийнятних за критерієм $\mu_{Gi}(P_1) \in [0;1]$ – ступінь належності альтернативи P_j до множини C_i, тобто ступінь виконання критерію G_i цією альтернативою [5; 8; 9].

У дискретному випадку це означає, що кожному проєкту P_j поставлено у відповідність число $\mu_{Gi}(P_j)$, яке відображає «силу» виконання критерію G_i цією альтернативою. Для таких множин використовується додаткове обмеження:

$$\sum_{j=1}^{m} \mu_{Gi}(P_j) = 1 \quad (2.2)$$

де m – кількість альтернативних проєктів системи захисту інформації.

Тобто всі проєкти ділять між собою «одиницю» належності за кожним критерієм.

На практиці, у сфері інформаційної безпеки для багатьох критеріїв відсутні точні кількісні дані або вони мають приблизний характер, експертні судження природно задаються через лінгвістичні терміни, між критеріями існують суперечності, а думки різних експертів можуть розходитися й містити внутрішні неузгодженості.

Адекватно описати таку ситуацію дозволяє нечіткий підхід. Нехай X – множина можливих значень деякого показника (наприклад, витрат чи рівня захищеності). Нечітка підмножина $A \subseteq X$ задається функцією належності, де для кожного значення $x \in X$ відображає ступінь, у якому це значення відповідає певній властивості [9; 10]:

$$\mu A(x): X \rightarrow [0; 1], \tag{2.3}$$

На основі цих величин формується матриця рішень і в подальшому здійснюється нечіткий багатокритеріальний аналіз. Щоб не змушувати експертів працювати з числами, вводиться впорядкована лінгвістична шкала інтенсивності переваги альтернативи P_i над альтернативою P_j . Наприклад, можна використати шкалу наведену у таблиці 2.1.

Таблиця 2.1 – Лінгвістична шкала інтенсивності переваги

Лінгвістичний терм	**Оцінка важливості**
Рівнозначна перевага	1
Дуже слабка перевага	3
Помірна перевага	5
Значна перевага	7
Дуже значна перевага	9

Для множини елементів $x_1, x_2, ..., x_n$ будується матриця парних порівнянь:

$$A = (a_{ij})_{n \times n} \tag{2.4}$$

де A – матриця парних порівнянь альтернатив за критерієм G_i;

a_{ij} – інтенсивність переваги альтернативи P_j над альтернативою P_k за критерієм G_i.

Матриця має такі властивості:

$$a_{ii} = 1, \ a_{ij} = \frac{1}{a_{ji}}, \tag{2.5}$$

Перша умова означає, що кожен елемент вважається рівнозначним самому собі. Друга умова забезпечує зворотність оцінок: якщо x_i у певній мірі переважає x_j, то x_j у відповідній мірі поступається x_i.

Отже, для кожного критерію ми маємо квадратну матрицю експертних чисел, що відображають попарні відносини переваги між альтернативами.

2.3 Побудова функцій належності на основі парних порівнянь альтернатив

Далі використовується стандартна для такого підходу процедура: з матриці парних порівнянь виділяється власний вектор, пов’язаний з найбільшим власним значенням [11; 12]:

$$A^{(i)} w^{(i)} = \lambda_{max}^{(i)} w^{(i)} \tag{2.6}$$

де $\lambda_{max}^{(i)}$ найбільше власне значення матриці A^i.

Для наочного подання процедури визначення власного вектора матриці парних порівнянь розглянемо її запис у вигляді розгорнутої системи рівнянь. Нехай для деякого критерію G_i матриця парних порівнянь альтернатив має вигляд:

$$A^i = \begin{pmatrix} a_{11}^{(i)} a_{12}^{(i)} & \cdots & a_{1m}^{(i)} \\ a_{21}^{(i)} a_{22}^{(i)} & \ddots & a_{2m}^{(i)} \\ \vdots \quad \vdots & \cdots & \vdots \\ a_{m1}^{(i)} a_{m2}^{(i)} & \ldots & a_{mm}^{(i)} \end{pmatrix}$$

Вектор відносних оцінок альтернатив w = (w_1, w_2, ..., w_n) та найбільше власне значення $\lambda_{max}^{(i)}$ визначаються із системи (2.6).

У розгорнутому вигляді це рівняння еквівалентне системі:

$$\begin{cases} a_{11}^{(i)} w_1^{(i)} + a_{12}^{(i)} w_2^{(i)} + \cdots + a_{1m}^{(i)} w_m^{(i)} = \lambda_{max}^{(i)} w_1^{(i)}; \\ a_{21}^{(i)} w_1^{(i)} + a_{22}^{(i)} w_2^{(i)} + \cdots + a_{2m}^{(i)} w_m^{(i)} = \lambda_{max}^{(i)} w_2^{(i)}; \\ \cdots \\ a_{m1}^{(i)} w_1^{(i)} + a_{m2}^{(i)} w_2^{(i)} + \cdots + a_{mm}^{(i)} w_m^{(i)} = \lambda_{max}^{(i)} w_m^{(i)}. \end{cases}$$

Найбільше власне значення $\lambda_{max}^{(i)}$ у цьому випадку відіграє роль коефіцієнта узгодженості суджень експертів щодо порівняння альтернатив за критерієм G_i. Якщо всі парні порівняння виконані узгоджено, матриця $A^{(i)}$ є узгодженою, і значення $\lambda_{max}^{(i)}$ практично $\lambda_{max}^{(i)}$ відхиляється від m, тим сильніша неузгодженість експертних оцінок і тим більше суперечливих порівнянь міститься в матриці. У разі значного відхилення $\lambda_{max}^{(i)}$ від m матрицю парних порівнянь доцільно переглянути й скоригувати, уточнивши відповідні експертні судження [13].

Компоненти вектора $w^{(i)}$ мають природну інтерпретацію: вони показують «відносну силу» кожного проєкта для заданого критерію. Щоб привести ці значення до вигляду функції належності, їх нормують:

$$\sum_{j=1}^{m} w^{(i)} = 1, \qquad (2.7)$$

Після чого приймають:

$$\mu_{Gi}(P_j) = w^{(i)}\text{j}, \quad \text{j} = 1, ..., \text{m} \tag{2.8}$$

Таким чином, для кожного критерію G_i маємо нечітку множину C_i на множині проєктів P, отриману безпосередньо з експертних суджень.

Запропонована методика ґрунтується на принципі Беллмана–Заде, згідно з яким найкраще рішення в умовах нечіткої постановки задачі обирається як альтернатива, що має максимальний ступінь належності до нечіткої множини «допустимих» рішень. У розглянутому випадку така множина задається перетином нечітких множин критеріїв C_i. Ступінь належності альтернативи P_j перетину. На першому етапі аналізу припускається, що всі критерії однаково важливі для особи, яка приймає рішення. У цьому випадку нема сенсу додатково зважувати критерії – застосовується підхід на основі перетину нечітких множин.

Сукупна множина рішень, які є прийнятними одночасно за всіма критеріями, задається як перетин нечітких множин:

$$D = C_1 \cap C_2 \cap \ldots \cap C_n \tag{2.9}$$

де D – нечітка множина альтернатив, прийнятних за всіма критеріями одночасно.

Для перетину нечітких множин використовується оператор мінімуму їхніх функцій належності. Отже, для кожного проєкта ступінь належності до множини «загально прийнятних» рішень обчислюється як:

$$\mu_{Gi}(P_j) = \min \mu_{Gi}(P_j) \tag{2.10}$$

де $\mu_{Gi}(P_j)$ – інтегральна оцінка альтернативи P_j при однаковій важливості критеріїв.

Це правило має просту інтерпретацію, загальна оцінка проєкта за всіма критеріями визначається найслабшим місцем. Якщо система захисту чудово виглядає майже за всіма показниками, але радикально «провалює» один

важливий критерій, значення $\mu_{Gi}(P_j)$ буде низьким, і така альтернатива не розглядатиметься як найкраща.

Після обчислення $\mu_{Gi}(P_j)$ для всіх альтернатив, якщо одна з альтернатив Pj* помітно перевершує всі інші, то такий проєкт вважається оптимальним варіантом СЗІ при однаковій важливості критеріїв. Якщо ж кілька альтернатив мають зіставні значення $\mu_{Gi}(P_j)$ і однозначного лідера немає, то необхідно перейти до уточненого етапу, де враховується відносна важливість критеріїв.

2.4 Багатокритеріальна оцінка альтернатив на основі нечітких множин

Щоб формально врахувати той факт, що одні критерії більш значущі, а інші – менш, експерти виконують попарне порівняння самих критеріїв. Застосовується той же підхід, що й для альтернатив: судження «цей критерій важливіший» задаються лінгвістично й потім переводяться у числа [6].

Формується матриця у якій елемент b_{ij} характеризує, наскільки критерій G_i важливіший за критерій G_j:

$$B = (b_{ij})_{n\times n} \tag{2.11}$$

Використовується та сама дев’ятибальна шкала, а матриця має властивості:

$$b_{ii} = 1,\ b_{ij} = \frac{1}{b_{ji}}, \tag{2.12}$$

Як і раніше, для матриці парних порівнянь вирішують задачу на власний вектор:

$$\mathrm{Bw} = \lambda_{\max}\mathrm{w} \tag{2.13}$$

де w – власний вектор матриці B;

λ_{max} – найбільше власне значення матриці B.

У розгорнутому вигляді рівняння відповідає системі

$$\begin{cases} b_{11}w_1 + b_{12}w_2 + \cdots + b_{1n}w_n = \lambda_{max}\, w_1; \\ b_{21}w_1 + b_{22}w_2 + \cdots + b_{2n}w_n = \lambda_{max}\, w_2; \\ \cdots \\ b_{n1}w_1 + b_{n2}w_2 + \cdots + b_{1n}w_n = \lambda_{max}\, w_n. \end{cases}$$

Розв’язання цієї системи дає власний вектор $w = (w_1, w_2, ..., w_n)$ компоненти якого інтерпретуються як відносні оцінки важливості критеріїв [14]. Далі вектор w нормують, задаючи умову:

$$\sum_{i=1}^{n} \mathrm{w_i} = 1,$$

Після чого коефіцієнти відносної важливості критеріїв визначаються співвідношенням:

$$b_i = n \cdot w_i, i = 1, \dots, n.$$

Компоненти цього вектора використовують для побудови коефіцієнтів відносної важливості. Таким чином, маємо, яку «частку впливу» на остаточне рішення має відповідний критерій G_i.

Щоб перенести отримані коефіцієнти важливості у сферу нечітких множин, множини C_i перетворюють [15]. Для цього застосовується степенева зміна функцій належності для кожного критерію G_i формують нову нечітку множину:

$$\mathrm{C}_i^{b_i} = \{ (\mu_{Gi}(P_1))^{b_i}/P_1, \dots, (\mu_{Gi}(P_m))^{b_i}/P_m \} \qquad (2.14)$$

$$\mu_{G_i}^{(b)}(P_j) = (\mu_{Gi}(P_j))^{b_i} \quad (2.15)$$

де $C_i^{b_i}$ – модифікована нечітка множина альтернатив за критерієм G_i з урахуванням його важливості.

Піднесення до степеня b_i змінює «жорсткість» критерію: для більш важливих критеріїв (великих α_i) низькі значення $\mu_{Gi}(P_j)$ ще сильніше зменшуються, а високі залишаються близькими до одиниці. Таким чином, вплив важливих критеріїв на підсумкову оцінку посилюється.

Після модифікації нечітких множин виконується зважений перетин:

$$D = {C_1}^{b_1} \cap {C_2}^{b_2} \cap \ldots \cap {C_n}^{b_n} \quad (2.16)$$

де D* – нечітка множина рішень, прийнятних за всіма критеріями з урахуванням їхньої важливості.

Як і раніше, для перетину використовується оператор мінімуму. Отримане значення є зваженою інтегральною оцінкою прийнятності проєкта P_j, яка враховує як ступені виконання окремих критеріїв, так і їхню відносну важливість. Остаточний вибір проєкта СЗІ здійснюється за правилом:

$$\mu_{D*}(P_{j*}) = \max_{j = 1,\ldots,m} \mu_{D*}(P_{j*}) \quad (2.17)$$

де P_{j*}– альтернатива, що має найбільший ступінь належності до множини D*.

Тобто обирається альтернатива з найбільшим ступенем належності до зваженої множини прийнятних рішень.

Висновки до розділу 2

У розділі обґрунтовано, що вибір проєкту системи захисту інформації є

багатокритеріальною задачею з істотною часткою лінгвістичних і неповних експертних даних, тому застосування лише «чітких» оптимізаційних підходів є обмеженим. Показано доцільність використання апарату нечітких множин для формалізації розпливчастих суджень, відображення невизначеності та забезпечення інтерпретованого порівняння альтернативних архітектур СЗІ.

Запропоновано структуру постановки задачі у вигляді множини альтернативних проєктів P = {P1, P2, ..., Pm} та системи узагальнених критеріїв G = {G1, G2, ..., G6}, які охоплюють ключові аспекти якості СЗІ: конфіденційність/цілісність, доступність/відмовостійкість, відповідність стандартам і вимогам, інтегрованість, експлуатаційні характеристики, економічна доцільність (ТСО). Така декомпозиція дозволяє узгодити вимоги безпеки з критеріальною моделлю та забезпечує можливість подальшої деталізації через підкритерії.

Сформовано механізм отримання оцінок на основі групового експертного оцінювання із застосуванням методу парних порівнянь. Введено впорядковану лінгвістичну шкалу інтенсивності переваги, що дозволяє експертам задавати судження у звичній вербальній формі з подальшим коректним переходом до числових значень та побудови матриць порівнянь для критеріїв і альтернатив.

Розроблено методику побудови функцій належності альтернатив за кожним критерієм на основі власного вектора матриці парних порівнянь, отриманого для найбільшого власного значення. Передбачено нормування ваг, що забезпечує інтерпретацію результатів як розподілу ступенів належності альтернатив у межах кожного критерію. Підкреслено значення контролю узгодженості суджень через відхилення λ_{max} (та відповідні індикатори узгодженості) як умови надійності експертних даних.

Реалізовано інтеграцію критеріїв на основі принципу Беллмана–Заде шляхом формування нечіткої множини прийнятних рішень як перетину нечітких множин критеріїв. На початковому етапі розглянуто випадок рівної важливості критеріїв, де агрегування здійснюється оператором мінімуму, що інтерпретується як підхід «за найслабшим місцем» і дозволяє відсіювати

альтернативи з критичними провалами за окремими показниками.

Запропоновано уточнений етап оцінювання із врахуванням різної важливості критеріїв. Ваги критеріїв визначаються з матриці парних порівнянь критеріїв, після чого реалізується їх перенесення у нечітку постановку через степеневу модифікацію функцій належності та виконання зваженого перетину. Такий механізм посилює вплив більш значущих критеріїв і забезпечує отримання зваженої інтегральної оцінки прийнятності кожної альтернативи.

Визначено правило фінального вибору як знаходження альтернативи з максимальним ступенем належності до зваженої множини прийнятних рішень. У підсумку сформовано цілісну методичну схему, яка поєднує: експертне попарне порівняння → побудову нечітких оцінок → агрегування за принципом Беллмана–Заде → ранжування та вибір проєкту СЗІ, що створює основу для подальшої практичної апробації та аналізу результатів у наступних розділах.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Обґрунтування вибору об’єкту та постановка задачі

Практична цінність методу багатокритеріального вибору проявляється не лише у формальному обчисленні інтегральної оцінки, а й у можливості пояснити, які саме фактори формують перевагу тієї чи іншої альтернативи в реальному організаційно-технічному середовищі. У межах третього розділу здійснюється апробація запропонованого підходу на прикладі конкретного підприємства із визначеним набором загроз, обмежень і вимог до системи захисту інформації. Це дозволяє перейти від теоретичного опису нечіткого аналізу до його прикладного застосування: сформувати множину альтернатив, узгодити критерії оцінювання, організувати експертне опитування, виконати розрахунок локальних і інтегральних показників, а також оцінити стійкість отриманого ранжування до варіювання ваг.

Вибір проєкту системи захисту інформації для промислового підприємства є багатокритеріальною задачею прийняття рішень, у якій технічні, організаційні та економічні вимоги мають різну природу і не зводяться до одного інтегрального показника без попередньої експертної інтерпретації. У межах магістерської роботи така задача розглядається для ТОВ «ГРІН КУЛ» (завод холодильного обладнання), чия інформаційна інфраструктура поєднує корпоративний IT-сегмент (служби каталогів, пошта, файлові та прикладні сервери, ERP/CRM, електронний документообіг, віддалений доступ) і виробничий OT-сегмент (мережі технологічного рівня, PLC/SCADA-вузли, контролери, датчики, шлюзи IT/OT) [1; 18]. Критичними активами є технологічні рецептури та креслення, конструкторська документація, планово-логістичні дані, персональні й комерційні відомості, а також безперервність виробничого циклу як така.

Виходячи з галузевих умов, формується узагальнена модель загроз, що охоплює несанкціонований доступ і зловживання привілеями, зараження

шкідливим ПЗ, витоки конфіденційних даних через електронну пошту, хмарні сервіси або некоректні налаштування, порушення цілісності технологічних параметрів унаслідок помилок персоналу чи компрометації віддалених підключень, мережеві збої та відмови окремих вузлів, ризики ланцюга постачання і сервісного обслуговування обладнання, інциденти на межі IT/OT, де некоректна сегментація або моніторинг призводять до поширення впливу. Оцінювання наслідків надалі здійснюватиметься через вплив на конфіденційність, цілісність і доступність (CIA) та показники безперервності (RPO/RTO) [25].

