МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

ТЕОРІЯ ПРИЙНЯТТЯ РІШЕНЬ

Методичні вказівки
до виконання циклу лабораторних робіт
«**Моделі та методи експертного оцінювання
під час розв'язання задач прийняття рішень
в умовах невизначеності**»
для здобувачів першого (бакалаврського) рівня
вищої освіти галузі знань 12 «Інформаційні технології»
спеціальностей 125 «Кібербезпека та захист інформації»
123 «Комп'ютерна інженерія»

Київ 2024

УДК 681.3.06 (075.8)
Т30

Укладач О. В. Ізмайлова, канд. техн. наук, доцент

Рецензент Є.Є. Шабала, канд. техн. наук, доцент

Відповідальний за випуск Ю. І. Хлапонін д-р техн. наук, професор

Затверджено на засіданні кафедри кібербезпеки та комп'ютерної інженерії, протокол №3 від 22 жовтня 2024 року.

Видається в авторській редакції.

Теорія прийняття рішень [Електронний ресурс]: методичні вказівки
Т30 / уклад. О.В. Ізмайлова. –Київ : КНУБА, 2024. – 36 с.

Містять зміст, порядок оформлення і вказівки до виконання циклу лабораторних робіт «Моделі та методи експертного оцінювання під час розв'язання задач прийняття рішень в умовах невизначеності».

Призначено для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 «Інформаційні технології» спеціальностей125 «Кібербезпека та захист інформації» 123 «Комп'ютерна інженерія».

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Мета дисципліни «Теорія прийняття рішень» в освітній програмі підготовки спеціалістів за спеціальностями 125 «Кібербезпека та захист інформації» та 123 «Комп'ютерна інженерія» полягає в набутті студентами теоретичних знань та практичних навичок, оволодіння інструментарієм розв'язання задач прийняття рішень при системному аналізі об'єкта комп'ютеризації, проєктуванні та експлуатації захищених інформаційно-комунікаційних систем і технологій.

Завдання дисципліни – вивчення основних положень теорії прийняття рішень, набуття вмінь визначення структури проблеми та її аналізу, генерування та оцінювання можливих альтернатив, прийнятя рішення по оцінці та вибору альтернатив, вміння оцінювати результати, надавати аргументовані рішення та відстоювати їх прийняття.

При розробці структури курсу «Теорія прийняття рішень» ставилось завдання навчити студентів організовувати власну професійну діяльність з оцінки та вибору ефективних рішень по реалізації спеціалізованих задач та практичних проблем у визначеній предметної області, що характеризуються комплексністю, багатоваріантністю, потребою в багатофакторному аналізі, різним ступенем визначеності даних та умов прийняття рішень. Студенту надається теоретичні основи та практичні навики для розв'язання слабко структурованих та неструктурованих задач прийняття рішень по оцінці й аналізу рішень на різних етапах життєвого циклу об'єктів дослідження. Наприклад, аналіз та оцінка ефективності проєктів інформаційно-комунікаційних систем та їх структурних компонентів, оцінка ефективності рівня захищеності ресурсів різних класів, оцінювання можливостей (ймовірностей) реалізації різних типів потенційних загроз інформаційних активів, їх вразливостей та очікуваних збитків, аналіз та оцінку засобів захисту.

Для реалізації поставлених завдань в рамках дисципліни «Теорія прийняття рішень» студенти розглядають методи багатокритерійного оцінювання, методи експертних оцінок, однокрокові та багатокрокові процедури оцінювання, методи прийняття рішень на умовах ризиків та невизначеності, методи теорії ігор.

1. МОДЕЛІ ТА МЕТОДИ ЕКСПЕРТНОГО ОЦІНЮВАННЯ ПІД ЧАС РОЗВ'ЯЗАННЯ ЗАДАЧ ПРИЙНЯТТЯ РІШЕНЬ В УМОВАХ НЕВИЗНАЧЕНОСТІ

1.1. Загальна характеристика методів експертного оцінювання

Експертні оцінки – це якісні оцінки, засновані на інформації, які можуть бути отримані тільки за допомогою експертів – найбільш компетентних осіб у предметній області прийняття рішень. Експерт – це висококваліфікований фахівець, що покладається на свої знання, досвід, інтуїцію і вміння оцінювати складні фактори (явища) і здатний створити власну обґрунтовану (інтуїтивну) модель аналізованого явища (проблеми).

Метод експертного оцінювання пов'язаний з встановленням та об'єднанням знань різних експертів. Він потребує визначення індивідуальних точок зору кожного зі сформованої групи і формування на їхній основі єдиного рішення. Метод експертних оцінок об'єднує організаційні, логічні та математико-статистичні процедури, що спрямовані на одержання від спеціалістів інформації, її аналіз та узагальнення для підготовки та прийняття ефективних рішень. Наведемо приклади застосування методів експертного оцінювання в предметній області наших спеціальностей:

- Встановлення рангів об'єктів, що оцінюються, за ступенем їх відповідності встановленій властивості. Наприклад, ранжування інформаційних активів за ступенем їх цінності, ранжування міри критичності загроз та наслідків їх реалізації.
- Прийняття рішень на основі якісних критеріїв. Наприклад, застосування якісної шкали оцінки експертами ймовірності реалізації загрози, оцінки вразливості інформаційного активу, цінності активу.
- Визначення структури критеріїв ефективності рішень та їх відносної ваги, Наприклад, експертна оцінка ваги критеріїв втрат при реалізації загрози, оцінка значущості критеріїв оцінки засобів захисту даних, оцінка ваги критеріїв варіантів побудови мережевої структури.
- Кількісна оцінка в балах або в встановленій бальні шкалі окремих властивостей альтернатив. Наприклад, застосування кількісної шкали оцінки експертами ймовірності реалізації загрози, оцінки вразливості інформаційного активу, цінності активу, очікуваних втрат при реалізації загрози. Другий приклад. На кожному з рівнів тестування на проникнення нерідко доводиться оцінювати параметри

інформаційно-комунікаційної системи. Такі оцінки знаходять як безпосереднім вимірюванням, обчисленням за відомими аналітичними формулами, так і завдяки застосуванню експертних методів безпосереднього оцінювання відповідних параметрів.

Експертні оцінки проводяться в декілька етапів:

- постановка та формулювання задачі;
- формування групи експертів;
- проведення опитування ;
- обробка результатів опитувань.

Достовірність результату експертної оцінки багато в чому залежить від слушності вибору експертів, часткового складу різноманітних спеціалістів, характеристик експертів. У цьому випадку під час добору експертів необхідно враховувати їхню компетентність в необхідній предметній області. Якість формування групи експертів може бути значно підвищено, якщо використовувати методи формалізованої оцінки ступеня компетентності експертів, що засновані на спеціальних тестах, взаємооцінці експертів і їхньої самооцінці.

Визначення індивідуальних точок зору та формування на їх основі єдиної думки можно проводити різними методами. Наведемо можливу класифікацію цих методів на основі двох класифікаційних ознак: методи опитування експертів та методи оцінювання результатів (рис. 1.1).
Надамо коротку характеристику методам опитування.

1.2. Методи опитування експертів

Очні та заочні методи опитування. Очні методи опитування передбачають спілкування опитувача з членами групи, другі – ні.

Індивідуальний метод опитування. Робота зі збору інформації ведеться окремо з кожним експертом, водночас експертів не інформують про думки та оцінки інших членів експертної групи. Первага цього метода – виключення можливості впливу в оцінках «лідерів» експертів на інших членів групи.

