МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук,
управління та адміністрування
Кафедра інформаційних технологій

Кваліфікаційна робота бакалавра

на тему: Аналіз системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки

Виконав студент групи КН-19
спеціальності 122 Комп'ютерні науки
Бєломєстнов Михайло Валерійович

Керівник к.т.н., доцент
Казакова Надія Феліксівна

Рецензент Начальник ІВЦ ОНЕУ
к.т.н., Домаскін Олег Михайлович

Одеса 2023

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

ІБ – інформаційна безпека

ІС – інформаційна система

ОПР – особа яка приймає рішення

ПЗ – програмне забезпечення

СППР – системи підтримки прийняття рішень

СТЗ – спеціальні технічні засоби

AI – Artificial intelligence, штучний інтелект

IDS – Intrusion Detection System, системи виявлення вторгнень

MCDM – Multi-Criteria Decision-Making, багатокритеріальні методи прийняття рішень

SIEM – Security information and event management , системи управління подіями та інформаційною безпекою

TCO – Total Cost of Ownership, сукупна вартість володіння.

ВСТУП

У сучасному світі зростає значущість аналізу загроз інформаційній безпеці, оскільки залежність від комп'ютерних систем неперервно збільшується. Інформаційні системи стають предметом зловмисних дій, які можуть призвести до значних фінансових втрат, порушення конфіденційності та пошкодження репутації. Аналіз та оцінка загроз інформаційній безпеці є надзвичайно важливим завданням для підтримки безпеки та стабільності комп'ютерних систем.

З метою ефективного виявлення та аналізу загроз інформаційній безпеці, в рамках даної дипломної роботи була розроблена програма Система Підтримки Прийняття Рішень (СППР). Головною метою цієї програми є надання засобів для систематичного аналізу загроз інформаційній безпеці та визначення відповідних заходів для їх запобігання та протидії. СППР забезпечує користувачам зручну та просту інтерфейс для проведення аналізу загроз, враховуючи їх вплив, вірогідність виникнення та інші параметри.

Однією з головних переваг програми СППР є її легка адаптованість до вимог та потреб користувача. Завдяки динамічній обчислювальній структурі та інтуїтивному інтерфейсу, користувачі можуть змінювати параметри та налаштування програми, враховуючи їх власні пріоритети та потреби. Це дозволяє кожному користувачеві отримати індивідуальне рішення, оптимізоване під їхні вимоги та унікальні умови.

Функціонал програми СППР включає такі можливості, як збір та аналіз інформації про потенційні загрози, визначення ризику та його категоризація, розробка рекомендацій та стратегій для запобігання загрозам, а також моніторинг та оновлення інформації про загрози з метою постійного покращення безпеки. Головною перевагою програми є її здатність забезпечувати оперативність та точність аналізу, а також зручний доступ до результатів та рекомендацій через інтерфейс СППР.

Метою даної дипломної роботи є розробка програми СППР для аналізу

загроз інформаційній безпеці. Основним завданням є створення функціонально готового програмного забезпечення, яке забезпечить користувачам зручну інформаційну систему для ефективного управління безпекою та прийняття рішень в галузі інформаційної безпеки. Під час дослідження дипломної роботи будуть розглянуті різні аспекти аналізу загроз, методи та алгоритми їх виявлення, а також розробка та впровадження програми СППР з урахуванням сучасних підходів та технологій. Очікується, що робота принесе вагомий внесок у сферу інформаційної безпеки та сприятиме підвищенню рівня захищеності комп'ютерних систем від загроз.

В результаті виконання дипломної роботи очікується отримання функціонально готової програми СППР, яка буде використовуватись для аналізу загроз інформаційній безпеці. Така програма забезпечить користувачам зручні та ефективні засоби для аналізу та управління загрозами, а також покращить рівень безпеки комп'ютерних систем. Дипломна робота виявиться корисною для організацій, які прагнуть забезпечити безпеку своїх інформаційних ресурсів та мереж, а також для спеціалістів у галузі інформаційної безпеки, які цікавляться розробкою та використанням програмних засобів для аналізу загроз.

