Хмельницький національний університет
Факультет інформаційних технології
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система оцінювання прийняття рішень в системах інформаційної безпеки
Назва теми

КвРКІ. 20210299.01.26.02 ПЗ
Шифр

Галузь знань 12 «*Інформаційні технології*»
Шифр, назва

Спеціальність 123 «*Комп'ютерна інженерія*»
Шифр, назва

Освітня програма «*Комп'ютерна інженерія та програмування*»
Назва

Виконав: студент IV курсу, група КІ2–19–2 _____ Н.В. Войталюк
Підпис — Ініціали, прізвище

Керівник _____ 22.06.23 _____ М.В. Капустян
Підпис, дата — Ініціали, прізвище

Нормоконтролер _____ С.М. Лисенко
Підпис, дата — Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Т.О. Говорущенко
Підпис — Ініціали, прізвище

«26» червня 2023 р.

Хмельницький 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"11" 01 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Войталюку Назару Володимировичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система оцінювання прийняття рішень в системах інформаційної безпеки

Керівник проекту (роботи) Капустян М.В., доцент кафедри КІІС.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.03.2023 р. № 5

2. Строк подання студентом проекту (роботи) на кафедру 07.06.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Теоретичні основи системи оцінювання прийняття рішення

Модель оцінювання прийняття рішення та визначення елементів даних для системи оцінювання прийняття рішення

Структура, алгоритми та результати роботи системи оцінювання прийняття рішень для систем інформаційної безпеки

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Алгоритми роботи системи оцінювання прийняття рішень для систем інформаційної безпеки

Структура системи оцінювання прийняття рішення

Креслення вигляду екранних форм системи оцінювання прийняття рішення

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_11_»_____01_____2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітк
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2023	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2023	виконав
3	Робота над розділом 1 – теоретичні основи системи оцінювання прийняття рішення	01.03.2023	виконан
4	Робота над розділом 2 – модель оцінювання прийняття рішення та визначення елементів даних для системи оцінювання прийняття рішення	01.04.2023	виконан
5	Робота над розділом 3 – Структура, алгоритми та результати роботи системи оцінювання прийняття рішень для систем інформаційної безпеки	30.04.2023	виконан
6	Оформлення пояснювальної записки згідно вимог	26.05.2023	виконан
7	Попередній захист ВКР	26.05.2023	виконан
8	Захист ВКР на засіданні ЕК	Червень 2023 року	

Студент _____ Войталюк Н.В.
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Капустян М.В.
Підпис Ініціали, прізвище

№ рядка	формат
1	
2	
3	
4	

Зм	Ар
Розроби	
Перевір	
Н. конт	
Затв.	

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ. 20210299.01.26.02 ПЗ	Пояснювальна записка	55		
			Графічні матеріали			
2		КвРКІ20210299.01.26.02Е8	Алгоритми роботи системи оцінювання прийняття рішень для систем інформаційної безпеки	1		
3		КвРКІ. 20210299.01.26.02Е8	Структура системи оцінювання прийняття рішення	1		
4		КвРКІ. 20210299.01.26.02Е8	Креслення вигляду екранних форм системи оцінювання прийняття рішення	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ. 20210299.01.26.02 ПЗ		
Розробив		Войталюк		22.06.23	Відомість проекту	Літера	Аркуш 1 / Аркушів 1
Перевір.		Капустян		22.06.23		У	
Н. контр.		Лисенко		26.06		ХНУ, КІ2-19-2	
Затв.		Говорущенко					

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система оцінювання прийняття рішень в системах інформаційної безпеки».

Автор роботи: *Войталюк Назар Володимирович.*

Керівник роботи: *Капустян Марія Вікторівна.*

Пояснювальна записка: *55 с.*, 16 *рис.*, 9 *табл.*, 3 *дод.*, 40 *джерела.*

Графічна частина: 3 креслення

СИСТЕМА ОЦІНЮВАННЯ ПРИЙНЯТТЯ РІШЕННЯ, ЗАГРОЗИ, СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета кваліфікаційної роботи: реалізація прототипу системи оцінювання прийняття рішень для системи інформаційної безпеки ІТ інфраструктури.

Використання системи оцінювання прийняття рішень в системах інформаційної безпеки дозволяє підвищити ефективність заходів безпеки, зменшити ризики й економічні затрати та забезпечити надійний захист інформаційних ресурсів ІТ інфраструктури. Це стає особливо важливим у контексті зростаючої кількості кіберзагроз та постійно змінюваного середовища інформаційних технологій.

Отже, система оцінювання прийняття рішень в системах інформаційної безпеки є необхідним інструментом для забезпечення ефективного та надійного захисту інформаційних систем від потенційних загроз. Вона дозволяє зробити обґрунтовані рішення та вибрати оптимальні заходи безпеки, що сприяє забезпеченню стійкості та безпеки в цифровому середовищі.

Підпис студента

22.06.23
Дата

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БД – База даних

ІС – Інформаційна система

ІТ – Інформаційні технології

КС – Комп’ютерна система

МАІ – Метод аналізу ієрархій

СОПР – Система оцінювання прийняття рішення

СІБ – Система інформаційної безпеки

IDS – Intrusion detection systems

ВСТУП

В сучасному цифровому світі, де інформація відіграє вирішальну роль, забезпечення безпеки комп'ютерних та інформаційних систем стає надзвичайно важливим завданням. Інформаційна безпека включає в себе комплекс заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації, а також запобігання несанкціонованому доступу, втраті даних та ризикам від кібератак.

Для ефективного забезпечення безпеки інформаційних систем, потрібна система оцінювання прийняття рішень, яка допомагає визначити оптимальні заходи та стратегії для запобігання загрозам і реагування на них. Система оцінювання прийняття рішень в системах інформаційної безпеки є інструментом, який дозволяє аналізувати, визначати та порівнювати альтернативи щодо їхньої ефективності, надійності, вартості та інших критеріїв.

Основна мета системи оцінювання прийняття рішень полягає в тому, щоб забезпечити оптимальне використання ресурсів та ефективний захист інформаційних систем від потенційних загроз. Це досягається шляхом визначення конкретних цілей безпеки, встановлення критеріїв оцінки та вибору оптимальних альтернатив.

Система оцінювання прийняття рішень включає в себе різноманітні елементи, такі як визначення цілей, виявлення загроз, аналіз ризиків, вибір заходів та контроль їхньої ефективності. Вона базується на аналітичних методах, моделях та інструментах, які допомагають приймати обґрунтовані рішення на основі доступної інформації.

Використання системи оцінювання прийняття рішень в системах інформаційної безпеки дозволяє підвищити ефективність заходів безпеки, зменшити ризики й економічні затрати та забезпечити надійний захист інформаційних ресурсів IT інфраструктури. Це стає особливо важливим у

контексті зростаючої кількості кіберзагроз та постійно змінюваного середовища інформаційних технологій.

Отже, система оцінювання прийняття рішень в системах інформаційної безпеки є необхідним інструментом для забезпечення ефективного та надійного захисту інформаційних систем від потенційних загроз. Вона дозволяє зробити обґрунтовані рішення та вибрати оптимальні заходи безпеки, що сприяє забезпеченню стійкості та безпеки в цифровому середовищі.

Метою роботи є реалізація прототипу системи оцінювання прийняття рішень для системи інформаційної безпеки IT інфраструктури.

Об’єкт дослідження є процес оцінювання прийняття рішення для систем інформаційної безпеки IT інфраструктур.

Предметом дослідження є система оцінювання прийняття рішень в системах інформаційної безпеки.

1 ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ОЦІНЮВАННЯ ПРИЙНЯТТЯ РІШЕННЯ

1.1 Прийняття рішень у системах оцінки прийняття рішень

Впровадження автоматизованих процедур оцінки прийняття рішень призвело до розробки різних методів створення систем оцінки прийняття рішень (СОПР). Ці системи використовують сучасні математичні методи, різноманітні математичні моделі, технічні та програмні ресурси. У результаті, СОПР пов'язані з цими методами, моделями та ресурсами.

СОПР – це комп’ютеризована, інтерактивна автоматизована система, яка складається із набору програмного забезпечення. Вона призначена для допомоги та оцінки різних рішень, пов'язаних з вирішенням невизначених або нечітких проблем. Використання СОПР забезпечує всебічне та об’єктивне дослідження предмета прийняття рішень в складних ситуаціях.

Сучасні інтелектуальні СОПР відрізняються широким використанням інтелектуальних методів обробки даних та прийняття рішень, а також дизайном інтерфейсу, що відповідає принципам інтелектуалізації взаємодії користувача з системою. В інтелектуалізації системи враховуються відгуки та вподобання користувача щодо представлення результатів обробки даних, зручного режиму введення, редагування та оновлення бази знань і даних, що відповідають потребам конкретного користувача.

ІСОПР належать до категорії інформаційних обчислювальних систем для обробки даних, які є комплексними та ефективними, що дозволяють інтегрувати різні типи даних. Інтелектуальні методи та алгоритми, включаючи алгоритми пошуку даних на основі специфічних ознак, алгоритми перетворення даних, ігрові методи пошуку та обробки даних, а також методи представлення знань у базі знань, є складовими даного системного класу. Окрім того, даний клас включає також різноманітні методи планування, методи обробки невизначеності, методи прийняття рішень на основі нейронних мереж, імовірнісні моделі та

судження, а також чітку та нечітку логіку. До цього класу також входять методи навчання, засновані на попередньому досвіді та спостереженнях, ймовірнісні методи обробки лінгвістичної інформації, байєсовські мережі, методи сприйняття та розпізнавання образів, а також методи керування в робототехніці.

Природа та різноманітні системи, включаючи біологічні, екологічні, соціальні та економічні, представляють собою постійний потік завдань з прийняття рішень, що виникають і розв'язуються. Ці завдання можуть виникати внаслідок функціонування живих організмів та їхніх колоній, уподобань споживачів, стихійних лих та інших явищ.

Рішення, у цьому контексті, відноситься до обґрунтованого набору дій, вжитих особою, яка приймає рішення для досягнення конкретної мети або приведення об'єкта чи системи керування в бажаний стан. Це вид розумової діяльності, що відображає волю людини.

При розробці СОПР важливо досить точно класифікувати рішення. Відомі підходи пропонують систему класифікації рішень, що представлена у таблиці 1.1.

Таблиця 1.1 – Класифікація видів рішень

Ознака	Вид рішення		
Ступінь структуризації проблеми	Гарно структуроване	Погано структуроване	Не структуроване
Кількість етапів реалізації рішення	Статичне (один етап)	Динамічне	
Рівень інформованості про стан проблеми	Умови визначеності	Умови ризику	Умови невизначеності
Кількість ОПР	Одна особа	Багато осіб	
Зміст рішення	Стратегічне	Тактичне	

Прийняття рішень включає процес вибору найбажанішого варіанту з набору задовільних альтернатив або визначення пріоритетності серії рішень. Для того, щоб приймати обґрунтовані рішення, необхідно мати знання про предмет, поточні та майбутні процеси, а також враховувати різні показники, які відображають ефективність та якість обраного варіанту. Таким чином, важливо мати відповідну модель предмета та структуру для прийняття та оцінки обраного варіанту.

Модель прийняття рішень є формальним представленням проблеми та процесу прийняття рішень. Встановлення формальних засад для відбору, зокрема критерію оптимальності, є одним з основних викликів теорії прийняття рішень (ТПР), яка зародилася в епоху Відродження. ТПР вивчає проблеми категоризації та аналізу різних типів вибору, а також розвиває теоретичні конструкції, такі як поняття корисності і переваги.

Процес прийняття рішень включає кілька важливих етапів, які включають постановку проблеми, формування рішення та вибір оптимального варіанту.

На етапі постановки проблеми проводиться аналіз і діагностика проблеми, а також встановлюються цілі для визначення напрямку пошуку рішень. Збирається релевантна інформація та дані, а рішення, які не відповідають цілям, відкидаються.

Етап формування рішення включає кілька фаз, таких як формулювання обмежень, критеріїв прийняття рішення та визначення альтернатив. На цьому етапі встановлюються обмеження, які відокремлюють прийнятні варіанти від неприйнятних, формулюються критерії, що допоможуть вибрати найкраще рішення з наявних варіантів, і генеруються прийнятні альтернативи шляхом розробки та пошуку рішень.

Наступним етапом є етап вибору рішення, на якому проводиться оцінка альтернатив та прийняття остаточного рішення. На цьому етапі прийнятні варіанти оцінюються за певними заздалегідь визначеними критеріями, і обирається найкращий варіант. Варто зауважити, що кожна альтернатива може

мати свою власну цінність, і існує можливість, що один варіант може мати неявну перевагу над іншим, що може виникнути складнощі.

Процес прийняття рішень складається з кількох важливих етапів. Спочатку необхідно визначити цілі, критерії відбору кандидатів, які мають право на отримання ресурсів, і критерії оптимальності. Після цього формується набір прийнятних альтернатив і вибираються методики вирішення проблеми. Далі проводиться порівняння і ранжування варіантів за обраними критеріями, а потім обираються найкращі варіанти відповідно до критерію оптимальності і приймається рішення.

Проте, в процесі прийняття рішень часто можуть виникати помилки. Деякі з них включають одностороннє прийняття рішень, відсутність системного підходу, надмірну упередженість до звичних альтернатив, недостатнє урахування потенційних ризиків, розгляд тільки позитивних результатів і ігнорування негативних наслідків, прийняття рішень на емоційній основі, спонтанність і поспішність. Крім того, у процесі прийняття рішень часто керуються припущеннями, прихованими бажаннями та помилковими припущеннями, замість того, щоб базуватися на достовірній та об'єктивній інформації. Також можуть статися помилкові тлумачення фактів і прийняття непродуктивних рішень, які не є відповідними контексту.

Слід також відзначити, що дієвість рішення залежить від його ефективності. Двома основними компонентами, які впливають на ефективність рішення, є якість рішення (Q) та людський фактор прийняття рішень (A). Дані фактори можуть бути кількісно визначені та взаємопов’язані за допомогою аналітичних зв’язків, таких як адитивні або мультиплікативні формули.

У випадку зниження будь-якої із зазначених змінних (особливо досягнення мінімального рівня) ефективність рішення буде знижуватися. Фактор Q для якості рішення пов’язаний із вибором найбільш підходящого варіанту із тих, які доступні у даному сценарії проблеми. Цей сценарій враховує умови прийняття рішень і здібності тих, хто приймає рішення.

Людський фактор А для прийняття рішень може мати різні прийнятні рівні для окремих варіантів.

Щоб підвищити ефективність прийняття рішень, слід зосередитися на покращенні фактора якості, зокрема шляхом відповідного вибору обмежень і критеріїв прийняття рішень, створення набору прийнятних альтернатив і вибору найкращого варіанту на основі умов завдання.

Наприклад, у вирішенні проблеми розподілу ресурсів ефективність вимірюється мірою співмірності цілей з ресурсами, витраченими на їх досягнення, що визначається коефіцієнтом якості рішення Q. Коефіцієнт Q суттєво залежить від якості та повноти проблеми формулювання та вибір відповідних моделей і методів вирішення проблем.

1.2 Невизначеність прийняття рішень

Поняття невизначеності стосується наявності факторів, які призводять до невизначеності результатів дій, і ступінь їх впливу є невідомим. Щоб оцінити наявність невизначеності, можна провести аналіз на теоретичному або практичному рівні, залежно від контексту прийняття рішень у конкретному сценарії. Математичні моделі часто використовуються для дослідження теоретичних невизначеностей, тоді як практичні невизначеності оцінюються шляхом оцінки доступної інформації для прийняття рішень.

Підбір відповідних моделей враховує умови, при яких вони застосовні, а оцінка інформації для прийняття рішень часто ґрунтується на концепції інформаційної ентропії, яка вимірює міру невизначеності в процесі прийняття рішень.

Категорія невизначеності характеризується кількома параметрами, що вказують на різні типи невизначеності, такі як загальна невизначеність, ситуаційна невизначеність, політична невизначеність, соціальна невизначеність та інші. Для ефективного розв'язання проблем прийняття

рішень при наявності невизначеностей важливо визначити рівень аналізу та типи невизначеностей, які враховуються.

Варто зауважити, що невизначеність часто неправильно розглядають просто як відсутність повної інформації про об'єкт. Насправді, невідповідність знань про стани об'єктів не є єдиним джерелом невизначеності. Крім того, невизначеність може виникати через неоднозначні цілі та невизначені критерії вибору рішень.

У багатьох практичних ситуаціях прийняття рішень є складним завданням через велику кількість альтернативних варіантів і різноманітність критеріїв, які використовуються для їх оцінки. Коли ми говоримо про системний аналіз, прийняття рішень і дослідження операцій, основні типи невизначеностей, що визнаються, включають невизначеність цілей, ситуаційну невизначеність, стратегічну невизначеність та інформаційну невизначеність.

Розглянемо основні характеристики первинних типів невизначеностей у процесі прийняття рішень.

Перший тип невизначеності – це невизначеність цілей. Вона виникає, коли вибір цілей в задачах з багатьма критеріями є непевним і оточений невизначеністю.

Другий тип – ситуаційна невизначеність. Вона виникає через неконтрольовані фактори, що впливають на практичні процеси. Ситуаційна невизначеність може походити з різних причин, таких як недостатня інформація про навколишнє середовище, непередбачувані зовнішні фактори або непевні очікування стосовно майбутніх подій.

Третій тип – стратегічна невизначеність. Вона пов'язана із невизначеністю щодо цілей і дій активного чи пасивного партнера або супротивника, відома також як невизначеність конфлікту.

Нарешті, інформаційна невизначеність означає невизначеність і неоднозначність процесів, явищ та інформації щодо аналізованої системи, а також відсутність достовірної інформації.

Окрім того, існують додаткові класифікації невизначеностей, зокрема такі як:

– Структурна невизначеність, яка відноситься до невизначеності моделі структури досліджуваної системи.

– Параметрична невизначеність, яка передбачає невизначеність параметрів моделі системи. Оцінка і аналіз якості цих параметрів можуть бути складними.

– Статистична невизначеність, яка виникає внаслідок невизначеності статистичних даних. Це може бути наслідком різних факторів, таких як обсяг даних, пропуски, випадкові вимірювання та помилки або шуми впливу.