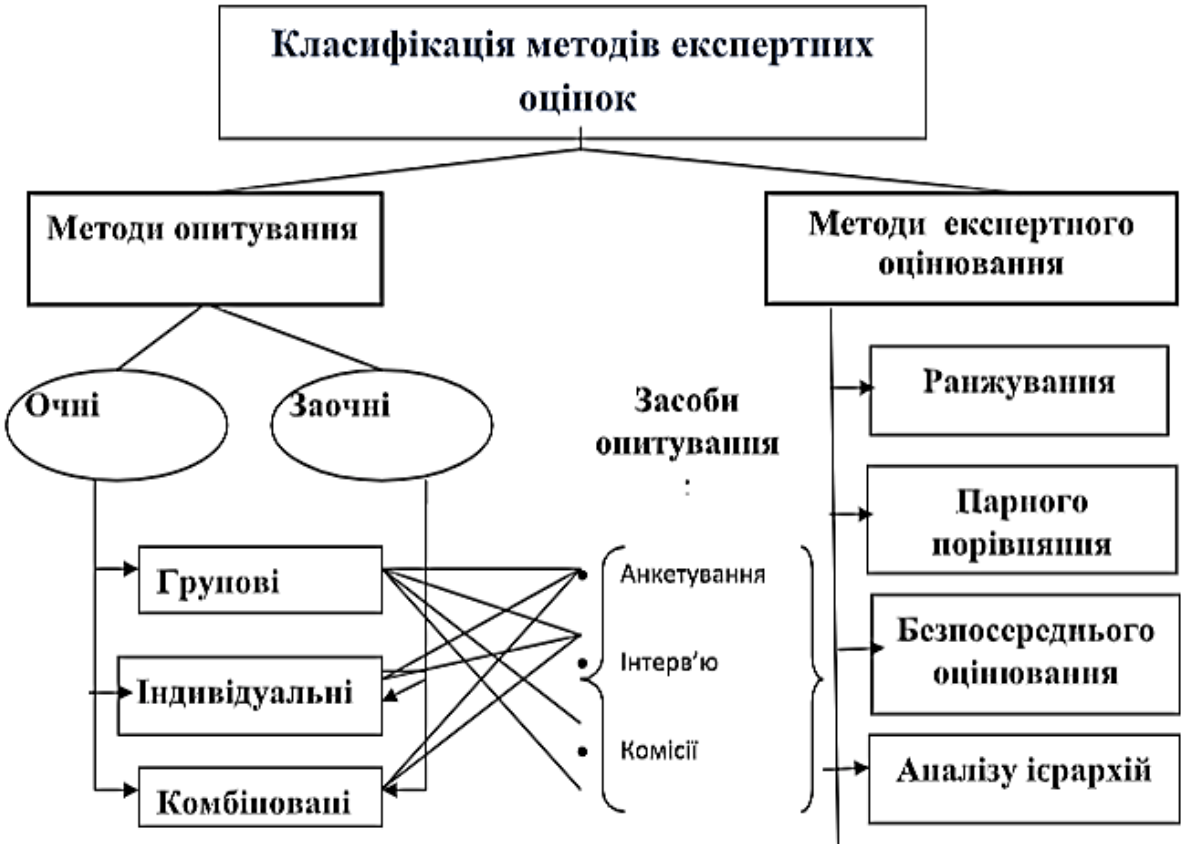

Рис.1.1. Класифікація методів експертних оцінок

Груповий метод опитування. Передбачає збір групи експертів та їх сумісне опитування. Групові методи опитування можуть проводитися засобами анкетування, інтерв'ювання, а також за рахунок проведення засідань відповідних комісій, мозкових атак. Перевага метода – можливість експертів обговорити поставлену задачу, аргументувати свої думки. Недолік можливість зниження об'єктивності оцінок за рахунок деякого впливу так званих «лідерів» групи.

Комбінований метод опитування. Застосовується з мктою використання переваг групових та індивідуальних методів та зменшення їх недоліків. Найбільш розповсюджений та корисний з методів цього класу є метод **Дельфи.** Головна особливість методу Дельфи полягає у тому, що думка кожного експерту може бути підвергнута критиці з боку інших експертів, водночас експерти фактично не зустрічаються один з іншим. Перевага метода полягає в збереженні анонімності точок зору кожного фахівця і тим самим зменшення загрози впливу на поведінку групи експертів так званих «лідерів» – найбільш авторитетних або наполегливих та красномовний. Суть метода полягає в тому, що після опитування експертів проводится аналіз міри розбіжності думок. Якщо вона надмірна,

автори полярних точок зору в письмовому вигляді аргументують свої точки зору. З цими обґрунтуваннями знайомляться всі члени групи.та проводиться повторно процедура опитування. .Ітерації опитування проводяться до тих пір, доки не буде досягнута необхідна міра погодженості думок експертів

1.3. Методи експертного оцінювання

Надамо загальну характеристику методам експертного оцінювання.

Метод ранжування [2; 4; 6; 9] – це процедура впорядкування об'єктів, яку виконує експерт. На основі знань та досвіду, експерт розташовує об'єкти, які він оцінює, в порядку надання їм переваги, керуючись одним чи кількома обраними показниками порівняння.

Метод парних порівнянь [1-4] базується на аналізі і встановленні експертом бінарних відношень між елементами множини об'єктів, що оцінюються.

Метод безпосереднього оцінювання [1; 2; 7; 9; 11] найбільш розповсюджений в практиці прийняття рішень. Він дає змогу експерту застосувати більш чутливий інструмент взаємного порівняння варіантів. Використовуючи цей метод перед експертом ставиться задача – оцінити якісну або кількісну властивість критерію в балах (попередньо встановлюється діапазон змін бальної оцінки) або в визначеній одиниці вимірювання. Останні мають відображати ступень відповідності варіанта властивості, що розглядається. Бали – це штучні числові оцінки якісної властивості.

Метод аналізу ієрархій (МАІ) [8-12] – математичний інструмент системного підходу до складних проблем прийняття рішень. МАІ не наказує особі, що приймає рішення (ОПР), якого-небудь «правильного» рішення, а дозволяє йому в інтерактивному режимі на основі встановлених правил експертного оцінювання знайти такий варіант (альтернативу), який найкращим чином узгоджується з його розумінням суті проблеми і вимогами до її вирішення.

2. МЕТОД РАНЖУВАННЯ

2.1. Змістовна постановка задачі

Можуть бути запропоновані різні варіанти змістовної постановки задачі прийняття рішень з застосуванням метода ранжування:

- ранжування об’єктів або варіантів рішень та вибір найкращого варіанта рішень з числа альтернатив, що розглядаються;
- введення бальних оцінок відповідності варіантів властивостям, що розглядаються;
- визначення значущості (ваги) об’єктів, що оцінюються.

Ранжування об’єктів та вибір найкращого варіанта рішень з числа альтернатив, що розглядаються. Метод ранжування застосовують, зазвичай, тоді, коли необхідно впорядкувати в часі або просторі певні чинники (об’єкти), які визначають кінцеві результати, але не піддаються безпосередньому вимірюванню. Для цього експерт має розташувати їх у тому порядку, який він вважає найбільш раціональним (порядку зростання або спадання) і приписати кожному з чинників (об’єктів) певне число натурального ряду – порядковий номер, або ранг. Порядковий номер, що дорівнює 1, отримує найкращий (або найгірший) чинник (об’єкт), а найменш важливому присвоюється порядковий номер n. Параметри $x1$, $x2$, ..., xn можуть включати в себе групи чинників (об’єктів), рівнозначних щодо їхньої важливості. Для кожної групи рівнозначних чинників (об’єктів) їхні ранги однакові. Їх обчислюють як середнє арифметичне відповідної вибірки порядкових номерів чинників, що входять до певної групи. Якщо ранжування виконують кілька, скажімо m, експертів, то для кожного чинника спочатку обчислюють суму рангів, отриману від усіх експертів, а потім згідно зі здобутим результатом установлюють його остаточний ранг. Найвищий (перший) ранг присвоюють чиннику, який набрав найменшу суму рангів, і, навпаки, чиннику, який набрав найбільшу суму рангів, присвоюють найнижчий ранг. Решту чинників упорядковують згідно зі значенням суми рангів того чинника, який має перший ранг. На підставі здобутих даних формують матрицю рангів.

Нехай є n варіантів рішень, окрему властивість l яких оцінює m експертів. Обозначим через X_{ij}^{l} ранг l-тої властивості j-того варіанта в оцінці i-того експерта. Сума рангів у ранжуванні i-того експерта:

$$X_i^l = \sum_{j=1}^{n} X_{ij}^l = 0.5n(n+1) \qquad (2.1)$$

Якщо експерт однаково оцінює декілька варіантів, то їм повинні бути привласнені однакові ранги. При цьому для можливості використання математичного апарата методу, необхідно дотримуватися наступного правила - однаковим в оцінці варіантам він надає ранг, що рівний середньому арифметичному значенню місць, що між собою поділяють. У результаті опитувань експертів будується матриця X^l що відображають результати оцінок експертами об'єктів по властивості l. Елементом матриці буде значення X_{ij}^l.