Для практичного відбору пропонується множина чотирьох реальних архітектурних альтернатив, релевантних масштабу підприємства та доступним ресурсам.

Альтернатива A1 – базова on-prem платформа: міжмережевий екран класу NGFW/UTM із сегментацією на периметрі, корпоративний антивірус/EDR, VPN для віддаленого доступу, локальні резервні копії за змішаною схемою (повні та інкрементні), мінімальні засоби журналювання (полегшений SIEM/OSS).

Альтернатива A2 – комерційна інтегрована платформа середнього класу: NGFW з IPS/IDS та контролем застосунків, корпоративний EDR/XDR, DLP на поштових і файлових сервісах, повноцінний SIEM з кореляцією подій, керування привілейованими доступами , базова аварійна готовність для критичних сервісів.

Альтернатива A3 – гібридний підхід on-prem + хмара з опорою на екосистему Microsoft 365 E5: використання засобів Defender, політик Zero-Trust із Conditional Access у Entra ID, SIEM/SOAR на базі Microsoft Sentinel, хмарні сервіси резервування й відновлення (Azure Backup/ASR) із інтеграцією OT-подій через шлюзи.

Альтернатива A4 – аутсорсинг SOC-as-a-Service під угодами рівня сервісу, планами аварійного відновлення і безперервності бізнесу (BCP), цілодобовий моніторинг постачальника, керовані NGFW/EDR/XDR, SIEM провайдера з кореляцією та сценаріями реагування, сенсори й агенти на майданчику замовника, спільно погоджені метрики MTTD/MTTR.

Узагальнену структурну характеристику альтернатив подано в таблиці 3.1.

Таблиця 3.1 – Опис і порівняння альтернативних архітектур СЗІ

А	**Короткий опис архітектури**	**Ключові компоненти**	**Очікувані сильні сторони**	**Потенційні ризики**
А1	Локальна інфраструктура захисту з мінімально необхідним функціоналом.	NGFW/UTM (периметр, сегментація), корпоративний AV/EDR, VPN, локальні бекапи, базовий журналінг/OSS-SIEM.	Повний контроль на майданчику; просте розгортання; низький поріг входу.	Обмежена глибина виявлення; вищий MTTD/MTTR; ручне реагування; обмежене покриття ОТ.
А2	Розширений набір засобів моніторингу та реагування в межах on-prem.	NGFW з IPS/IDS, EDR/XDR, DLP (пошта/файли), SIEM з кореляцією, PAM, базовий DR.	Краща видимість та кореляція подій; скорочення часу інцидент-менеджменту.	Потреба у кваліфікованому супроводі; зростання CAPEX/OPEX; складність інтеграції з ОТ.
А3	Локальні засоби плюс хмарні Defender/Sentinel і DR-сервіси.	Defender (Endpoint/Identity/Office), Entra ID/Conditional Access, Microsoft Sentinel (SIEM/SOAR), Azure Backup/ASR, шлюзи IT/OT.	Швидке масштабування; автоматизація реагування; сильні можливості аналітики.	Залежність від провайдера; вимоги до якості інтеграції IT/OT; питання суверенності даних.
А4	Керовані NGFW/EDR/XDR і SIEM постачальника, 24×7 моніторинг і реагування.	Сенсори/агенти на об’єкті, керовані NGFW/EDR/XDR, SIEM/UEBA провайдера, процеси за SLA, плани DR/BCP.	Зниження навантаження на штат; експертний моніторинг 24×7; прогнозований MTTR.	Залежність від якості телеметрії і каналу; вимоги до SLA; розмежування доступів.

Багатокритеріальна оцінка альтернатив виконується за шістьма узагальненими критеріями, що відображають кращі практики галузі та вимоги підприємства. Перелік критеріїв та приклади операційних індикаторів подано в таблиці 3.2.

Таблиця 3.2 – Система узагальнених критеріїв і операційні індикатори вимірювання

Код	Назва критерію	Операційні індикатори/приклади метрик	Нормування
G1	Ефективність захисту (CIA, покриття загроз, реагування)	Частка заблокованих атак; MTTD/MTTR; якість плейбуків SOAR; частота помилкових спрацювань.	«Більше – краще» (покриття); «менше – краще» (час/помилки).
G2	Відмовостійкість і безперервність (BCP/DR)	RPO/RTO; частка сервісів під DR; успішність тестів відновлення; ізоляція резервів.	«Більше – краще» (охоплення/успішність); «менше – краще» (RTO/RPO).
G3	Відповідність і аудит	Покриття політик; трасованість журналів; готовність до аудитів; відповідність ISO 27001/IEC 62443/внутр. регламентам.	«Більше – краще».
G4	Інтегрованість і сумісність	Інтеграції з ERP/CRM/AD; відкритість API; збір OT-подій; інтеграції без кастомного коду.	«Більше – краще».
G5	Експлуатаційні характеристики	Трудомісткість адміністрування; масштабованість; частка автоматизованих операцій; навантаження на ІБ-команду.	«Менше – краще» (трудомісткість); «більше – краще» (автоматизація).
G6	Сукупна вартість володіння	CAPEX+OPEX на 3–5 років; вартість навчання/підтримки; ліцензії/супровід.	«Менше – краще».

Оцінювання здійснює міжфункціональна експертна група з п’яти ролей: керівник з інформаційної безпеки, мережевий інженер, інженер з OT/автоматизації, фахівець із аудиту, а також економіст/фінансист. Кожен експерт формує власні матриці парних порівнянь для критеріїв і для альтернатив за кожним критерієм, далі перевіряється узгодженість кожної матриці та у разі потреби, повертаються зауваження для уточнення. Склад і зони відповідальності експертів подано в таблиці 3.3.

При формуванні множини альтернатив важливо підкреслити, що розглянуті варіанти не є абстрактними конфігураціями, а відображають типові практичні стратегії впровадження СЗІ для підприємств із обмеженнями щодо

бюджету, кадрового забезпечення та сумісності з наявною інфраструктурою. Тому кожна альтернатива описується не лише переліком технологій, а й очікуваними експлуатаційними властивостями: складністю розгортання, вимогами до компетенцій персоналу, характером супроводу та потенціалом масштабування. Такий спосіб подання забезпечує коректність подальшого порівняння, оскільки переводить обговорення з рівня “наявності окремих засобів” на рівень цілісної архітектури.

Таблиця 3.3 – Склад експертної групи і зони відповідальності

Експерт	**Роль/посада**	**Зона компетенції у виборі СЗІ**	**Ключовий внесок в оцінювання**
E1	Керівник з ІБ / CISO	Політики безпеки, ризики, пріоритети захисту.	Матриці критеріїв; пріоритизація G1-G3; валідація сценаріїв реагування.
E2	Мережевий інженер	Периметр, сегментація, NGFW/VPN, DR-мережі.	Оцінка A1-A4 за G1/G4; вимоги до телеметрії і каналів.
E3	Інженер OT/автоматизації	PLC/SCADA, шлюзи IT/OT, безпека технологічних мереж.	Оцінка впливу на безперервність; ризики інтеграції; покриття OT-подій.
E4	Аудитор/комплаєнс	Відповідність стандартам, журналінг, докази аудиту.	Оцінка за G3; вимоги до логування/зберігання та репортингу.
E5	Економіст/фінансист	Бюджетування, TCO, SLA/DR/BCP-угоди.	Оцінка G6; CAPEX/OPEX; економічна стійкість альтернатив.

Система критеріїв, що використовується для оцінювання альтернатив, орієнтується на потреби підприємства та водночас узгоджується з загальноприйнятими принципами інформаційної безпеки: забезпеченням конфіденційності, цілісності та доступності, а також вимогами до відповідності, керованості та економічної доцільності. Важливо, що критерії інтерпретуються операційно – через індикатори, які експерти здатні порівнювати на основі досвіду (наприклад, повнота покриття загроз, забезпечення резервування,

зрілість журналювання та аудиту, сумісність з типовими сервісами підприємства, прогнозована сукупна вартість володіння). Це знижує ризик “формального” оцінювання та підвищує валідність експертних суджень.

Окремо варто зазначити, що сформована експертна група є мультидисциплінарною: представлена ролями, які відповідають як технічним, так і організаційно-економічним аспектам функціонування СЗІ. Це принципово, оскільки вибір проєкту системи захисту не може вважатися обґрунтованим, якщо він базується лише на ІТ-погляді без урахування комплаєнсу, операційних процесів і бюджетних обмежень. У результаті сформовано основу для коректного застосування методу нечіткого багатокритеріального вибору, де надалі виконуються порівняння та агрегування неоднорідних експертних оцінок.

3.2. Алгоритм багатокритеріального вибору для ТОВ «ГРІН КУЛ»

Подальша практична реалізація методу спирається на узгоджений збір експертних суджень та їх подальшу формалізацію в матрицях попарних порівнянь. Локальні пріоритети альтернатив розраховуються окремо за кожним узагальненим критерієм G_i (i = 1..6) і для кожного експерта E_k (k = 1..5). Для кожної матриці передбачено обов’язкову перевірку внутрішньої узгодженості. Неузгоджені матриці повертаються експерту для доопрацювання. Далі локальні пріоритети агрегуються між експертами з урахуванням якості їхніх суджень; після цього визначаються ваги критеріїв і виконується інтегральна агрегація за правилом перетинів нечітких множин. Агрегації виконуються за зваженим середнім із вагами експертів, що отримані з індексів узгодженості їхніх матриць.

Для введення суджень використовується лінгвістична шкала інтенсивності переваги, яку конвертовано у числові значення. Надалі ці значення утворюють елементи матриць попарних порівнянь. Значення на діагоналі дорівнюють одиниці [11; 17].

Шкала з таблиці 3.4 забезпечує узгодженість семантики експертних висловлювань і дозволяє заповнювати матриці порівнянь без нав’язування точних фізичних вимірів.

Таблиця 3.4 – Лінгвістична шкала інтенсивності переваги (1-9)

Число	**Лінгвістичний термін**	**Пояснення**
1	Рівнозначна перевага	Альтернативи однаково бажані за критерієм
3	Слабка перевага	Є незначна аргументована перевага
5	Помірна перевага	Перевага добре відчутна
7	Сильна перевага	Докази переваги суттєві
9	Абсолютна перевага	Перевага безсумнівна
2, 4, 6, 8	Проміжні значення	Уточнюють інтенсивність між наведеними рівнями

Локальні пріоритети отримуються як нормований власний вектор, що відповідає найбільшому власному значенню λ_{max} системи $Aw = \lambda w$, після чого виконується перевірка узгодженості: $CI = (\lambda_{max} - m)/(m - 1)$, $CR = CI\ RI(m)$, де $RI(m)$ – випадковий індекс. Умова прийнятності: $CR \leq 0{,}10$ [23].

Узгодженість експертних суджень у методі попарних порівнянь є критичною умовою коректності отриманих ваг і подальших інтегральних висновків. З цієї причини процедура включає контроль логічної несуперечності: для кожної матриці попарних порівнянь визначається найбільше власне значення λ_{max}, після чого обчислюється індекс узгодженості CI та відношення узгодженості CR. Застосування порогової вимоги $CR \leq 0{,}10$ забезпечує відсікання оцінок, у яких суб’єктивні переваги задані непослідовно (наприклад, коли одночасно декларується перевага P_1 над P_2, P_2 над P_3, але при цьому P_3 – над P_1 із “високою інтенсивністю”). У таких випадках матриця повертається експерту на уточнення, що підвищує надійність і відтворюваність підсумкових результатів.

З метою зменшення впливу суб’єктивних викривлень, у процедурі передбачено зважування експертів за якістю їх суджень через коефіцієнти β_k, які нормуються до одиниці. Такий підхід дозволяє коректно агрегувати групові

оцінки навіть у разі, коли окремі експерти демонструють вищу непослідовність, а отже й меншу інформаційну цінність своїх матриць порівнянь.

Відповідно, групова оцінка $\overline{w}_{G_i}$ відображає не просте середнє, а агрегований результат із урахуванням надійності джерел [23].

Для забезпечення відтворюваності експертного оцінювання та мінімізації суб'єктивних суперечностей процедура заповнення матриць попарних порівнянь доповнюється обов'язковим контролем узгодженості. Послідовність формування матриці, обчислення локальних пріоритетів та перевірки показника узгодженості узагальнено подано на рисунку 3.1.

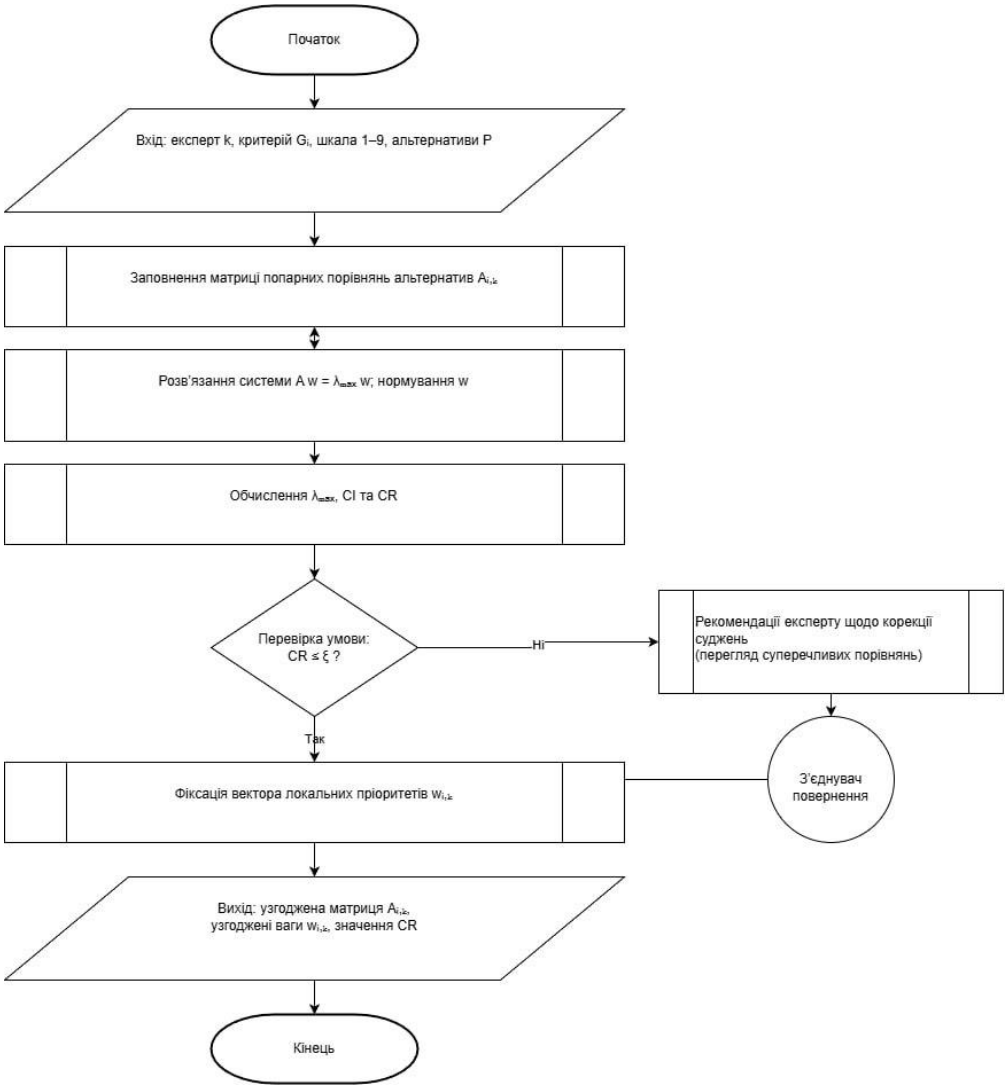


Рисунок 3.1 – Процедура експертного оцінювання та контролю узгодженості матриць

Якщо значення CR перевищує допустимий поріг, матриця повертається експерту для коригування окремих порівнянь, після уточнення розрахунки повторюються до отримання узгоджених оцінок. У подальшому для всіх узгоджених матриць визначаються вагові коефіцієнти, що відображають якість експертних суджень.

Після відбору узгоджених матриць виникає потреба отримати групову оцінку за кожним критерієм на основі п’яти експертних суджень. Агрегування здійснюється з урахуванням “якості” заповнення матриць: чим нижче CR, тим більш надійними вважаються судження експерта, а його внесок у груповий результат задається ваговим коефіцієнтом β_k. Узагальнену схему обчислення β_k та агрегування локальних пріоритетів наведено на рисунку 3.2.