– Методична невизначеність, яка відноситься до невизначеності або неоднозначності у обробці даних або методах розв'язання проблем.

– Комбінаторна невизначеність, яка виникає через неможливість знати всі можливі варіанти. Цей тип невизначеності часто пов'язаний з іншими типами невизначеностей і виникає від них.

Важливо відзначити, що під час прийняття рішень і системного аналізу різні типи невизначеностей часто взаємодіють і утворюють складну системну невизначеність.

1.3 Людино-машинні системи оцінювання прийняття рішень

Важливо відзазначити, що людський процес прийняття рішень має свої обмеження в аналізі, обробці даних, якості рішень і швидкості. Люди обмежені в своїй здатності працювати з обмеженою кількістю інформації одночасно і часто стикаються з непослідовністю, невизначеністю, нелогічністю і спрощеннями під час аналізу складних проблем. У порівнянні з людьми, обчислювальні машини здатні ефективно працювати в таких ситуаціях. Це призвело до розвитку систем, що поєднують сильні сторони людей і машин, компенсуючи їхні слабкі сторони.

Сучасні системи "людина-машина" включають автоматизовані системи керування, експертні системи та системи прийняття рішень, які особливо корисні для вирішення проблем розподілу ресурсів. Системи прийняття рішень дозволяють людям проектувати, порівнювати та вибирати альтернативні рішення за допомогою обчислювальних засобів.

Сьогодні неможливо уявити застосування нових методологій для створення та прийняття високоякісних рішень без використання електронних інформаційних систем та інформаційних технологій. Розширення використання інформаційних технологій в суспільстві стало ключовим фактором впровадження таких систем. Використання сучасних методів, заснованих на інформаційних технологіях, сприяє використанню обчислювальної потужності комп'ютерів для обчислень, обробки даних, аналізу та прогнозування в режимі реального часу, що допомагає в прийнятті рішень.

Отже, акцент перейшов на автоматизацію інтелектуальних завдань, що призвело до поширення систем прийняття рішень "людина-машина", які є ефективними для розв'язання практичних проблем. При автоматизації процесу прийняття рішень рекомендується використовувати системи прийняття рішень, які дозволяють створювати різні сценарії і визначати оптимальні варіанти дій. Такі системи є цінними для управління та оцінки рішень, а також для аналізу даних в сучасному економічному середовищі.

При автоматизації процесів прийняття рішень досить часто рекомендується використовувати СОПР, щоб полегшити прийняття критичних рішень на основі очікуваних подій. Ці стандартні операційні процедури дозволяють створювати кілька потенційних сценаріїв і визначати оптимальні варіанти дій. Крім того, СОПР володіють якостями, які роблять їх не лише цінними для системних завдань управління та оцінки прийняття рішень, але також є ключовими інструментами для аналізу даних у сучасному економічному кліматі.

1.4 Вимоги до сучасних систем оцінки прийняття рішень

З огляду на сучасний етап розвитку, системи СОПР повинні відповідати наступним критеріям:

– Повинна мати можливість обробляти нечіткі та неструктуровані дані.

– Функціонувати з слабо структурованими рішеннями.

– Підтримувати як послідовні, так і взаємозалежні рішення.

– Повинна мати можливість застосовувати знання.

– Має полегшувати моделювання та прогнозування.

– Логіку системи має бути легко сформульовано для легкої розробки.

– Має бути простою у використанні та модифікації.

– Повинна підтримувати три фази прийняття рішень, тобто інтелектуальну, проектну та відбіркову.

– Система має бути призначена для ОПР різного рівня.

– Систему можна налаштувати як для індивідуального, так і для групового використання.

– СОПР підтримує кілька методів і стилів рішень, які можуть бути корисними для команд ОПР.

– Є адаптивною та гнучкою до змін в організації та її середовищі.

– Дозволяє людям керувати процесом прийняття рішень за допомогою комп’ютера, а не навпаки.

– Система підтримує еволюційне застосування та легко адаптується до мінливих вимог.

– Використання СОПР підвищує ефективність процесу прийняття рішень.

1.5 Особливості застосування сучасних СОПР

Захоплення СОПР як перспективною сферою впровадження комп’ютерних технологій і засобом підвищення продуктивності праці в сфері

інформаційної безпеки зростає щодня. Останніми роками сучасні СОПР з'явилися з кількома розширеними функціями, які роблять їх більш ефективними для забезпечення процесу прийняття рішень.

– Інтеграція штучного інтелекту (ШІ) і машинного навчання (МН). Сучасні СОПР включають алгоритми штучного інтелекту та машинного навчання, щоб надавати точнішу та надійнішу інформацію. AI і ML можуть допомогти визначити закономірності, тенденції та аномалії у великих і складних наборах даних і надати рекомендації на основі такого аналізу. Ця інтеграція дозволяє приймати більш обґрунтовані та керовані даними рішення.

– Візуалізація даних і приладна панель. Нові СОПР створені для забезпечення чіткого та короткого перегляду даних за допомогою графічних зображень. Використання інтерактивних інформаційних панелей, діаграм і графіків полегшує особам, які приймають рішення, швидке розуміння складних даних і тенденцій.

– Хмарна архітектура. СОПР зазвичай базуються на хмарі, що забезпечує більшу гнучкість і доступність. Доступ до хмарної DSS можна отримати з будь-якого місця, де є підключення до Інтернету, і вона може збільшуватися або зменшуватися залежно від потреб користувача.

– Аналіз даних у реальному часі. Сучасні СОПР забезпечують аналіз даних у режимі реального часу, що дозволяє швидко приймати рішення. Аналіз даних у режимі реального часу може допомогти визначити проблеми та можливості, щойно вони виникають, що дозволить компаніям швидко реагувати.

– Спільне прийняття рішень. Системи оцінювання прийняття рішень підтримують співпрацю між членами команди, дозволяючи багатьом зацікавленим сторонам надавати внесок і відгуки. Функції співпраці можуть включати спільні робочі області, чат у реальному часі та контроль версій.

Мобільна сумісність. Сучасні системи розроблені таким чином, щоб бути сумісними з мобільними пристроями, дозволяючи користувачам отримувати доступ до даних і приймати обґрунтовані рішення зі своїх

мобільних пристроїв. Ця функція дозволяє тим, хто приймає рішення, бути в курсі та приймати рішення, навіть коли вони не в офісі.

Таким чином можна відзначити, що сучасні СОПР включають передові технології та функції, які роблять їх ефективнішими для сприяння процесам прийняття рішень. Інтеграція штучного інтелекту та машинного навчання, візуалізація даних і приладна дошка, хмарна архітектура, аналіз даних у режимі реального часу, спільне прийняття рішень і сумісність із мобільними пристроями – це лише деякі з ключових особливостей СОПР, які дозволяють компаніям робити більш інформовані та керовані даними рішення.

1.6 Метод оцінки прийняття рішення

Одним із широко використовуваних підходів для математичного моделювання процесу прийняття рішень є теорія прийняття рішень із використанням методу аналізу ієрархій (Analytic Hierarchy Process, AHP). MAI є методом, розробленим Томасом Сааті для ранжування альтернатив і прийняття рішень в умовах багатокритеріального вибору. Аналітичний метод ієрархії, створений Томасом Сааті, здобув світове визнання та знаходить широке застосування в рішеннях проблем у різних галузях. Цей метод має різні модифікації, які враховують специфіку конкретних завдань і можуть знизити наявні обмеження.

Метод MAI відрізняється високою гнучкістю, що дозволяє його застосування для виявлення зв'язків між критеріями та альтернативами шляхом найпростішого підходу. Цей метод враховує актуальність критеріїв у реальному світі та розкриває їх взаємодію у випадках складних проблем з багатьма критеріями та значною кількістю альтернатив. Використовуючи метод аналізу ієрархій, можна розкласти складні проблеми на конкретні ієрархії, включаючи кількісні та якісні аспекти проблеми в аналізі. Метод MAI поєднує всі рівні ієрархій, що дозволяє встановити, як зміна одного критерію впливає на інші критерії та альтернативи.

Математичний апарат MAI базується на парних порівняннях критеріїв та альтернатив і дозволяє визначити ваги кожного критерію та альтернативи. Основна ідея полягає у використанні показників важливості, які порівнюються з одиницею, і визначають ступінь переваги одного елементу над іншим.

Даний метод включає виконання таких кроків:

Створення ієрархії: Ієрархія складається з критеріїв, підкритеріїв та альтернатив. Критерії і підкритерії представляють рівні вищого порядку, альтернативи – рівень нижчого порядку.

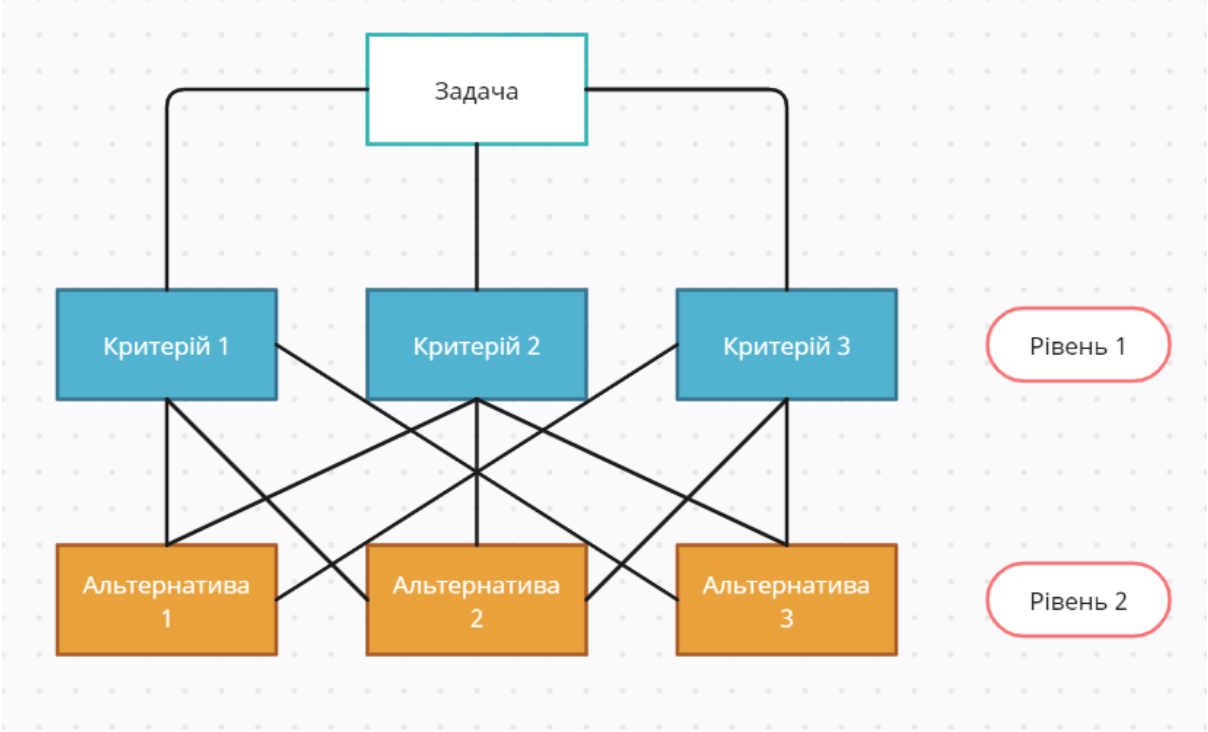


Рисунок 1.1 – Метод аналізу ієрархій

Парні порівняння: Кожен критерій та альтернатива порівнюється з іншими за допомогою шкали важливості, наприклад, від 1 до 9. Ваги визначаються на основі цих парних порівнянь.

Створення матриці парних порівнянь: Кожне парне порівняння записується у вигляді матриці, де елемент (i, j) представляє вагу, яку d критерій або альтернатива мають в порівнянні з елементом (j, i).

Обчислення ваг: Застосовуються математичні методи для обчислення ваг критеріїв та альтернатив на основі матриці парних порівнянь.

Оцінка сумарної важливості: Сумарна важливість альтернативи визначається шляхом обчислення добутку ваг кожного рівня ієрархії.

Вибір оптимальної альтернативи: Альтернатива з найвищою сумарною важливістю вважається оптимальною.

MAI дозволяє систематизувати процес прийняття рішень, розкриває вагу кожного критерію та альтернативи й допомагає зробити інформований вибір на основі математичних розрахунків. Цей підхід використовується в багатьох галузях, включаючи економіку, бізнес, інженерію тощо.

Ієрархічна структура представляє собою графічне відображення завдання у вигляді дерева, де кожен елемент, за винятком найвищого рівня, залежить від одного або більше елементів, що знаходяться на вищих рівнях. Подібні структури широко застосовуються в різних сферах життя, наприклад, в організаційній структурі компаній, системі підпорядкування працівників у магазині та інших. Ієрархічні структури використовуються для досягнення більш глибокого розуміння реальності: ми розкладаємо складні проблеми на менші складові частини. На кожному кроці цього процесу важливо зосередитися на поточному елементі. Цей аналіз дозволяє нам зрозуміти всю багатогранність досліджуваного об'єкта і виявити всі його складності.

Створення ієрархії є першим кроком у застосуванні методу AHP для прийняття рішень. Ієрархічна структура допомагає систематизувати критерії, підкритерії та альтернативи, а також визначити їх взаємозв'язки і вагомість. Зазвичай, ієрархія має трьох рівнів: критерії, підкритерії і альтернативи.

Критерії є основними факторами, за допомогою яких будуть оцінюватись альтернативи.

У процесі прийняття рішень, експерт має враховувати набір критеріїв, які виступають як характеристики, що впливають на перевагу однієї альтернативи над іншою відносно встановленої мети. Врахування цих критеріїв дозволяє експерту узгоджувати свої вирішення з конкретним

контекстом і забезпечує об'єктивність та системність процесу прийняття рішень. Покладаючись на цей набір критеріїв, експерт здатен оцінювати і порівнювати альтернативи на основі їхнього впливу на досягнення мети, що сприяє прийняттю найбільш ефективних рішень.

В контексті систем інформаційної безпеки можуть бути визначені такі критерії: надійність, конфіденційність, цілісність, доступність, ефективність та інші. Кожен критерій має відповідний ваговий коефіцієнт, який відображає його важливість відносно інших критеріїв.

Підкритерії є деталізацією кожного критерію і допомагають розкрити його сутність. Наприклад, для критерія "надійність" можуть бути визначені такі підкритерії: стійкість до атак, виявлення та усунення помилок, резервне копіювання тощо. Важливо врахувати, що підкритерії повинні бути взаємно виключними і вичерпними для кожного критерію.

Альтернативи є варіантами, які будуть порівнюватись між собою для прийняття рішень. У контексті систем інформаційної безпеки альтернативи можуть включати різні технології, програмні рішення, методи захисту, політики безпеки тощо. Кількість альтернатив може бути довільною, але важливо забезпечити повноту та вичерпність варіантів.

Після визначення критеріїв, підкритеріїв та альтернатив необхідно побудувати ієрархічну структуру. Це може бути представлено у вигляді дерева, де кожен рівень відображає критерії, підкритерії та альтернативи. З'являється батьківський вузол, який відображає критерій, а його дочірні вузли представляють підкритерії та альтернативи. Вагові коефіцієнти надаються кожному вузлу для відображення їх відносної вагомості.

Парні порівняння – це процес порівняння двох елементів за допомогою шкали, що відображає їх відносну важливість. У контексті нашої дипломної роботи, ми використовуємо парні порівняння для визначення важливості різних критеріїв і альтернатив в системах інформаційної безпеки.

1.7 Постановка задачі

Створення системи оцінки прийняття рішень для систем інформаційної безпеки має велику актуальність у забезпеченні безпеки даних, захисту від атак та забезпечення відповідності вимогам законодавства. Вона допомагає організаціям забезпечувати ефективний та цілісний підхід до безпеки інформації у постійно змінюючому цифровому середовищі.

Таким чином вирішення поставленого завдання потребує виконання наступних етапів:

1. Дослідити теоретичні основи оцінки прийняття рішення.
2. Визначеити елементи даних для системи оцінювання прийняття рішення для систем інформаційної безпеки.
3. Провести розрахунок оцінки прийняття рішення на основі методу аналізу ієрархій.
4. Виконати проєктування структури системи оцінювання прийняття рішення для систем інформаційної безпеки.
5. Виконати реалізації прототипу системи оцінювання прийняття рішення для систем інформаційної безпеки.

2 МОДЕЛЬ ОЦІНЮВАННЯ ПРИЙНЯТТЯ РІШЕННЯ ТА ВИЗНАЧЕННЯ ЕЛЕМЕНТІВ ДАНИХ ДЛЯ СИСТЕМИ ОЦІНЮВАННЯ ПРИЙНЯТТЯ РІШЕННЯ

2.1 Взаємозв’язок загроз, системи інформаційної безпеки та системи оцінки прийняття рішення

У сфері інформаційної безпеки концепція загроз, систем інформаційної безпеки та систем оцінки прийняття рішення тісно поєднанні між собою. Якщо розглядати будь-яку IT інфраструктуру із розгорнутою для неї системою інформаційної безпеки (СІБ), то загрози є чинниками, які здійснюють зловмисний вплив на IT інфраструктуру, тоді як СІБ є сукупністю рішень для протидії цьому. З іншого боку для своєчасного та найбільш оптимального прийняття рішення про застосування комплексу контрзаходів із протидії загрозам використовуються системи оцінювання прийняття рішення для систем інформаційної безпеки. Взаємозв’язок загроз, системи інформаційної безпеки та системи оцінки прийняття рішення наведено на рис. 3.1.