Дипломна робота містить в собі 62 сторінок, 12 таблиць, 10 рисунків, 16 посилань.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Різновиди підходів до визначення рівня інформаційної безпеки

Система інформаційної безпеки має на меті організацію безпечного та надійного доступу до інформації, передачі та зберігання інформаційних даних, обробки інформації, контролю доступу до неї, відновлення інформації та резервування даних. Основні завдання системи інформаційної безпеки включають забезпечення безпечного зберігання та передачі електронної інформації, забезпечення надійного доступу до неї, обмеження і контроль доступу співробітників до інформації, розробку правил безпечної роботи з даними, проведення заходів з резервування та відновлення інформації в аварійних ситуаціях, а також підтримку інформаційної безпеки на потрібному рівні. Забезпечення інформаційної безпеки стає критично важливим для успішного функціонування підприємств у сучасній постіндустріальній економіці. Однак, виникає потреба у визначенні поточного стану інформаційної безпеки підприємства, включаючи характеристики та відповідні значення показників, що забезпечують належний рівень захисту інформації. Важливо також оцінити ці значення в умовах невизначеності, яка є невід'ємною частиною сфери безпеки. Для забезпечення належного рівня інформаційної безпеки необхідно використовувати комплексний підхід, який включає в себе різноманітні заходи, такі як використання спеціальних технічних і програмних засобів, організаційні заходи, нормативно-правові акти тощо. Головна мета будь-якої системи інформаційної безпеки полягає в створенні умов для безпечного функціонування підприємства, захисті його інтересів від протиправних посягань, запобіганні ризикам, пов'язаним з розкраданням фінансових ресурсів, розголошенням, втратою, витоком, спотворенням або знищенням конфіденційної інформації, а також забезпеченні інформаційної безпеки в усіх підрозділах підприємства. Завдання

службам захисту інформації полягає не лише у створенні, але й у постійному вдосконаленні заходів для забезпечення безпеки інформації. Тому важливо постійно відстежувати та аналізувати стан інформаційної безпеки для досягнення належного рівня захисту .

Удосконалення інформаційної безпеки (ІБ) у підприємстві вимагає належної оцінки ІБ, що включає ряд ключових аспектів (рис.1.1).

Перше, важливе завдання полягає в розумінні контексту оцінки, яке включає в себе визначення цілей оцінки та встановлення обмежень, які дозволять здійснити комплексний аналіз ІБ. Крім того, наявність свідоцтв оцінки відіграє важливу роль, оскільки вони підтверджують ефективність і реалізацію заходів щодо забезпечення ІБ, а також можуть включати в себе різноманітні документи, звіти та результати аудиту. Іншим важливим компонентом є модель оцінки, яка надає рамки для проведення оцінки ІБ, включаючи визначення параметрів та механізмів оцінки. Критерії оцінки встановлюють вимоги ІБ, процедури ІБ та витрати, необхідні для забезпечення адекватного рівня захисту. Нарешті, результат оцінки включає виявлення слабких місць, оцінку ризиків та надання конкретних рекомендацій щодо поліпшення ІБ. Правильне використання всіх цих аспектів оцінки ІБ дозволяє підприємству досягти належного рівня захищеності інформації, а також пристосувати заходи безпеки до власних потреб і вимог.

Рисунок 1.1 − Процес оцінки інформаційної безпеки в організації

Оцінка інформаційної безпеки (ІБ) включає в себе процес визначення та оцінювання критичних елементів, ефективності захисних заходів та доцільності інвестицій для забезпечення необхідного рівня ІБ. Основна мета оцінки полягає у створенні інформаційної потреби, яка сприятиме покращенню ІБ. Крім цього, існують інші цілі, такі як [2]:

- визначення відповідності окремих областей ІБ, процесів забезпечення ІБ і захисних заходів встановленим критеріям;
- виявлення впливу критичних елементів та їх взаємодії на ІБ організації;
- порівняння зрілості різних процесів забезпечення ІБ і ступеня відповідності різних захисних заходів вимогам;
- використання результатів оцінки ІБ для порівняння рівня ІБ між схожими організаціями.