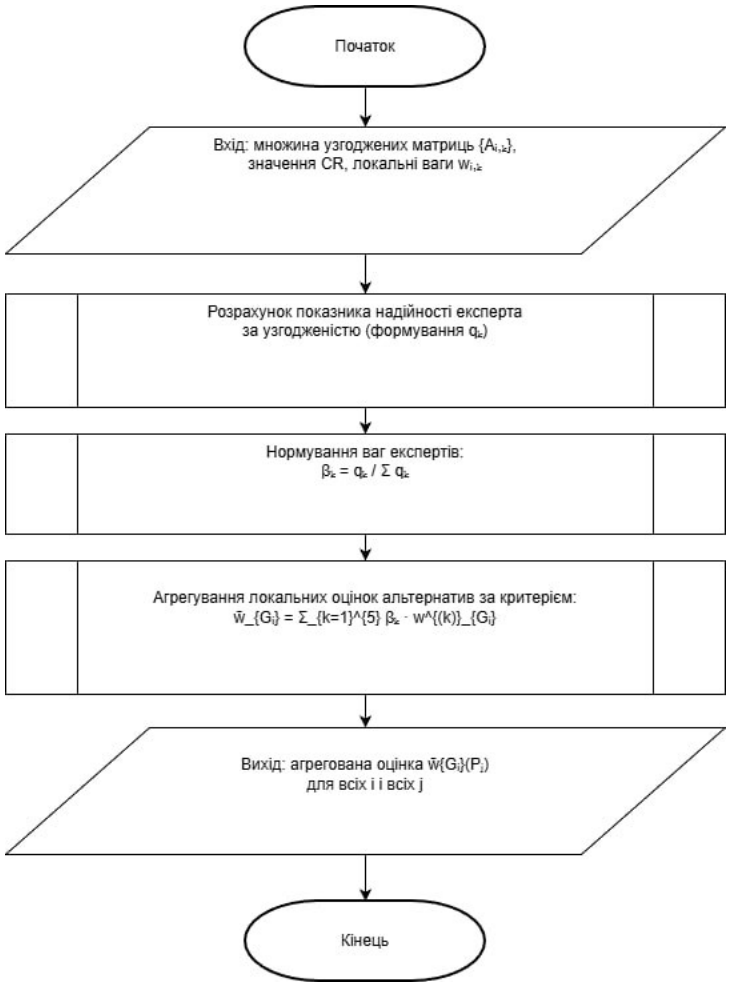


Рисунок 3.2 – Агрегування експертних оцінок з урахуванням якості матриць

Після отримання локальних пріоритетів для кожного критерію формується інтерпретація цих значень як функцій належності $\mu_{G_i}(P_j)$, що дозволяє перейти до нечіткого багатокритеріального інтегрування. Важливо підкреслити, що така інтерпретація є методологічно обґрунтованою: нечітка модель тут виступає не “декоративною” надбудовою, а математичним інструментом узгодженого поєднання неоднорідних критеріїв за умов неповної та суб’єктивної інформації.

Далі агреговані локальні пріоритети $\bar{\mu}_{G_i}(P_j)$ поєднуються з вагами критеріїв в інтегральному узагальненні за правилом перетинів нечітких множин.

Блок-схема алгоритму наведена на рисунку 3.3.

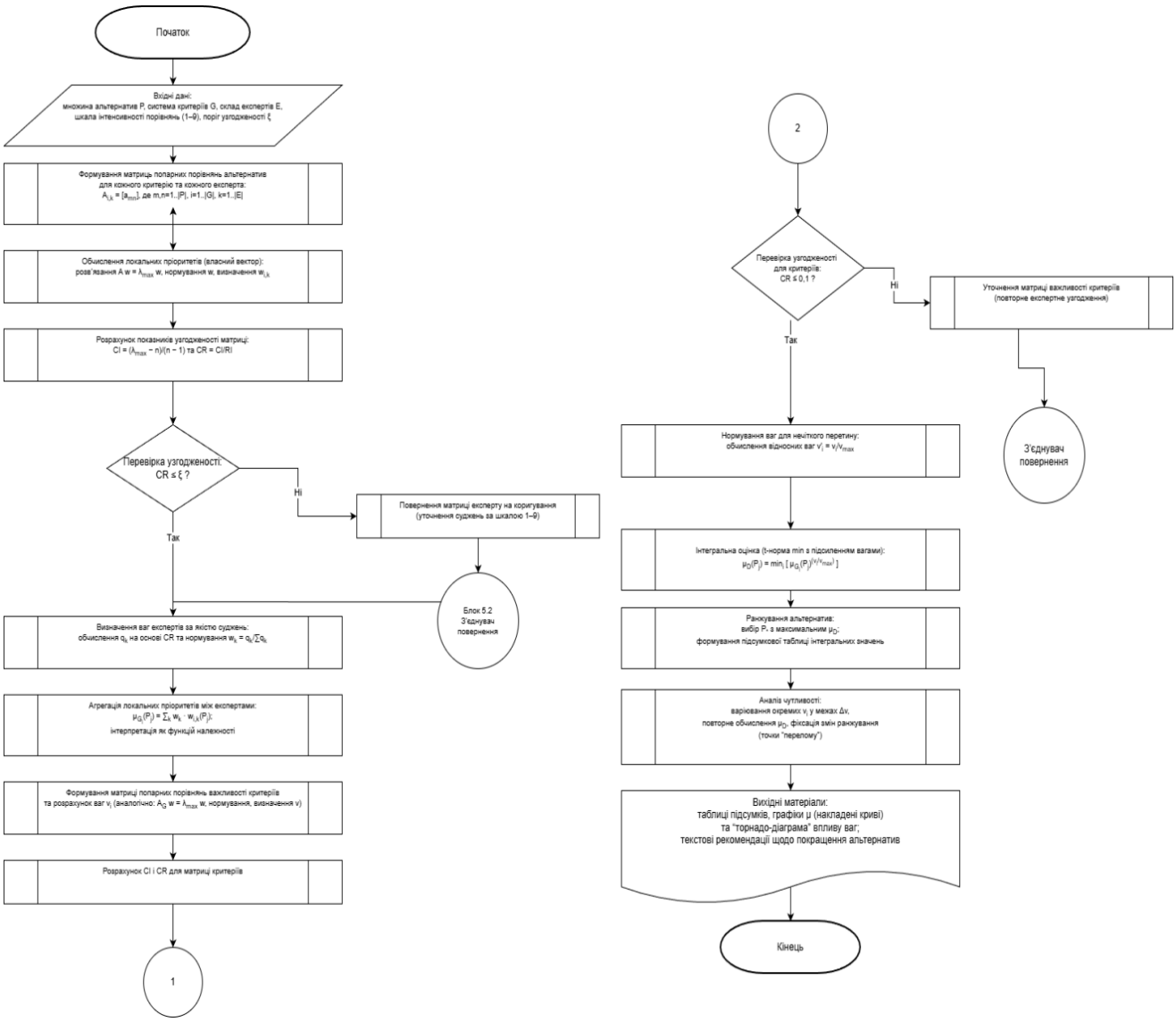


Рисунок 3.3 – Блок-схема алгоритму розрахунку

Зазначена послідовність забезпечує прозорість прийняття рішень: якість кожного окремого судження впливає на вагу відповідного експерта, а значущість критеріїв керує «жорсткістю» перетину. У підсумку метод є відтворюваним, перевіряним і сумісним із вимогами стандартів ISO/IEC 27001 та ISO/IEC 27005.

3.3 Реалізація методу на прикладі ТОВ «ГРІН КУЛ»

Нижче подано послідовне застосування запропонованого методу до вхідних даних підприємства: 5 експертів, 4 альтернативи (A1-A4), 6 критеріїв (G1-G6), лінгвістична шкала інтенсивності переваги.

Таблиця 3.5 – Консолідовані коефіцієнти належності $\mu_{Gi}(P_j)$ за результатами зваженої агрегації експертних оцінок

Критерій / Альтернатива	**A1**	**A2**	**A3**	**A4**
G1 Конфіденційність/цілісність	0.60	0.78	0.86	0.72
G2 Доступність/відмовостійкість	0.58	0.75	0.83	0.70
G3 Відповідність стандартам	0.55	0.82	0.80	0.70
G4 Інтегрованість/сумісність	0.62	0.77	0.85	0.68
G5 Експлуатаційні характеристики	0.65	0.80	0.78	0.73
G6 Економічна доцільність	0.85	0.70	0.65	0.60

Значення $\mu_{Gi}(P_j)$ інтерпретуються як ступені виконання критерію G_i альтернативою P_j після перевірки узгодженості індивідуальних матриць та їх зваженої агрегації [20].

Таблиця 3.6 – Нормовані ваги критеріїв v_i та показники узгодженості (λ_{max}, CI, CR)

Критерій	**Вага**	**Експонента v_i / v_{max}**
G1 Конфіденційність/цілісність	0.23	1.000
G2Доступність/відмовостійкість	0.18	0.783
G3 Відповідність стандартам	0.16	0.696
G4 Інтегрованість/сумісність	0.17	0.739
G5 Експлуатаційні характеристики	0.14	0.609
G6 Економічна доцільність	0.12	0.522

Параметри узгодженості: $\lambda_{max} = 6.32$; CI = 0.064; CR = 0.052 ≤ 0,10 – умова узгодженості виконується.

Таблиця 3.7 – Локальні мінімальні значення за правилом перетинів

Критерій / Альтернатива	**A1**	**A2**	**A3**	**A4**
G1Конфіденційність/цілісність	0.600	0.780	0.860	0.790
G2 Доступність/відмовостійкість	0.4508	0.6876	0.864	0.787
G3 Відповідність стандартам	0.660	0.871	0.856	0.780
G4 Інтегрованість/сумісність	0.702	0.824	0.887	0.782
G5 Експлуатаційні характеристики	0.769	0.873	0.860	0.826
G6 Економічна доцільність	0.919	0.830	0.799	0.766
$\min_i \mu_{Gi}(P_j)$	0.4508	0.6876	0.799	0.782

Інтегральна належність альтернатив визначається як мінімум профільних значень по критеріях: $\mu_D(P_j) = \min_{i\epsilon\{1\ldots6\}} \left\{ \mu_{\{G_i\}} (P_j)^{\frac{v_i}{v_{max}}} \right\}$.

Таблиця 3.8 — Інтегральні оцінки $\mu_D(P_j)$ та ранжування альтернатив

Альтернатива	**μD(Pj)**	**Місце**
A3	0.799	1
A2	0.6876	3
A4	0.7803	2
A1	0.4508	4

Найбільше значення $\mu D(P_j)$ отримала архітектура «Гібрид + MDR» (A3), що свідчить про її найкраще узгоджене задоволення всіх критеріїв за обраним правилом перетинів; далі слідують «Комерційна платформа» (A2), «Аутсорсинг SOC» (A4) та «On-prem базова» (A1) [21].

Отримані в процесі розрахунків локальні пріоритети демонструють, що різні альтернативи формують переваги за різними групами критеріїв, що є типовою ситуацією для задач вибору СЗІ: рішення, яке забезпечує максимальний технічний рівень захисту, нерідко поступається за економічною доцільністю або експлуатаційною керованістю. Саме тому інформативним є не лише визначення лідера за інтегральною оцінкою, а й аналіз профілю альтернатив – виявлення “провалів” за окремими критеріями та причин їх виникнення.

З практичної точки зору, агреговані значення $\mu_{Gi}(P_j)$ слід інтерпретувати як кількісне відображення рівня відповідності альтернативи критерію G_i за умови колективного експертного судження. Якщо для певної альтернативи спостерігається висока оцінка за критеріями ефективності та відповідності, але нижча за експлуатаційними характеристиками, то це вказує на потенційну потребу в додаткових організаційних заходах (наприклад, підготовці персоналу, регламентації процесів супроводу або залученні зовнішньої підтримки) [22]. Таким чином, проміжні результати мають прикладне значення: вони дозволяють не лише “обрати найкраще”, а й сформувати цільові рекомендації щодо посилення альтернатив, які близькі до лідера.

Окремо доцільно відзначити, що процес перевірки узгодженості матриць та застосування коефіцієнтів β_k знижує ризик випадковості результатів. Це забезпечує підвищену довіру до підсумкового ранжування, оскільки воно спирається на контрольовані та відфільтровані експертні судження, а не на “неперевірену” думку окремих учасників оцінювання.

3.4. Підсумкова оцінка та аналіз чутливості

На завершальному етапі багатокритеріального відбору альтернатив для ТОВ «ГРІН КУЛ» узагальнюються результати попередніх розрахунків. Значення відповідності $\mu_D(P_j)$, агреговані між експертами для кожного критерію G_i та альтернативи P_j, перетворюються згідно з правилом перетинів нечітких множин

з урахуванням вагових показників v_i. Для мінімізації впливу «вузького місця» використано t-норму min з підсиленням важливості через показник v_i/v_{max} [14].

Інтегральна оцінка $\mu_{Gi}(P_j)$, розрахована за правилом перетинів із ваговими показниками, відображає компромісний результат: альтернатива отримує високий рівень належності лише тоді, коли демонструє прийнятний рівень за всіма ключовими критеріями з урахуванням їх важливості [18]. На відміну від методів, що допускають “компенсацію” слабких місць надмірними перевагами в одному параметрі, застосований підхід є більш консервативним і краще відповідає практиці проєктування СЗІ: критично слабкий елемент (наприклад, відсутність надійного DR або суттєві прогалини у відповідності) не повинен “перекриватися” лише технічними перевагами в іншому сегменті [25].

Результати інтегрального оцінювання та ранжування альтернатив наведено в табл. 3.9. Найвище значення μ_D отримала альтернатива A3 ($\mu_D\ (A3) = 0.8008$), що підтверджує стійку перевагу гібридної архітектури, яка поєднує on-prem контроль із хмарними сервісами моніторингу та керованим реагуванням (MDR). Другою за інтегральною оцінкою виступає SOC-as-a-Service (A4) ($\mu_D\ (A4) = 0.7803$), що пояснюється високими показниками за критеріями G2-G3.

Таблиця 3.9 – Інтегральні значення $\mu_D(P_j)$ та ранжування альтернатив

№	**Альтернатива**	**μD(Pj)**
1	A3	0.8008
2	A4	0.7803
3	A2	0.6876
4	A1	0.4508

Для наочного порівняння профілів альтернатив побудовано накладені графіки перетинів за критеріями G1-G6 (рис. 3.4). З рисунка 3.4 видно, що профіль A3 є найбільш збалансованим: значення перетинів залишаються

високими за більшістю критеріїв, а виражених «провалів», які могли б стати обмеженням у межах t-норми min, практично не спостерігається. Натомість А1 має помітні слабкі місця за окремими критеріями, що й зумовлює мінімальне інтегральне значення. Альтернатива А4 демонструє високі результати за частиною критеріїв, однак поступається А3 за сукупністю параметрів, тоді як А2 займає проміжну позицію.

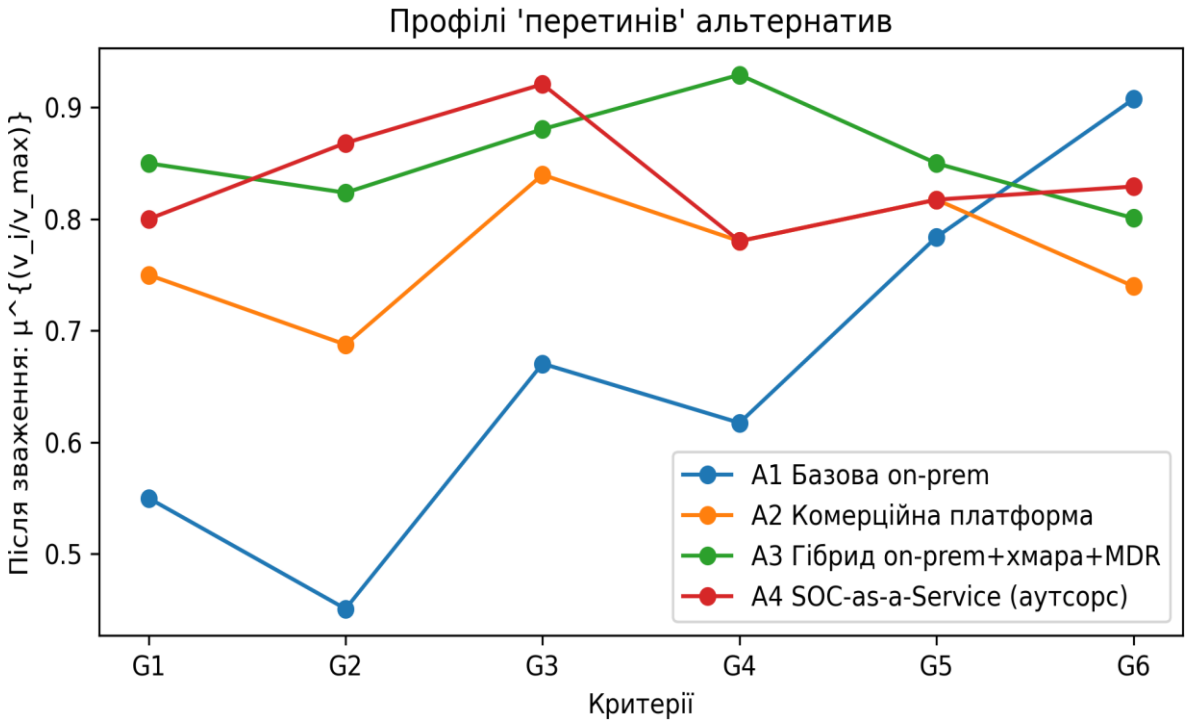


Рисунок 3.4 – Накладені графіки перетинів профілів для альтернатив А1-А4

Оскільки ранжування альтернатив залежить від ваг критеріїв v_i, доцільно перевірити стійкість отриманого рішення до зміни пріоритетів підприємства. Для цього виконується аналіз чутливості, що полягає у варіюванні ваг критеріїв у заданих межах із повторним обчисленням інтегральних оцінок та фіксацією можливих змін лідера. Загальну послідовність сценарного аналізу та побудови графічних матеріалів наведено на рис. 3.5.