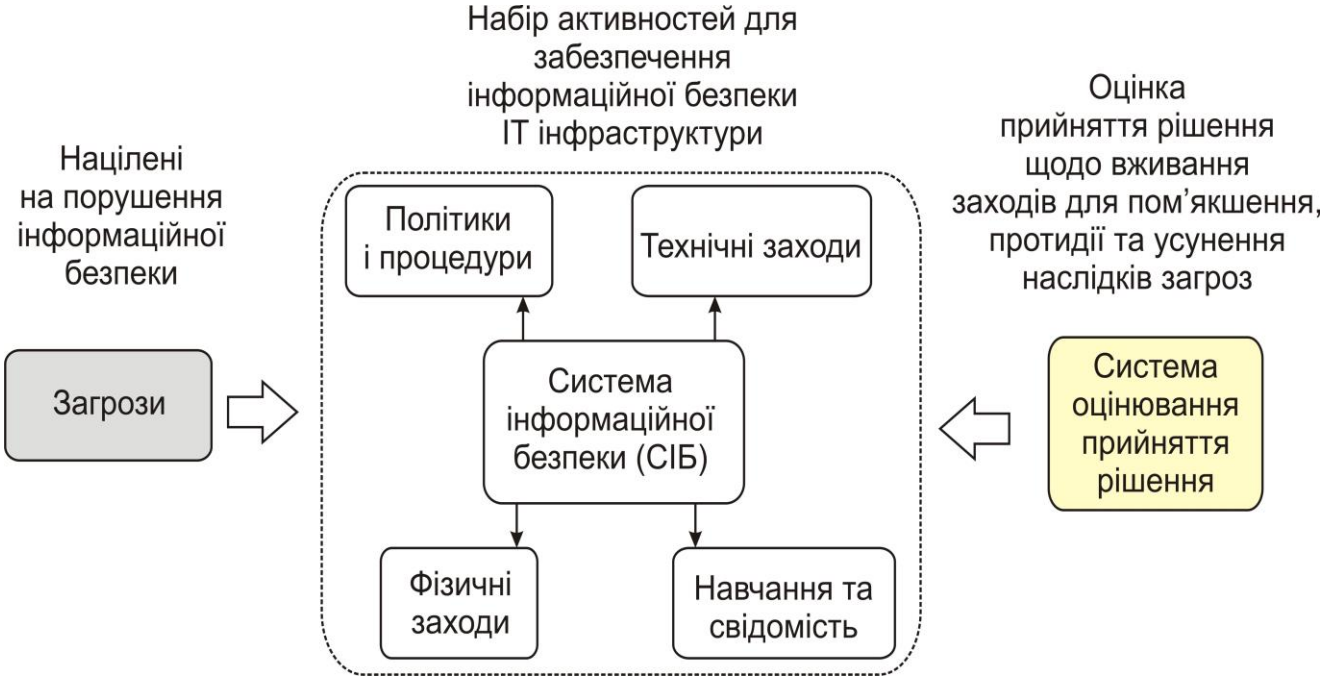


Рисунок 2.1 – Взаємозв’язок загроз, системи інформаційної безпеки та системи оцінки прийняття рішення

Визначимо систему інформаційної безпеки (СІБ) як комплекс організаційних, технічних та технологічних заходів, спрямованих на захист інформації від незаконного доступу, використання, руйнування, розголошення, зміни та перешкоджання доступу до неї. Основна мета системи інформаційної безпеки полягає в забезпеченні конфіденційності, цілісності та доступності інформації.

Система інформаційної безпеки може включати в себе такі структурні компоненти:

– Політики і процедури: Встановлення правил, стандартів та процедур, які визначають стратегію та підхід до захисту інформації. Це включає політики доступу, управління паролями, обмеження прав доступу та інші правила, які встановлюються для забезпечення безпеки інформації.

– Технічні заходи: Використання різноманітних технічних засобів для захисту інформації, таких як файрволи, системи виявлення вторгнень, антивірусне програмне забезпечення, шифрування даних, системи аутентифікації та інші технології.

– Фізичні заходи: Заходи, спрямовані на захист фізичного доступу до приміщень, комп'ютерів, серверів та інших фізичних активів, які містять інформацію. Це можуть бути системи контролю доступу, відеоспостереження, біометричні системи і т. д.

– Навчання та свідомість: Навчання співробітників щодо правил безпеки, свідомого використання технологій та виявлення потенційних загроз. Цей комплекс заходів включає проведення навчальних програм, тренінгів та свідомість персоналу щодо безпеки інформації.

Основним чинником порушення цілісності, конфіденційності та/або доступності даних для ІТ інфраструктури є загрози. Це можуть бути хакерські атаки, віруси, фішинг, соціальний інжиніринг та інші види кіберзагроз. Тому з метою протидії загрозам, аналізу ризиків, визначення пріоритетів та прийняття обґрунтованих рішень з питань безпеки інформаційної системи залучаються системи оцінки прийняття рішення. Вони оцінюють потенційні

загрози, вплив на безпеку інформації, ефективність заходів забезпечення безпеки та інші фактори для прийняття оптимальних рішень з покращення безпеки.

Таким чином, система оцінки прийняття рішень використовується для аналізування загроз, оцінки ефективності системи інформаційної безпеки та прийняття рішень щодо вдосконалення безпеки. Взаємодія між цими елементами допомагає забезпечити ефективний захист інформаційних систем від потенційних загроз.

2.2 Модель оцінювання прийняття рішень в системах інформаційної безпеки

Модель оцінювання прийняття рішень в системах інформаційної безпеки використовується для систематичного аналізу та оцінки різних аспектів безпеки інформаційної системи. Головною метою цієї моделі є надання підтримки прийняття обґрунтованих рішень, спрямованих на забезпечення високого рівня безпеки інформаційних систем.

Подамо модель оцінювання прийняття рішень в системах інформаційної безпеки на основі методу аналізу ієрархій через наступні складові (рис. 2.2):

– Цілі: Визначення основних цілей оцінювання, таких як покращення безпеки інформаційної системи, запобігання атакам, зниження ризиків, забезпечення конфіденційності тощо.

– Критерії: Встановлення критеріїв, за якими будуть оцінюватись альтернативи. Критерії повинні відображати важливі аспекти безпеки ІТ інфраструктури, зокрема такі як надійність, конфіденційність, цілісність, доступність, швидкодія та ефективність.

– Альтернативи: Визначення можливих альтернативних рішень або заходів, що можуть бути прийняті для забезпечення безпеки інформаційної системи. Це можуть бути технологічні рішення, заходи зі зміни процесів, впровадження нових систем безпеки, навчання персоналу тощо.

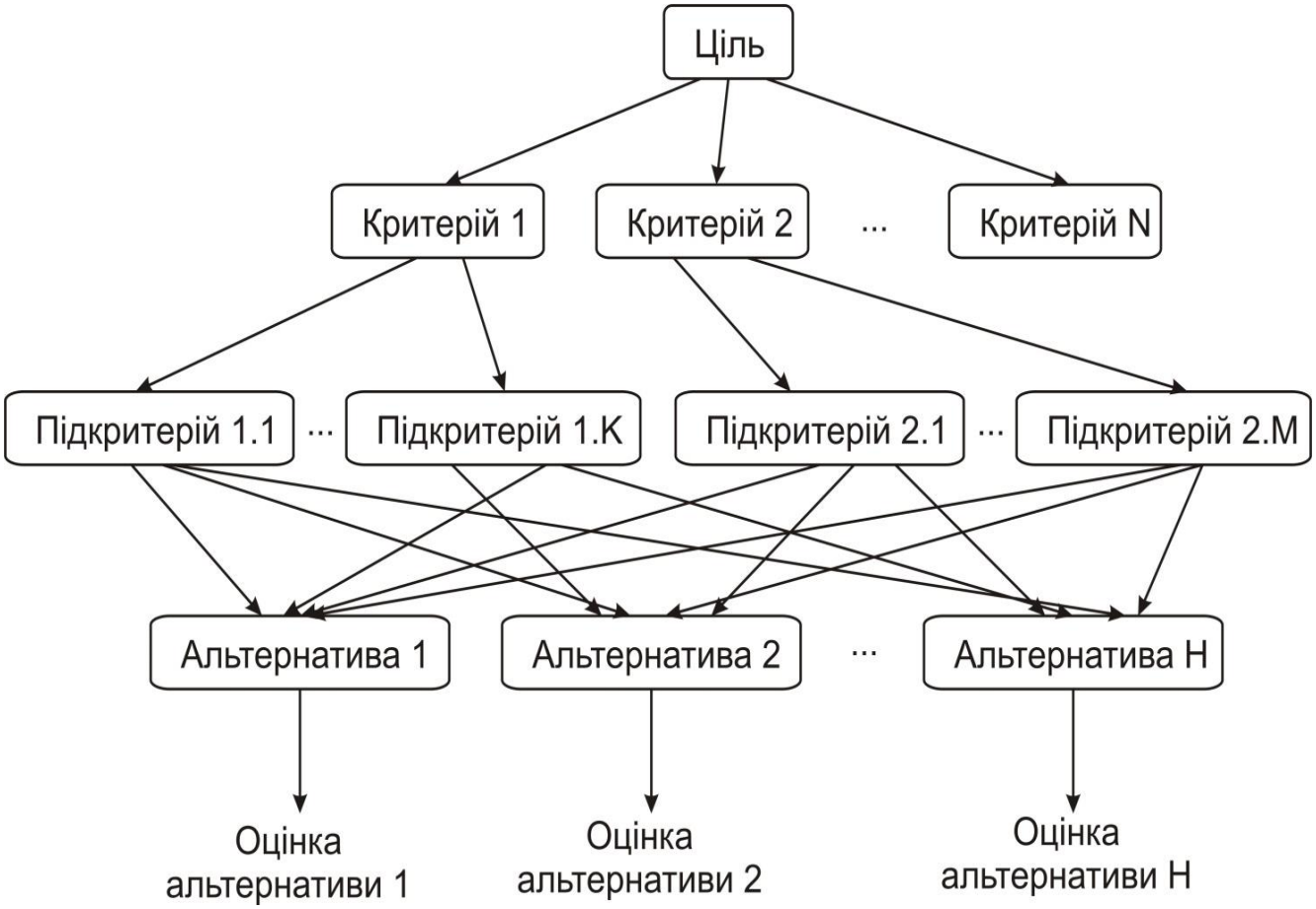


Рисунок 2.2 – Модель оцінювання прийняття рішень в системах інформаційної безпеки

– Ваги критеріїв: Встановлення ваг кожного критерію, щоб відобразити їх відносну важливість у виборі альтернативи. Це може бути зроблено шляхом проведення попарних порівнянь критеріїв і використання матриці парних порівнянь.

– Оцінювання альтернатив: Оцінювання кожної альтернативи відповідно до встановлених критеріїв. Це включає збір інформації, проведення аналізу, використання відповідних метрик та шкал оцінювання.

– Аналіз та порівняння: Порівняння оцінок альтернатив за кожним критерієм, враховуючи їх ваги. Це допомагає визначити, яка альтернатива є найбільш оптимальною з точки зору безпеки інформаційної системи.

– Вибір оптимальної альтернативи: Вибір альтернативи, яка має найвищий рівень безпеки на основі проведеного аналізу і порівняння. Ця альтернатива буде рекомендована для прийняття рішення.

Таким чино представлена модель оцінювання на основі методу аналізу ієрархій допомагає систематично аналізувати, порівнювати та вибирати оптимальні альтернативи для забезпечення високого рівня безпеки інформаційних систем.

2.3 Визначення елементів даних для системи оцінювання прийняття рішення

Відповідно до запропонованої моделі оцінки прийняття рішення розглянемо набір даних, що використовуватиметься у системі оцінки прийняття рішення для систем інформаційної безпеки. В якості прикладу будуть розглянуті цілі, критерії та альтернативи для категорії «Технічні заходи».

Розглянемо набір даних у вигляді цілі, набору критеріїв та альтернатив.

Ціль: «Забезпеченні безпеки інформаційної системи від атаки відмова в обслуговуванні»

1. Функціональні критерії (K1):

– Ефективність виявлення DoS-атак: Оцінка здатності альтернативи вчасно виявляти DoS-атаки і реагувати на них. (K1_1).

– Ефективність блокування DoS-атак: Оцінка здатності альтернативи блокувати небажані атакуючі пакети та запобігати відмовам в обслуговуванні. K1_2).

– Відновлення послуг: Оцінка здатності альтернативи швидко відновлювати нормальну роботу системи після DoS-атаки (K1_3).

– Мінімальний вплив на легітимних користувачів: Оцінка здатності альтернативи забезпечити нормальний доступ до системи для легітимних користувачів навіть під час DoS-атак (K1_4).

2. Технологічні критерії (K2):

– Масштабованість: Оцінка здатності альтернативи масштабуватися для захисту від різних рівнів інтенсивності DoS-атак та забезпечення стабільної роботи системи (K2_1).

– Швидкодія: Оцінка швидкості реакції альтернативи на DoS-атаки та відновлення нормального функціонування системи (K2_2).

– Надійність: Оцінка надійності альтернативи у виявленні та блокуванні DoS-атак (K2_3).

– Сумісність: Оцінка сумісності альтернативи з існуючою інфраструктурою та іншими захисними заходами (K2_4).

3. Економічні показники: (K3):

– Вартість впровадження: Оцінка вартості реалізації та впровадження альтернативи (K3_1).

– Вартість підтримки: Оцінка вартості підтримки та обслуговування альтернативи на протязі її експлуатації (K3_2).

– ROI (повернення інвестицій): Оцінка потенційного виграшу від інвестицій в альтернативу з точки зору уникнення можливих втрат, збільшення продуктивності або покращення репутації (K3_3).

Тоді альтернативи для забезпечення безпеки інформаційної системи при атаках відмова в обслуговуванні можуть включати:

– Використання мережевих брандмауерів та систем фільтрації пакетів (A1).

– Встановлення систем виявлення і запобігання вторгнень (IDS/IPS) (A2).

– Використання CDN (Content Delivery Network) (A3).

– Використання облікових записів з обмеженими правами та контролем доступу (A4).

Сформуємо набір даних для цілі «Забезпечення безпеки інформаційної системи від атаки Man in the Middle». Тоді критерії визначимо наступним чином:

1. Функціональні критерії:

– Здатність виявлення атаки Man in the Middle: Оцінка здатності альтернативи вчасно виявляти атаки Man in the Middle та реагувати на них.

– Здатність блокування атаки Man in the Middle: Оцінка здатності альтернативи блокувати небажані атакуючі з'єднання та запобігати атакам Man in the Middle.

– Забезпечення конфіденційності даних: Оцінка здатності альтернативи забезпечити конфіденційність передачі даних та уникнення перехоплення інформації атакуючими.

2. Технологічні критерії:

– Відповідність протоколам безпеки: Оцінка використання альтернативою відповідних протоколів та механізмів шифрування для захисту з'єднань та даних від атак Man in the Middle.

– Підтримка сертифікатів та ідентифікація: Оцінка здатності альтернативи підтримувати сертифікати та засоби ідентифікації для перевірки легітимності комунікаційних сторін.

– Захист від перехоплення: Оцінка здатності альтернативи запобігати перехопленню трафіку та викриттю конфіденційної інформації.

3. Економічні показники:

– Вартість впровадження: Оцінка вартості реалізації та впровадження альтернативи для захисту від атак Man in the Middle.

– Вартість підтримки: Оцінка вартості підтримки та обслуговування альтернативи на протязі її експлуатації.

– ROI (повернення інвестицій): Оцінка потенційного виграшу від інвестицій в альтернативу з точки зору уникнення можливих втрат, збільшення продуктивності або покращення репутації.

Альтернативи для забезпечення безпеки інформаційної системи від атак Man in the Middle можуть включати:

– Використання протоколів шифрування, таких як SSL/TLS (A1).

– Встановлення системи двофакторної аутентифікації (A2).

– Використання віртуальних приватних мереж (VPN) (A3).

– Використання системи моніторингу трафіку та виявлення аномалій (A4).

Сформуємо ціль для забезпечення безпеки інформаційної системи від шкідливого програмного забезпечення. Далі здійснимо визначення критеріїв:

1. Функціональні критерії:

– Ефективність виявлення шкідливого програмного забезпечення: Оцінка здатності альтернативи вчасно виявляти шкідливе програмне забезпечення та інші загрози безпеці.

– Ефективність блокування шкідливого програмного забезпечення: Оцінка здатності альтернативи блокувати і запобігати виконанню шкідливого програмного забезпечення в системі.

– Відновлення та відновлення послуг: Оцінка здатності альтернативи швидко відновлювати нормальну роботу системи та виправляти наслідки атак шкідливого програмного забезпечення.

– Мінімальний вплив на продуктивність: Оцінка здатності альтернативи забезпечувати нормальну продуктивність та функціональність системи навіть під час виявлення та блокування шкідливого програмного забезпечення.

2. Технологічні критерії:

– Ефективність сканування та виявлення: Оцінка швидкості та точності альтернативи в скануванні системи на наявність шкідливого програмного забезпечення.

– Швидкодія: Оцінка швидкості реакції альтернативи на нові загрози та шкідливе програмне забезпечення.

– Надійність: Оцінка надійності альтернативи у виявленні та блокуванні шкідливого програмного забезпечення.

– Сумісність: Оцінка сумісності альтернативи з існуючою інфраструктурою та іншими заходами безпеки.

3. Економічні показники:

– Вартість впровадження: Оцінка вартості реалізації та впровадження альтернативи.

– Вартість підтримки: Оцінка вартості підтримки та обслуговування альтернативи протягом її експлуатації.

– ROI (повернення інвестицій): Оцінка потенційного виграшу від інвестицій в альтернативу з точки зору уникнення можливих втрат, збільшення продуктивності або покращення репутації.

Альтернативи для забезпечення безпеки інформаційної системи від шкідливого програмного забезпечення можуть включати:

– Використання антивірусного програмного забезпечення (A1).

– Використання системи виявлення і запобігання вторгнень (IDS/IPS) (A2).

– Впровадження системи білого списку для контролю програмного забезпечення (A3).

– Регулярні оновлення та патчі для оперативних систем та програмного забезпечення (A4).

Сфомуємо набір данних для цілі «Забезпечення безпеки інформаційної системи від фішингових атак»

1. Функціональні критерії:

– Ефективність виявлення фішингових атак: Оцінка здатності альтернативи вчасно виявляти фішингові атаки та інші форми соціального шахрайства.

– Ефективність блокування фішингових атак: Оцінка здатності альтернативи блокувати фішингові веб-сторінки, шкідливі посилання та інші методи атаки фішингом.

– Захист інформації користувачів: Оцінка здатності альтернативи забезпечувати конфіденційність інформації користувачів та запобігати витоку особистих даних через фішингові атаки.