Поліпшення інформаційної безпеки (ІБ) в організації може бути досягнуто через різноманітні підходи до оцінки, які враховують конкретні критерії:

1. Оцінка за еталоном: Цей підхід заснований на порівнянні діяльності та заходів забезпечення ІБ організації з встановленими еталонами. Шляхом вимірювання відповідності системи забезпечення ІБ вимогам еталону, можна отримати оцінку її ефективності.
2. Ризик-орієнтована оцінка: Цей підхід враховує потенційні загрози та ризики, пов'язані з інформаційною сферою організації,, та оцінює ефективність заходів, спрямованих на управління цими ризиками. Результатом оцінки є оцінка здатності організації ефективно управляти ризиками ІБ.
3. Оцінка за економічними показниками: Цей підхід визначає ефективність та доцільність витрат на заходи забезпечення ІБ, порівнюючи їх з економічними вимогами та очікуваними користями. Це дозволяє організації раціонально використовувати ресурси для досягнення оптимального рівня ІБ.

Процес оцінки ІБ за еталоном включає вибір відповідного еталону, формування критеріїв оцінки, збір свідоцтв оцінки, вимірювання критичних елементів об'єкта оцінки та формування оцінки ІБ. Це дозволяє організації отримати об'єктивну оцінку стану її інформаційної безпеки і визначити можли ві напрямки подальшого поліпшення.

Ризик-орієнтована оцінка інформаційної безпеки включає кілька важливих кроків. По-перше, необхідно ідентифікувати потенційні ризики, які можуть виникнути в сфері інформаційної безпеки. По-друге, слід визначити відповідні процеси управління ризиками та ключові індикатори ризиків інформаційної безпеки. По-третє, на основі цих процесів та індикаторів формуються критерії оцінки інформаційної безпеки. Далі проводиться збір свідчень для оцінки і вимірювання факторів ризику. Завершальним етапом є формування оцінки інформаційної безпеки на основі отриманих даних.

Оцінка інформаційної безпеки на основі економічних показників використовує аргументи, зрозумілі для бізнесу, щодо необхідності забезпечення та вдосконалення інформаційної безпеки. Один з таких показників – сукупна вартість володіння (Total Cost of Ownership – TCO). TCO включає прямі і непрямі витрати, пов'язані з впровадженням, експлуатацією та супроводом системи захисту інформації. Прямі витрати охоплюють матеріальні витрати, такі як закупівля обладнання та програмного забезпечення, а також трудові витрати відповідних співробітників. Непрямі витрати включають витрати на обслуговування системи захисту інформації та втрати, пов'язані з інцидентами. Збір і аналіз статистичних даних щодо прямих і непрямих витрат проводиться протягом року. Отримані дані порівнюються з критеріями TCO аналогічних організацій галузі, що дозволяє оцінити витрати на інформаційну безпеку і порівняти їх з типовим профілем захисту. Така оцінка допомагає управляти витратами для досягнення необхідного рівня захищеності.

Оцінка ефективності системи захисту інформації на основі моделі TCO включає декілька етапів. Спочатку збираються дані про поточний рівень TCO.

Потім проводиться аналіз областей, пов'язаних з інформаційною безпекою. Наступним кроком є вибір порівняльної моделі ТСО як критерію оцінки, а також порівняння показників з цим критерієм. Завершальним етапом є формування оцінки інформаційної безпеки на основі отриманих даних. Проте, цей спосіб оцінки вимагає створення загальної інформаційної бази даних щодо ефективності систем захисту інформації в організаціях зі схожим бізнесом, а також постійного підтримання актуальної бази даних. Такий обмін інформацією між організаціями, як правило, не відповідає бізнес-цілям. Тому оцінка інформаційної безпеки на основі показника ТСО майже не використовується на практиці.

1.2 Методології оцінки ризику в галузі інформаційної безпеки

Оцінка інформаційної безпеки - це складний процес, який включає кілька етапів. Перш за все, необхідно визначити контекст оцінки, що охоплює цілі, призначення, тип оцінки (незалежна або самооцінка), об'єкт та області оцінки, а також обмеження та ролі, пов'язані з оцінкою. Це допомагає уточнити рамки і вимоги до процесу оцінки [3].

Наступним кроком є встановлення критеріїв оцінки та створення моделі оцінки. Критерії визначаються на основі важливих атрибутів безпеки, які необхідно враховувати при оцінці. Модель оцінки визначає, як будуть збиратися дані, які методи оцінки будуть використовуватися та які процедури перевірки будуть застосовуватися.