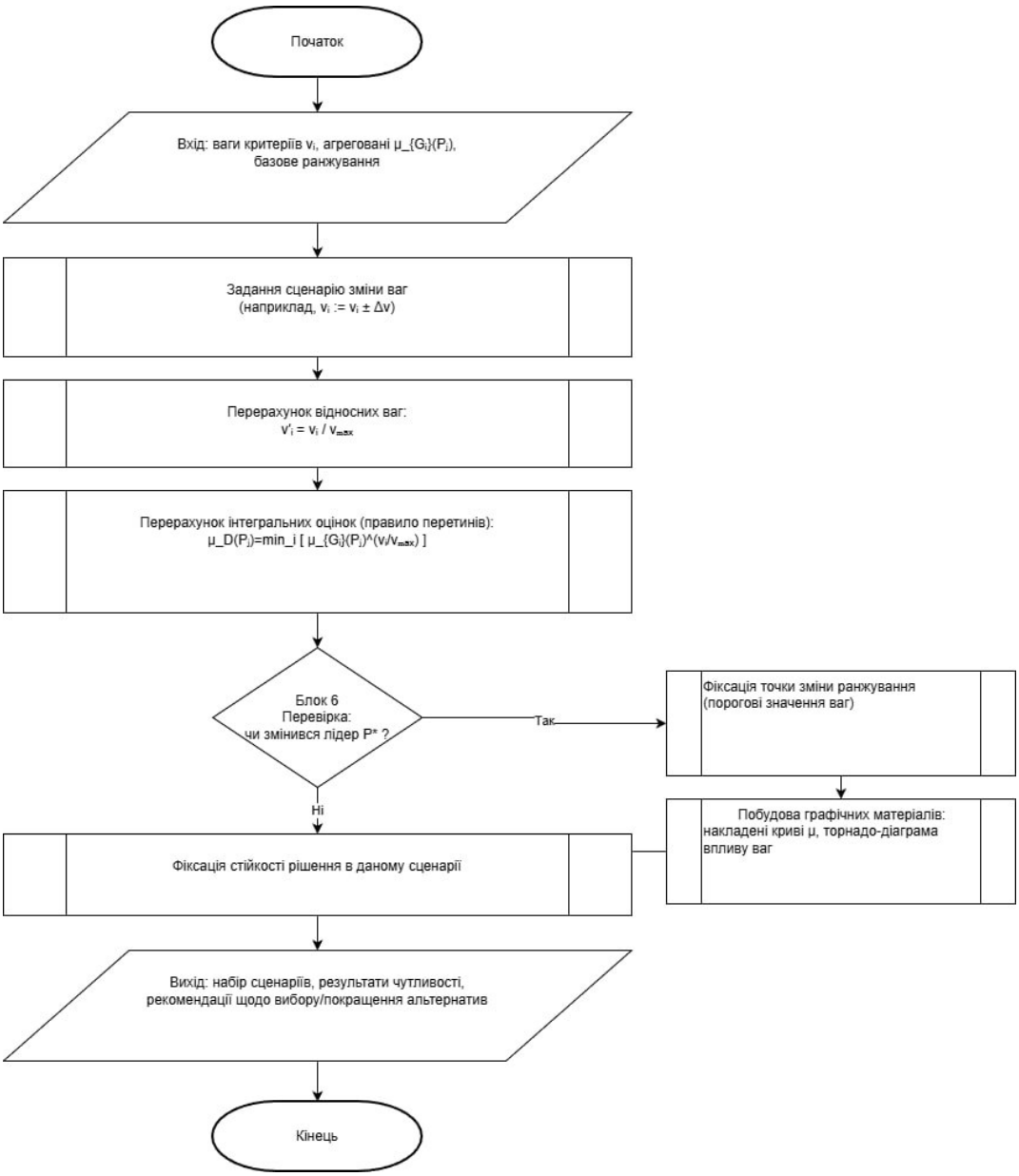


Рисунок 3.5 – Сценарний аналіз і аналіз чутливості (перевірка стійкості ранжування)

Результати аналізу чутливості подаються графічно у вигляді накладених кривих $\mu_D(P_j)$ та діаграми впливу ваг, що дозволяє виділити критерії, які найбільшою мірою визначають підсумкове рішення. На основі цього формуються практичні рекомендації щодо підсилення альтернатив, які мають високий потенціал, але поступаються через окремі “вузькі місця”.

Для оцінки стійкості висновків виконано аналіз чутливості до зміни ваг критеріїв v_i. Аналіз проводився шляхом локального варіювання ваги одного критерію на ±20% із подальшим нормуванням вектора ваг до умови $\sum v_i = 1$ та

повторним обчисленням інтегральної оцінки μ_D. Такий підхід дозволяє перевірити, чи не є лідер «артефактом» конкретного набору ваг, а також сформувати сценарні рекомендації для випадків зміни пріоритетів підприємства.

Таблиця 3.10 – $\mu D(P_j)$ у базовому та сценарних варіантах ваг

Альтернатива	**Base**	**G2 +20%**	**G6 +20%**
A3	0.8008	0.8000	0.7660
A4	0.7803	0.7884	0.7803
A2	0.6876	0.6500	0.6876
A1	0.4508	0.4000	0.4508

Так, рисунок 3.7 ілюструє реакцію інтегральної оцінки лідера на зміну ваг окремих критеріїв. Оскільки агрегування виконано за t-нормою min з підсиленням важливості через v_i/v_{max}, метод є «вузькомісцевим»: найбільший вплив на μ_D мають ті критерії, які формують мінімальні (або близькі до мінімальних) значення в профілі лідируючої альтернативи, тоді як зміна ваг «некритичних» критеріїв може майже не позначатися на підсумковому результаті.

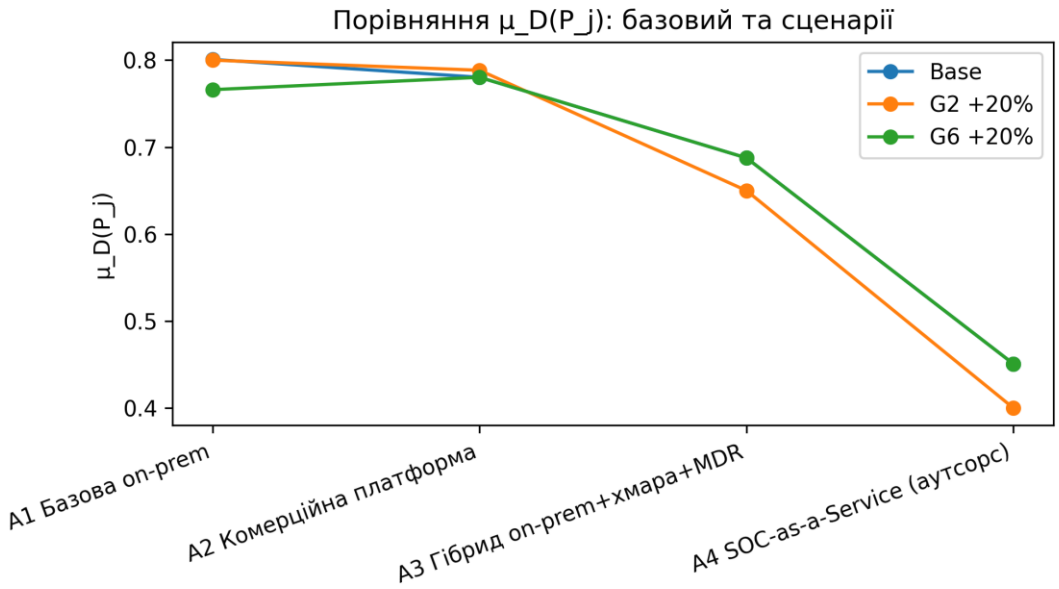


Рисунок 3.6– Порівняння $\mu D(P_j)$ за базовою моделлю та сценаріями зміни ваг

Кількісні результати аналізу чутливості наведено в таблиці 3.10. Як видно, підсилення G6 (сукупна вартість володіння) призводить до зменшення інтегральної оцінки лідера, тобто скорочує «запас переваги» і зближує значення конкурентних альтернатив за сценарію жорсткішого бюджетного пріоритету. Натомість підсилення G1 (ефективність захисту) підвищує μ_D лідера, посилюючи домінування у базовому ранжуванні. Нульові або близькі до нуля зміни для частини критеріїв свідчать, що в межах обраного правила агрегування вони не є визначальними обмеженнями для лідируючої альтернативи в поточному профілі.

Таблиця 3.11 – «Торнадо»-аналіз: вплив варіювання ваг на μ_D лідера

Критерій	**Зміна ваги**	**Δ μD лідера**
G1 Ефективність захисту	20%	0.0302
G6 Сукупна вартість володіння	−20%	0.0228
G2 Відмовостійкість	−20%	0.0000
G3 Відповідність/аудит	−20%	0.0000
G3 Відповідність/аудит	20%	0.0000
G4 Інтегрованість/сумісність	−20%	0.0000
G4 Інтегрованість/сумісність	20%	0.0000
G5 Експлуатаційність	−20%	0.0000
G5 Експлуатаційність	20%	0.0000
G2 Відмовостійкість/DR	20%	-0.0008
G1 Ефективність захисту	−20%	-0.0262
G6 Сукупна вартість володіння	20%	-0.0348

На основі профілів перетинів та аналізу чутливості рекомендовано пріоритет A3 як базової архітектури. Для підвищення запасу стійкості альтернативи A4 варто деталізувати SLA, регламент DR-тестів та контроль ланцюжка постачання постачальника SOC. Для A1 доцільно посилити EDR/бекопіювання і автоматизацію реагування, для A2 – розширити інтеграцію з AD/ERP та підвищити рівень DR-готовності. Відтворюваність розрахунків забезпечується фіксацією матриць попарних порівнянь, нормувальних правил і порогів консистентності, що наведено в попередніх підпунктах.

Висновки до розділу 3

У розділі 3 здійснено практичну реалізацію та апробацію запропонованого методу нечіткого багатокритеріального вибору проєкту системи захисту інформації на прикладі ТОВ «ГРІН КУЛ» — підприємства зі змішаною IT/OT-інфраструктурою та визначеними загрозами, обмеженнями і вимогами до СЗІ. У межах розділу забезпечено перехід від теоретичної постановки задачі до прикладного застосування методу шляхом формування множини альтернатив, побудови системи критеріїв, організації експертного оцінювання та виконання повного циклу розрахунків локальних і інтегральних показників.

Сформовано множину з чотирьох архітектурних альтернатив (A1–A4), релевантних масштабу підприємства й доступним ресурсам, а також систему з шести узагальнених критеріїв, що охоплюють технічні, організаційні та економічні аспекти функціонування СЗІ. Для зменшення суб’єктивних викривлень використано групову експертну процедуру з контролем узгодженості матриць попарних порівнянь та зваженою агрегацією експертних суджень, що забезпечує коректність отриманих ваг критеріїв і локальних пріоритетів альтернатив.

Локальні оцінки інтерпретовано як ступені належності альтернатив до нечітких множин критеріїв, після чого виконано інтегральне узагальнення за правилом перетину з t-нормою min з урахуванням ваг. Застосована схема згортки має некомпенсаційний характер, що методично відповідає задачам проєктування СЗІ, де критично низький рівень виконання окремого критерію повинен обмежувати підсумкову придатність альтернативи.

За результатами інтегрального оцінювання отримано ранжування альтернатив, відповідно до якого найвищу оцінку має альтернатива A3, що свідчить про її найбільш збалансоване задоволення системи критеріїв у заданих умовах підприємства. Для перевірки стійкості висновків виконано аналіз чутливості до варіювання ваг критеріїв. Результати підтверджують загальну стабільність вибору лідера та демонструють залежність запасу переваги від зміни пріоритетів, насамперед у частині економічної доцільності та ефективності

захисту. Таким чином, підсумковий результат розглядається як обґрунтована основа для управлінського рішення, доповнена сценарною інтерпретацією можливих змін пріоритетів, а у розділі 3 доведено прикладну придатність запропонованого методу для задач вибору СЗІ в умовах неоднорідності критеріїв, неповноти інформації та необхідності узгодженого врахування технічних, організаційних і економічних чинників. Метод забезпечує прозорість процедури оцінювання, відтворюваність розрахунків і можливість перевірки стійкості отриманого ранжування.

4 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження лише за умови відповідності вимогам часу як у площині науково-технічного прогресу, так і з позицій економіки. Тому для науково-дослідних робіт необхідним є оцінювання економічної ефективності отриманих результатів.

Магістерська кваліфікаційна робота на тему «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» належить до науково-технічних розробок, що орієнтовані на подальше впровадження у практику (або рішення про комерціалізацію може бути ухвалено в процесі виконання самої роботи). Йдеться про створення програмно-методичного підходу для вибору СЗІ, яким можуть користуватися інші організації, отримуючи економічний ефект за рахунок зниження ризиків, оптимізації витрат та скорочення часу ухвалення рішень. Для реалізації такого потенціалу необхідно визначити зацікавленого замовника/інвестора (напр., інтегратор або підприємство) та обґрунтувати економічну доцільність впровадження.

Для наведеного випадку передбачаються такі етапи робіт:

1) проведення комерційного та технологічного аудиту розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу;

2) розрахунок витрат на виконання та впровадження науково-технічної розробки (методу і прототипу засобу підтримки прийняття рішень);

3) визначення економічної ефективності у разі практичного застосування/комерціалізації потенційним інвестором і підготовка обґрунтування доцільності такого кроку.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Метод вибору проєкту системи захисту інформації на основі

експертного оцінювання» є оцінювання науково-технічного рівня запропонованого методу та рівня його комерційного потенціалу як рішення для підтримки прийняття управлінських рішень у сфері СЗІ.

Оцінювання науково-технічного рівня та комерційного потенціалу рекомендується здійснювати за 5-бальною шкалою за 12 критеріями, наведеними в табл. 4.1 [29].

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою

Продовження табл. 4.1

7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовують ся у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	**Експерт (ПІБ, посада)**		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	5	5	5
2. Ринкові переваги (наявність аналогів)	3	3	3
3. Ринкові переваги (ціна продукту)	4	4	4
4. Ринкові переваги (технічні властивості)	4	4	4
5. Ринкові переваги (експлуатаційні витрати)	4	4	4
6. Ринкові перспективи (розмір ринку)	4	3	3
7. Ринкові перспективи (конкуренція)	3	3	3
8. Практична здійсненність (наявність фахівців)	4	4	4
9. Практична здійсненність (наявність фінансів)	4	4	4
10. Практична здійсненність (необхідність нових матеріалів)	5	5	5
11. Практична здійсненність (термін реалізації)	4	4	4
12. Практична здійсненність (розробка документів)	4	4	4
Сума балів	48	47	47
Середньоарифметична сума балів $СБ_с$	47,3		

За результатами розрахунків, наведених в таблиці 4.2, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в табл. 4.3 [29].

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	**Науково-технічний рівень та комерційний потенціал розробки**
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» становить 47,3 бала, що, відповідно до таблиці 4.3, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий).

4.2 Розрахунок узагальненого коефіцієнта якості розробки

Окрім комерційного аудиту розробки доцільно також розглянути технічний рівень якості розробки, розглянувши її основні технічні показники. Ці показники по-різному впливають на загальну якість проектної розробки.

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення розрахуємо за формулою [30]:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i , \tag{4.1}$$

де k – кількість найбільш важливих технічних показників, які впливають на якість нового технічного рішення;

α_i – коефіцієнт, який враховує питому вагу *і-го* технічного показника в загальній якості розробки. Коефіцієнт α_i визначається експертним шляхом і при цьому має виконуватись умова $\sum_{i=1}^{k} \alpha_i = 1$;

β_i – відносне значення *і-го* технічного показника якості нової розробки.

Відносні значення β_i для різних випадків розраховуємо за такими формулами:

– для показників, зростання яких вказує на підвищення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{нi}}{I_{ai}} , \tag{4.2}$$

де $I_{ні}$ та $I_{на}$ – чисельні значення конкретного *і*-го технічного показника якості відповідно для нової розробки та аналога;

– для показників, зростання яких вказує на погіршення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{ai}}{I_{ні}}, \tag{4.3}$$

Використовуючи наведені залежності можемо проаналізувати та порівняти техніко-економічні характеристики аналогу та розробки на основі отриманих наявних та проектних показників, а результати порівняння зведемо до таблиці 4.4.

Таблиця 4.4 – Порівняння основних параметрів розробки та аналога.

Показники (параметри)	**Одиниця вимірю-вання**	**Аналог**	**Проєкто-ваний метод**	**Відношення (βі)**	**Питома вага (αі)**
Час підготовки рішення (повний цикл: збір → узгодж. → ранжування) – *менше краще*	год	24	8	3.00	0.20
Середній коеф. узгодженості CR (до корекцій) – *менше краще*	%	15	8	1.88	0.20
Прозорість/ аудитованість обчислень (наявність CR-контролю, розв'язання систем відносних рівнянь, відтворюваність) – *більше краще*	бал (0-10)	6	9	1.50	0.15
Підтримка аналізу перетинів і чутливості (what-if, графіки) – *більше краще*	бал (0-10)	5	9	1.80	0.20
Інтегрованість/придатність до застосування (Excel/API, специфіка IT/OT) – *більше краще*	бал (0-10)	6	8	1.33	0.10

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення складе:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i = 0{,}20 \cdot 3{,}00 + 0{,}20 \cdot 1{,}88 + 0{,}15 \cdot 1{,}50 + 0{,}20 \cdot 1{,}80 + 0{,}10 \cdot 1{,}33 + 0{,}15 \cdot 1{,}43 \approx 1{,}91$$

$B_н$ 1 свідчить, що проєктований метод має суттєву перевагу над аналогом за сукупністю ключових параметрів: він швидше готує рішення, забезпечує кращу узгодженість та прозорість розрахунків, містить обов'язковий аналіз перетинів/чутливості, простіше інтегрується у наявні процеси та має нижчі витрати на цикл.