– Підвищення свідомості користувачів: Оцінка здатності альтернативи надавати навчання та освіту користувачам щодо виявлення та запобігання фішинговим атакам.

2. Технологічні критерії:

– Ефективність виявлення шкідливих посилань: Оцінка здатності альтернативи виявляти шкідливі посилання в електронних повідомленнях, веб-сторінках та інших джерелах.

– Перевірка достовірності веб-сайтів: Оцінка здатності альтернативи перевіряти достовірність веб-сайтів та ідентифікувати фішингові сторінки.

– Захист від перехоплення даних: Оцінка здатності альтернативи захищати дані користувачів від перехоплення під час фішингових атак.

– Механізми анти-фішингу: Оцінка наявності та ефективності механізмів анти-фішингу, таких як попередження перед відвідуванням потенційно шкідливих веб-сторінок або ідентифікація підроблених веб-сайтів.

– Аналіз поведінки: Оцінка здатності альтернативи аналізувати поведінку користувачів та виявляти незвичайні дії, що можуть вказувати на фішингову атаку.

– Перевірка безпеки електронної пошти: Оцінка наявності та ефективності механізмів перевірки безпеки електронної пошти для виявлення та блокування фішингових повідомлень.

3. Економічні показники:

– Вартість впровадження: Оцінка вартості реалізації та впровадження альтернативи для захисту від фішингових атак.

– Вартість підтримки: Оцінка вартості підтримки та обслуговування альтернативи протягом її експлуатації.

– ROI (повернення інвестицій): Оцінка потенційного виграшу від інвестицій в альтернативу з точки зору уникнення можливих втрат, збільшення продуктивності або покращення репутації.

Альтернативи для забезпечення безпеки інформаційної системи від фішингових атак можуть включати:

– Використання анти-фішингових фільтрів та блокування шкідливих посилань (A1)

– Впровадження системи навчання та свідомості користувачів щодо фішингу (A2)

– Використання двофакторної аутентифікації та сильних паролів (A3)

– Застосування механізмів аналізу поведінки для виявлення фішингових атак (A4)

Сформуємо ціль "Забезпечення безпеки інформаційної системи від атак прослуховування каналу зв’язку". Тоді критеріями для системи оцінювання прийняття рішення будуть:

1. Функціональні критерії:

– Ефективність виявлення атак прослуховування: Оцінка здатності альтернативи вчасно виявляти атаки прослуховування каналу зв'язку та інші загрози безпеки.

– Ефективність блокування атак: Оцінка здатності альтернативи блокувати та запобігати виконанню атак прослуховування каналу зв'язку в системі.

– Відновлення та відновлення послуг: Оцінка здатності альтернативи швидко відновлювати нормальну роботу системи та виправляти наслідки атак прослуховування каналу зв'язку.

– Мінімальний вплив на продуктивність: Оцінка здатності альтернативи забезпечувати нормальну продуктивність та функціональність системи навіть під час застосування заходів проти атак прослуховування.

2. Технологічні критерії:

– Ефективність використання шифрування: Оцінка ефективності використання шифрування для захисту каналу зв'язку від прослуховування.

– Використання захищених протоколів: Оцінка використання протоколів, що забезпечують безпеку передачі даних через канал зв'язку.

– Використання фізичних заходів безпеки: Оцінка використання фізичних методів, таких як контроль доступу та захищені комунікаційні засоби, для запобігання атакам прослуховування.

– Забезпечення інтеграції з існуючою інфраструктурою: Оцінка здатності альтернативи інтегруватися з існуючими системами та інфраструктурою зв'язку.

3. Економічні показники:

– Вартість впровадження: Оцінка вартості реалізації та впровадження альтернативи для запобігання атакам прослуховування каналу зв'язку.

– Вартість підтримки: Оцінка вартості підтримки та обслуговування альтернативи протягом її експлуатації.

– ROI (повернення інвестицій): Оцінка потенційного виграшу від інвестицій у альтернативу з точки зору уникнення можливих втрат, збільшення продуктивності або покращення репутації.

Альтернативи для забезпечення безпеки інформаційної системи від атак прослуховування каналу зв'язку можуть включати:

– Використання шифрування з криптографічними протоколами (A1).

– Використання віртуальних приватних мереж (VPN) (A2).

– Використання захищених комунікаційних протоколів, таких як SSL / TLS (A3).

– Фізичний контроль доступу до приміщень з комунікаційними засобами (A4).

Таким чином сформовано приклади основних елементів даних для системи оцінювання прийняття рішення. В подальшому цілі, критерії та альтернативи можна доповнювати та змінювати.

2.4 Розрахунок оцінки прийняття рішення на основі методу аналізу ієрархій

Виконаємо оцінювання прийняття рішення на основі методу аналізу ієрархій для цілі «Забезпеченні безпеки інформаційної системи від атаки відмова в обслуговуванні» (критерії та набір альтернатив зазначені у розділі 2.3.).

Для початку визначимо вагу кожної групи вибраних критеріїв. Для цього виконаємо попарне їх порівняння із використанням наступної шкали оцінювання:

1 – критерії рівнозначні.

3 – один критерій має дещо більшу значимість ніж інший.

5 – один критерій має значно більшу роль ніж інший.

7 – один критерій має безперечно більшу значимість ніж інший, підтверджується не тільки експертним шляхом, але і на практиці.

9 – один критерій має більшу роль ніж інший.

Наприклад якщо пріоритет критерію А над Б дорівнює 7, то пріоритет критерію Б над А складатиме 1/7.

Нехай для заданої цілі забезпечення безпеки інформаційної системи при атакх відмова в обслуговуванні в межах системи інформаційної безпеки важливим аспектом є мінімізація економічних витрат (наприклад підприємство має обмежений бюджет), тому при попарному порівнянні пар критеріїв «Економічна критерії» – «Функціональні критерії» та «Економічна критерії» – «Технологічні критерії» виставимо 5 балів (та 1/5 відповідно). При оцінці пари «Функціональні критерії» – «Технологічні критерії» виставимо оцінку 7 балів, оскільки функціональність при забезпечення високого рівня безпеки інформаційної системи при атаках відмова в обслуговуванні є дуже важливим критерієм. Результати попарного порівняння критеріїв наведено у таблиці 3.1.

Таблиця 3.1 – Результати попарного порівняння критеріїв

Вага критерію в ієрархії	Економічні показники	Функціональні критерії	Технологічні критерії
Економічні показники	1	5	5
Функціональні критерії	0,2	1	7
Технологічні критерії	0,2	0,143	1

Потім необхідно оцінити вагу критерію серед усіх, що розглядаються в групі. Іншими словами це означає, що необхідно визначити вектор пріоритетів по матрицях, тобто обчислити головний власний вектор, який після нормалізації стає вектором пріоритетів.

Виконаємо нормалізацію стовпця. Для цього розділю значення елементів у вибраному рядку на суму значень елементів у відповідних стовпцях. Потім виконаємо сумування отримані значення і поділю результат на кількість елементів у рядку.

Наприклад розрахуємо за описаним вище методом вагу критерію «Економічні показники» у групі критеріїв «Економічні показники», «Функціональні критерії» та «Технологічні критерії»:

$$\frac{\frac{1}{1+0,2+0,2}+\frac{5}{5+1+0,143}+\frac{5}{5+7+1}}{3}=63,76\% \qquad (1.1)$$

Результати оцінки кожного критерію представлені в таблиці 3.2

Таблиця 3.2 – Ваги критеріїв у групі

Критерій	Вага критерію в групі,%
Економічні показники	63,76
Функціональні критерії	28,14
Технологічні критерії	8,10

На наступному кроці слід визначити вагу кожного із підкритеріїв у своїй групі критеріїв. Розглянемо детальніше процес визначення ваги підкритеріїв у групі «Технологічні критерії» – масштабованість, швидкодія, надійність, сумісність.

Нехай в рамках даної системи інформаційної безпеки підкритерій мастшабованості буде менш важливим у порівнянні із критеріями швидкодія, надійсність та сумісність. Причому останні два критерії нехай матимуть ще більшу вагу (по 5).

Результати попараного порівняння критеріїв у підгрупі «Технологічні критерії» наведено у таблиці 3.3.

Таблиця 3.3 – Результати попараного порівняння критеріїв у підгрупі «Технологічні критерії»

Вага критеріїв в ієрархії	Масштабованість	Швидкодія	Надійність	Сумісність
Масштабованість	1	3	5	5
Швидкодія	0,33	1	3	3
Надійність	0,2	0,33	1	3
Сумісність	0,2	0,33	0,33	1

Слід відзначити, що при формуванні матриці попарного порівняння потрібно враховувати, що чим більше вона вийде (більше критеріїв), тим складніше буде зробити попарне порівняння критеріїв, тому рекомендується обирати не більше 10-15 найважливіших критеріїв. В даному випадку ця умова

виконана. Ваги підкритеріїв у групі «Технологічні критерії» наведено у таблиці 3.4.

Таблиця 3.4 – Ваги підкритеріїв у групі «Технологічні критерії»

Критерій	Вага критерію в групі,%
Масштабованість	0,55
Швидкодія	0,24
Надійність	0,14
Сумісність	0,07

Наступник кроком розглянемо процес визначення ваги підкритеріїв у групі «Функціональні критерії» – ефективність виявлення, ефективність блокування, відновлення послуг та мінімальний вплив на легітимних користувачів. Результати попараного порівняння критеріїв у підгрупі «Функціональні критерії» наведено у таблиці 3.5.

Таблиця 3.5 – Результати попараного порівняння критеріїв у підгрупі «Функціональні критерії»

Вага критеріїв в ієрархії	Ефективність виявлення	Ефективність блокування	Відновлення послуг	Мінімальний вплив на легітимних користувачів
Ефективність виявлення	1	1	7	5
Ефективність блокування	1	1	3	5
Відновлення послуг	0,14	0,33	1	3
Мінімальний	0,2	0,2	0,33	1

вплив на легітимних користувачів				

Ваги підкритеріїв у групі «Функціональні критерії» подано у таблиці 3.6. Цілком очевидно, що найбільшу вагу матимуть критерії, що стосуються процесу безпосереднього виявлення та блокування шкідливої активності.

Таблиця 3.6 – Ваги підкритеріїв у групі «Функціональні критерії»

Критерій	Вага критерію в групі,%
Ефективність виявлення	0,45
Ефективність блокування	0,36
Відновлення послуг	0,12
Мінімальний вплив на легітимних користувачів	0,07

В результаті виконання цього етапу було визначено вагу кожного критерію у відповідній групі. Проте слід відзначити, що власну вагу має кожна група критеріїв. Таким чином, при формуванні остаточної оцінки альтернативи буде враховуватися вага критерію з урахуванням ваги його групи, тобто підсумкова вага критерію дорівнюватиме добутку ваги групи на вагу критерію у групі. Наприклад, підсумкова вага критерію «Масштабованість», що входить до групи критеріїв «Технологічні критерії», складатиме (8,1*0,55)/100 = 0,04%.

На наступному етапі виконаємо перевірку виконання критеріїв. Для цього застосуємо градацію за ступенем досяжності результатів тестів, при цьому наведені нижче бали служитимуть коефіцієнтом для результуючої оцінки. Це дозволить оцінити проміжні значення. Для цього скористаємось школою, що подана у таблиці 3.7.

Таблиця 3.7 – Шкала оцінювання відповідності

Бал	Оцінка
0	Повністю не відповідає
3	Майже не відповідає
5	Відповідає на достатньому рівні
7	Майже відповідає
10	Повністю відповідає

Після внесення отриманих результатів до порівняльної таблиці отримується підсумковий бал для кожного критерію та рішення обраної альтернативи. Цей бал дорівнюватиме добутку підсумкової ваги критерію та балу оцінки. Наприклад одне із порівнюваних рішень за групою критеріїв «Функціональні критерії» подано у таблиці 3.8.

Таблиця 3.8 – Результат оцінки функціональних критеріїв для альтернативи 1

Функціональні критерії	Результуюча вага критерію	Альтернатива 1	
		Оцінка	Результуючий бал
Ефективність виявлення	0,13	7	0,91
Ефективність блокування	0,10	3	0,3
Відновлення послуг	0,03	7	0,21
Мінімальний вплив на легітимних користувачів	0,01	3	0,03
Підсумковий бал оцінки за групою критеріїв:			1,45

Таким чином в результаті результуючі значення оцінок для всіх альтернатив наведено у таблиці 3.9.

Таблиця 3.9 – Результати оцінювання альтернатив

Критерій	Альтернатива 1	Альтернатива 2	Альтернатива 3	Альтернатива 4
Економічні показники	6,48	6,12	6,78	6,64
Функціональні критерії	1,45	1,50	1,45	1,65
Технологічні критерії	0,52	0,58	0,48	0,54

Таким чином було проведено оцінювання прийняття рішення на основі методу аналізу ієрархій для цілі «Забезпеченні безпеки інформаційної системи від атаки відмова в обслуговуванні». Сформовані оцінки дозволяються кількісно визначити відносну важливість або пріоритетність кожного елементу відносно інших.

2.5 Висновки до розділу 2

Таким чином визначено взаємозв’язок загроз, системи інформаційної безпеки та системи оцінки прийняття рішення. Основним призначенням системи оцінки прийняття рішень є аналіз загроз, оцінка ефективності системи інформаційної безпеки та прийняття рішень щодо вдосконалення безпеки. Взаємодія між цими елементами допомагає забезпечити ефективний захист інформаційних систем від потенційних загроз. Розглянуто модель оцінювання прийняття рішень в системах інформаційної безпеки на основі методу аналізу ієрархій. Сформовані множини даних для системи оцінювання прийняття рішення. Проведено розрахунок оцінки прийняття рішення на основі методу аналізу ієрархій на прикладі цілі «Забезпеченні безпеки інформаційної системи від атаки відмова в обслуговуванні».

3 СТРУКТУРА, АЛГОРИТМИ ТА РЕЗУЛЬТАТИ РОБОТИ СИСТЕМИ ОЦІНЮВАННЯ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Структура системи оцінювання прийняття рішень для систем інформаційної безпеки

Основним завдання проектованої системи оцінювання прийняття рішень для систем інформаційної безпеки є формування кількісних оцінок для альтернатив, що представлені у формі множини заходів із протидії та усуненні наслідків зловмисної активності. Представимо структуру системи оцінювання прийняття рішень для систем інформаційної безпеки у вигляді двох підсистем: підсистеми оцінювання прийняття рішення та підсистеми визначення зловмисної активності. Структуру системи оцінювання прийняття рішень для систем інформаційної безпеки наведено на рис. 3.1.

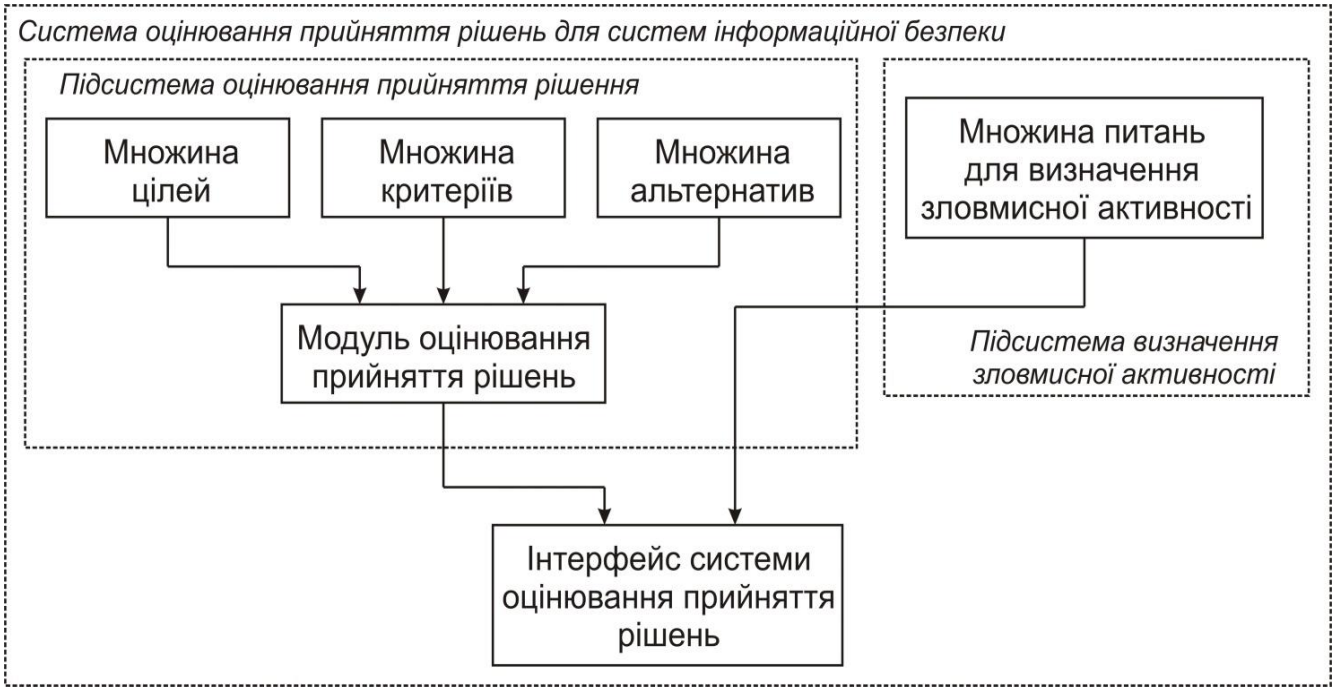


Рисунок 3.1 – Структура системи оцінювання прийняття рішень для систем інформаційної безпеки

Підсистема оцінювання прийняття рішення є основною складовою, що дозволяє оцінити заходи із протидії та усуненні наслідків зловмисної активності. Ця підсистема складається із таких складових:

– Множина цілей. Представлена у формі набору визначених цілей, що відповідають видам зловмисної активності. Всі цілі згруповані відповідно до складових системи інформаційної безпеки таких як політики та процедури, технічних заходів, фізичних заходів, а також заходів по навчанню. Таким чином в рамках кожної групи визначено набір цілей, що надаються користувачу для оцінювання заходів по їх протидії або усуненні наслідків.