Проведення оцінки включає збір свідчень та перевірку їх достовірності. Це означає, що інформація, яка використовується для оцінки, повинна бути достовірна та підтверджена. Крім того, проводяться вимірювання та оцінювання атрибутів об'єкта оцінки згідно з встановленими критеріями.

На виході отримується результат оцінки, який відображає ступінь безпеки інформації або ідентифікує вразливість. Цей результат може включати числові значення, ранжування, висновки або рекомендації.

Процес оцінки інформаційної безпеки може бути представлений на процесній моделі, яка відображає послідовність кроків та залежності між ними.

Перед розглядом конкретних методів оцінки інформаційної безпеки для підприємств важливо враховувати загальні компоненти процесу оцінки, такі як контекст оцінки, збір свідчень та їх перевірку, вимірювання та оцінювання атрибутів, а також вихідні дані оцінки. Це допоможе забезпечити правильність та об'єктивність оцінки безпеки інформації (рис.1.2) .

Рисунок 1.2 – Основні елементи процесу оцінювання ІБ

1.3 Побудова моделі загроз

Одним з основних етапів оцінки безпеки інформації є проведення оцінки загроз інформаційної безпеки. Для цього використовується модель загроз, яка визначає вимоги до системи захисту. Наявність адекватної моделі загроз є необхідною умовою для розробки ефективної системи захисту, яка забезпечує безпеку інформації. В систему захисту включаються лише ті заходи, які нейтралізують актуальні загрози. Модель загроз є основою для проектування

майбутніх систем захисту та прийняття рішень щодо їх захищеності. Тому добре складена модель загроз дозволяє адекватно захистити інформацію та забезпечує реалізацію мети відповідних нормативних актів. З іншого боку, недостатньо точна або поверхнева модель загроз робить подальшу роботу невдалим, ускладнює правильне формулювання технічного завдання для розробки системи захисту і може призвести до непотрібних витрат на засоби захисту.

При розробці моделі загроз інформаційній системі (ІС) необхідно керуватися певними принципами. Забезпечення безпеки інформації в ІС залежить від системи захисту, яка контролює її обіг. Варто зазначити, що технічні засоби захисту самі по собі не можуть забезпечити повну безпеку інформації, оскільки не усувають можливість порушення доступу відповідно до наданих повноважень. Тому використання організаційних заходів в поєднанні з технічними є важливим аспектом. При створенні моделі загроз необхідно враховувати як прямі загрози, що безпосередньо становлять загрозу для інформаційної безпеки, так і непрямі загрози, які створюють умови для виникнення прямих або непрямих загроз. Інформація в ІС обробляється і зберігається за допомогою різних технологій і технічних засобів, які потребують захисту на різних рівнях. Ці об'єкти стикаються з прямими або непрямими загрозами безпеки інформації. Для розробки моделі загроз потрібно виконати кілька послідовних кроків, таких як категоризація об'єкту інформаційної діяльності, аналіз послідовності логічних кроків процесу порушення інформаційної безпеки, ідентифікація компонентів моделі загроз і їх порівняння, а також дослідження актуальності порівняних компонентів. Остаточні результати аналізу оформляються відповідно до підготовленого шаблону, що дозволяє сформувати модель загроз. Розробка моделі загроз відбувається на основі детального аналізу атрибутів. У випадку побудови моделі загроз, атрибутами є загрози, джерела цих загроз та вразливості.

Після виконання всіх цих кроків буде сформована модель загроз.

1.4 Підходи до підвищення рівня ІБ

Для аналізу процесів порушення інформаційної безпеки рекомендується використовувати логічну послідовність «загроза – джерело загрози – вразливість – наслідки» [4].

Ця послідовність показує, що порушення інформаційної безпеки є послідовним процесом і залежить від різних складових. Тому, для забезпечення ефективного захисту, необхідно детально аналізувати ці складові. Покращення системи захисту інформації можливе за умови комплексного підходу до побудови моделі загроз і розуміння ступеня її відповідності потрібним результатам. Для такого комплексного підходу потрібні детальні класифікації цих складових.

У сучасній науковій дискусії в цій галузі існує багато класифікацій за різними ознаками. З усієї різноманітності була обрана класифікація, яка є найбільш повною і легко сприймається. Відповідно до обраної класифікації розглянемо докладно кожну складову моделі загроз.