4.3 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов'язані з виконанням НДР за темою «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання», під час планування, обліку та калькулювання собівартості групуються за встановленими статтями витрат відповідно до чинних методичних рекомендацій.

4.3.1 Витрати на оплату праці

До статті «Витрати на оплату праці» відносяться суми основної та додаткової заробітної плати учасників, безпосередньо залучених до виконання теми: керівника НДР, студентів-виконавців, консультантів з ІБ, системних адміністраторів, аналітиків/документаторів, лаборантів та інших фахівців. Розрахунок здійснюється за посадовими окладами, відрядними розцінками та тарифними ставками згідно з діючими в установі системами оплати праці.

Основна заробітна плата дослідників.

Витрати на основну заробітну плату дослідників ($З_о$) визначаються на підставі посадових окладів і планової трудомісткості робіт за формулою [29]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.4)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=22 дні.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.5 – Витрати на заробітну плату дослідників

Найменування посади	**Місячний посадовий оклад, грн**	**Оплата за робочий день, грн**	**Число днів роботи**	**Витрати на заробітну плату, грн**
Аналітик-студент (основний виконавець)	18 000,00	818,18	24	19 636,32
Консультант з ІБ (часткова зайнятість)	25 000,00	1 136,36	6	6 818,16
Системний адміністратор / технік (часткова зайнятість)	19 000,00	863,64	10	8 636,40
Керівник НДР (методичний супровід)	20 000,00	909,09	6	5 454,54
Всього	-	-	-	40 545,42

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Метод та засіб захисту програмного забезпечення з апаратною прив'язкою до USB-носіїв» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \qquad (4.5)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \quad (4.6)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо *Мм*=8000,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду [29];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 22 дн;

$t_{зм}$ – тривалість зміни, год.

$$C_1 = 8000{,}00 \cdot 1{,}10 \cdot 1{,}15 / (22 \cdot 8) = 57{,}50 \text{ грн.}$$

$$З_{р1} = 57{,}50 \cdot 6{,}00 = 345{,}00 \text{ грн.}$$

Таблиця 4.6 – Величина витрат на основну заробітну плату робітників

Найменування робіт	**Тривалість роботи, год**	**Розряд роботи**	**Тарифний коефіцієнт (K_t)**	**Погодинна тарифна ставка, грн**	**Величина оплати на робітника, грн**
Інсталяція робочого середовища (OS, Office/Excel, Python)	6	2	1,1	110	660
Збір і верифікація експертних матриць	8	2	1,1	110	880
Розробка шкал і шаблонів у Excel (критерії, матриці, перевірка CR)	10	3	1,3	130	1 300,00
Реалізація розв'язання систем рівнянь та агрегування (скрипти/макроси)	14	4	1,5	150	2 100,00
Побудова графіків перетинів і аналізу чутливості	8	3	1,3	130	1 040,00

Продовження табл. 4.6

Документування та верстка звітів (таблиці, пояснення, висновки)	10	2	1,1	110	1 100,00
Всього	-	-	-	-	7 080,00

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.7)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод}$ = (40 545,42+ 7 080,00) · 11 / 100% = 5238,76 грн.

4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.8)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (40 545,42+ 7 080,00+ 5238,76) · 22 / 100% = 10596,11 грн.

4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» відносимо витрати на канцелярські та витратні матеріали, друк та недорогі носії/кабелі, що необхідні для старту реалізації теми: підготовки анкет і матриць парних порівнянь, друку методичних інструкцій для експертів, тимчасового зберігання даних оцінювання та мінімальної підготовки робочих місць (кабелі/патч-корд). Ціни підібрані на рівні середніх роздрібних по Україні і не є завищеними.

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}\,, \qquad (4.9)$$

де H_j – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 ... 1,15*);

B_j – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$М_1$ = 2,000 · 185,00 · 1,05 - 0 · 0 = 388,50 грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на матеріали

Найменування матеріалу; марка, тип, сорт	**Ціна за 1 од., грн**	**Норма витрат, од.**	**Величина відходів, од.**	**Ціна відходів, грн/од.**	**Вартість витраченого матеріалу, грн**
Папір офісний А4, 500 арк.	200	1	0	0	200
Заправка картриджа (лазерний)	600	1	0	0	600
Папки-швидкозшивачі (картон/пластик)	25	5	0	0	125
Стікери клейкі 76×76 (блок)	50	3	0	0	150
Маркери перманентні (набір 4 шт.)	120	1	0	0	120
Ручки кулькові (набір 10 шт.)	80	1	0	0	80
USB флеш-накопичувач 32 ГБ	300	1	0	0	300
Кабель USB-A – USB-C, 1 м	150	1	0	0	150
Патч-корд Ethernet Cat5e, 3 м	120	1	0	0	120
Всього	-	-	-	-	1 845,00

4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, що використовуються під час виконання теми «Метод вибору проєкту СЗІ на основі експертного оцінювання», визначаємо за номенклатурою закупівель за формулою

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (4.10)$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ *= 1,1 ... 1,15*).

$К_в = 1 \cdot 209{,}00 \cdot 1{,}05 = 219{,}45$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.8– Витрати на комплектуючі

Найменування комплектуючих	**Кількість, шт.**	**Ціна за штуку, грн**	**Коеф. трансп. витрат $К_j$**	**Сума, грн**
Адаптер USB → RJ45 (гігабітний)	1	600,00	1,05	630,00
Патч-корд Ethernet Cat5e, 10 м	1	300,00	1,05	315,00
Флеш-накопичувач USB 3.0, 32 ГБ	1	300,00	1,03	309,00
Кабель USB-A – USB-C, 1 м	1	150,00	1,03	154,50
Всього (Кв)	-	-	-	1 408,50

4.3.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення. Втрати на «Спецустаткування» відсутні.

4.3.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» відносять витрати на створення та/або придбання спеціалізованих

програмних продуктів і компонентів (прикладних програм, алгоритмів, баз даних), потрібних для виконання досліджень, а також на їх проєктування, підготовку, інсталяцію й налаштування.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.11)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, (K_i = *1,10…1,12);*

k – кількість найменувань програмних засобів.

$B_{прг} = 2\,699{,}00 \cdot 1 \cdot 1{,}05 = 2\,833{,}95$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	**Кількість (період/од.)**	**Ціна одиниці, грн**	**Сума, грн**
Доступ до мережі Internet (високошвидкісний) грн/місяць	1	439,00	460,95
Microsoft 365 Personal (Excel/Word/PowerPoint/OneDrive 1 ТБ) – річна підписка	1 рік	2 699,00	2 833,95
ESET NOD32 Antivirus – 1 ПК, 1 рік	1 ліцензія	899,00	943,95
SuperDecisions (AHP/ANP) – академ. доступ	1 од.	0,00	0,00
Visual Studio Community (IDE)	1 од.	0,00	0,00
Anaconda/Python (NumPy, pandas, matplotlib)	1 од.	0,00	0,00
Всього	-	-	4 238,85

4.3.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.12)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (31\ 499{,}00 \cdot 1) / (3 \cdot 12) = 1\ 749{,}94грн.$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання / активу (модель/тип)	**Балансова вартість, грн**	**Строк корисного використання, років**	**Термін використання під час НДР, міс**	**Амортизаційні відрахування, грн**
Ноутбук Lenovo IdeaPad 5 15IAL7, 16 ГБ/512 ГБ, FHD, Windows 11 Home	31 499,00	3	2	1 749,94
БФП HP Laser MFP 135a (4ZB82A)	11 000,00	5	2	366,67
Маршрутизатор TP-Link Archer AX55 (AX3000, Wi-Fi 6)	2 999,00	4	2	124,96
Windows 11 Home (ESD-ліцензія, 1 ПК), якщо ноутбук без ОС	5 599,00	1	2	933,17
Приміщення лабораторії	420 000,00	30	2	1 333,33
Всього амортизація	-	-	-	4 508,07

4.3.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.13)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e$ = 12,56 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,060 \cdot 352 \cdot 4,32 \cdot 0,90 / 1,00 = 82,12$ грн..

Проведені розрахунки зведемо до таблиці.

Таблиця 4.11 – Витрати на електроенергію

Найменування обладнання	**Встановлена потужність, кВт**	**Тривалість роботи, год**	**Тариф, грн/кВт·год**	**Сума, грн**
Ноутбук Lenovo IdeaPad 5 15IAL7	0,060	352	4,32	82,12
Маршрутизатор TP-Link Archer AX55	0,012	1 440	4,32	74,65
БФП HP Laser MFP 135a (друк/скан)	0,365	15	4,32	14,19
Разом	—	—	—	170,96

4.3.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, здобувачів, зайнятих розробленням досліджень, пов’язані з проведенням

випробувань макетів та приладів, а також витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних експериментів. Витрати за статтею «Службові відрядження» розраховуємо як 0…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.14)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св} = 0\%$.

$В_{св}$ (58 354,55 + 5 636,31) · 0 / 100 = 0,00 грн.

4.3.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.15)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$В_{сп}$ = (58 354,55 + 5 636,31) · 20 / 100 = 12 798,17 грн.

4.3.11 Інші витрати

До статті «Інші витрати» належать платежі банків, оплатні послуги, витрати на публікації, дрібні послуги та витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.16)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів} = 50\%$.

$I_в$ = (58 354,55 + 5 636,31) · 50 / 100 = 31 995,43 грн.

4.3.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винагороди та різноманітні виплати; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банку; витрати, пов'язані з основним виробництвом продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.17)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв} = 100\%$.

$В_{нзв}$ = (58 354,55 + 5 636,31) · 100 / 100 = 63 990,86 грн,

4.3.13 Загальні витрати на проведення науково-дослідної (науково-технічної) роботи

Витрати на проведення науково-дослідної роботи на тему «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» приймемо як:

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (4.18)$$

$В_{заг}$ = 63 990,86 + 7 038,99 + 15 626,57 + 1 748,00 + 1 455,30 + 3 598,00 + 17 174,74 + 0,00 + 0,00 + 12 798,17 + 31 995,43 + 63 990,86 = 219 416,92 грн,

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.19)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,9.

ЗВ = 219 416,92 / 0 9 = 243 796,58 грн,

4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати досліджень, проведені за темою «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання», передбачають комерціалізацію протягом 4-х років реалізації на ринку.

Розробка є сукупністю методичних та програмних рішень (програмного забезпечення, програмного продукту) для використання масовими споживачами. В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів продукту, у періоди часу, що аналізуються, від покращення його певних характеристик;

Показник	**1-й рік**	**2-й рік**	**3-й рік**	**4-й рік**
Збільшення кількості споживачів, осіб	50	120	200	300

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, приймемо 200000 осіб;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, приймемо 6 000грн/рік;

$\pm\Delta Ц_о$ – зміна вартості програмного продукту від впровадження результатів науково-технічної розробки, приймемо 67,81 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 4-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [29]:

$$\Delta П_i = (\pm\Delta Ц_о \cdot N + Ц_о \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.20)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2025 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту). Приймемо ρ =40%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2025 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1 = (67,81 \cdot 200000 + 277,81 \cdot 4000) \cdot 0,83 \cdot 0,40 \cdot (1 - 0,18) = 3994642,86$ грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2 = (67,81 \cdot 200000 + 277,81 \cdot 8000) \cdot 0,83 \cdot 0,40 \cdot (1 - 0,18) = 4297166,84$ грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3 = (67,81 \cdot 200000 + 277,81 \cdot 5000) \cdot 0,83 \cdot 0,40 \cdot (1 - 0,18) = 4070273,85$ грн.

Збільшення чистого прибутку 4-го року:

$\Delta П_4 = (67,81 \cdot 200000 + 277,81 \cdot 2000) \cdot 0,83 \cdot 0,40 \cdot (1 - 0,18) = 3843380,87$ грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.21)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ=0,12;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

ПП = 3994642,86/(1+0,12)[1] + 4297166,84/(1+0,12)[2]+ +4070273,85/(1+0,12)[3] + 3 843 380,87/(1+0,12)[4] = 3 566 645,41 + 3 425 675,10 + 2 897 140,53 + 2 442 538,03 = 12 331 999,06 грн.

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \quad (4.22)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=1,5;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 243 796,58 грн.

$PV = k_{інв} \cdot ЗВ$ *=1,5 · 243 796,58 = 365 694,87грн.*

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \quad (4.23)$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 12 331 999,06 грн.

PV – теперішня вартість початкових інвестицій, 365 694,87грн.

$E_{абс} = ПП - PV = 12\ 331\ 999{,}06 - 365\ 694{,}87 = 11\ 966\ 304{,}19$ *грн.*

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \quad (4.24)$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 11 966 304,19 грн.

PV – теперішня вартість початкових інвестицій, 365 694,87грн.

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 4 роки.

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1 = (1+11\ 966\ 304{,}19/365\ 694{,}87)^{1/4} = 2{,}41.$$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \quad (4.25)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2025 році в Україні d =0,11;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,3.

$\tau_{мін}$= 0,11+0,3 = 0,41 < 1,46 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності.

Тобто інвестувати в науково-дослідну роботу за темою «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \tag{4.26}$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$= 1 / 2,41= 0,41 р.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Висновки до розділу 4

За підсумками проведених розрахунків рівень комерційного потенціалу розробки за темою «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» становить 47,3 бала, що відповідно до шкали

інтерпретації свідчить про високий комерційний потенціал і доцільність подальшої реалізації.

За техніко-економічними параметрами узагальнений коефіцієнт якості методу відносно аналога дорівнює $V_n \approx 1{,}91$, тобто запропоноване рішення переважає наявні підходи майже вдвічі за сукупністю ключових властивостей (швидкість підготовки рішень, контроль узгодженості CR, прозорість обчислень через розв'язання систем відносних рівнянь, наявність аналізу перетинів/чутливості, інтегрованість у робочі процеси).

Розрахунок економічної ефективності при можливої комерціалізації показав, що приведена вартість зростання чистих прибутків інвестора за 4 роки становить ПП = 12 331 999,06 грн, початкові інвестиції (з урахуванням коефіцієнта впровадження) – PV = 365 694,87 грн, а абсолютний економічний ефект – E_{abc} = 11 966 304,19 грн. Внутрішня економічна дохідність за прийнятою методикою дорівнює $E_v \approx 2{,}41$, що суттєво перевищує мінімально допустимий рівень (≈0,41 за d=0,11 та f=0,30).

Період окупності інвестицій становить $T_{ok} \approx 0{,}41$ року (< 1 року), що істотно менше за порогові 3 роки і підтверджує комерційну привабливість розробки для потенційного інвестора.

Отже, можна зробити висновок про доцільність виконання НДР за темою «Метод вибору проєкту системи захисту інформації на основі експертного оцінювання» та перспективність її впровадження як інструмента підтримки прийняття рішень у сфері СЗІ. Рекомендовано перейти до пілотного впровадження (апробації на реальному підприємстві) з подальшою підготовкою до масштабування.

ВИСНОВКИ

У магістерській кваліфікаційній роботі розв’язано актуальну задачу обґрунтованого вибору проєкту системи захисту інформації для організації в умовах багатокритеріальності, невизначеності та неповноти вихідних даних. Мета роботи полягала у покращенні ефективності та апробації методу, який поєднує експертне оцінювання, попарні порівняння та апарат нечітких множин для отримання відтворюваного рейтингу альтернатив СЗІ.

У ході виконання роботи проведено аналіз предметної області інформаційної безпеки та узагальнено підходи до опису загроз, стандартів і практик побудови СЗІ. Показано, що в задачах вибору архітектури СЗІ експертні оцінки часто мають лінгвістичну природу, а частина показників не може бути визначена точними метриками на ранніх етапах проєктування, що обґрунтовує застосування нечіткого підходу. Сформовано постановку задачі багатокритеріального вибору у вигляді ранжування множини альтернативних проєктів за системою узагальнених критерії. Критерії структуровано у шість логічних груп. Така декомпозиція забезпечує зрозумілість і керованість експертного оцінювання та полегшує інтерпретацію результатів.

Покращенно метод одержання локальних оцінок альтернатив на основі попарних порівнянь і подальшої нечіткої інтерпретації результатів. Для кожного критерію G_i побудовано функції належності $\mu_{Gi}(P_j)$, що відображають ступінь виконання критерію альтернативою. Показано, що нормування $\sum_{j=1}^{m} \mu_{Gi}(P_j) = 1$ використовується як наслідок застосування вектора пріоритетів, отриманого з матриць попарних порівнянь, і забезпечує порівнюваність оцінок у межах критерію.

Удосконалено процедуру експертного оцінювання за рахунок контролю узгодженості суджень. Запропоновано використовувати показники узгодженості CI та CR для матриць попарних порівнянь критеріїв і альтернатив, що дозволяє виявляти суперечливі судження та підвищує надійність і відтворюваність підсумкового рішення. Загальну логіку методу подано у вигляді блок-схеми

алгоритму, яка відображає послідовність етапів від формування вихідних даних до отримання інтегральної оцінки та ранжування.