– Множина критеріїв. Представлена у формі набору критеріїв для кожної цілі та визначає набір ознак за якими можна оцінити заходи по протидії або усуненні наслідків зловмисної активності.

– Множина альтернатив. Складає набір заходів, що дозволяють пом’якшити, протидіяти або виявити зловмисну активність. Кожній цілі відповідає власна множина альтернатив, проте у частині випадків вони можуть перетинатись (наприклад альтернатива, що представлена у вигляді використання правил обмеження вхідного трафіку для мережевого екрану буде спільною для декількох цілей – при атаці відмова в обслуговуванні, атаці Man in the Middle, тощо).

– Модуль оцінювання прийняття рішень. Представляє ядро системи оцінювання прийняття рішень для систем інформаційної безпеки, що реалізує метод аналізу ієрархій.

У випадку коли користувачу системи не вдається однозначно ідентифікувати зловмисну активність передбачено підсистему визначення зловмисної активності. Ця підсистема складається із множини питань для визначення зловмисної активності, давши відповідь на які, користувачу буде запропоновано набір цілей, яким притаманна спостережувана поведінка.

Результати роботи обох підсистем відображають за допомогою інтерфейсу системи оцінювання прийняття рішень.

3.2 Алгоритми роботи системи оцінювання прийняття рішень для систем інформаційної безпеки

В основі запропонованої системи оцінювання прийняття рішень для систем інформаційної безпеки закладено метод аналізу ієрархій. Це є структурований метод організації, що використовується аналізу складних рішень у різних галузях. Даний метод включає виконання наступних кроків (рис. 3.2):

1. Визначення цілі прийняття рішення. Робота методу починається із формулювання чіткої ціль (мети), яку слід досягти в системі інформаційної безпеки. Наприклад, це можу бути забезпечення високого рівня безпеки даних або мінімізація ризиків втрати конфіденційності.

2. Створення ієрархії критеріїв. Наступним кроком є визначення основних критеріїв та підкритеріїв, які впливають на досягнення цілі безпеки інформаційної системи. Високорівневими критеріями можуть бути наприклад, доступність, конфіденційність та цілісність. Ранжування критеріїв та підкритеріїв здійснюється на основі вагових коефіцієнтів від 1 до 9, де значення 1 означає, що критерій немає значення, а значення 9 – найважливіший критерій.

3. Створення ієрархії альтернатив. На цьому кроці здійснюється визначення можливих альтернатив, які можуть бути використані для досягнення цілі забезпечення безпеки інформаційної системи. Наприклад, це можуть бути різні технології шифрування, системи перевірки доступу або мережеві файрволи. Далі слід оцінити кожну альтернативу відносно кожного критерію, використовуючи числову шкалу. Наприклад, від 1 до 9, де 1 означає найнижчий рівень задоволення критерію, а 9 – найвищий рівень.

4. Розрахунок ваг критеріїв. Використовуючи методи математичних обчислень, здійснюється розрахунок ваг критеріїв на основі їх відносної важливості, яка була зазначена на кроці 2. Розрахунок ваг критеріїв можна здійснити наприклад за методом Сааті.

5. Розрахунок ваг альтернатив. Використовуючи отримані ваги критеріїв і оцінки альтернатив, здійснюється розрахунок ваг альтернатив для кожного

критерію. Для цього виконується множення ваги критерію на оцінку альтернативи та сумування цих значення для кожного критерію.

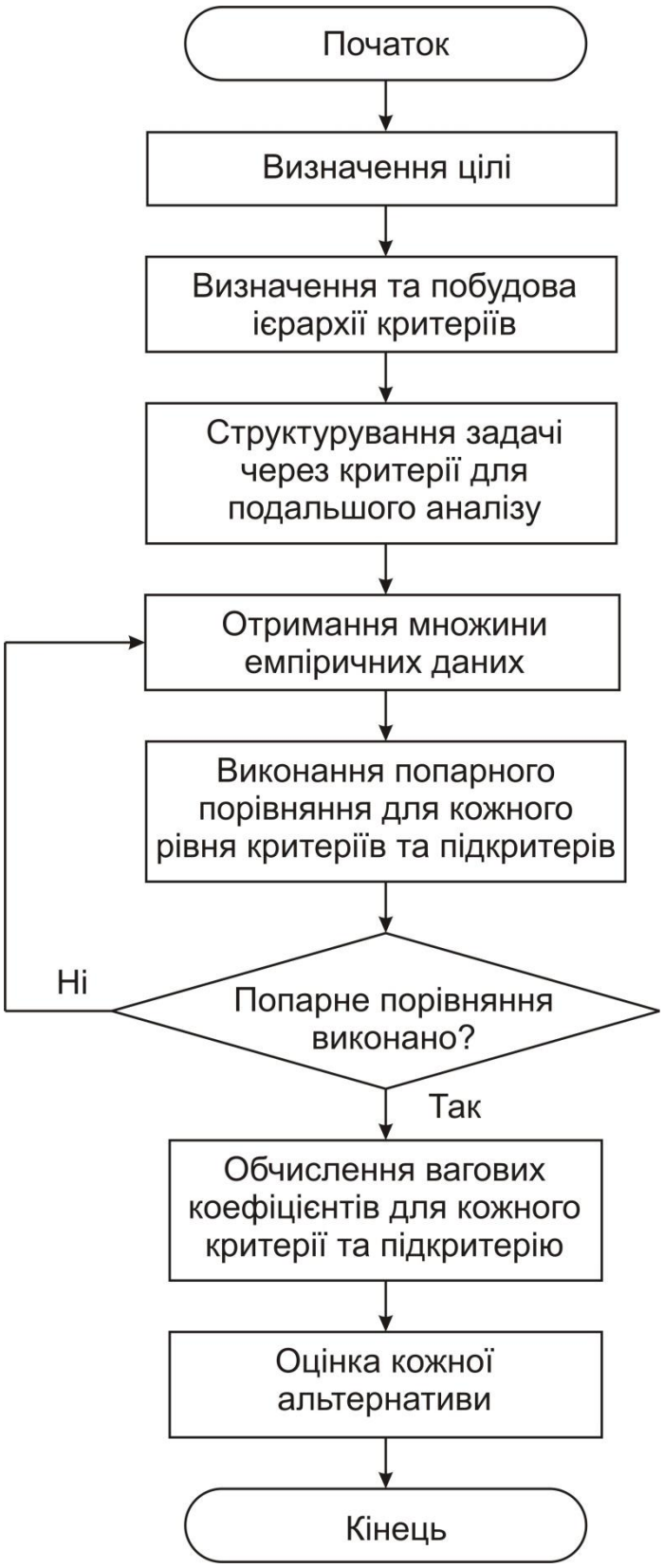


Рисунок 3.2 – Блок-схема роботи методу аналізу ієрархій

6. Обчислення загальних оцінок альтернатив. Обчислення загальних оцінок альтернатив, складаючи ваги альтернатив для кожного критерію. Це дозволить порівняти альтернативи та визначити найбільш оптимальну з точки зору безпеки інформаційної системи.

Таким чином в результаті буде сформовано кількісну оцінку для кожного критерію. Слід відзначити, що даний метод є ітеративним процесом, і результати можуть бути змінені або покращені на основі нової інформації або ревізії критеріїв та альтернатив.

В результаті загальний алгоритм роботи системи оцінювання прийняття рішень для систем інформаційної безпеки, що заснована на методі MAI, наведено на рис. 3.3.

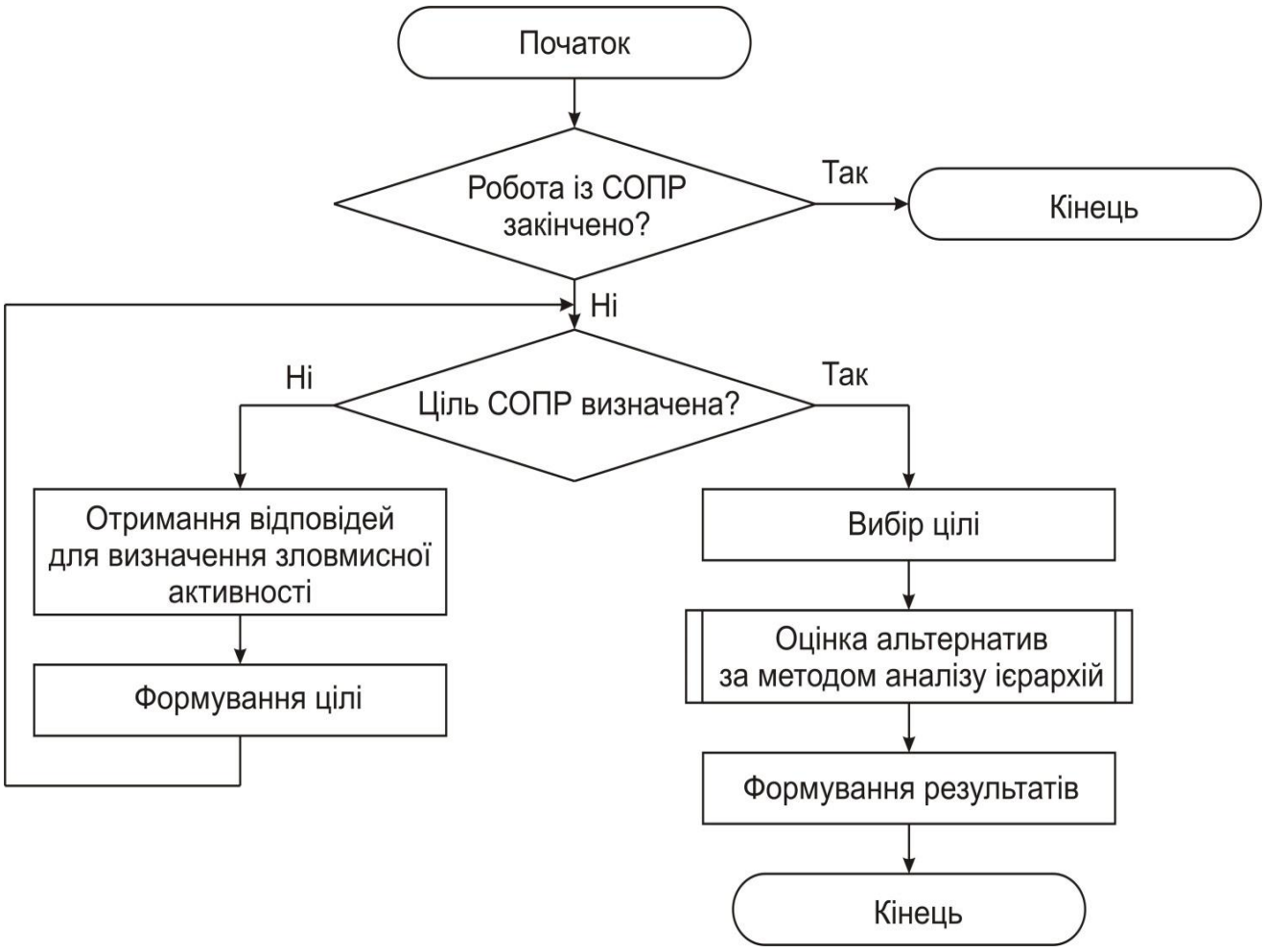


Рисунок 3.3 – Блок-схема роботи методу аналізу ієрархій

3.3 Модель вимог до системи оцінювання прийняття рішень для систем інформаційної безпеки

Для наглядності представлення роботи запропонованої системи оцінювання прийняття рішення для систем інформаційної безпеки використаємо UML (Unified Modeling Language) – стандартну мову моделювання, яка використовується розробниками ПЗ для візуалізації процесів та роботи систем. Використання UML-діаграм дозволяє візуалізувати структуру розробленої СОПР, оскільки це графічний спосіб відображення її структури та поведінки, а також це допомагає зрозуміти систему в цілому та легко виявити взаємозв'язки між її компонентами.

Представимо модель вимог до запропонованої системи у вигляді UML-діаграми варіантів використання (рис. 3.4). У представлені системиі оцінювання прийняття рішення можна виділити два актори: користувача та адміністратора системи. Основними функціями користувача системи оцінювання прийняття рішення є безпосередньо оцінка прийняття рішення стосовно заходів забезпечення безпеки для IT інфраструктури, визначення зловмисної активності (у випадку, якщо не вдається одразу визначити ціль) та перегляд інформації про систему.

З іншого боку адміністратор системи оцінки прийняття рішеня має можливість по зміні елементів даних системи (створення, читання, видалення, редагування – CRUD), зокрема цілей, критеріїв та альтернатив. Також адміністратор має можливість змінити набір питань для визначення зловмисної активності, тобто створити, змінити або видалити. UML діаграму варіантів використання для запропонованої системи оцінювання прийняття рішення наведено на рис. 3.4.

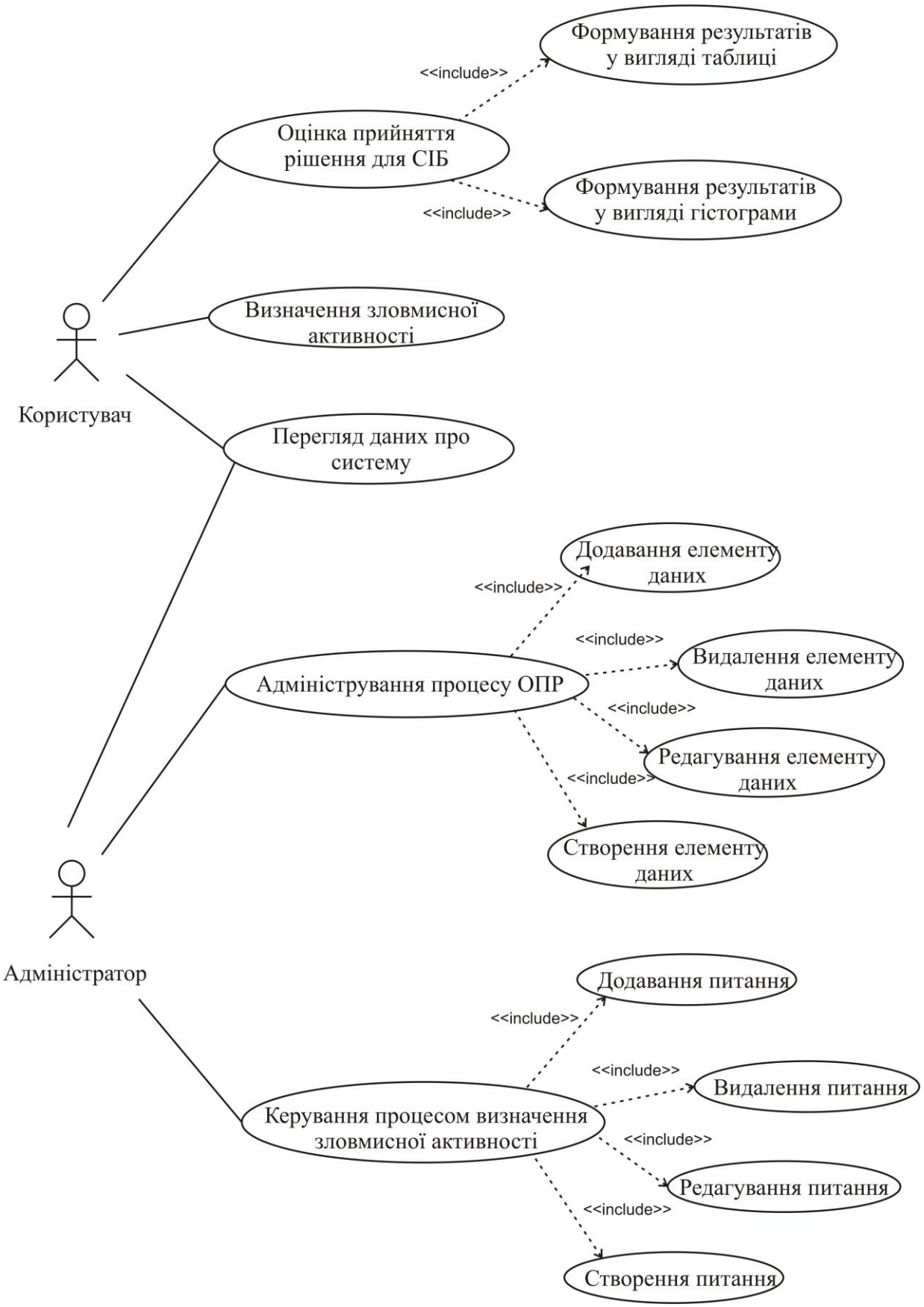


Рисунок 3.4 – UML діаграма варіантів використання для запропонованої системи оцінювання прийняття рішення

3.4 Вибір засобів реалізації

Для реалізації прототипу системи оцінювання прийняття рішень для систем інформаційної безпеки було використано Windows Forms. Windows Forms в C++/CLI – це технологія, яка дозволяє розробляти графічні користувацькі інтерфейси (GUI) для програм на основі платформи Windows, використовуючи мову програмування C++/CLI. Основним призначенням Windows Forms є створення віконних додатків з інтерактивними елементами керування, такими як кнопки, тексти, списки, таблиці та інші.

Windows Forms містить різноманітні елементи керування, які можна додати до форм: елементи керування, які відображають текстові поля, кнопки, розкривні поля, перемикачі та навіть веб-сторінки. Якщо існуючий елемент керування не відповідає вашим потребам, Windows Forms також підтримує створення власних власних елементів керування за допомогою класу UserControl.

Основні особливості роботи з WinForms у C++/CLI:

– Створення форм: Windows Forms дозволяє легко створювати графічний інтерфейс за допомогою різних контейнерів та елементів керування, які можна розташовувати на формі.

– Події: Ви можете прив'язувати обробники подій до елементів керування, таких як натискання кнопки або введення тексту. Це дозволяє реагувати на дії користувача та виконувати певні дії відповідно.

– Керування властивостями елементів керування: Ви можете змінювати властивості елементів керування, такі як розміри, положення, колір, шрифт та інші, за допомогою програмного коду.

– Графічний рендеринг: Windows Forms використовує систему графічного рендерингу GDI+ для відображення елементів керування на екрані. Це дозволяє створювати приємний, зручний та професійний графічний інтерфейс настільного застосунку.

– Підтримка клавіатури та миші: Windows Forms дозволяє обробляти взаємодію з клавіатурою та мишею, включаючи натискання клавіш, переміщення миші та кліки.