1.5 Джерела ризиків та загроз в ІБ

Концепція інформаційних загроз є ключовою у теорії та практиці інформаційного захисту. Аналіз загроз є першим і одним з головних етапів при створенні моделі загроз. Його метою є виявлення можливих загроз інформації та вказівка, з якого боку та в якій частині системи слід очікувати атаку. Джерелами загроз безпеки інформації є джерела загроз (рис.1.2) . Ці джерела можуть бути як суб'єктами (особи), так і об'єктивними проявами [5].

Важливо відзначити, що джерела загроз можуть знаходитися як всередині організації - внутрішні джерела, так і поза нею – зовнішні джерела. Розмежування на внутрішні та зовнішні джерела є обґрунтованим, оскільки для однієї і тієї ж загрози можуть використовуватися різні методи захисту від зовнішніх та внутрішніх джерел.

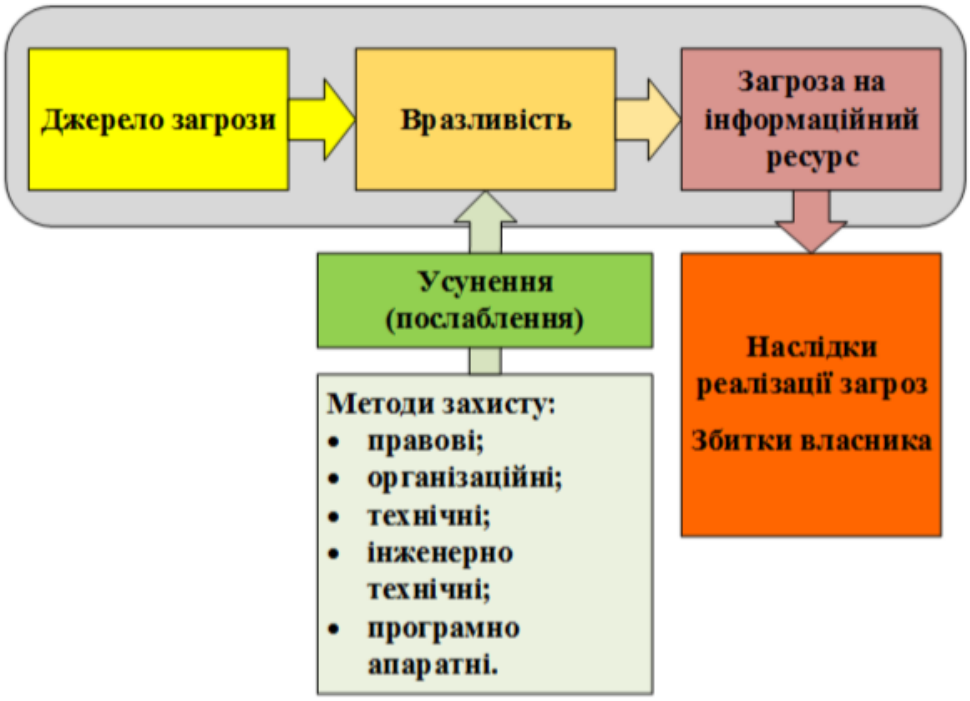

Рисунок 1.2 −Модель реалізації загроз ІБ

Усі джерела загроз безпеки інформації можна класифікувати на три основні групи [6]:

1. Джерела загроз, що виникають внаслідок дій суб'єкта (антропогенні джерела загроз).
2. Джерела загроз, що виникають внаслідок застосування технічних засобів (техногенні джерела загроз).
3. Джерела загроз, що виникають внаслідок стихійних явищ (стихійні джерела загроз).

Антропогенні загрози ІБ пов'язані з діяльністю людей, які можуть викликати небезпеку для безпеки інформації. Основні джерела антропогенних загроз включають такі:

1. Зловмисники (хакери): Це люди, які мають знання та навички для незаконного доступу до інформації, викрадення даних, розповсюдження шкідливих програм тощо. Зловмисники можуть бути

мотивовані фінансовими перевагами, політичними або особистими мотивами.