Найкращий варіант A^* буде той, що відповідає умові:

$$\min_j \{X^l j\}, \qquad (2.2)$$

де X^l_j – сумарний ранг j-того варіанту по властивості l :

$$X_j^l = \sum_{i=1}^{m} X_{ij}^l .$$

Необхідний етап опрацювання результатів опитуваннння - оцінка узгодженості думок експерта. Для цього визначається значення коефіцієнта конкордації (згоди) K^l.:

$$K^l = \frac{12\ S^l}{m^2\left(n^3 - n\right) - m\sum_{i=1}^{m} T_i^l}; \qquad (2.3)$$

при цьому $0 \le K^l \le 1;$

$$S^l = \sum_{j=1}^{n} d_j^{\,l}; \quad d_j^{\,l} = \left(X_j^{\,l} - X_{cp}\right)^2; \quad X_{cp} = 0.5\,m(n+1);$$

$$T_i^l = \sum_{\mu=1}^{m}\left(t_{\mu_i}^{\ 3} - t_{\mu_i}\right),$$

де $t_{\mu i}$ - число повторень μ - рангу в ранжуванні i-го експерта.

У разі повної узгодженості думок експертів під час оцінки варіантів по властивості l коефіцієнт конкордації K^l дорівнює одиниці, а у разі повної розлагодженості – нулю. Розглянемо приклад на рис. 2.1.

Експерт	Варіант 1	Варіант 2	Варіант 3
1	1	2	3
2	1	2	3
3	1	2	3

а

Експерт	Варіант 1	Варіант 2	Варіант 3
1	1	2	3
2	3	2	1
3	2	2	2

б

Рис.2.1. Результати ранжування експертами трьох варіантів по одній властивості

Розраховуємо коефіцієнт конкордації для випадку повної погодженості думок експертів (див. рис. 2.1, *а*):

K^l =(12 (3-6)^2 + (6-6)^2 + (9-6)^2)/9 (27-3) = 1.

Розраховуємо коефіцієнт конкордації для випадку повної розлагодженості думок експертів (див. рис. 2.2, *б*):

K^l = (*12* (6-6)^2 + (6-6)^2 + (6-6)^2)/ (9 (27-3) – 3 (27-3)) = 0.

У реальних умовах K^l знаходиться в межах від нуля до одиниці, і по його значенню можна судити про більшу або меншу узгодженість думок експертів. Умовно припускається, що думки експертів можна вважати узгодженими, якщо K^l>0.55. Але узгодженість думок експертів можна оцінити на основі більш детального і точного аналізу. Він засновується на наступному. Всі можливі значення ранжування вважається рівно ймовірними. Тому значенням K^l може бути приведена у відповідність деяка статистика *Y* при випадковому порядку варіантів в ранжуванні, що залежить від значень *m* та *n*. Висувається *Но* гіпотеза про те, що думки експертів розлагоджено. Статистика *Y* має дві області значень: критичну область та область прийняття гіпотези. Критична область – це сукупність значень *Y* , для яких *Но* гіпотезу відкидають. Область прийняття гіпотези включає в себе ті значення *Y* , при яких гіпотезу приймають.

Головний принцип перевірки гіпотези – якщо розраховане значення *Y*р належить критичній області, то гіпотезу відкидають. Як правило, для перевірки *Но* гіпотези використовують критичні точки розподілення *Yкр.* Критичними називаються точки, що відокремлюють критичну область від області прийняття гіпотези. Якщо *Yр* ≥ *Yкр*, то *Но* гіпотезу відкидають,

думки експертів вважають узгодженими. Під час перевірки *Но* гіпотези треба враховувати імовірність помилки α, що передбачає ситуацію, коли вірна гіпотеза *Но* буде відкинута. Найчастіше враховують такі значення α: 0.1; 0.05; 0.01.

Залежно від значень *m* та *n Yp* розраховують за різними формулами і його значення порівнюється з *Yкр,* що визначається на основі різних розподілень (табл. 2.1)

Таблиця 2.1

Дані для визначення *Yp*

n	***m***	***Yp***	**Розподілення, що рекомендується; ступень свободи**
3 4 5 6 7 7	2…15 2…8 2…8 2…8 7 8	$Y^{(1)}$	Таблиці критичних значень (ГОСТ 23584-81)
≥20	≥13	$Y^{(1)}$	χ^2- розподілення зі ступенем свободи $\nu = n-1$
$7 \le n \le 19$	≥13	$Y^{(2)}$	*F*-розподілення Фішера зі ступенем свободи $\nu_1 = n-1$; $\nu_2 = (n-1)(m-1)$
≤ 7	≥8	$0.5[Y^{(1)}+(n-1)\,Y^{(2)}]$	χ^2- розподілення зі ступенем свободи $\nu = n-1$; *F*-розподілення Фішера зі ступенем свободи $\nu_1 = n-1$; $\nu_2 = (n-1)(m-1)$; $Yкр=0.5[\chi^2+(n-1)F]$
≥ 8	$7 \le m \le 12$	$Y^{(2)}$	*F*-розподілення Фішера зі ступенем свободи $\nu_1 = n-1$; $\nu_2 = S^2/[(m-1)\sum_{j=1}^{n} vj^2]-(m-1)$, де $S = (m-1)\sum_{j=1}^{n} vj$, $vj = 1/(m-1)\mp\sum_{i=1}^{m} (Yij-Yj_{cep})^2$; $Yj_{cep}=\frac{1}{m}\sum_{i=1}^{m} Yij$
8 ≥7	3…6 2…6	$0.5[Y^{(1)}+(m-1)(n-1)\,Y^{(2)}]$	χ^2- розподілення зі ступенем свободи $\nu = n-1$; *F*-розподілення Фішера зі ступенем свободи $\nu_1 = n-1$; $\nu_2 = (n-1)(m-1)$; Yкр=0.5[χ^2+(m-1)(n-1)*F*]

Примітка 1. $Y^{(1)}=m(n-1)K^l$; $Y^{(2)}=[(m-1)Y^{(1)}]/m(n-1)-Y^{(1)}]$.

Примітка 2. Значення розподілення χ^2 наведені в таблиці Д1.1 (див. дод. 1), розподілення Фішера – в табл.Д2.1 та Д2.2 (див. дод. 2).

Приклад 2.1. Припустимо треба вибрати найкращий з семи варіантів захисту конфіденційності даних інформаційного активу. В результаті опитування восьми експертів побудована така матриця ранжування (табл. 2.2).

Перевіримо узгодженість думок експертів. Для визначення коефіцієнта конкордації (1.3) треба розрахувати значення *Xcp, S* та *Ti.*(ф.1.4).

Таблиця 2.2

Матриця ранжування варіантів захисту конфіденційності даних

Експерт	**Варіанти захисту конфіденційності даних**						
	1	2	3	4	5	6	7
1	1	4	5	6	2.5	2.5	7
2	2	4	5	6	1	3	7
3	1.5	5	4	6.5	1.5	3	6.5
4	2	4	5	6	1	3	7
5	1	4	5	6	2.5	2.5	7
6	1.5	5	4	6.5	1.5	3	6.5
7	2	4	5	6	1	3	7
8	1	5	4	6	2	3	7
Xj	12	35	37	49	13	23	55
X_j'	44	21	19	7	43	33	1

$$Xcp = 0.5m(n+1) = 0.5x8x8 = 32;$$

$$S= (12-32)^2+(35-32)^2+(37-32)^2+(49-32)^2+(13-32)^2+(23-32)^2+(55-32)^2=1334$$

$$T_1=2^3-2=6\ ;$$

$$T_2=0\ ;$$

$$T_3=(2^3-2)+(2^3-2)=12;$$

$$T_4=0\ ;$$

$$T_5=2^3-2=6\ ;$$

$$T_6=(2^3-2)+(2^3-2)=12;$$

$$T_7=0\ ;$$

$$T_8=0$$

$$K = \frac{12x1334}{8^2(7^3-7)-8(6+0+12+0+6+12+0+0)} = 0.753 \ .$$

Згідно з табл. 2.1 значення *Yp* розраховується за формулою:

$$Yp = 0.5[Y^{(1)} + (n-1)\ Y^{(2)}] = 0.5x(42+6x49) = 168,$$

де $Y^{(1)} = m(n-1)K = 8x6 = 42$; $Y^{(2)} = [(m-1)Y^{(1)}]/m(n-1) - Y^{(1)}] = 7x42/(8x6-42) = 49.$

$$Yкр = 0.5[\chi^2 + (n-1)F] = 0.5(16.8+6x7.14) = 29.82,$$

де значенняχ^2 та F встановлені згідно з таблицею Д1.1 (див. дод. 1) та таблицею.Д2.1 (див. дод. 2), якщо значення $\alpha = 0.01$.