– Робота з базами даних: Windows Forms надає підтримку для з'єднання з базами даних та виконання запитів, дозволяючи розробникам створювати програми з можливістю виконання основних операцій із базами даних – створення, видалення, редагування та додавання (CRUD).

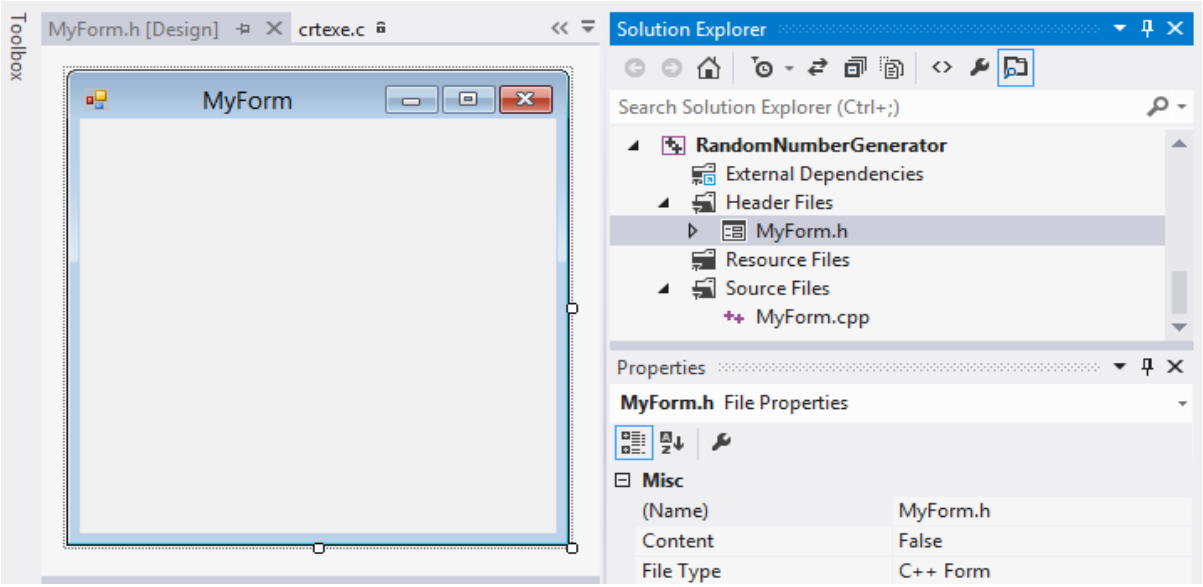


Рисунок 3.5 – Середовище розробки Win Forms у Visual Studio

3.5 Результати роботи системи оцінювання прийняття рішення системи інформаційної безпеки

З метою демонстрації роботи системи оцінювання прийняття рішення для систем інформаційної безпеки було виконано реалізацію її прототипу у вигляді програмного забезпечення за допомогою Win Forms. Інтерфейсні вікна розробленого прототипу системи оцінювання прийняття рішення для систем інформаційної безпеки представлено на рис. 3.5-3.12.

Для початку роботи із розробленої СОПР слід вибрати складову системи інформаційної безпеки для якої потрібно буде оцінити прийняття рішення (рис. 3.6). На вибір користувачу СОПР надається чотири складові:

– Політики і процедури.

– Технічні заходи.

– Фізичні заходи.

– Навчання та свідомість.

Фактично ці чотири складові є чотирма наборами асетів у системі інформаційної безпеки. Наприклад складова технічні заходи включає в себе набір цілей, що проявляються у забезпеченні безпеки інформаційної системи від конкретного типу загрози, зокрема:

– Атака відмова в обслуговуванні.

– Атака Man in the Middle.

– Фішингові атаки.

– Атака прослуховування.

– Атака «грубої сили».

– Зловмисне програмне забезпечення.

Інтерфейсне вікно вибору цілі, що представляє собою конкретний тип зловмисної активності наведено на рис. 3.7.

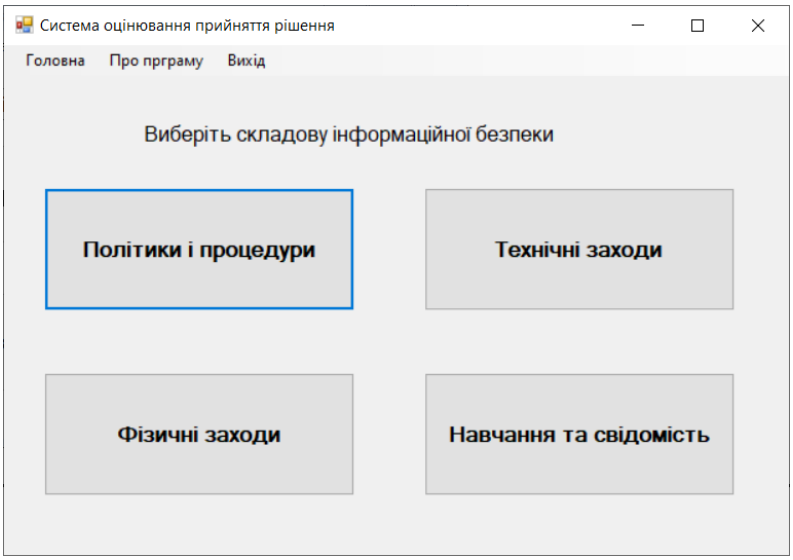


Рисунок 3.6 – Головне інтерфейсне вікно системи оцінювання прийняття рішення системи інформаційної безпеки

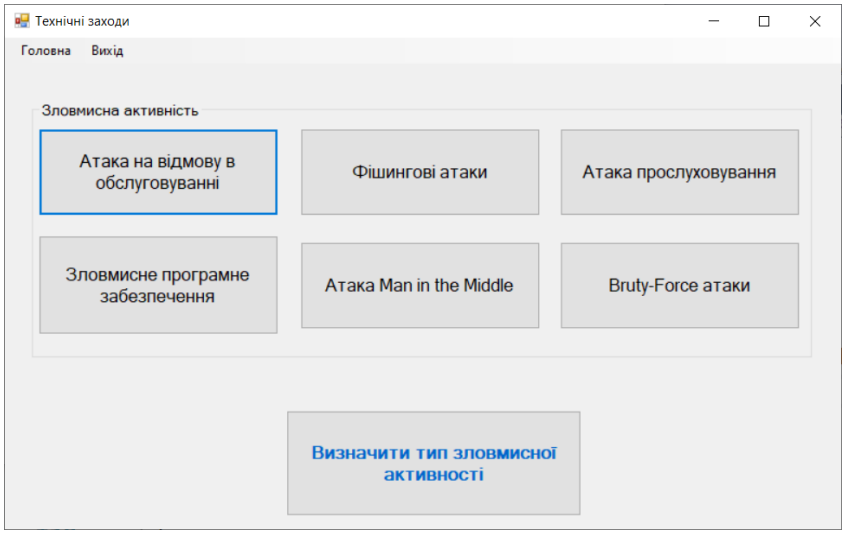


Рисунок 3.7 – Інтерфейсне вікно вибору зловмисної активності

Після вибору цілі, користувачу пропонується заповнити матрицю важливості критеріїв, виконавши попарне порівняння кожної із них. На рис. 3.8 наведено інтерфейсне вікно попарного порівняння критеріїв для забезпечення цілі «Забезпеченні безпеки інформаційної системи від атаки відмова в обслуговуванні». Користувачу пропонується виставляти оцінки:1, 3, 5, 7, 9. Слід відзначити, якщо користувач оцінивши наприклад критерії «Економічні показники» і «Функціональні критерії» виставляє оцінку 5, то у комірці, що відповідає за перетин «Функціональні критерії» та «Економічні показники» буде автоматично встановлено значення 1/5.

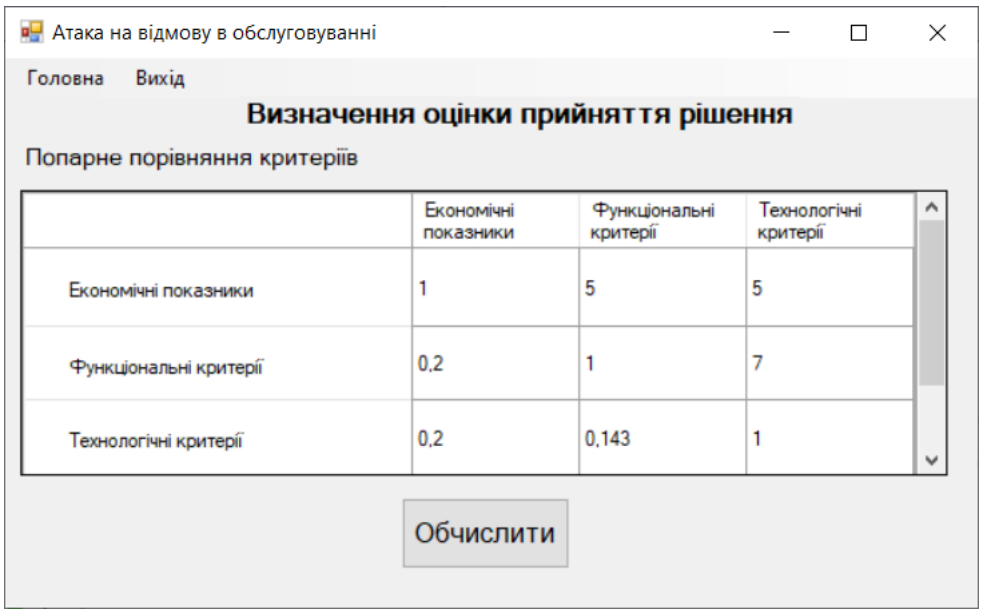


Рисунок 3.8 – Інтерфейсне вікно попарного порівняння критеріїв

Після заповнення матриці та натискання кнопки «Обчислити» система оцінювання прийняття рішення здійснює обчислення вагових коефіцієнтів для кожного критерію у цій групі. Інтерфейсне вікно результатів попарного порівняння критеріїв наведено на рис. 3.9. Якщо така оцінка не задовольняє користувача є можливість повернутись назад та змінити значення у матриці попарного порівняння критеріїв. Після цього відбудеться повторне обчислення вагових коефіцієнтів.

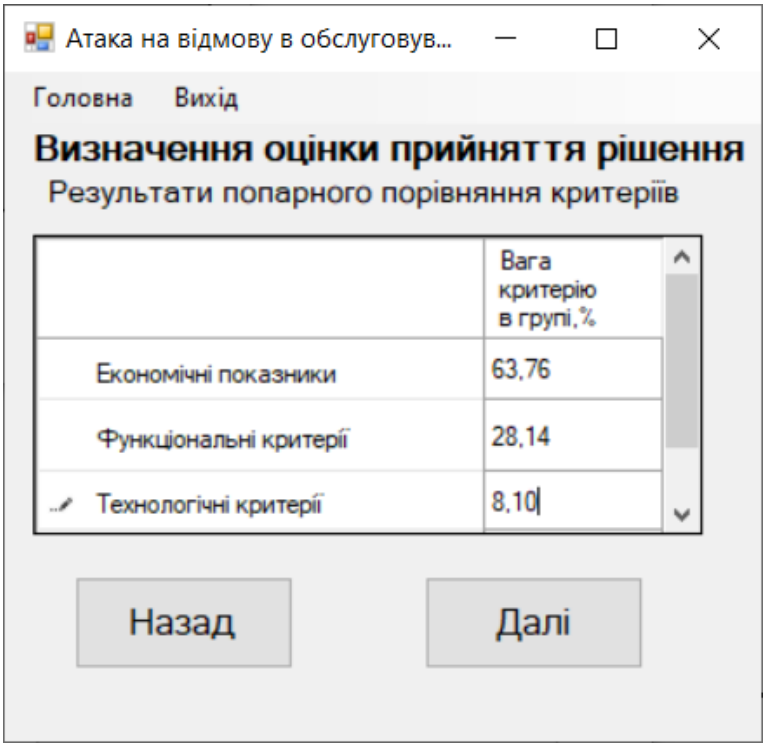


Рисунок 3.9 – Інтерфейсне вікно результатів попарного порівняння критеріїв

Якщо користувач погоджується із сформованими ваговими коефіцієнтами для кожного із критерію, здійснюється аналогічна процедура для підкритеріїв у кожній групі. Наприклад інтерфейсне вікно попарного порівняння підкритерії у групі «Технологічні критерії» наведено на рис. 3.10.

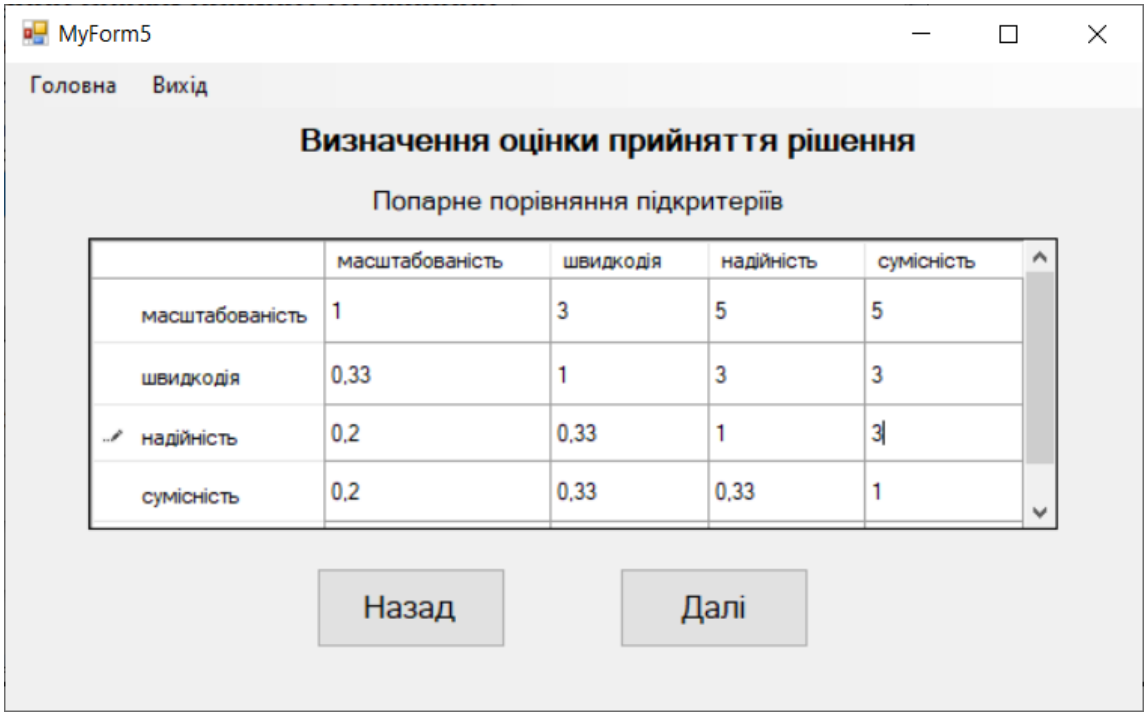


Рисунок 3.10 – Інтерфейсне вікно попарного порівняння під критерії у групі «Технологічні критерії»

Таким чином після обрахунку всіх вагових коефіцієнтів для критеріїв та під критеріїв здійснюється формування остаточних оцінок для кожної із альтернатив. Наприклад, на рис. 3.11 наведено інтерфейсне вікно результатів оцінювання для цілі «Забезпеченні безпеки інформаційної системи від атаки відмова в обслуговуванні». Як видно із результатів СОПР формує числові оцінки для кожної із числових альтернатив:

– Використання мережевих брандмауерів та систем фільтрації пакетів (Альтернатива 1).

– Встановлення систем виявлення і запобігання вторгнень (IDS/IPS) (Альтернатива 2).

– Використання CDN (Content Delivery Network) (Альтернатива 3).

– Використання облікових записів з обмеженими правами та контролем доступу (Альтернатива 4).

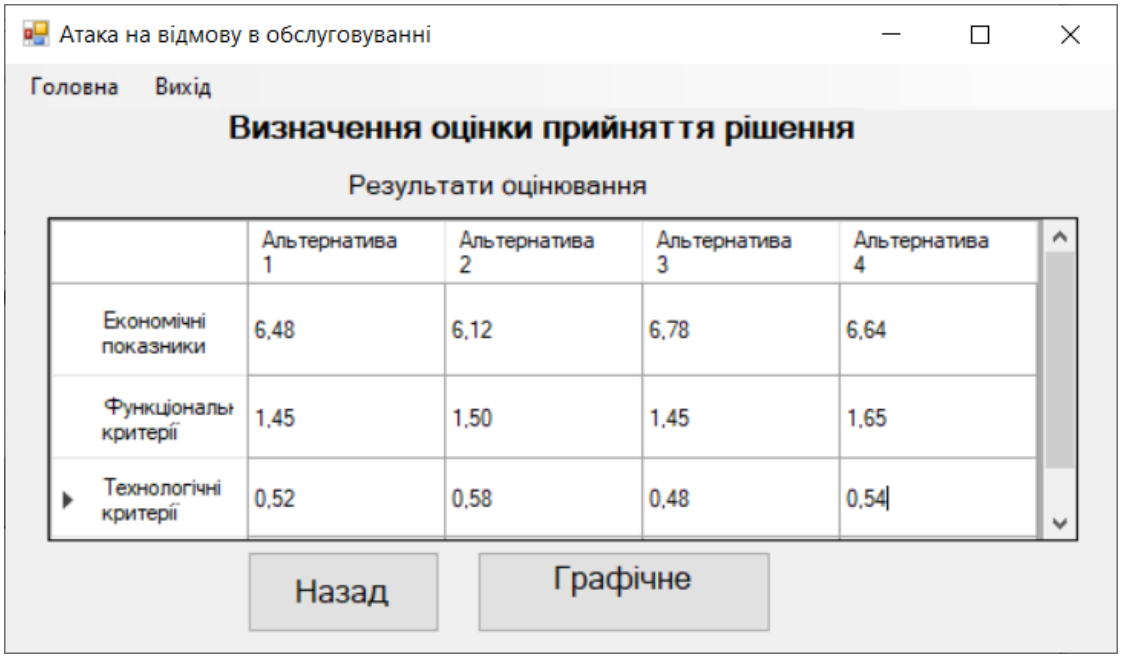


Рисунок 3.11 – Інтерфейсне вікно результатів оцінювання

Також є можливість графічного відображення результатів оцінювання (у вигляді гістограми). Інтерфейсне вікно результатів оцінювання, що подані у формі гістограми подано на рис. 3.12.