2. Внутрішні загрози: Це загрози, що виникають зсередини організації. Працівники, які мають доступ до конфіденційної інформації, можуть зловживати своїм статусом, викрадати дані, розголошувати інформацію або неправомірно використовувати ресурси компанії.
3. Соціальний інжиніринг: Це метод маніпулювання людьми, щоб отримати конфіденційну інформацію. Шахраї можуть використовувати соціальний інжиніринг, щоб отримати доступ до паролів, номерів кредитних карток або інших конфіденційних даних шляхом використання підступів, вманювання та обману.

Техногенні загрози ІБ пов'язані з використанням технологій та інфраструктури. Основні джерела техногенних загроз включають такі:

4. Вразливості програмного забезпечення: Недоліки та вразливості в програмах та операційних системах можуть бути використані для незаконного доступу до інформації або впровадження шкідливих програм.
5. Комп'ютерні віруси та шкідливі програми: Шкідливі програми, такі як віруси, черв'яки, троянські коні та шпигунські програми, можуть інфікувати комп'ютери та мережі, викрадати дані, розповсюджуватися та завдавати шкоди.
6. Дефекти в мережевій інфраструктурі: Недоліки у мережевій інфраструктурі, такі як недостатня захищеність мережевих пристроїв, неправильна конфігурація мережі або слабкі паролі, можуть створювати ризики для безпеки інформації.
7. Стихійні загрози ІБ виникають в результаті природних або непередбачуваних подій. Основні стихійні джерела загроз включають такі:
8. Природні бедствія: Повені, землетруси, урагани, пожежі та інші природні бедствія можуть спричинити втрату даних, знищення

інфраструктури та порушення роботи систем, що може викликати загрози для безпеки інформації.

9. Аварії в енергетичній та комунікаційній інфраструктурі: Відмови електропостачання, збої мережі зв'язку або інших комунікаційних систем можуть призвести до перерви у доступі до інформації, втрати даних або порушення функціонування систем.
10. Несанкціоновані дії третіх сторін: Невідомі особи або організації, не пов'язані з конкретною організацією, можуть бути джерелом загроз ІБ шляхом фізичного доступу до приміщень, викрадення обладнання або здійснення інших дій, що ставлять під загрозу безпеку інформації

1.6 Вразливості інформаційних систем

Можливі загрози, спрямовані на порушення безпеки інформації на конкретному об'єкті інформатизації, виникають через існуючі вразливості (фактори). Вразливості є невід'ємною частиною об'єкта інформатизації і виникають внаслідок недоліків у процесі функціонування, архітектурних особливостей автоматизованих систем, протоколів обміну даними, програмного забезпечення та апаратних платформ, умов експлуатації та розташування. Джерела загроз можуть використовувати ці вразливості для незаконного доступу до інформації та отримання неправомірної вигоди. Крім того, можливі ненавмисні дії з боку загроз, що активізують вразливості і завдають шкоди. Кожна загроза може експлуатувати різні вразливості. Вирішення або значне зменшення вразливостей впливає на здатність реалізувати загрози щодо безпеки інформації.

З метою спрощення аналізу, вразливості поділяються на різні категорії, включаючи класи, групи і підгрупи. Вразливості, пов'язані з безпекою інформації, можна розділити на об'єктивні, суб'єктивні та випадкові.

Об'єктивні вразливості, які можна відокремити, включають наступне:

1. Електромагнітне випромінювання, що походить від технічних

пристроїв, яке може бути наведене на лінії, кабелі, генератори або підсилювачі, і впливає на конфіденційність, цілісність та доступність інформації.

2. Керуючі вразливості, такі як апаратні та програмні закладки, які можуть бути встановлені у телефонних лініях, електроживленні, приміщеннях або технічних пристроях, порушуючи безпеку інформації.
3. Вразливості, пов'язані з елементами, які мають електроакустичні перетворення або піддаються впливу електромагнітного поля, що може спричинити пошкодження або неправильну роботу системи.
4. Вразливості, пов'язані з особливостями захищеного об'єкта, такі як його розташування та організація каналів обміну інформацією, що можуть ускладнити захист інформації.