Думки експертів вважаються достатньо погодженим, тому що *Yp>Yкр.*

Таким чином найкращим варіантом згідно з умовою (ф. 2.2) буде перший.

Введення бальних оцінок відповідності варіантів властивостям, що розглядаються. На основі метода ранжування може бути запропонований шлях введення бальних числових оцінок відповідності варіантів властивостям, що розглядаються. В якості таких оцінок, наприклад, можуть розглядатися сумарні ранги кожного варіанта $\{X_j^l\}$. Значення X_j^l залежить від числа експертів, що приймають участь в опитуванні. Допустима ситуація, коли при порівнянні варіантів по різним властивостям може брати участь різна кількість експертів. Тому може бути доцільним перевести ранги варіантів в деякий загальних для всіх властивостей діапазон можливих значень на основі встановленої шкали оцінювання. Припустимо буде заданий діапазон значень від U_{min} до U_{max}. При чому U_{max}^l присвоюється найкращому варіанту рішень з кожної властивості (варіанта з мінімальним значенням X^lj), U_{min}^l – найгіршому варіанту рішень з кожної властивості (варіанта з максимальним значенням X^lj). Тоді перетворений ранг варіантів може бути визначений так:

$$Uj^l = U_{\min} + \frac{x_{\max}{}^l - x^l{}_J}{X_{max}{}^l - X_{\min}{}^l}(U_{\max} - U_{\min}), \qquad (2.5)$$

де X_{max}^l та X_{min}^l відповідно максимальні та мінімальні сумарні ранги, що отримані при оцінці експертами варіантів по властивості l.

Наявність штучних оцінок варіанта з кожної властивості Uj^l надає можливість використовувати методи пошуку рішень з застосуванням чисельних критеріїв.

Приклад 2.3. Припустимо, дані, що при ранжуванні експертами варіантів захисту конфіденційності даних (табл. 2.2.) вони керувались оцінкою міри вразливості об'єкта під час застосування кожного варіанта захисту. Шкала оцінки вразливості рівня вразливості наведена в табл. 2.3.

Таблиця 2.3

Шкала оцінювання рівня вразливості

Якісна оцінка	Діапазон оцінки в балах	Змістовна характеристика
Дуже низька вразливість	0-0,1	Відсутня ймовірність впливу на конфіденційність інформації
Низька вразливість	0,2-0,4	Можливе незначне розкриття інформації, але масштаби втрати обмежені таким чином, що доступні не всі дані.
Середня вразливість	0,4-06	Помірна вразливість
Висока вразливсть	0,6-0,8	Значна вразливість, ліквідація якого повязана зі значними втратами
Дуже висока вразливість	0,8-1	Критична вразливість

Експертами був визначений рівень вразливості U_{max} = 0,5 для варіанта 7 (найгіршого варіанта захисту) та U_{min}=0,1 для варіанта 1 (найкращого варіанта) (див. табл. 2.2).

Розраховуючи в балах міри вразливості інформаційного активу X_j' при застосуванні ф.2.5, застосовується значення X_j' – перетворений рангу сумарний ранг критерію $l; X'_l = nm - X_l$. (див. табл.2.2) :

$$U_1 = 0{,}1 + \frac{(44-44)}{(44-1)} \times (0{,}5 - 0{,}1) = 0{,}1;$$

$$U_2 = 0{,}1 + \frac{(44-21)}{(44-1)} \times (0{,}5 - 0{,}1) = 0{,}31;$$

$$U_3 = 0{,}1 + \frac{(44-19)}{(44-1)} \times (0{,}5 - 0{,}1) = 0{,}33;$$

$$U_4 = 0{,}1 + \frac{(44-7)}{(44-1)} \times (0{,}5 - 0{,}1) = 0{,}44;$$

$$U_5 = 0{,}1 + \frac{(44-43)}{(44-1)} \times (0{,}5 - 0{,}1) = 0{,}11;$$

$$U_6 = 0{,}1 + \frac{(44-33)}{(44-1)} \times (0{,}5 - 0{,}1) = 0{,}2;$$

$$U_7 = 0{,}1 + \frac{(44-1)}{(44-1)} \times (0{,}5 - 0{,}1) = 0{,}50;$$

Визначити значущість (вагу) об'єктів, що оцінюються. В разі, коли на думку особи, що приймає рішення (ОПР), під час розв'язання поставленої задачі слід враховувати різну значущість окремих об'єктів, на основі метода ранжування можна визначити «вагу» β_l (ступень значущості) кожного з них. При цьому $(\sum_{l=1}^{L} \beta_l = 1)$.

Приклад 2.4. Припустимо треба оцінити «вагу» (значущість) таких трьох показників оцінки ефективності системи захисту інформації: ідентифікація ризиків кібербезпеки (*ID*); кіберзахист (*PR*.); виявлення кіберінцидентів (*DE*) У результаті опитування семи експертів побудована така матриця ранжування (табл.2.3.).

У результаті ранжування буде визначений сумарний ранг кожного критерію X_l. «Удільна вага» критерію розраховується за формулою:

$$\beta_l = \frac{X'_l}{\sum_{l=1}^{L} X'_l}, \qquad (2.6)$$

де X'_l – перетворений сумарний ранг критерію l; $X'_l = nm - X_l$.

Визначаємо середній ранг критеріїв:

$$Xcp = 0.5x7x4=14.$$

Таблиця 2.3

Ранжування показників оцінки захисту інформації

Критерії	**Експерти**							X_l
	1	*2*	*3*	*4*	*5*	*6*	*7*	
ID	2	1	2	2	1	1	1	10
PR	2	2	1	2	2	2	2	13
DE	2	3	3	2	3	3	3	19

Визначаємо дисперсію думок експертів S та значення $\sum_{ш=1}^{b} Ti$ (1.4):

$$S= (10\text{-}14)^2+(13\text{-}14)^2+(19\text{-}14)^2=42;$$

$$\sum_{ш=1}^{b} Ti= (3^3\text{-}3)+0+0+(3^3\text{-}3)+0+0+0= 48$$

Визначаємо коефіцієнт конкордації думок експертів (ф.2.3):

$$K = \frac{12x42}{7^2(3^3-3)-7x48} = 0.6$$

K>0.55, тому вважаємо думки експертів достатньо погодженими.

Знаходимо перетворені ранги критеріїв:

X'_R=7x3- 10=11; $X'к$ =7x3- 13=8; X'_T =7x3- 19=2.

Згідно з формулою (2.6) знаходимо "удільну вагу " критеріїв:

$$\beta_R = \frac{11}{11+8+2} = 0.524; \quad \beta_K = \frac{8}{11+8+2} = 0.381; \beta_T = \frac{2}{11+8+2} = 0.095$$

2.2. Лабораторна робота «Метод ранжування»

2.2.1. Мета роботи. Мета роботи – закріплення теоретичних знань та набуття навичок розв'язання задач експертного оцінювання рішень побудови захищених інформаційних систем та засобів комп'ютерної інженерії з застосуванням одного з базових методів експертного оцінювання – метода ранжування .

2.2.2. Зміст лабораторної роботи

Студент отримує завдання на побудови модуля прийняття рішень для системи, де виникає проблема оцінювання і є можливість її розв'язання з застосуванням метода ранжування. На основі заданого прикладу студенту необхідно виконати такі етапи:

- проаналізувати зміст поставленої задачі, розглядаючи її як складову частину системи – функціональний модуль її побудови;
- побудувати модель «чорної скриньки» модуля розв'язання задачі, в якій відображається її назва, перелік вхідної інформації, необхідної для її реалізації та її джерела; перелік вихідної інформації, що повинна бути отримана в результаті реалізації;
- побудувати дерево функцій, необхідних для реалізації модуля;
- визначити прецеденти роботи модуля;
- побудувати діаграму діяльності модуля на рівні прецедентів;
- надати математичну постановку реалізації задачі з застосуванням схеми алгоритму або діаграми діяльності по реалізації відповідного прецеденту;
- надати інфологічну модель предметної області на основі діаграми класів або діаграми Чена
- провести розрахунки з метою розв'язання поставлених задач з застосуванням одного з трьох альтернативних варіантів:
  1. На основі Microsoft Excel
  2. На основі інших мов програмування
  3. Розрахунки без застосування програмування

2.3. Приклади варіантів завдань

Приклад 1. З метою мінімізації уразливих місць у системному й прикладному програмному забезпеченні, програмно-апаратних пристроях експертам запропоновано провести ранжування сканерів з точки зору пропуску вразливостей Результати опитувань наведені в табл. 2.4.