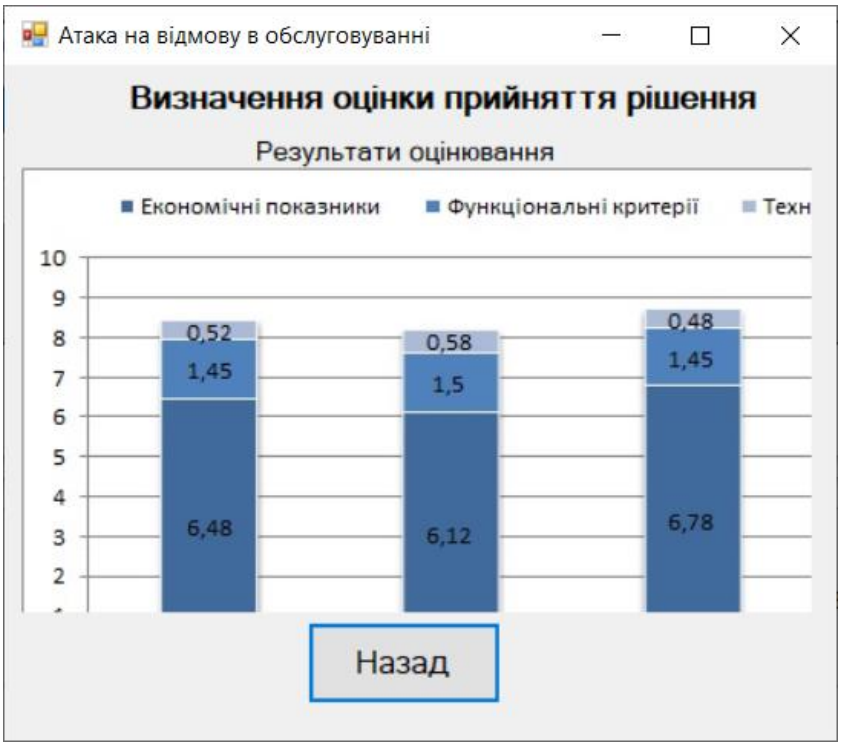


Рисунок 3.12 – Інтерфейсне вікно результатів оцінювання, що подані у формі гістограми

У випадку, якщо користувач не може обрати ціль, є можливість пройти послідовність тестових питань. На рис. 3.13 наведено інтерфейсне вікно визначення зловмисної активності.

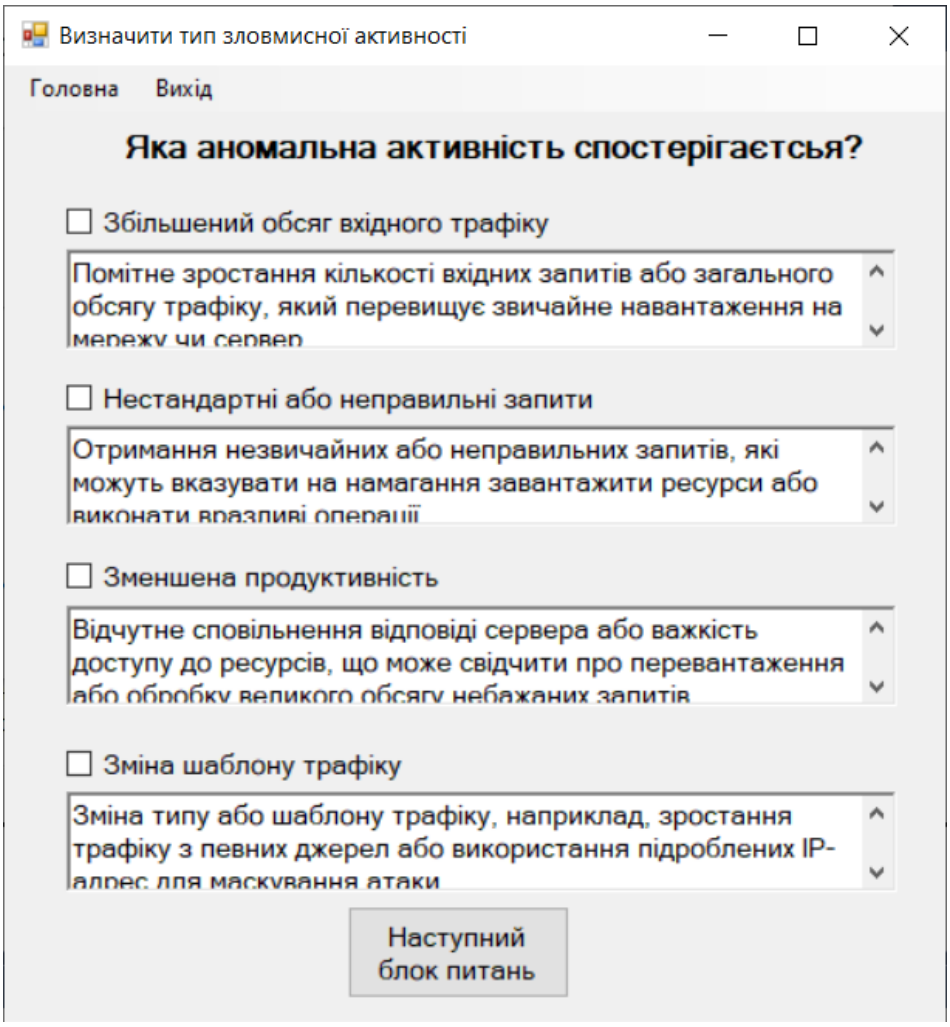


Рисунок 3.13 – Інтерфейсне вікно визначення зловмисної активності

Таким чином реалізований прототип системи оцінювання прийняття рішення дозволяє сформувати кількісну оцінку для заходів, які можна використати для пом’якшення, протидії та усунення наслідків впливу атак на ІТ інфраструктуру. Особливістю даної системи оцінювання підтримки рішення є наявність функції визначення зловмисної активності, у випадку, якщо користувач не може одразу ідентифікувати загрозу.

3.6 Висновки за розділом 3

Представлено структуру системи оцінювання прийняття рішень для систем інформаційної безпеки у вигляді двох підсистем. Запропонована СОПР складається із двох підсистем: підсистеми оцінювання прийняття рішення та підсистеми визначення зловмисної активності. Наведено алгоритми роботи системи оцінювання прийняття рішень для систем інформаційної безпеки (алгоритми роботи методу аналізу ієрархій та роботи всієї СОПР). Здійснено вибір засобів реалізації та виконано реалізацію прототипу системи оцінювання прийняття рішення системи інформаційної безпеки. Реалізований прототип системи оцінювання прийняття рішення дозволяє сформувати кількісну оцінку для заходів, які можна використати для пом’якшення, протидії та усунення наслідків впливу атак на IT інфраструктуру. Особливістю даної системи оцінювання підтримки рішення є наявність функції визначення зловмисної активності, у випадку, якщо користувач не може одразу ідентифікувати загрозу.

ВИСНОВКИ

З метою ефективного забезпечення безпеки інформаційних систем, потрібна система оцінювання прийняття рішень, яка допомагає визначити оптимальні заходи та стратегії для запобігання загрозам і реагування на них. Система оцінювання прийняття рішень в системах інформаційної безпеки є інструментом, який дозволяє аналізувати, визначати та порівнювати альтернативи щодо їхньої ефективності, надійності, вартості та інших критеріїв.

Основна мета системи оцінювання прийняття рішень полягає в тому, щоб забезпечити оптимальне використання ресурсів та ефективний захист інформаційних систем від потенційних загроз. Це досягається шляхом визначення конкретних цілей безпеки, встановлення критеріїв оцінки та вибору оптимальних альтернатив.

Використання системи оцінювання прийняття рішень в системах інформаційної безпеки дозволяє підвищити ефективність заходів безпеки, зменшити ризики й економічні затрати та забезпечити надійний захист інформаційних ресурсів ІТ інфраструктури. Це стає особливо важливим у контексті зростаючої кількості кіберзагроз та постійно змінюваного середовища інформаційних технологій.

В результаті виконання даної кваліфікаційної роботи було запропоновано прототип системи оцінювання прийняття рішення для систем інформаційної безпеки.

У першому розділі розглянуто концепцію прийняття рішень у системах оцінки прийняття рішень, сутність людино-машинних систем оцінювання прийняття рішень, а також класифікацію СОПР. Сформульовано постановку завдання.

У другому розділі визначено взаємозв’язок загроз, системи інформаційної безпеки та системи оцінки прийняття рішення. Основним призначенням системи оцінки прийняття рішень є аналіз загроз, оцінка ефективності системи

інформаційної безпеки та прийняття рішень щодо вдосконалення безпеки. Взаємодія між цими елементами допомагає забезпечити ефективний захист інформаційних систем від потенційних загроз. Розглянуто модель оцінювання прийняття рішень в системах інформаційної безпеки на основі методу аналізу ієрархій. Сформовані множини даних для системи оцінювання прийняття рішення. Проведено розрахунок оцінки прийняття рішення на основі методу аналізу ієрархій на прикладі цілі «Забезпеченні безпеки інформаційної системи від атаки відмова в обслуговуванні».

У третьому розділі запропонована структура системи оцінювання прийняття рішень для систем інформаційної безпеки складається з двох підсистем: підсистеми оцінювання прийняття рішень і підсистеми визначення зловмисної активності. Подано алгоритми роботи системи оцінювання прийняття рішень для систем інформаційної безпеки, зокрема алгоритми роботи методу аналізу ієрархій та всієї системи оцінювання прийняття рішень. Вибрано засоби реалізації і реалізовано прототип системи оцінювання прийняття рішень для системи інформаційної безпеки. Прототип дозволяє надати кількісну оцінку для заходів, яку можна використовувати для послаблення, протидії та усунення наслідків атак на IT-інфраструктуру. Особливістю цієї системи оцінювання прийняття рішень є наявність функції визначення зловмисної активності, яка активується у випадку, коли користувач не може одразу ідентифікувати загрозу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Daniati E., Firliana R., Wardani A. S. and Zarkasi A. C., Evaluation Framework for Decision Making Based On Sentiment Analysis in Social Media, *2021 International Conference on Advanced Mechatronics, Intelligent Manufacture and Industrial Automation (ICAMIMIA)*, Surabaya, Indonesia, 2021, 47-51.

2. Zaburko J., Szulżyk-Cieplak J., Information security risk assessment using the AHP method, *IOP Conference Series Materials Science and Engineering*, 710(1):012036

3. Agustinia I. and Sari P. K., Measument of Information Security Awareness Among Social Media Path User in Indonesis, *Asia Pacific Institute of Advanced Research*, 2, 2, 2016, 114-123.

4. Petrova V. A cybersecurity risk assessment, *International Scientific Journal Industry 4.0*., 1, 2021, 37-40.

5. Bhol S. and Mohanty J. R. Cyber Security Metrics Evaluation Using Multi-criteria Decision-Making Approach, *Smart Intelligent Computing and Applications*, 2020, 665-675.

6. Muhirwe J. and White N., Cyberscurity Awareness and Practice of Next Generation Corperate Technology Users, *Issues in Information Systems*, 17, 2016 183-192.

7. Thaduri A., Aljumaili M., Kour R. and Karim R., Cybersecurity for eMaintenance in railway infrastructure: risks and consequences, *Int J Syst Assur Eng Manag*, 10, 2, 2019, 149-159.

8. Stefanescu D. C. and Papoi A., New Threats to The National Security of States Cyber Threat, *Scientific Journal of Silesian University of Technology. Series Transport*, 107, 2020, 177-182.

9. McCormac A., Calic D., Butavicius M., Parsons K., Zwaans T. and Pattinson M., A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses, *Australasian Journal of Information Systems*, 2017, 21.

10. Ungkap P. and Daengsi T., Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand, *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, Chiangrai, Thailand, 2022, 1359-1362.

11. Sum R., Risk Prioritisation Using The Analytic Hierarchy Process. *Innovation and Analytics Conference and Exhibition (IACE 2015)*, AIP Conf. Proc. 1691

12. Muhammad N., N. Fuzzy DEMATEL method for identifying LMS evaluation criteria. 9th International Conference on Theory and application of Soft Computing, *Computing with Words and Perception*, 2017.

13. Adebiaye R. and Ajani T., Information Technology Usage: Quantitative Analysis of Smartphone Security Awareness and Pratice Among Undergraduate Student in The United States, *International Journal of Engineering Technologies and Management Research*, 5, 3, 2018, 270-284.

14. Jing H., Wang J., Chen C.L., Detection of DDoS Attack within Industrial IoT Devices Based on Clustering and Graph Structure Features, *Security and Communication Networks* 2022 (2022), 1401683.

15. Serrano B., Fernando J., Song W., et al, A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Engineering Science and Technology, an International Journal*. 31, 2021.

16. Pacheco L. D. S., Mobility and Cloud Management in Wireless Heterrogeneous 5G Networks, *Dissertation Institute of Technology Federal University of Para*, 2020.

17. Stocker F., Villar E. G., Roglio K. D. D. and Abib G., Dismissal: Important Criteria in Managerial Decision-Making, *RAE-Revista de Administração de Empresas (Journal of Business Management)*, 58, 2. 2018. 116-129.

18. Kafke J., Viana T., Call Me Maybe: Using Dynamic Protocol Switching to Mitigate Denial-of-Service Attacks on VoIP Systems, *Network* 2022, 2(4), 545-567.

19. Ali B. Internet of Things based Smart Homes: Security Risk Assessment and Recommendations, Master's Thesis, Luleå University of Technology, Department of Computer Science, *Electrical and Space Engineering*, 2016, 98 p.

20. Bugeja J., Jacobsson A. and Davidsson P., On Privacy and Security Challenges in Smart Connected Homes, *Proceedings of the 2016 European Intelligence and Security Informatics Conference (EISIC)*, IEEE, Uppsala, Sweden, 2016, 172-175.

21. Kovacevic A., Putnik N. and Toskovic O., Factors Related to Cybersecurity Behavior, *IEEE Access*, 8, 2020, 23-57.

22. Sadik M., Akkari N. and Aldabbagh G., QoS/QoE Based Handover Decision in Multi-Tier LTE Networks, *Int J Digit Inform Wirel Commun*, 8, 2, 2018, 133-138.

23. Fatokun F. B., Hamid S., Norman A. and Fatokun J. O., The Impact of Age Gender and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities, *Journal of Physics*, 1339, 2019, 1-13.

24. Zwilling M., Klien G., Lesjak D., Wiechetek L., Cetin F. and Basim H. N., Cybersecurity Awareness Knowledge and Behavior: A Comparative Study, *Journal of Computer Information Systems*, 2020, 1-16.

25. Ahmed N., Kulsum U., Azad I. B., Momtaz Z., Haque M. E. and Rahman M. S., Demographic Factors of Cybersecurity Awareness in Bangladesh, *IEEE Region 10 Humanitarian Technology Conference*, 2017.

26. Adebiaye R. and Ajani T., Information Technology Usage: Quantitative Analysis of Smartphone Security Awareness and Pratice Among Undergraduate Student in The United States, *International Journal of Engineering Technologies and Management Research*, 5, 3, 2018, 270-284.

27. Li L., Xu L., He W., Chen Y. and Chen H., Cybersecurity Awareness and Its Impact on Employee's Behavior, *10th International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS)*, 2016, 103-111.

28. Anwar M., He W., Ash I., Yuan X., Li L. and Xu L., Gender Difference and Employees' Cybersecurity Behaviors, *Computers in Human Behavior*, 69, 2017, 437-443, 2017.

29. Venter I. M., Blignaut R. J., Renaud K. and Venter M. A., Cybersecurity education is as essential as the three R's, *Heliyon*, 5, 2019, 1-8, Nov 2019.

30. Garba A. A., Siraj M., Othman S. H. and Musa M. A., A Study on Cybersecurity Awareness Among Students in Yobe State University Nigeria: A Quantitative Approach, *International Journal on Emerging Technologies*, 5, 2020, 41-49.

31. Daengsi T., Pornpongtechavanich P. and Wuttidittachotti P., Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks, *Education and Information Technologies*, 27, 2022 4729–4752.

32. Albladi S. M., and Weir G. R. S. User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1) 2018, 1-24.

33. Aoyama T., Nakano T., Koshijima I., Hashimoto Y., and Watanabe K. On the complexity of cybersecurity exercises proportional to preparedness. Journal of Disaster Research, 12(5), 2017, 1081-1090.

34. Bahnsen A. C., Bohorquez E. C., Villegas S., Vargas, J., and Gonzalez F. A. Classifying phishing URLs using recurrent neural networks. *ECrime Researchers Summit, ECrime*, 2017, 1-8

35. Baillon A., De Bruin J., Emirmahmutoglu A., Van De Veer E., and Van Dijk B. Informing, simulating experience, or both: A field experiment on phishing risks. *PLoS ONE*, *14*(12), 1–15

36. Aleroud A. and Zhou L. Phishing environments, techniques, and countermeasures: A survey. *Computers and Security*, *68*, 2017, 160-196

37. Anwar M., He W., Ash I., Yuan X., Li L., and Xu L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 2017, 437-443.

38. Bin Othman Mustafa M. S., Nomani Kabir M., Ernawan F., & Jing W.. An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks. *2019 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2019,* 10-14.