Суб'єктивні вразливості можуть бути описані таким чином:

1. Помилки, пов'язані з розробкою, встановленням та використанням програмного забезпечення, а також введенням даних.
2. Помилки в управлінні складними системами, такими як самонавчання, налаштування сервісів та організація управління обміном інформацією.
3. Помилки, що виникають під час експлуатації технічних засобів, включаючи включення/виключення, використання засобів охорони та обміну інформацією.
4. Порушення режиму охорони і захисту, які стосуються доступу до об'єкта та технічних засобів.
5. Порушення режиму експлуатації технічних засобів, включаючи енергозабезпечення та життєзабезпечення.
6. Порушення режиму використання інформації, такі як обробка, обмін, зберігання та знищення носіїв інформації.
7. Порушення режиму конфіденційності, зокрема співробітниками поза робочим часом або після звільнення.

Випадкові вразливості можна узагальнити наступним чином:

1. Збої і відмови технічних засобів, що відповідають за опрацювання інформації, забезпечення працездатності засобів обробки, охорони та контролю доступу.
2. Старіння і розмагнічування носіїв інформації, таких як дискети, жорсткі диски, кабелі і мікросхеми.
3. Збої у програмному забезпеченні, включаючи операційні системи, системи управління базами даних, прикладні програми та антивірусні програми.
4. Збої в електропостачанні, що можуть впливати на обладнання та обробку інформації.
5. Пошкодження життєзабезпечуючих комунікацій, таких як електропостачання, водопостачання, газопостачання, каналізація, кондиціювання та вентиляція.
6. Пошкодження огороджувальних конструкцій, включаючи огорожі територій та будівельні конструкції.

1.7 Загрози інформаційній безпеці

У сучасній літературі поняття «інформаційна загроза» розглядається як можливість вплинути на безпеку інформації або ступінь ймовірності виникнення такої небажаної ситуації, наслідком якої можуть бути негативні наслідки для інформації. Наприклад, загроза зйому і перехоплення інформації з дисплею може привести до витоку таємниць або порушення конфіденційності, загроза пожежі може призвести до пошкодження або втрати доступу до інформації, а загроза переривання каналу передачі інформації може спричинити недоступність інформації. Існує багато підходів до класифікації загроз, але найпоширенішими у літературі та законодавстві є два підходи: базовані на основних властивостях та базовані на складі незаконних дій.

У першому випадку, можна виділити наступні типи загроз, які можуть впливати на інформацію [7]:

– незаконне розкриття конфіденційної інформації;
– неправомірна зміна або пошкодження даних, що порушує цілісність інформації;
– недоступність інформації для легітимних користувачів або відмова в обслуговуванні;
– неправомірне отримання контролю або вплив на систему безпеки, що порушує спостережність або керованість.

У другому випадку, можна виділити наступні загрози:

– крадіжка або незаконне копіювання інформації;
– руйнування або пошкодження інформації;
– неправомірна модифікація або спотворення інформації;
– блокування доступу до інформації;
– відкидання або заперечення автентичності інформації;
– розповсюдження недостовірної інформації.

Другий підхід є більш практичним і конкретним, а також лаконічним і зрозумілим. Тому для аналізу більш вигідною є класифікація загроз за складом незаконних дій. В першій класифікації є певна абстракція і необхідність побудови ієрархічної системи для розкриття змісту кожного пункту. Це робить її менш зручною для аналізу. З іншого боку, друга класифікація є конкретною і практичною, а також лаконічною. Тому вона є більш придатною для аналізу.

Розкрадання – це незаконне, з корисливою метою, безоплатне заволодіння або використання чужого майна на шкоду його власника або інших осіб. Ці дії призводять до збитків і втрати власності.

Знищення – це дії, які призводять до безповоротного видалення інформації з системи. Це порушує цілісність і доступність інформації, і відновлення її стає неможливим.

Спотворення – це зміна змісту повідомлення під час передачі по зв'язку. Інформація може бути спотворена через вплив зовнішніх чинників, технічні

помилки апаратури або недбалість обслуговуючого персоналу.

Порушення доступності інформації – це дії, які унеможливлюють доступ до інформації в системі. Це може бути наслідком технічних проблем, атак або інших факторів, що перешкоджають нормальному функціонуванню системи.

Термін «автентичний» означає, що інформація є достовірною і базується на першоджерелах.

Заперечення автентичності інформації – це відмова суб'єкта прийняти відповідальність за надану інформацію або повідомлення.

Нав'язування неправдивої інформації – це надання некоректної інформації, приховуючи її справжній характер і підводячи отримувача до невірних висновків.