Результат роботи:

1. Встановлення міри погодженості думок експертів.
2. В умовах недостатнього рівня погодженості – оцінки «авторів крайніх точок» відхиляються з подальших розрахунків
3. Провести ранжування сканерів з точки зору пропуску вразливостей.
4.

Таблиця 2.4

Ранжування сканерів з точки зору пропуску вразливостей

Експерт	**Вимоги**				
	MaxPatrol	**Internet Scanner**	**Retina**	**Nessus**	**Shadow Security Scanne**
	1	4.5	4.5	2.5	2.5
	1	4	5	2	3
	1	4	5	2	3
	1	5	4	3	2

Приклад 2. Визначені такі вимоги до системи захисту даних в інформаційній технології управління медичною установою:

A – права доступу повинні гранулюватися з точністю до користувача. Всі об’єкти повинні піддаватися контролю доступу;

B – під час виділення об’єкта, що зберігається, з пулу ресурсів довіреної обчислювальної бази необхідно ліквідовувати всі сліди його використання;

C – кожен користувач системи повинен унікальним чином ідентифікуватися. Кожна реєстрована дія має асоціюватися з конкретним користувачем;

D – довірена обчислювальна база повинна створювати, підтримувати і захищати журнал реєстраційної інформації, що стосується доступу до об’єктів, контрольованих базою;

E – тестування повинне підтвердити відсутність очевидних недоліків у механізмах ізоляції ресурсів і захисту реєстраційної інформації.

Матеріали експертного оцінювання ступеня важливості кожної вимоги наведені в табл. 2.5.

Таблиця 2.5

Ранжування вимог до системи захисту

Експерт	Вимоги				
	A	B	C	D	E
	1.5	5	1.5	3	4
	2	5	2	2	4
	1	5	2	3	4
Студент, що виконує роботу	Надати свої оцінки				

Результат роботи:

1. Встановлення міри погодженості думок експертів.
2. В умовах недостатнього рівня погодженості – оцінки «авторів крайніх точок» відхиляються з подальших розрахунків
3. Встановлення ваги вимог до побудови системи.

Приклад завдання 3. Визначені такі вимоги до побудови системи захисту даних в інформаційній технології управління медичною установою.

A –права доступу повинні гранулюватися з точністю до користувача. Всі об’єкти мають піддаватися контролю доступу;

B – під час виділення об’єкта, що зберігається, з пулу ресурсів довіреної обчислювальної бази необхідно ліквідовувати всі сліди його використання;

C – кожен користувач системи повинен унікальним чином ідентифікуватися. Кожна реєстрована дія повинна асоціюватися з конкретним користувачем;

D – довірена обчислювальна база повинна створювати, підтримувати і захищати журнал реєстраційної інформації, що стосується доступу до об’єктів, контрольованих базою;

E – тестування повинне підтвердити відсутність очевидних недоліків у механізмах ізоляції ресурсів.

Матеріали експертного оцінювання ступеню важливості кожної вимоги наведені в табл. 2.6.

Таблиця 2.6

Ранжування вимог до системи захисту

Експерт	Вимоги				
	A	B	C	D	E
	1	4	1	2	3
	1	3	2	2	4
	2	5	2	2	4
	1	5	2	3	4
Студент, що виконує роботу	Надати свої оцінки				

Результат роботи:

1. Нормалізація представлення даних.
2. Встановлення міри погодженості думок експертів.
3. Встановлення ваги вимог до побудови системи.

Приклад 4. Для підприємства визначені сім стратегій його можливого розвитку ($Z_1, Z_i, \ldots Z_7$), що впливають на глобальну мету розвитку підприємства. Для визначення міри перспективності кожної стратегії для досягнення мети системний аналітик провів опитування шести експертів. Результати опитування представлені в матриці ранжування перспективності стратегій (табл .2.7).

Таблиця 2.7

Ранжування стратегій розвитку підприємства

Експерти	Стратегії розвитку підприємства						
	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7
1	7	2	1	4,5	6	3	4,5
2	6	2	1	4,5	7	3	4,5
3	7	2	1	4	6	3	5
4	7	1	2	4,5	6	3	4,5
5	7	2	1	4,5	6	3	4,5
6	7	1.5	1.5	4,5	6	3	4,5

Результат роботи:

1. Міру погодженості думок експертів.
2. Міру перспективності кожної стратегії для досягнення глобальної мети розвитку підприємства($X_1, X_i, \ldots X_7$) в діапазоні від 0 до 100.

3. Ступень важливості кожної стратегії для досягнення глобальної мети розвитку підприємства ($\beta_{1...}\ \beta_{i...}\ \beta_7$) ; $\sum\ \beta_i = 1$.

Приклад 5. Чотири експерти залучені до оцінки ступеня впливу восьми вхідних змінних на вихідну змінну об'єкта керування (табл.2.8).

Таблиця 2.8

Ранжування ступеню впливу вхідних змінних

Експерт	К1	К2	К3	К4	К5	К6	К7	К8
	1	3	2	3	4	5	6	7
	1	2	3	3	4	5	5	5
	2	1	3	5	4	6	8	7
	1	8	7	3	5	6	4	2

Потрібно виконати:

1. Нормалізувати представлення матриці
2. Перевірити міру погодженості думок експертів.
3. Встановити ступень впливу в шкалі 100-40.

Приклад завдання 6. Результати оцінювання експертами ймовірності відбуття рівнів збитку від реалізації загрози порушення конфіденційності інформаційного активу представлені в табл. 2.9.

Таблиця 2.9

Оцінка експертами ймовірності відбуття рівня збитку

Експерт	**Ймовірність відбуття рівня збитку**						
	S1	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**
	0,3406	0,2215	0,0390	0,0653	0,0967	0,1214	0,1636
	0,3580	0,346	0,041	0,012	0,1112	0,1314	0,022
	0,244	0,2512	0,1133	0,054	0,0812	0, 1133	0,1431
	0,3506	0,2115	0,0390	0,0653	0,0967	0,1636	0,1214
	0,2251	0,1834	0,051	0,1121	0,1231	0,2113	0,094

Проранжуйте результати оцінювання експертів та проаналізуйте достатність рівня погодженості оцінок на основі коефіцієнта конкордації.

Приклад 7. Результати ранжування експертами активів інформаційно-телекомунікаційної системи за ступенем їхньої цінності наведені в табл. 2.10.

Потрібно виконати:

1. Нормалізувати представлення матриці
2. Перевірити міру погодженості думок експертів.
3. Визначте цінність активів в в діапазоні оцінювання від 7 до 10.
4.

Таблиця 2.10

Ранжування активів за ступенем їх цінності

Експерт	Стратегічні плани розвит-ку	Картка об'єкта	Звіт про динаміку основних ключових показників підприємства	Звіт про прибутки і збитки Компанії в динаміці	Аналітика продажів	Звіт за основними ключовими показниками регіонів	Комерційні умови роботи з постачаль-никами	Дані про клієнтів
	1	3	2	3	4	5	6	7
	1	2	3	3	4	5	5	5
	2	1	3	5	4	6	7	7
	1	7	7	3	5	6	4	2

3. МЕТОД БЕЗПОСЕРЕДНЬОГО ОЦІНЮВАННЯ

3.1. Змістовна постановка задачі

Метод безпосереднього оцінювання – найбільш розповсюджений в практиці прийняття рішень на основі експертного оцінювання. Він надає можливість експерту застосувати чутливий інструмент взаємного порівняння об’єктів, тому що дозволяє не тільки впорядкувати (ранжувати) об'єкти за встановленою властивістю, а й визначити більш точно рівень їх взаємної переваги. При цьому методі перед *i*-тим експертом ставиться задача – оцінити властивість *j*-того критерію X_{iy} в балах (попередньо встановлюється діапазон змін бальної оцінки) або в визначеній одиниці вимірювання. Реалізуються такі етапи метода безпосереднього експертного оцінювання:

- визначення об’єктів оцінювання та властивостей, що оцінюються;
- формування групи експертів;
- встановлення шкали оцінювання властивості об’єкта;
- проведення опитування експертів;
- оцінка ступеню узгодженості думок експертів;
- узагальнення оцінок експертів.