Запропоновано підхід до багатокритеріальної агрегації локальних оцінок з урахуванням важливості критеріїв. Інтегральну оцінку альтернативи подано у вигляді $\mu_D(P_j)$, що інтерпретується як ступінь прийнятності альтернативи за всіма критеріями. Застосування "консервативної" логіки агрегації дозволяє уникнути небажаної компенсації критично слабких характеристик надмірними перевагами за окремими параметрами, що є важливим для задач інформаційної безпеки.

Виконано практичну апробацію методу на прикладі підприємства ТОВ «ГРІН КУЛ» з використанням групи експертів, набору альтернатив та критеріїв. За результатами розрахунків отримано підсумковий рейтинг альтернатив і визначено найбільш доцільний проєкт СЗІ для заданих умов. Проведено аналіз чутливості, який підтвердив стійкість лідера до помірних змін ваг критеріїв, що додатково підвищує довіру до прийнятого рішення. Отримані результати мають практичне значення для задач обґрунтування вибору архітектури СЗІ, планування модернізації захисної інфраструктури, підготовки техніко-економічного обґрунтування та підтримки управлінських рішень у сфері кібербезпеки. Запропонований метод є гнучким: він допускає розширення набору критеріїв і альтернатив, зміну шкал оцінювання, уточнення правил агрегації та інтеграцію з ризик-орієнтованими підходами.

Перспективами подальших досліджень є: розширення моделі за рахунок кількісного врахування ризиків і збитків, автоматизація збору частини метрик з систем моніторингу, використання нечітких чисел трикутного/трапецієподібного типу для більш природного опису лінгвістичних оцінок, а також порівняння результатів із альтернативними методами ранжування для підвищення обґрунтованості та перевірки узгодженості висновків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023: July 2022 to June 2023. Luxembourg: Publications Office of the European Union, 2023. URL: https://data.europa.eu/doi/10.2824/782573 (date of access: 01.11.2025).

2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva: International Organization for Standardization, 2022. URL: https://www.iso.org/standard/82875.html (date of access: 04.11.2025).

3. Архипов О., Касперький І. Проблеми методики отримання та обробки оціночних суджень членів експертних комісій, створюваних державними експертами з питань таємниць. *Правова інформатика.* 2006. № 4(12). С. 54-60. URL: https://ippi.org.ua/sites/default/files/06aoept.pdf (дата звернення: 04.11.2025).

4. Пасічник В.В., Юнчик В.Л., Кунанець Н.Е., Федонюк А.А. Використання нечіткої логіки у процесі експертного оцінювання електронних навчальних ресурсів. *Науковий вісник НЛТУ України.* 2022. Т. 32, № 1. С. 112-121. URL: https://nv.nltu.edu.ua/index.php/journal/article/view/2439 (дата звернення: 04.11.2025).

5. Zadeh L.A. Fuzzy Sets. *Information and Control.* 1965. Vol. 8. P. 338-353. URL:https://www.dcsc.tudelft.nl/~sc4081/2016/Materials/Zadeh_1965_fuzzy_sets.pdf (date of access: 05.11.2025).

6. Bellman R.E., Zadeh L.A. Decision-Making in a Fuzzy Environment. *Management Science.* 1970. Vol. 17(4). P. B-141–B-164. URL: https://www.jstor.org/stable/2629367 (date of access: 05.11.2025).

7. Zimmermann H.-J. Fuzzy programming and linear programming with several objective functions. *Fuzzy Sets and Systems.* 1978. Vol. 1(1). P. 45-55. URL: https://doi.org/10.1016/0165-0114(78)90031-3 (date of access: 05.11.2025).

8. Klir G.J., Yuan B. Fuzzy Sets and Fuzzy Logic: Theory and Applications. Upper Saddle River, NJ: Prentice Hall, 1995.

9. Dubois D., Prade H. Fuzzy Sets and Systems: Theory and Applications. New York: Academic Press, 1980.

10. Ross T.J. Fuzzy Logic with Engineering Applications. 3rd ed. Chichester: Wiley, 2010.

11. Saaty T.L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: McGraw-Hill, 1980.

12. Buckley J.J. Fuzzy hierarchical analysis. *Fuzzy Sets and Systems.* 1985. Vol. 17(3). P. 233-247. URL: https://doi.org/10.1016/0165-0114(85)90090-9 (date of access: 05.11.2025).

13. Chang D.-Y. Applications of the extent analysis method on fuzzy AHP. *European Journal of Operational Research.* 1996. Vol. 95(3). P. 649-655. URL: https://doi.org/10.1016/0377-2217(95)00300-2 (date of access: 05.11.2025).

14. Hwang C.-L., Yoon K. Multiple Attribute Decision Making: Methods and Applications. Berlin: Springer, 1981.

15. Chen C.-T. Extensions of the TOPSIS for group decision-making under fuzzy environment. *Fuzzy Sets and Systems.* 2000. Vol. 114(1). P. 1-9. URL: https://doi.org/10.1016/S0165-0114(97)00377-1 (date of access: 05.11.2025).

16. NIST. The NIST Cybersecurity Framework (CSF) 2.0. 2024. URL: https://www.nist.gov/cyberframework (date of access: 05.11.2025).

17. NIST. Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (date of access: 05.11.2025).

18. NIST. Guide for Conducting Risk Assessments (SP 800-30 Rev. 1). 2012. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (date of access: 05.11.2025).

19. NIST. Guide to Computer Security Incident Handling (SP 800-61 Rev. 2). 2012. URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final (date of access: 05.11.2025).

20. Center for Internet Security. CIS Critical Security Controls. URL: https://www.cisecurity.org/controls (date of access: 05.11.2025).

21. MITRE. ATT&CK® Knowledge Base. URL: https://attack.mitre.org/ (date of access: 05.11.2025).

22. OWASP Foundation. OWASP Top 10 – 2021. URL: https://owasp.org/Top10/ (date of access: 05.11.2025).

23. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection. Information security controls. Geneva: ISO, 2022. URL: https://www.iso.org/standard/75652.html (date of access: 05.11.2025).

24. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks. Geneva: ISO, 2022. URL: https://www.iso.org/standard/80585.html (date of access: 05.11.2025).

25. ISO 31000:2018 Risk management – Guidelines. Geneva: ISO, 2018. URL: https://www.iso.org/standard/65694.html (date of access: 05.11.2025).

26. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 05.11.2025).

27. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 05.11.2025).

28. ISO/IEC 27002 та ISO/IEC 27005 (онлайн-огляд стандартів ISO/IEC 27k). ISO/IEC 27k family. URL: https://www.iso.org/isoiec- 27001-information-security.html (date of access: 05.11.2025).

29. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт. Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. Вінниця : ВНТУ, 2021. 42 с.

30. Кавецький В. В. Економічне обґрунтування інноваційних рішень: практикум. В. В. Кавецький, В. О. Козловський, І. В. Причепа. Вінниця : ВНТУ, 2016. 113 с.

ДОДАТКИ

Додаток А. ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Метод вибору проєкту системи захисту інформації на основі експертного оцінювання

Автор роботи: Дмитришин Єгор Тарасович
Тип роботи: магістерська кваліфікаційна робота
Підрозділ кафедра захисту інформації ФІТКІ, група І БС-24м

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism 1,3 %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

√ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

В. о. зав. кафедри ЗІ д. т. н., проф. _____ Володимир ЛУЖЕЦЬКИЙ

Гарант освітньої програми «Безпека інформаційних і комунікаційних систем» к.т.н., доцент _____ Олеся ВОЙТОВИЧ

Особа, відповідальна за перевірку _____ Валентина КАПЛУН

З висновком експертної комісії ознайомлений(-на)

Керівник _____ Наталія КОНДРАТЕНКО

Здобувач _____ Єгор ДМИТРИШИН

ДОДАТОК Б. ВХІДНІ МАТРИЦІ ЕКСПЕРТІВ ТА ХІД

Б.1. Матриці попарних порівнянь критеріїв (E1–E5)

Кожен експерт заповнює матрицю 6×6 за шкалою Сааті 1–9. Узгодженість перевіряється за CR.

Матриця Б.1.1 – Порівняння критеріїв експертом E1

Показник	G1	G2	G3	G4	G5	G6
G1	1.000	2.000	2.000	2.000	2.000	3.000
G2	0.500	1.000	1.000	1.000	2.000	2.000
G3	0.500	1.000	1.000	1.000	2.000	1.000
G4	0.500	1.000	1.000	1.000	2.000	2.000
G5	0.500	0.500	0.500	0.500	1.000	2.000
G6	0.333	0.500	1.000	0.500	0.500	1.000

E1: λmax=6.161; CI=0.032; CR=0.026.

Матриця Б.1.2 – Порівняння критеріїв експертом E2

Показник	G1	G2	G3	G4	G5	G6
G1	1.000	2.000	3.000	2.000	2.000	2.000
G2	0.500	1.000	2.000	1.000	2.000	2.000
G3	0.333	0.500	1.000	2.000	1.000	1.000
G4	0.500	1.000	0.500	1.000	1.000	2.000
G5	0.500	0.500	1.000	1.000	1.000	2.000
G6	0.500	0.500	1.000	0.500	0.500	1.000

E2: λmax=6.265; CI=0.053; CR=0.043.

Матриця Б.1.3 – Порівняння критеріїв експертом E3

Показник	G1	G2	G3	G4	G5	G6
G1	1.000	1.000	2.000	2.000	1.000	3.000
G2	1.000	1.000	0.500	1.000	2.000	2.000
G3	0.500	2.000	1.000	0.500	1.000	2.000
G4	0.500	1.000	2.000	1.000	2.000	2.000
G5	1.000	0.500	1.000	0.500	1.000	1.000
G6	0.333	0.500	0.500	0.500	1.000	1.000

E3: λmax=6.360; CI=0.072; CR=0.058.

Матриця Б.1.4 – Порівняння критеріїв експертом E4

Показник	G1	G2	G3	G4	G5	G6
G1	1.000	1.000	3.000	2.000	3.000	1.000
G2	1.000	1.000	2.000	2.000	1.000	2.000
G3	0.333	0.500	1.000	1.000	2.000	2.000
G4	0.500	0.500	1.000	1.000	1.000	2.000
G5	0.333	1.000	0.500	1.000	1.000	2.000
G6	1.000	0.500	0.500	0.500	0.500	1.000

E4: λmax=6.442; CI=0.088; CR=0.071.

Матриця Б.1.5 – Порівняння критеріїв експертом E5

Показник	G1	G2	G3	G4	G5	G6
G1	1.000	0.500	2.000	1.000	2.000	5.000
G2	2.000	1.000	0.500	2.000	2.000	2.000
G3	0.500	2.000	1.000	2.000	2.000	3.000
G4	1.000	0.500	0.500	1.000	3.000	2.000
G5	0.500	0.500	0.500	0.333	1.000	2.000
G6	0.200	0.500	0.333	0.500	0.500	1.000

E5: λmax=6.477; CI=0.095; CR=0.077.

Б.2. Агрегація критеріїв та отримання ваг vi

$a_{ij} = \prod_k (a_{ij}{}^k)^{\beta k}$, *де* $\beta k = 0.2$

Матриця Б.2.1 – Групова (зважено-геометрична) матриця критеріїв

Показник	G1	G2	G3	G4	G5	G6
G1	1.000	1.149	2.352	1.741	1.888	2.460
G2	0.871	1.000	1.000	1.320	1.741	2.000
G3	0.425	1.000	1.000	1.149	1.516	1.644
G4	0.574	0.758	0.871	1.000	1.644	2.000
G5	0.530	0.574	0.660	0.608	1.000	1.741
G6	0.407	0.500	0.608	0.500	0.574	1.000

Узгодженість групової матриці: CR=0.012 ≤ 0.10.

Таблиця Б.2 – Порівняння ваг критеріїв (розрахунок vs табл. 3.6)

Показник	vi (розрах.)	vi (у файлі)
G1	0.2634	0.2300
G2	0.1985	0.1800
G3	0.1628	0.1600
G4	0.1634	0.1700
G5	0.1217	0.1400
G6	0.0903	0.1200

Б.3. Матриці попарних порівнянь альтернатив за кожним критерієм (E1–E5)

Нижче наведено матриці 4×4 (шкала 1–9) для кожного критерію Gi та експертів E1–E5. З них обчислюються локальні пріоритети w методом геометричних середніх.

Б.3.1. Критерій G1

Матриця Б.3.1.1 – G1, експерт E1

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.333	0.500
A2	2.000	1.000	0.500	1.000
A3	3.000	2.000	1.000	1.000
A4	2.000	1.000	1.000	1.000

Таблиця Б.3.1.1 – w та показники узгодженості (E1)

Показник	w (локальні пріоритети)
A1	0.1252
A2	0.2330
A3	0.3647
A4	0.2771

E1: CR=0.017.

Матриця Б.3.1.2 – G1, експерт E2

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.500	0.500
A2	2.000	1.000	1.000	1.000
A3	2.000	1.000	1.000	2.000
A4	2.000	1.000	0.500	1.000

Таблиця Б.3.1.2 – w та показники узгодженості (E2)

Показник	w (локальні пріоритети)
A1	0.1416
A2	0.2833
A3	0.3369
A4	0.2382

Матриця Б.3.1.3 – G1, експерт E3

Показник	A1	A2	A3	A4
A1	1.000	0.333	0.500	1.000
A2	3.000	1.000	1.000	2.000
A3	2.000	1.000	1.000	2.000
A4	1.000	0.500	0.500	1.000

Таблиця Б.3.1.3 – w та показники узгодженості (E3)

Показник	w (локальні пріоритети)
A1	0.1477
A2	0.3618
A3	0.3270
A4	0.1635

E3: CR=0.008.

Матриця Б.3.1.4 – G1, експерт E4

Показник	A1	A2	A3	A4
A1	1.000	2.000	1.000	0.500
A2	0.500	1.000	2.000	0.500
A3	1.000	0.500	1.000	0.500
A4	2.000	2.000	2.000	1.000

Таблиця Б.3.1.4 – w та показники узгодженості (E4)

Показник	w (локальні пріоритети)
A1	0.2364
A2	0.1988
A3	0.1672
A4	0.3976

E4: CR=0.068.

Матриця Б.3.1.5 – G1, експерт E5

Показник	A1	A2	A3	A4
A1	1.000	1.000	1.000	2.000
A2	1.000	1.000	0.500	2.000
A3	1.000	2.000	1.000	2.000
A4	0.500	0.500	0.500	1.000

Таблиця Б.3.1.5 – w та показники узгодженості (E5)

Показник	w (локальні пріоритети)
A1	0.2833
A2	0.2382
A3	0.3369
A4	0.1416

E5: CR=0.022.

Б.3.2. Критерій G2

Матриця Б.3.2.1 – G2, експерт E1

Показник	A1	A2	A3	A4
A1	1.000	1.000	0.333	1.000
A2	1.000	1.000	1.000	2.000
A3	3.000	1.000	1.000	1.000
A4	1.000	0.500	1.000	1.000

Таблиця Б.3.2.1 – w та показники узгодженості (E1)

Показник	w (локальні пріоритети)
A1	0.1851
A2	0.2896
A3	0.3205
A4	0.2048

E1: CR=0.080.

Матриця Б.3.2.2 – G2, експерт E2

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.500	0.500
A2	2.000	1.000	0.500	1.000
A3	2.000	2.000	1.000	1.000
A4	2.000	1.000	1.000	1.000

Таблиця Б.3.2.2 – w та показники узгодженості (E2)

Показник	w (локальні пріоритети)
A1	0.1416
A2	0.2382
A3	0.3369
A4	0.2833

E2: CR=0.022.

Матриця Б.3.2.3 – G2, експерт E3

Показник	A1	A2	A3	A4
A1	1.000	2.000	0.500	2.000
A2	0.500	1.000	0.500	3.000
A3	2.000	2.000	1.000	2.000
A4	0.500	0.333	0.500	1.000

Таблиця Б.3.2.3 – w та показники узгодженості (E3)

Показник	w (локальні пріоритети)
A1	0.2741
A2	0.2145
A3	0.3876
A4	0.1238

E3: CR=0.080.

Матриця Б.3.2.4 – G2, експерт E4

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.500	1.000
A2	2.000	1.000	2.000	2.000
A3	2.000	0.500	1.000	1.000
A4	1.000	0.500	1.000	1.000

Таблиця Б.3.2.4 – w та показники узгодженості (E4)

Показник	w (локальні пріоритети)
A1	0.1672
A2	0.3976
A3	0.2364
A4	0.1988

E4: CR=0.022.

Матриця Б.3.2.5 – G2, експерт E5

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.250	1.000
A2	2.000	1.000	0.500	0.500
A3	4.000	2.000	1.000	3.000
A4	1.000	2.000	0.333	1.000

Таблиця Б.3.2.5 – w та показники узгодженості (E5)

Показник	w (локальні пріоритети)
A1	0.1306
A2	0.1847
A3	0.4862
A4	0.1985

E5: CR=0.076.