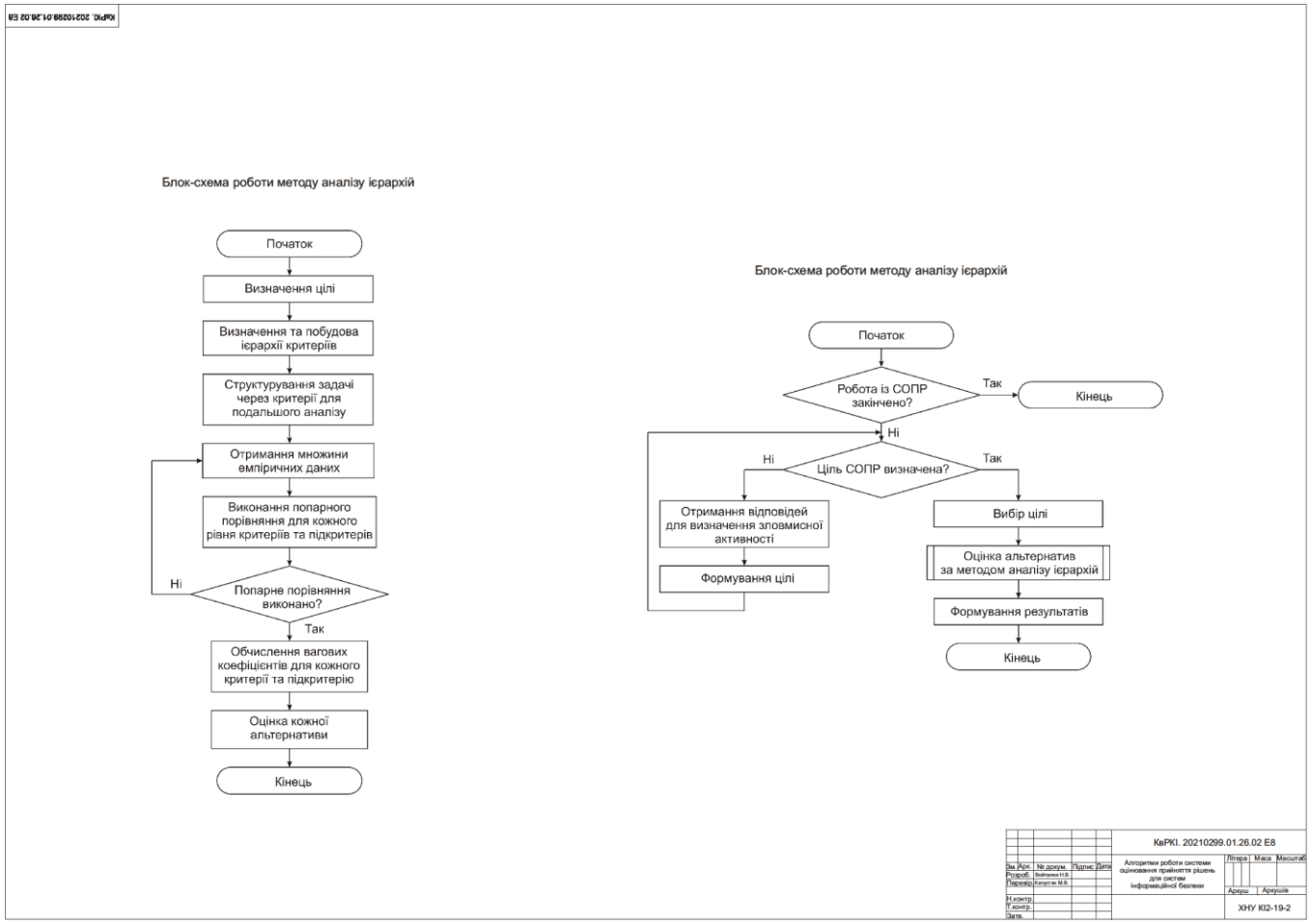
39. Bordonaba-Juste M. V, Lucia-Palacios L., & Pérez-López R. Generational differences in valuing usefulness, privacy and security negative experiences for paying for cloud services. *Information Systems and E-Business Management, 18*(1), 2020, 35-60.

40. Carella A., Kotsoev M., & Truta T. M. Impact of security awareness training on phishing click-through rates. *Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017*, 4458–4466.

ДОДАТОК А

(обов’язковий)

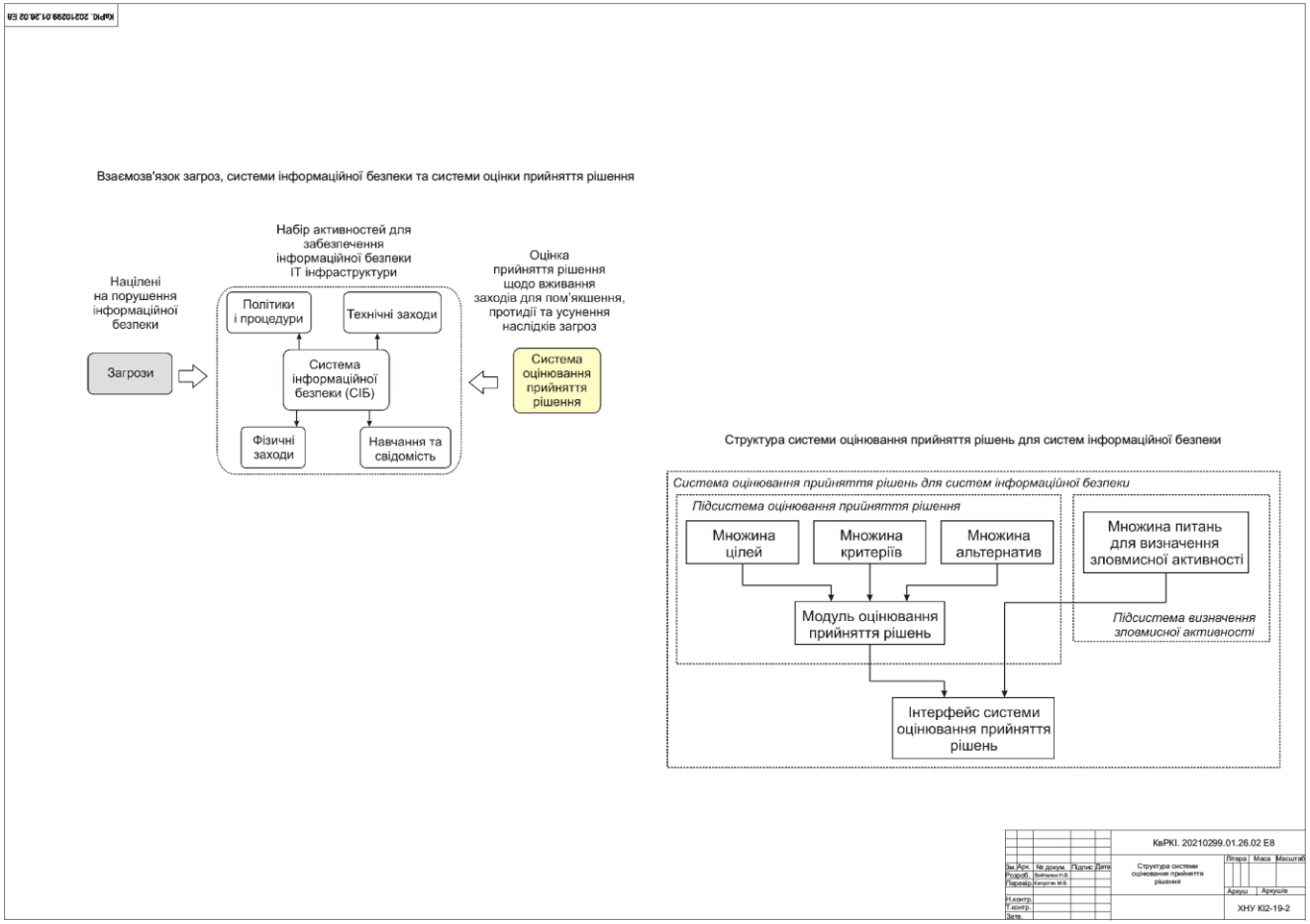
Копія креслення «Алгоритми роботи системи оцінювання прийняття рішень для систем інформаційної безпеки»



ДОДАТОК Б

(обовяз‘язковий)

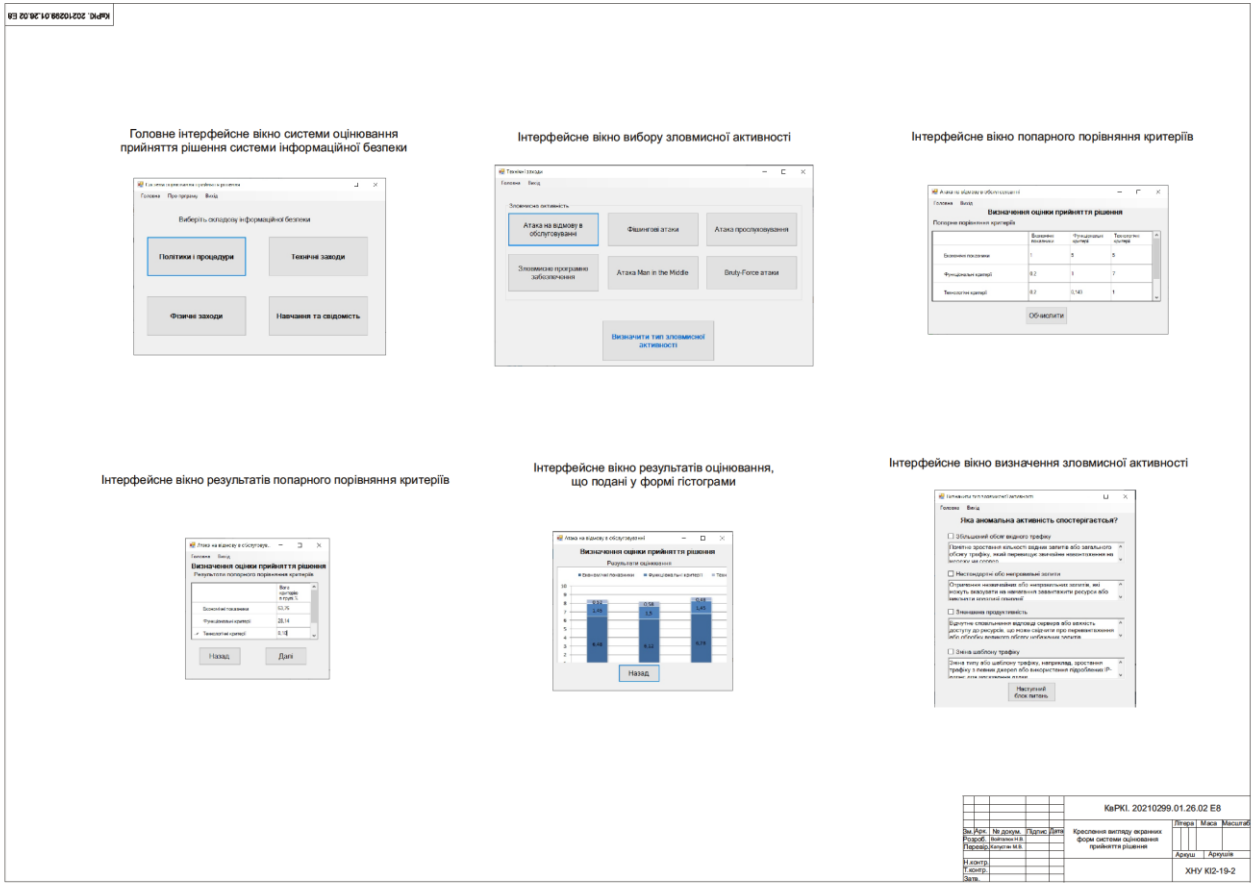
Копія креслення «Структура системи оцінювання прийняття рішення»

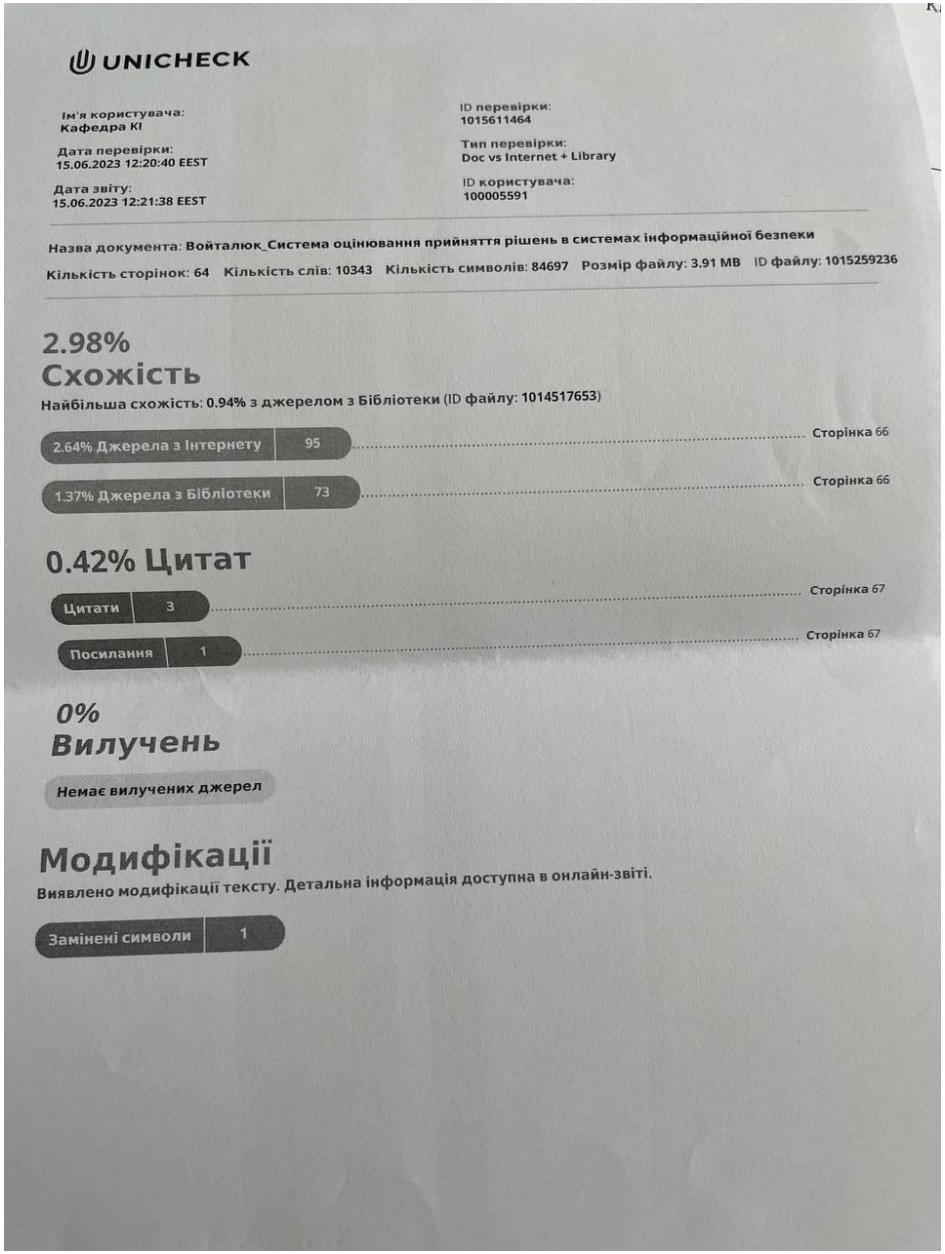


ДОДАТОК В

(обовяз‘язковий)

Копія креслення «Креслення вигляду екранних форм системи оцінювання прийняття рішення»





UNICHECK

Ім'я користувача:
Кафедра КІ

Дата перевірки:
15.06.2023 12:20:40 EEST

Дата звіту:
15.06.2023 12:21:38 EEST

ID перевірки:
1015611464

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100005591

Назва документа: Войталюк_Система оцінювання прийняття рішень в системах інформаційної безпеки

Кількість сторінок: 64 Кількість слів: 10343 Кількість символів: 84697 Розмір файлу: 3.91 MB ID файлу: 1015259236

2.98%
Схожість

Найбільша схожість: 0.94% з джерелом з Бібліотеки (ID файлу: 1014517653)

2.64% Джерела з Інтернету 95 ..... Сторінка 66

1.37% Джерела з Бібліотеки 73 ..... Сторінка 66

0.42% Цитат

Цитати 3 ..... Сторінка 67

Посилання 1 ..... Сторінка 67

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 1

Thu Jun 15 11:12:09 EEST 2023, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
D: 116466 азва: БКР Система оцінювання прийняття рішень в системах інформаційної безпеки одано в БД: 2023-06-15 втора: Н.В. Войталюк ерівники: М.В. Капустян онсультанти: поненти:	76398	590	483 (1%)	6 (1%)

	Джерело плагіату	Наявність плагіату в документі	
	Опис	Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Войталюк Назар Володимирович

Тема: Система оцінювання прийняття рішень в системах інформаційної безпеки

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 55

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є розробка системи оцінювання прийняття рішень в системах інформаційної безпеки.

2. Висновок про відповідність роботи дипломному завданню: *Дипломний проєкт* відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі розглянуто основні існуючі системи оцінювання прийняття рішень а також актуальність цієї тематики у сфері інформаційеої безпеки. Другий розділ присвячено аналізу предметної області та обгрунтованого вибору методики та засобів для реалізації поставленої задачі. У третьому розділі представлено розроблену систему оцінювання прийняття рішень в системах інформаційної безпеки.

4. Позитивні сторони роботи: У роботі приділено увагу необхідності та важливості даної теми в умовах війни в Україні.

5. Негативні сторони роботи: У роботі наявні певні недоліки із використанням усталеної термінології, присутні незначні граматичні помилки.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка та листи креслення оформлені коректно згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: В загальному робота виконана на достатньому рівні.

8. Інші зауваження: ---

9. Оцінка дипломної роботи: Розглянувши роботу в повному обсязі, та зваживши позивні та негативні сторони, вважаю що робота заслуговує оцінки «задов.» 3.25 (D)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) к.т.н., доцент кафедри АКІТтаР Корецька Л.

«22» червня 2023 р. (підпис)

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Войтович Назар Володимирович
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-19-2

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному *репозитарії університету*.

Також надаю університету право на передачу моєї роботи для обробки та *збереження* в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та *використання* роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

22.06.23
дата

підпис

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система оцінювання прийняття рішень в системах інформаційної безпеки

Автор: Войталюк Назар Володимирович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Капустян Марія Вікторівна, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділі аналізу існуючих аналогів та відомих рішень, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 2,98% і адресується до 168 першоджерела, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ М. В. Капустян

Гарант ОП _____ С. М. Лисенко

Завідувач кафедри КІІС _____ Т. О. Говорущенко