Надаємо характеристику кожного етапу і проілюструємо його реалізацію на основі прикладу.

Визначення об’єктів оцінювання та властивостей, що оцінюються. Визначається об’єкт оцінювання *X* (система, функція, процес, співробітник і т.д.) та властивості$\{ X_j\}, \mathrm{j} = \overline{1, G}$, за якими буде проводитись оцінка об’єкта. В нашому прикладі в якості об’єкта оцінювання *X* обирається система захисту інформації і кібербезпеки підприємства критичної інформаційної інфраструктури [7]. По об’єкту в якості властивостей розглядаються показники ефективності , що характеризують ступень досягнення системою захисту інформації і кібербезпеки поставлених перед нею завдань в рамках тауих функцій кібербезпеки:.

- ID Ідентифікація ризиків кібербезпеки;
- PR Кіберзахист;
- DE Виявлення кіберінцидентів;
- RS Реагування на кіберінциденти;
- RC Відновлення стану кібербезпеки.

Формування групи експертів. Група експертів має складатися з такої кількості осіб, що надає можливість отримати обґрунтовані висновки щодо всіх питань експертизи. В нашому прикладі група експертів буде складатися з 8 осіб. По кожному експерту може враховуватись пріоритет *Pi,* i=$\overline{1,n}$, що задається в установленій бальній шкалі оцінювання і відображає якісну компетентність експерта у встановленій предметній області об'єкта оцінювання і в подальшому впливає на вагу оцінок експерта при їх узагальненні.

Встановлення шкали оцінювання властивості об'єкта. Оцінка проводиться експертами на основі встановлено\ї ОПР шкали оцінювання , в якій може задаватися або діапазон бальних оцінок по кожній властивості *{Xj$_{min}$; Xj$_{max}$}, j*=$\overline{1,G}$; або діапазон бальних оцінок у рамках визначеного якісного рівня оцінювання по кожній властивості. У нашому прикладі шкала оцінювання задається для п'яти якісних рівнів (табл.3.1).

Таблиця 3.1

Шкала оцінювання властивості об'єкта

Рівень значень критеріїв	
Якісна оцінка	**Діапазон оцінок в балах**
Незадовільний	$0 \leq X_j < 0{,}25$
Низький	$0{,}25 \leq X_j < 0{,}5$
Середній	$0{,}5 \leq X_j < 0{,}75$
Високий	$0{,}75 \leq X_j < 0{,}9$
Найвищий	$0{,}9 \leq X_j < 1$

Експерт під час проведення оцінювання повинен обрати рівень відповідного показника і встановити значення цього показника в діапазоні встановлених значень обраного рівня.

Результати опитування експертів за встановленої шкалою наведені в табл. 3.2.

Таблиця 3.2

Оцінка експертами показників ефективності

Показники	Безпосередня оцінка експертами значень показників *Xij*								Xj= $X_{сер}$	σ_j	V_j
	1	2	3	4	5	6	7	8			
ID Ідентифікація ризиків кібербезпеки	0.7	0.8	0.7	0.6	0.75	0.8	0.75	0.7	0.725	0.061	0,085
PR Кіберзахист	0.3	0.4	0.5	0.7	0.7	0.45	0.4	0.6	0.556	0,14	0,25
DE Виявлення кіберінцидентів	0.8	0.9	0.9	0.75	0.8	0.9.	0.9	0.85	0,85	0,17	0,2
RS Реагування на кіберінциденти	0.55	0.6	0.6	0.65	0.6	0.55	0.6	0.65	0.6	0,1	0,16
RC Відновлення стану кібербезпеки.	0.8	0.9	0.9	0.95	0.7	0.95	0.7	0.65	0.82	0.015	0,018

Оцінка ступеня узгодженості думок експертів. Необхідною умовою вірогідності отриманої узагальненої оцінки об'єкта по кожній властивості $\{X_j\}, j = \overline{1,G}$, що враховує думки групи експертів, є достатній ступінь узгодженості думок експертів. Його можна перевірити різними шляхами. Наприклад, перший шлях – на основі аналізу коефіцієнта варіації з врахуванням дисперсії оцінок (див. табл. 3.1) і порівнянням останньої з заздалегідь визначеним її допустимим значенням або другий шлях – порівнянням проміжку між крайніми оцінками експертів з заздалегідь встановленою допустимою величиною. Наведемо приклад оцінки ступеня узгодженості на основі аналізу коефіцієнта варіації. Для того щоби визначити коефіцієнт варіації використовується така формула:

$$V = \sigma / Xсер, \quad (3.1)$$

де σ – середньоквадратичне відхилення;

$$\sigma = \sqrt[n]{\frac{\sum_{i1}^{n}(X_{сер} - X_i)^2}{n}}; \quad (3.2)$$

$X_{сер}$ – усереднена оцінка думок групи експертів:

$$Xсер = \frac{1}{n}\sum_{i}^{n} X_{ij}; \ i=\overline{1,n}; \ j=\overline{1,G}. \quad (3.3)$$

Мінливість думок експертів вважається слабкою, якщо ν<10%; якщо ν від 11-25%, то середньою і значною за ν>25%.

У табл.3.1 наведені результати оцінки ступеню узгодженості думок експертів по кожному показнику на основі коефіцієнта варіації. Якщо ОПР вважає недопустимим ступінь розбіжності виставлених оцінок, то авторам «крайніх точок», що не відповідають умовам встановленого рівня погодженості, пропонується аргументувати свої оцінки. Останнє може бути проведено в письмовому вигляді або на основі очного обговорення результатів. Після цього процедура експертного оцінювання повторюється. У нашому прикладі ОПР не допускає ступінь розбіжності думок експертів більш середнього, найбільший рівень розбіжності оцінок експертів відбувся по показнику PR Кіберзахист, що становить 25 %, він належить до середнього рівня. Тобто результати оцінювання, з погляду ступеня узгодженості вважаються готовими до подальшої обробки.

Узагальнення оцінок експертів. Пропонується застосування двох варіантів встановлення узагальненої оцінки об'єкта X_j за властивістю, що об'єднує оцінки групи експертів.

Перший варіант не передбачає врахуванні під час узагальнення оцінок пріоритету кожного експерта, а визначається як усереднена оцінка :

$$X_j = Xсер = \frac{1}{n}\sum_{i}^{n} X_{ij}; \ i=\overline{1,n}; \ j=\overline{1,G}. \quad (3.4)$$

Другий варіант передбачає врахуванні під час узагальнення оцінок порівняльного пріоритету кожного експерта:

$$X_j = \sum_i^n X_{ij} \times \beta_i, \quad (3.2)$$

де β_i – вага оцінки і-того експерту; $0 \leq \beta_i \leq 1; \sum_{i=1}^n \beta_i = 1$

$\beta_i = \frac{P_i}{\sum_{i=1}^n P_i;}$

де *Pi* -порівняльний пріоритет і-того експерту в установленій бальній шкалі.

У нашому прикладі застосовуємо перший варіант узагальнення оцінок експертів. Результати дивись в табл. 3.1.

3.2.Лабораторна робота «Метод безпосереднього оцінювання»

3.2.1. Мета роботи. Мета роботи – закріплення теоретичних знань та набуття навичок розв'язання задач експертного оцінювання рішень побудови захищених інформаційних систем та засобів комп'ютерної інженерії з застосуванням одного з базових методів експертного оцінювання – метода безпосереднього оцінювання .

3.2.2. Зміст і етапи лабораторної роботи

Студент отримує завдання на побудову модуля прийняття рішень для системи, е виникає проблема оцінювання і є можливість її розв'язання з застосуванням метода безпосереднього оцінювання. Для проведення лабораторної роботи група студентів розбивається на підгрупи, перед якою ставиться задача визначити на основі метода безпосереднього оцінювання властивость визначеного об'єкта. В кожній групі визначається ОПР (лідер групи) та експерти (студенти).

Етап 1. ОПР на основі метода безпосереднього оцінювання пропонується провести опитування групи експертів, яка надає оцінку показників у рамках встановленої шкали вимірювання (для якісного бального оцінювання), або у встановленій одиниці вимірювання кількісного показника.