Б.3.3. Критерій G3

Матриця Б.3.3.1 – G3, експерт E1

Показник	A1	A2	A3	A4
A1	1.000	2.000	1.000	1.000
A2	0.500	1.000	1.000	1.000
A3	1.000	1.000	1.000	1.000
A4	1.000	1.000	1.000	1.000

Таблиця Б.3.3.1 – w та показники узгодженості (E1)

Показник	w (локальні пріоритети)
A1	0.2951
A2	0.2087
A3	0.2481
A4	0.2481

E1: CR=0.022.

Матриця Б.3.3.2 – G3, експерт E2

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.500	0.500
A2	2.000	1.000	1.000	1.000
A3	2.000	1.000	1.000	2.000
A4	2.000	1.000	0.500	1.000

Таблиця Б.3.3.2 – w та показники узгодженості (E2)

Показник	w (локальні пріоритети)
A1	0.1416
A2	0.2833
A3	0.3369
A4	0.2382

E2: CR=0.022.

Матриця Б.3.3.3 – G3, експерт E3

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.500	1.000
A2	2.000	1.000	0.500	0.500
A3	2.000	2.000	1.000	2.000
A4	1.000	2.000	0.500	1.000

Таблиця Б.3.3.3 – w та показники узгодженості (E3)

Показник	w (локальні пріоритети)
A1	0.1672
A2	0.1988
A3	0.3976
A4	0.2364

E3: CR=0.068.

Матриця Б.3.3.4 – G3, експерт E4

Показник	A1	A2	A3	A4
A1	1.000	0.500	2.000	0.500
A2	2.000	1.000	2.000	2.000
A3	0.500	0.500	1.000	1.000
A4	2.000	0.500	1.000	1.000

Таблиця Б.3.3.4 – w та показники узгодженості (E4)

Показник	w (локальні пріоритети)
A1	0.1988
A2	0.3976
A3	0.1672
A4	0.2364

E4: CR=0.068.

Матриця Б.3.3.5 – G3, експерт E5

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.500	0.500
A2	2.000	1.000	2.000	2.000
A3	2.000	0.500	1.000	0.500
A4	2.000	0.500	2.000	1.000

Таблиця Б.3.3.5 – w та показники узгодженості (E5)

Показник	w (локальні пріоритети)
A1	0.1381
A2	0.3905
A3	0.1953
A4	0.2761

E5: CR=0.045.

Б.3.4. Критерій G4

Матриця Б.3.4.1 – G4, експерт E1

Показник	A1	A2	A3	A4
A1	1.000	1.000	0.500	1.000
A2	1.000	1.000	1.000	2.000
A3	2.000	1.000	1.000	2.000
A4	1.000	0.500	0.500	1.000

Таблиця Б.3.4.1 – w та показники узгодженості (E1)

Показник	w (локальні пріоритети)
A1	0.2026
A2	0.2865
A3	0.3407
A4	0.1703

E1: CR=0.022.

Матриця Б.3.4.2 – G4, експерт E2

Показник	A1	A2	A3	A4
A1	1.000	2.000	0.500	1.000
A2	0.500	1.000	1.000	1.000
A3	2.000	1.000	1.000	2.000
A4	1.000	1.000	0.500	1.000

Таблиця Б.3.4.2 – w та показники узгодженості (E2)

Показник	w (локальні пріоритети)
A1	0.2441
A2	0.2053
A3	0.3453
A4	0.2053

E2: CR=0.068.

Матриця Б.3.4.3 – G4, експерт E3

Показник	A1	A2	A3	A4
A1	1.000	2.000	0.500	0.500
A2	0.500	1.000	0.500	1.000
A3	2.000	2.000	1.000	2.000
A4	2.000	1.000	0.500	1.000

Таблиця Б.3.4.3 – w та показники узгодженості (E3)

Показник	w (локальні пріоритети)
A1	0.1988
A2	0.1672
A3	0.3976
A4	0.2364

E3: CR=0.068.

Матриця Б.3.4.4 – G4, експерт E4

Показник	A1	A2	A3	A4
A1	1.000	0.333	0.500	0.500
A2	3.000	1.000	0.500	1.000
A3	2.000	2.000	1.000	1.000
A4	2.000	1.000	1.000	1.000

Таблиця Б.3.4.4 – w та показники узгодженості (E4)

Показник	w (локальні пріоритети)
A1	0.1265
A2	0.2606
A3	0.3330
A4	0.2800

E4: CR=0.043.

Матриця Б.3.4.5 – G4, експерт E5

Показник	A1	A2	A3	A4
A1	1.000	0.500	3.000	1.000
A2	2.000	1.000	2.000	2.000
A3	0.333	0.500	1.000	0.500
A4	1.000	0.500	2.000	1.000

Таблиця Б.3.4.5 – w та показники узгодженості (E5)

Показник	w (локальні пріоритети)
A1	0.2558
A2	0.3888
A3	0.1242
A4	0.2312

E5: CR=0.043.

Б.3.5. Критерій G5

Матриця Б.3.5.1 – G5, експерт E1

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.500	0.500
A2	2.000	1.000	1.000	1.000
A3	2.000	1.000	1.000	2.000
A4	2.000	1.000	0.500	1.000

Таблиця Б.3.5.1 – w та показники узгодженості (E1)

Показник	w (локальні пріоритети)
A1	0.1416
A2	0.2833
A3	0.3369
A4	0.2382

E1: CR=0.022.

Матриця Б.3.5.2 – G5, експерт E2

Показник	A1	A2	A3	A4
A1	1.000	0.500	0.500	0.500
A2	2.000	1.000	2.000	2.000
A3	2.000	0.500	1.000	0.500
A4	2.000	0.500	2.000	1.000

Таблиця Б.3.5.2 – w та показники узгодженості (E2)

Показник	w (локальні пріоритети)
A1	0.1381
A2	0.3905
A3	0.1953
A4	0.2761

E2: CR=0.045.

Матриця Б.3.5.3 – G5, експерт E3

Показник	A1	A2	A3	A4
A1	1.000	1.000	1.000	2.000
A2	1.000	1.000	1.000	3.000
A3	1.000	1.000	1.000	1.000
A4	0.500	0.333	1.000	1.000

Таблиця Б.3.5.3 – w та показники узгодженості (E3)

Показник	w (локальні пріоритети)
A1	0.2870
A2	0.3176
A3	0.2413
A4	0.1542

E3: CR=0.043.

Матриця Б.3.5.4 – G5, експерт E4

Показник	A1	A2	A3	A4
A1	1.000	1.000	0.500	0.500
A2	1.000	1.000	1.000	2.000
A3	2.000	1.000	1.000	2.000
A4	2.000	0.500	0.500	1.000

Таблиця Б.3.5.4 – w та показники узгодженості (E4)

Показник	w (локальні пріоритети)
A1	0.1703
A2	0.2865
A3	0.3407
A4	0.2026

E4: CR=0.068.

Матриця Б.3.5.5 – G5, експерт E5

Показник	A1	A2	A3	A4
A1	1.000	2.000	0.500	1.000
A2	0.500	1.000	1.000	2.000
A3	2.000	1.000	1.000	2.000
A4	1.000	0.500	0.500	1.000

Таблиця Б.3.5.5 – w та показники узгодженості (E5)

Показник	w (локальні пріоритети)
A1	0.2426
A2	0.2426
A3	0.3431
A4	0.1716

E5: CR=0.091.

Б.3.6. Критерій G6

Матриця Б.3.6.1 – G6, експерт E1

Показник	A1	A2	A3	A4
A1	1.000	2.000	2.000	2.000
A2	0.500	1.000	2.000	1.000
A3	0.500	0.500	1.000	1.000
A4	0.500	1.000	1.000	1.000

Таблиця Б.3.6.1 – w та показники узгодженості (E1)

Показник	w (локальні пріоритети)
A1	0.3976
A2	0.2364
A3	0.1672
A4	0.1988

E1: CR=0.022.

Матриця Б.3.6.2 – G6, експерт E2

Показник	A1	A2	A3	A4
A1	1.000	2.000	3.000	2.000
A2	0.500	1.000	1.000	1.000
A3	0.333	1.000	1.000	1.000
A4	0.500	1.000	1.000	1.000

Таблиця Б.3.6.2 – w та показники узгодженості (E2)

Показник	w (локальні пріоритети)
A1	0.4326
A2	0.1954
A3	0.1766
A4	0.1954

E2: CR=0.008.

Матриця Б.3.6.3 – G6, експерт E3

Показник	A1	A2	A3	A4
A1	1.000	2.000	1.000	3.000
A2	0.500	1.000	1.000	1.000
A3	1.000	1.000	1.000	3.000
A4	0.333	1.000	0.333	1.000

Таблиця Б.3.6.3 – w та показники узгодженості (E3)

Показник	w (локальні пріоритети)
A1	0.3640
A2	0.1956
A3	0.3061
A4	0.1343

E3: CR=0.043.

Матриця Б.3.6.4 – G6, експерт E4

Показник	A1	A2	A3	A4
A1	1.000	2.000	2.000	2.000
A2	0.500	1.000	2.000	4.000
A3	0.500	0.500	1.000	1.000
A4	0.500	0.250	1.000	1.000

Таблиця Б.3.6.4 – w та показники узгодженості (E4)

Показник	w (локальні пріоритети)
A1	0.3824
A2	0.3216
A3	0.1608
A4	0.1352

E4: CR=0.068.

Матриця Б.3.6.5 – G6, експерт E5

Показник	A1	A2	A3	A4
A1	1.000	3.000	2.000	3.000
A2	0.333	1.000	2.000	2.000
A3	0.500	0.500	1.000	3.000
A4	0.333	0.500	0.333	1.000

Таблиця Б.3.6.5 – w та показники узгодженості (E5)

Показник	w (локальні пріоритети)
A1	0.4527
A2	0.2361
A3	0.2045
A4	0.1067

E5: CR=0.080.

Б.4. Отримання μGi(Pj) з матриць альтернатив

1) Для кожної матриці (Gi, Ek) обчислюємо локальні ваги w методом геометричних середніх.

2) Переводимо у шкалу [0;1] за лінійним приведенням до інтервалу [min; max] (параметри беруться з групової оцінки).

3) Агрегуємо експертів: $\hat{\mu}Gi(Pj)=\Sigma\ \beta k\cdot\mu k,Gi(Pj)$.

Таблиця Б.4 –Агреговані значення μGi(Pj)

Показник	A1	A2	A3	A4
G1	0.60	0.78	0.86	0.72
G2	0.58	0.75	0.83	0.70
G3	0.55	0.82	0.80	0.70
G4	0.62	0.77	0.85	0.68
G5	0.65	0.80	0.78	0.73
G6	0.85	0.70	0.65	0.60

Б.5. Подальші обчислення розділу 3: $\tilde{\mu}Gi(Pj)$ та $\mu D(Pj)$

$$\tilde{\mu}Gi(Pj) = (\mu Gi(Pj))^{\frac{vi}{vmax}}, \quad де \frac{vi}{vmax} - як у табл. 3.6$$

$$\mu D(Pj) = min_i \tilde{\mu}Gi(Pj)$$

Таблиця Б.5 – Ваги критеріїв та експоненти

Показник	vi	vi/vmax
G1	0.230	1.000
G2	0.180	0.783
G3	0.160	0.696
G4	0.170	0.739
G5	0.140	0.609
G6	0.120	0.522

Таблиця Б.6 – Перетворені значення $\tilde{\mu}Gi(Pj)$

Показник	A1	A2	A3	A4
G1	0.6000	0.7800	0.8600	0.7200
G2	0.6528	0.7983	0.8642	0.7563
G3	0.6596	0.8710	0.8562	0.7802
G4	0.7024	0.8244	0.8868	0.7520
G5	0.7692	0.8729	0.8596	0.8256
G6	0.9187	0.8301	0.7986	0.7659

Таблиця Б.7 – Інтегральні оцінки $\mu D(Pj)$ та ранжування

Показник	$\mu D(Pj)$	Ранг
A3	0.7986	1.0000
A4	0.7200	3.0000
A2	0.7800	2.0000
A1	0.6000	4.0000

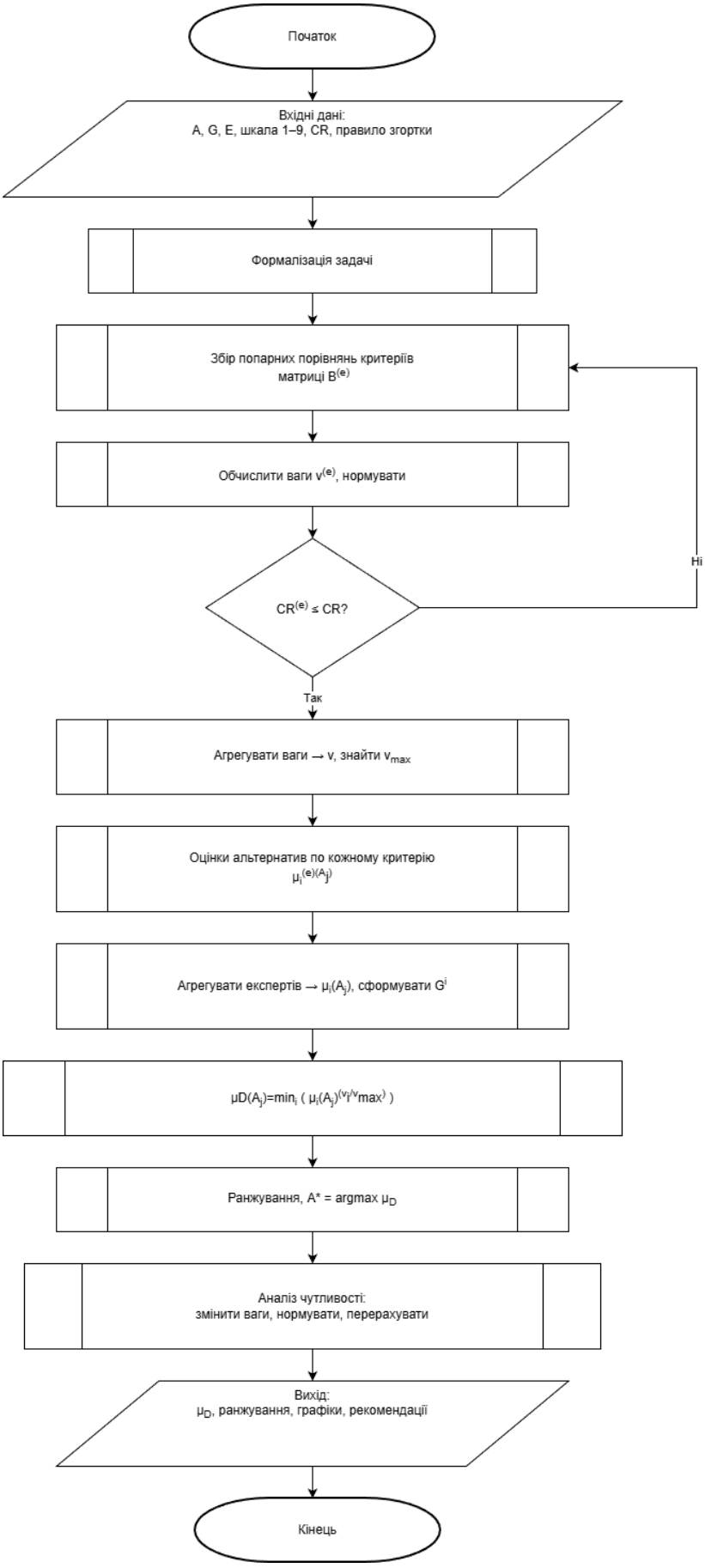
ІЛЮСТРАТИВНА ЧАСТИНА

МЕТОД ВИБОРУ ПРОЄКТУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЕКСПЕРТНОГО ОЦІНЮВАННЯ

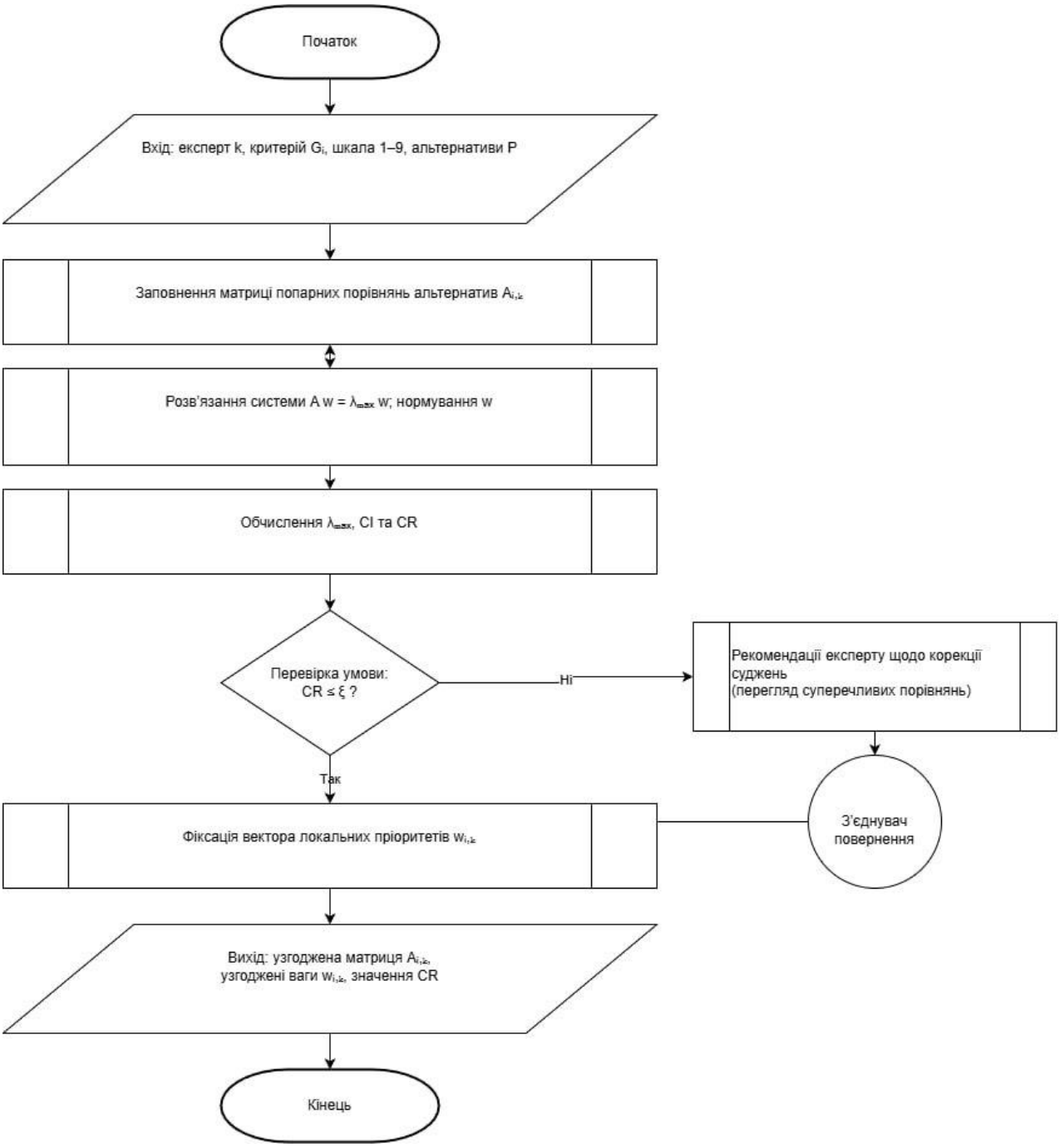
Виконав: студент 2 курсу групи 1БС-24м
спеціальності 125 Кібербезпека та захист інформації
_____ Єгор ДМИТРИШИН

Керівник: к. т. н., професор кафедри ЗІ
_____ Наталія КОНДРАТЕНКО
«19» грудня 2025 р.