Етап 2. На основі результатів опитування ОПР розподіляє між членами групи реалізацію наступним функцій:

1. На основі аналізу коефіцієнту варіації (ф.3.1.) з урахуванням дисперсії оцінок і порівнянням останньої з заздалегідь визначеним її допустимим значенням провести аналіз ступеня узгодженості думок експертів. Враховуючи дані аргументації ОПР, проводить обговорення ситуації з групою експертів. Згідно з методом Дельфі, експертам під час погодження з аргументами «авторів» крайніх точок надається можливість змінити свої оцінки і провести повторний етап оцінювання. Якщо відповідний рівень узгодженості думок не було досягнуто після повторного оцінювання, рішення про подальші кроки прийняття рішень приймає ОПР.

2. Провести узагальнення оцінок експертів з встановленням середньозваженого значення.

3. Побудувати модель «чорної скриньки» модуля прийняття рішень, в якій відображається його назва, перелік вхідної інформації, необхідної для реалізації, та її джерела; перелік вихідної інформації, що повинна бути отримана в результаті реалізації.

4. Визначити прецеденти роботи модуля.

5. Побудувати діаграму діяльності модуля на рівні прецедентів.

6. Надати математичну постановку реалізації задачі з застосуванням схеми алгоритму або діаграми діяльності по реалізації відповідного прецеденту.

7. Надати інфологічну модель предметної області на основі діаграми класів або діаграми Чена

Етап 3. Оформити звіт про виконання лабораторної роботи.

3.3. Приклади варіантів завдань

Приклад 1. Провести оцінку рівня вразливості визначеного інформаційного активу з погляду конфіденційності даних на основі встановленої шкали оцінювання (табл. 3.3).

Таблиця 3.3

Шкала оцінювання рівнів вразливості активу по впливу на конфіденційність

Назва рівня вразливості	Рівень вразливості активу				
	Дуже низький	Низький	Середній	Високий	Дуже високий
Діапазон значень	0-0.2	0.2-04	0.4-0.6	0.6-0,8	0.8 – 1.
Якісна характеристика рівня загрози при порушенні конфіденційності	Відсутній вплив на конфіденційність	Відбувається незначне розкриття інформації, але масштаби втрати обмежені таким чином, що доступні не основні дані	Відбувається значне розкриття інформації, але масштаби втрати обмежені таким чином, що доступні не всі дані	Відбувається розкриття до певної інформації з обмеженим доступом, але розкрита інформація має прямий серйозний вплив	Конфіденційність інформації не забезпечується

Приклад 2. Провести оцінку рівня ризику визначеного інформаційного активу під час реалізації загрози порушення конфіденційності даних на основі встановленої шкали оцінювання (табл. 3.4).

Таблиця 3.4

Шкала оцінювання рівнів ризику при реалізації загрози

Рівень ризику	Діапазон значень	Характеристика
Суто оптимістичний	0-1	Ризик відсутній. Реалізація загрози неможлива
Оптимістичний	1-2	Ризик майже відсутній. Успішна реалізація загрози практично неможлива, а наслідки відсутні.
Дуже низький	2-3	Ризиком можна знехтувати. Успішна реалізація загрози є рідкісною, а наслідки незначні.
Низький	3-4	Ризик є малим. Ймовірність реалізації загрози та її наслідки досить малі.
Помірний	4-5	Успішна реалізацій загрози можлива, наслідки будуть середніми
Середній	5-6	Ризик є серйозним. Потенційна реалізація загрози існує, наслідки будуть відчутливими.
Високий	6-7	Ризик реалізації загрози високий. реалізація загрози скоріш можлива, наслідки значні.
Песимістичний	7-8	Ризик реалізаії загрози дуже високий, успішна реалізація загрози можлива, а наслідки скоріше за все будуть катастрофічні
Суто песимістичний	8-10	Ризик та ймовірність реалізаці\ загрози дуже високі. Наслідки з глобальним впливом – надзвичайно високі, що можуть спричинити повний колапс системи, відновлення стабільної роботи майже неможливо

Завдання 2. Провести групою експертів оцінки якості Європейської системи «Полегшеної шкали оцінювання» (рис. 3.1). на основі такої шкали оцінювання (табл. 3.5).

Таблиця 3.5

Шкала оцінки якості Європейської системи «Полегшеної шкали оцінювання»

Рівень оцінки	Діапазон значень	Характеристика негативних факторів
Дуже високий	8-10	Не потребує поліпшення
Високий	6-8	Рівень високий але експерт вважає недоцільним встановлення обмежень на відсоток студентів, що відповідають встановленим оцінкам
Середній	4-6	Не формалізовані правила. які помилки мають яку значущість, але експерт вважає доцільним встановлення обмежень на відсоток студентів на встанволені оцінки як важель мотивації студентів
Низький	2-4	Не формалізовані правила. які помилки мають яку значущість, крім того, кесперт – вважає недоцільним встановлення обмежень на відсоток студентів на встанволені оцінки
Незадовільний	0-2	Експерт вважає, що потрібна більш досконалі правила побудови шкали і правил оцінювання знань студентів

Рис. 3.1. Європейської системи «Полегшеної шкали оцінювання»

СПИСОК ДЖЕРЕЛ

1. Бурячок В.Л. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов та ін. – Київ : ДУТ, 2015. – 345 с.
2. Грабовецький, Б. Є. Методи експертних оцінок: теорія, методологія, напрямки використання : монографія / Б. Є. Грабовецький. – Вінниця: ВНТУ, 2010. – 171 с.
3. Експертні методи в автоматизованих системах керування: Формування та напрями використання експертних знань: [Електронний ресурс] : навч. посіб. для студ. спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / КПІ ім. Ігоря Сікорського; уклад.: Л. Д. Ярощук. – 2-ге вид., допов. – Електронні текстові дані (1 файл: 0,90 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2022. – 43 с.
4. А. В. Катренко, В. В. Пасічник Прийняття рішень: теорія та практика : підручник / А. В. Катренко, В. В. Пасічник. – Львів: «Новий Світ – 2000», 2020. – 447 с.
5. Катренко А.В. Системний аналіз: підручник для ВНЗ / А. В. Катренко, В. В.Пасічник. – Львів: Вид-во «Новий світ-2000», 2020. – 396 с
6. Потьомкін М. М., Седляр А. А., Сірченко Р. С., Іщенко О. М. Нечіткий комплексний метод ранжування та його використання для багатокритерійного порівняння альтернатив. *Кібернетика та системний аналіз*. 2022. Т. 58, № 3. С. 83-90. doi: https://doi.org/10.1007/s10559-022-00471-0 URL: http://jnas.nbuv.gov.ua/article/UJRN-0001323859
7. Ю.І. Хлапонін, Л.М. Козубцова, І.М. Козубцов, Р.М. Штонда. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. Кібербезпека: освіта, наука, техніка №3(15), с.124-134
8. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. Front Cover. Thomas L. Saaty. McGraw-Hill International Book Company, 1980. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. Front Cover. Thomas L. Saaty. McGraw-Hill International Book Company, 1980.

9. Izmailova O. Assessing the Variety of Expected Losses upon the Materialisation of Threats to Banking Information /O.Izmailova, H. Krasovska, K. Krasovska ,V. Zaslavskyi// *Information & Security: An International Journal* , vol. 45 (2020): 89-118 https://doi.org/10.11610/isij.450
10. Khlaponin Y., Izmailova O., Krasovska H., Krasovska K., Bodnar N., Abbas S.Q. Base of models of the information security risks assessment systemBase of models of the information security risks assessment systemProceedings of FRUCT'35Tampere, Finland, 24-26 April 2024 Oy, Finland, ISSN 2305-7254, ISBN 978-952-65246-1-0, Issue 1, p.352-366 Scopus https://fruct.org/publications/volume-35/fruct35/files/Khl.pdf
11. Yurii Khlaponin, Olha Izmailova, Nameer Hashim Qasim, Hanna Krasovska, Kateryna Krasovska. Management risks of dependence on key employees: identification of personnel. Workshop on "Cybersecurity Providing in Information and elecommunication Systems" (CPITS 2021) http://sec.picst.org/ January 28, 2021 pp 295-308 http://ceur-ws.org/Vol-2923/paper33.pdf. Scopus https://fruct.org/publications/volume-35/fruct35/files/Khl.pdf
12. Методичні вказівки до виконання циклу прктичних практичних робіт «Метод аналізу ієрархій»для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 "Кібербезпека" (БІКС) та 123 «Комп'ютерна інженерія» з дисципліни «Системний аналіз» / Уклад. О.В. Ізмайлова,–Київ : КНУБА, 2024. – 28 с.

Додаток 1

Таблиця Д.1

Значення розподілення χ^2

ν	α=0.01	α=0.05
1	6.63	3.84
2	9.21	5.99
3	11.34	7.81
4	13.28	9.49
5	15.1	11.1
6	16.8	12.6
7	18.5	14.1
8	20.1	15.5
9	21.7	16.9
10	23.2	18.3
11	24.7	19.7
12	26.2	21.0
13	27.7	22.4
14	29.1	23.7
15	30.6	25.0
16	32	26.3
17	33.4	27.6
18	34.8	28.9
19	36.2	30.1
20	37.6	31.4
21	38.9	32.7
22	40.3	33.7
23	41.6	35.2
24	43	36.4
25	44.3	37.7
26	45.6	38.9
27	47	49.1
28	48.3	41.3
29	49.6	42.6
30	50.9	43.8
40	63.7	55.8
50	76.2	67.5
60	88.4	79.1
70	100.4	90.5
80	112.3	101.9
90	124.1	113.1
100	135.8	124

Додаток 2

Таблиця Д.2. 1

Значення розподілення F ($\alpha = 0..01$) (ν_1 в діапазоні від 1 до 10)

Ступень свободи ν_2	Ступень свободи ν_1									
	1	2	3	4	5	6	7	8	9	10
1	4.052	5.0	5.403	5.625	5.764	5.859	5.928	5.98	6.023	6.05
2	98.5	99	99.2	99.3	99.4	99.4	99.4	99.4	99.4	99.4
3	34.1	30.8	29.5	28.7	28.2	27.9	27.7	27.5	27.3	27.2
4	21.2	18.0	16.7	16	15.5	15.2	15	14.8	14.7	14.5
5	16.3	13.3	12.1	11.4	11	10.7	10.5	10.3	10.2	10.1
6	13.7	10.9	9.78	9.15	8.75	8.47	8.26	8.1	7.98	7.87
7	12.2	9.56	8.45	7.85	7.46	7.19	6.99	6.84	6.72	6.62
8	11.3	8.65	7.59	7.01	6.63	6.37	6.18	6.03	5.91	5.81
9	10.6	8.02	6.99	6.42	6.06	5.8	5.61	5.47	5.35	5.26
10	10	7.56	6.56	5.99	5.64	5.39	5.2	5.06	4.94	4.85
11	9.65	7.21	6.22	5.87	5.32	5.07	4.89	4.74	4.63	4.54
12	9.32	6.93	5.95	5.41	5.06	4.82	4.64	4.5	4.39	4.3
13	9.07	6.7	5.74	5.21	4.86	4.62	4.44	4.3	4.19	4.1
14	8.86	6.51	5.56	5.04	4.7	4.46	4.28	4.14	4.03	3.94
15	8.58	6.35	5.42	4.89	4.56	4.32	4.14	4	3.89	3.8
16	8.53	6.23	5.29	4.77	4.44	4.2	4.03	3.89	3.78	3.69
17	8.4	6.11	5.19	4.87	4.34	4.1	3.93	3.79	3.68	3.59
18	8.29	6.01	5.09	4.58	4.25	4.01	3.84	3.71	3.6	3.51
19	8.19	5.93	5.01	4.5	4.17	3.94	3.77	3.63	3.52	3.43
20	8.1	5.85	4.94	4.43	4.1	3.87	3.7	3.56	3.46	3.37
21	8.02	5.78	4.87	4.37	4.04	3.81	3.64	3.51	3.4	3.31
22	7.95	5.72	4.82	4.31	3.99	3.76	3.59	3.45	3.35	3.26
23	7.88	5.56	4.76	4.25	3.94	3.71	3.54	3.41	3.3	3.21
24	7.82	5.61	4.72	4.22	3.9	3.87	3.5	3.38	3.25	3.17
25	7.77	5.37	4.68	4.18	3.86	3.62	3.46	3.32	3.22	3.13
30	7.56	5.39	4.51	4.02	3.7	3.47	3.3	3.17	3.07	2.98
40	7.31	5.18	4.31	3.83	3.51	3.29	3.12	2.99	2.89	2.8
50	7.08	4.98	4.13	3.85	3.34	3.12	2.95	2.82	2.72	2.63
120	6.85	4.79	3.95	3.48	3.17	2.96	2.79	2.66	2.56	2.47
∞	6.63	4.81	3.78	3.32	3.02	2.8	2.64	2.51	2.41	2.32

Таблиця Д.2. 2

Значення розподілення F ($\alpha = 0..01$) (ν_1 в діапазоні від 11 до ∞)

Ступень свободи ν_2	Ступень свободи ν_1								
	12	15	20	24	30	40	60	120	∞
1	6.1	6.15	6.2	6.23	6.26	6.29	6.31	6.34	6.36
2	99.4	99.4	99.4	99.5	99.5	99.5	99.5	99.5	99.5
3	27.1	26.9	26.7	26.5	26.5	26.4	26.3	26.2	26.1
4	14.4	14.2	14	13.9	13.9	13.7	13.7	13.6	13.5
5	9.89	9.72	9.56	9.47	9.38	9.29	9.2	9.11	9.02
6	7.72	7.56	7.4	7.31	7.23	7.14	7.06	6.97	6.88
7	6.47	6.21	6.16	6.07	5.99	5.91	5.82	5.74	6.65
8	5.87	5.52	5.36	5.28	5.2	5.12	5.03	4.95	4.66
9	5.11	4.96	4.81	4.73	4.65	4.57	4.48	4.4	4.31
10	4.7	4.56	4.41	4.33	4.25	4.17	4.08	4	3.91
11	4.4	4.25	4.1	4.02	3.94	3.86	3.78	3.69	3.6
12	4.16	4.01	3.86	3.78	3.7	3.62	3.54	3.45	3.36
13	3.96	3.82	3.66	3.59	3.51	3.43	3.34	3.25	3.17
14	3.8	3.66	3.51	3.43	3.35	3.27	3.18	3.09	3
15	3.66	3.51	3.43	3.35	3.27	3.18	3.09	2.96	2.87
16	3.55	3.41	3.26	3.18	3.1	3.02	2.93	2.84	2.75
17	3.46	3.31	3.16	3.08	3	2.92	2.83	2.75	2.65
18	337	3.23	3.08	3	2.92	2.84	2.75	2.66	2.57
19	3.3	3.15	3	2.92	2.84	2.75	2.67	2.58	2.49
20	3.23	3.09	2.94	2.86	2.78	2.69	2.61	2.52	2.42
21	3.17	3.03	2.86	2.8	2.72	2.64	2.55	2.46	2.06
22	3.12	2.98	2.83	2.75	3.67	2.58	2.5	2.4	2.31
23	3.07	2.93	2.78	2.7	2.62	2.54	2.45	2.35	2.26
24	3.03	2.89	2.74	2.66	2.58	2.49	2.4	2.31	2.21
25	2.99	2.85	2.7	2.62	2.53	2.45	2.36	2.27	2.17
30	2.84	2.7	2.56	2.47	2.39	2.3	2.21	2.11	2.01
40	2.66	2.52	2.37	2.29	2.2	2.11	2.02	1.92	1.8
60	2.5	2.35	2.2	2.12	2..3	1.94	1.84	1.73	1.6
120	2.34	2.19	2.03	1.95	1.86	1.76	1.66	1.53	1.38
∞	2.18	2.04	1.88	1.79	1.7	1.59	1.47	1.32	1

Навчально-методичне видання

ТЕОРІЯ ПРИЙНЯТТЯ РІШЕНЬ

Методичні вказівки
до виконання циклу лабораторних робіт
«**Моделі та методи експертного оцінювання
під час розв'язання задач прийняття рішень
в умовах невизначеності**»
для здобувачів першого (бакалаврського) рівня
вищої освіти галузі знань 12 «Інформаційні технології»
спеціальностей 125 «Кібербезпека та захист інформації»
123 «Комп'ютерна інженерія»

Укладач **Ізмайлова** Ольга Василівна

Комп'ютерне верстання *А. П. Селівестрової*

Ум. друк. арк. 2,09. Обл.-вид. арк. 2,25
Електронний документ. Вид № 62/V-24.

Виконавець і виготовлювач
Київський національний університет будівництва і архітектури

Проспект Повітряних Сил, 31, Київ, Україна, 03037
Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи ДК № 808 від 13.02.2002 р