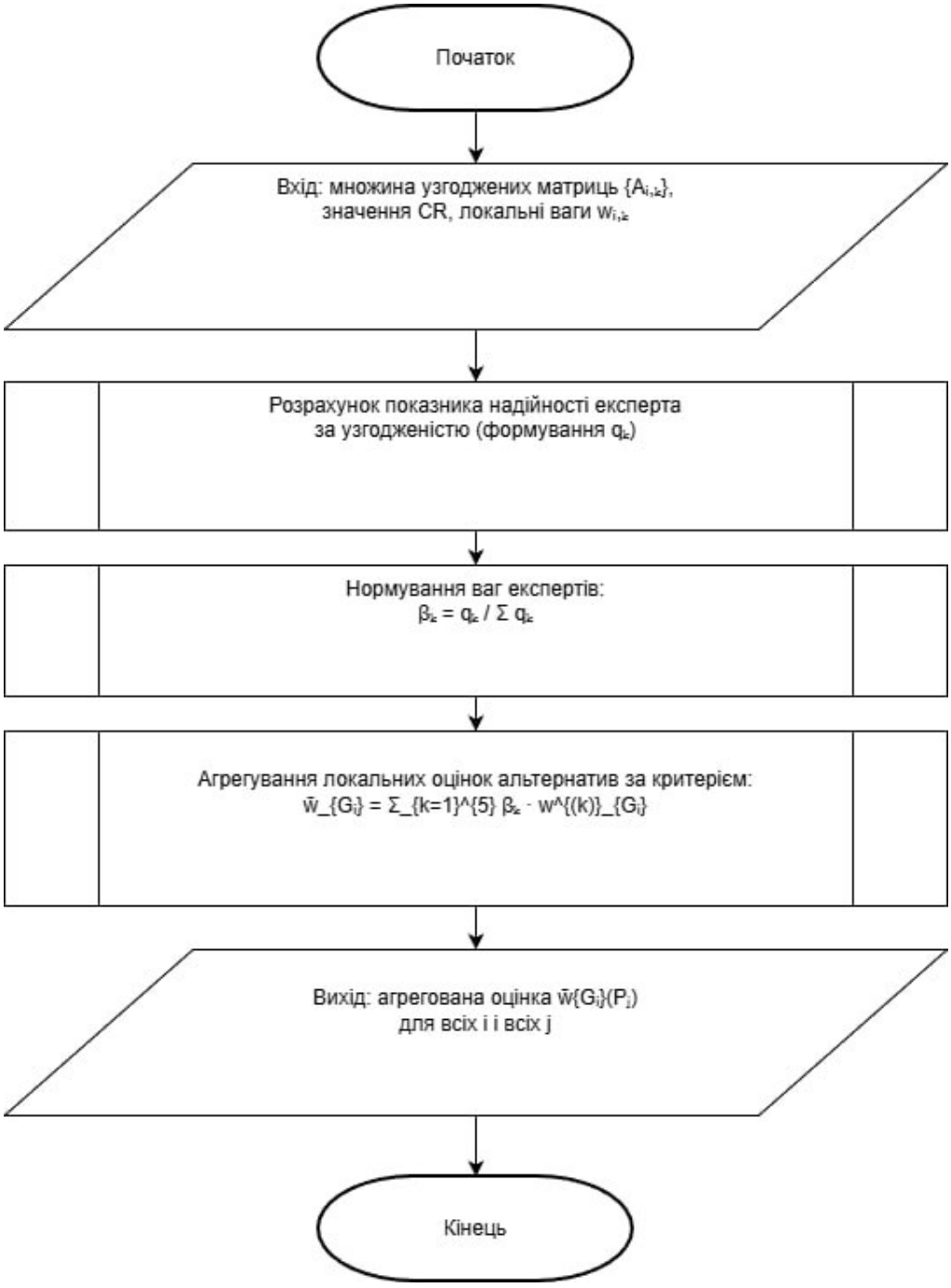
СХЕМА АЛГОРИТМУ ЗАПРОПОНОВАНОГО ПІДХОДУ



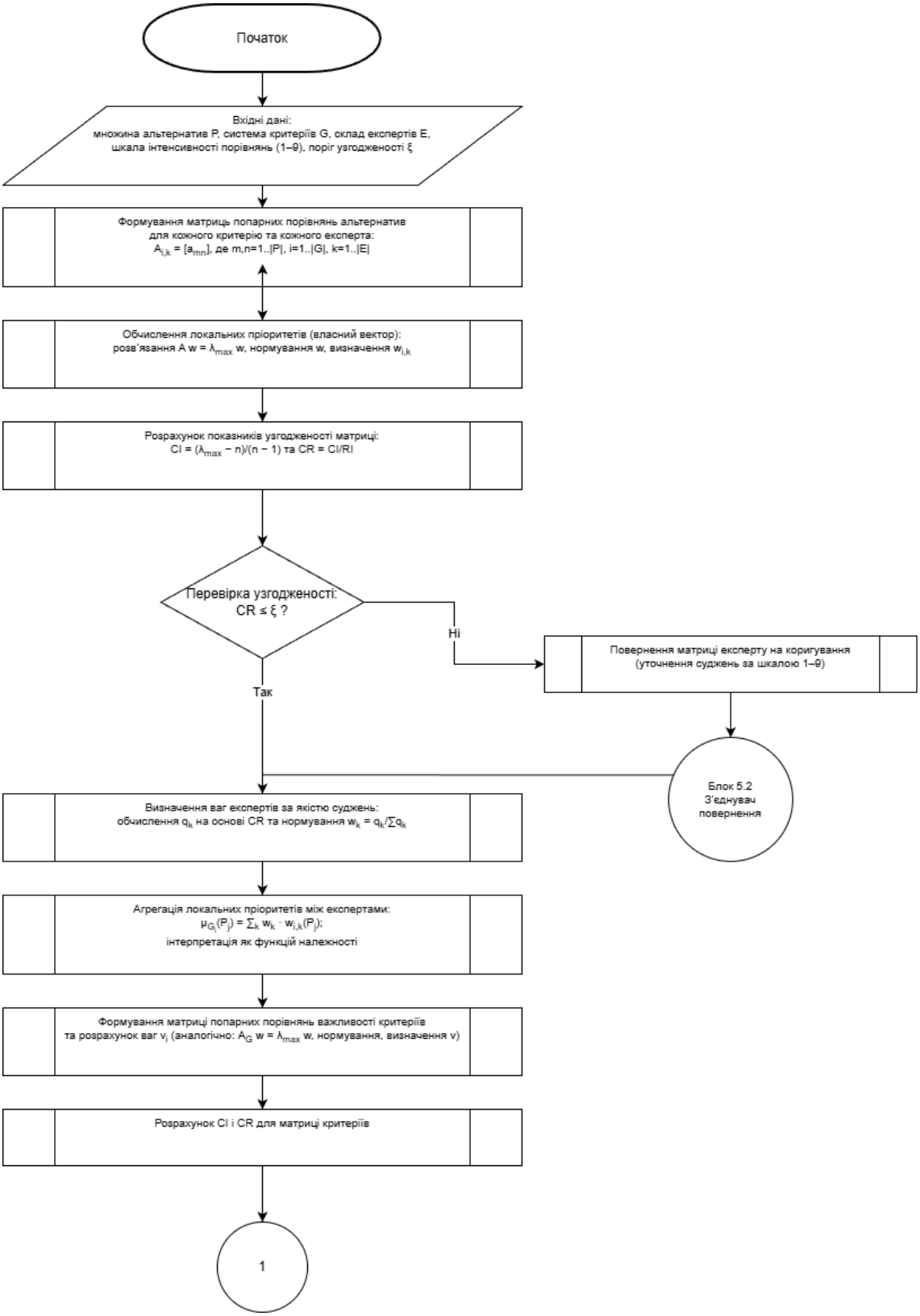
ПРОЦЕДУРА ЕКСПЕРТНОГО ОЦІНЮВАННЯ ТА КОНТРОЛЮ УЗГОДЖЕНОСТІ МАТРИЦЬ

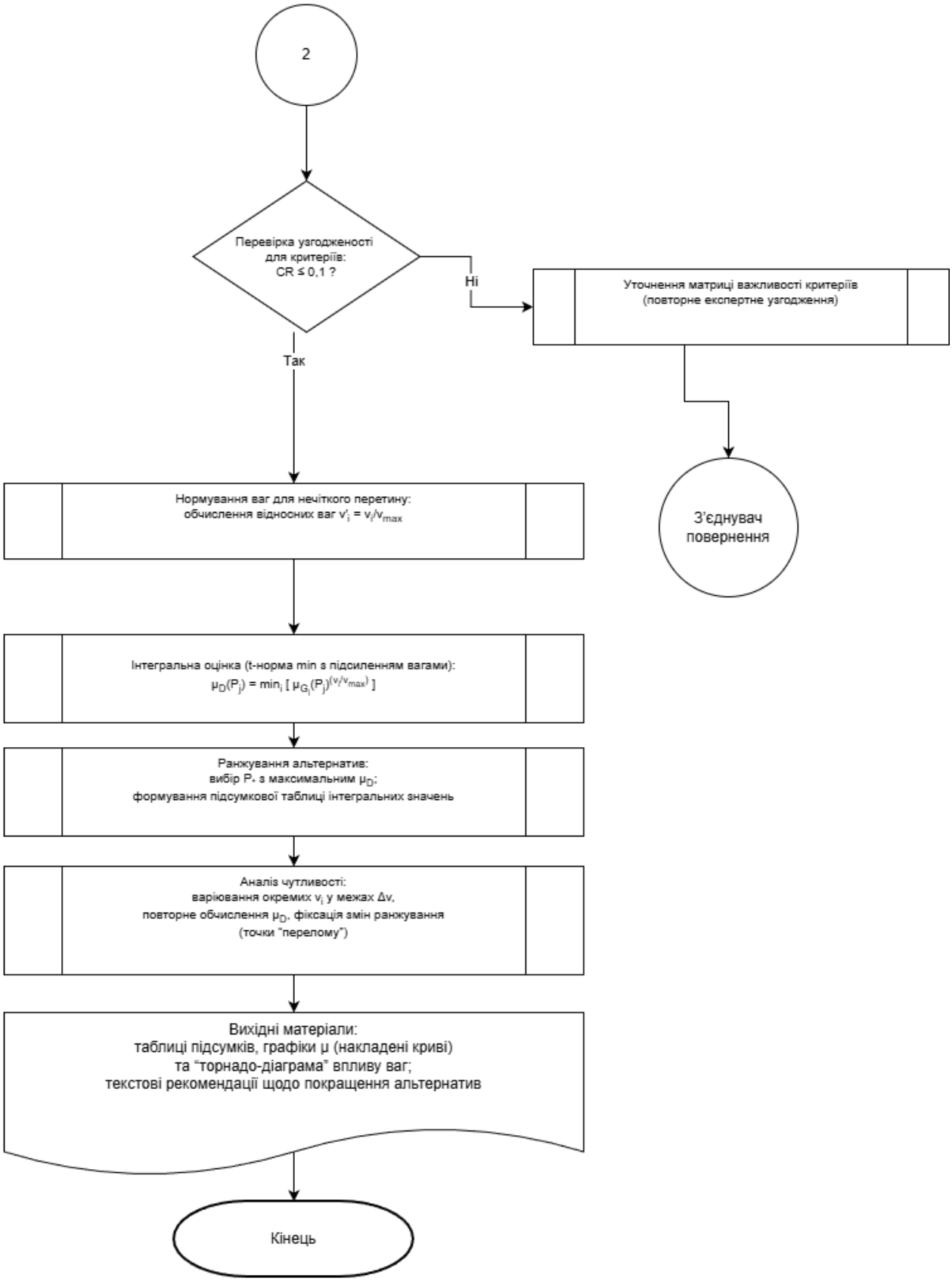


АГРЕГУВАННЯ ЕКСПЕРТНИХ ОЦІНОК З УРАХУВАННЯМ ЯКОСТІ МАТРИЦЬ

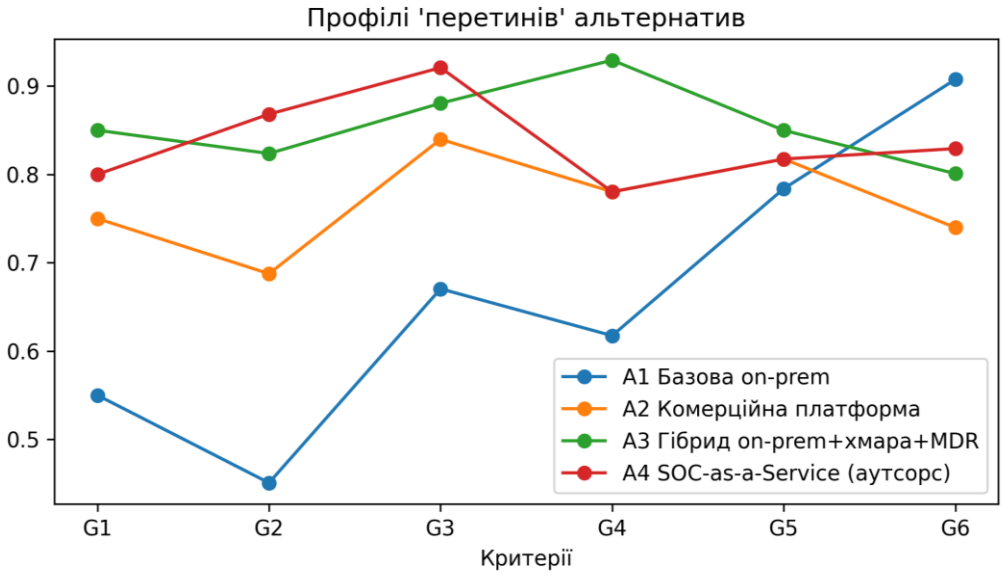


БЛОК-СХЕМА АЛГОРИТМУ РОЗРАХУНКУ




2
Перевірка узгодженості для критеріїв: CR ≤ 0,1 ?
Ні
Так
Уточнення матриці важливості критеріїв (повторне експертне узгодження)
З'єднувач повернення
Нормування ваг для нечіткого перетину: обчислення відносних ваг $v'_i = v_i/v_{max}$
Інтегральна оцінка (t-норма min з підсиленням вагами): $\mu_D(P_j) = \min_i [\mu_{G_i}(P_j)^{(v_i/v_{max})}]$
Ранжування альтернатив: вибір P_* з максимальним μ_D; формування підсумкової таблиці інтегральних значень
Аналіз чутливості: варіювання окремих v_i у межах Δv, повторне обчислення μ_D, фіксація змін ранжування (точки "перелому")
Вихідні матеріали: таблиці підсумків, графіки μ (накладені криві) та "торнадо-діаграма" впливу ваг; текстові рекомендації щодо покращення альтернатив
Кінець

ГРАФІК ПЕРЕТИНІВ ПРОФІЛІВ АЛЬТЕРНАТИВ



СЦЕНАРНИЙ АНАЛІЗ І АНАЛІЗ ЧУТЛИВОСТІ (ПЕРЕВІРКА СТІЙКОСТІ РАНЖУВАННЯ)