1.8 Аналіз існуючих способів виявлення загроз інформації

Як було вказано раніше, існують різні способи оцінки інформаційної безпеки (ІБ). Але два найбільш ефективних з них є наступні [8]:

1. Оцінка на основі еталону: в цьому випадку аналіз проводиться шляхом порівняння ситуації на підприємстві з еталонними або стандартизованими значеннями і даними. Після цієї процедури отримується список атрибутів і їх коефіцієнтів відповідності. Цей підхід застосовується, коли організація та її діяльність відповідають стандартам. В інших випадках дані, отримані в результаті оцінки, можуть не відображати реальний стан речей. Позитивним аспектом цього підходу є наявність розробленої та структурованої бази знань. Однак, негативним аспектом аналізу на основі еталону є можливі складнощі при інтерпретації еталонних даних та неможливість застосування цього підходу до нестандартно структурованих підприємств.
2. Ризик-орієнтована оцінка: в цьому випадку аналізується можливість порушення безпеки підприємства. Після проведення цієї процедури

отримується список атрибутів та їх коефіцієнтів ризику. Цей підхід можна використовувати в будь-якому випадку. Однак, зі зростанням розміру підприємства збільшується обсяг інформації, яку потрібно обробити. Позитивним аспектом цього підходу є можливість застосування його на будь-якому підприємстві. Однак, негативним аспектом ризик-орієнтованої оцінки є необхідність аналізувати існуючі загрози та складнощі при збільшенні розміру підприємства.

Існують різні варіації обох цих підходів, які можна знайти в різних джерелах. Однак, не існує єдиних стандартизованих методик використання цих підходів. Кожен спеціаліст втілює їх на свій розсуд, а великі компанії намагаються створити програмні комплекси, які поєднують ці два підходи.

2. СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Актуальність теми СППР

Актуальність теми «Аналіз системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки» полягає у важливості забезпечення ефективності та безпеки інформаційних ресурсів в умовах сучасного цифрового світу. Нижче наведено докладне пояснення актуальності даної теми [9]:

Зростання загроз інформаційній безпеці: У сучасному світі комп'ютерні системи та мережі є незамінними складовими підприємств, установ, організацій та навіть особистого життя людей. Разом зі зростанням технологічного прогресу також зростає кількість і складність загроз інформаційній безпеці, таких як хакерські атаки, крадіжка конфіденційної інформації, віруси та шкідливі програми тощо. Аналіз системи підтримки прийняття рішень є ключовим для ефективного виявлення, оцінки та управління цими загрозами.

Наслідки порушень інформаційної безпеки: Неадекватна оцінка та управління загрозами інформаційній безпеці може мати серйозні наслідки для організацій. Це можуть бути фінансові втрати, витік конфіденційної інформації, порушення репутації, втрата довіри клієнтів та партнерів, юридичні проблеми та інші. Аналіз системи підтримки прийняття рішень дозволяє зменшити ризики та мінімізувати наслідки порушень інформаційної безпеки.

Законодавчі вимоги та регулювання: Багато країн встановлюють законодавчі вимоги щодо захисту інформації та інформаційних систем. Організації зобов'язані виконувати ці вимоги та впроваджувати ефективні системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки, які дозволяють довести відповідність вимогам та забезпечити

належний рівень захисту.

Постійний розвиток технологій: Швидкий технологічний прогрес приводить до появи нових методів та засобів атак на інформаційні системи. При цьому, системи підтримки прийняття рішень повинні постійно вдосконалюватись, щоб впроваджувати нові методи аналізу, детекції та відповіді на загрози. Актуальність даної теми полягає у постійній потребі в оновленні та покращенні систем підтримки прийняття рішень для ефективного виявлення та протидії новим загрозам.

Конкурентний ринок технологій безпеки: Компанії, організації та установи з усього світу постійно шукають найкращі рішення для забезпечення інформаційної безпеки. Тому існує постійна потреба у вивченні, аналізі та порівнянні систем підтримки прийняття рішень для оцінки загроз інформаційної безпеки.

Таким чином, актуальність теми «Аналіз системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки» очевидна через зростаючу кількість загроз інформаційній безпеці, потребу в ефективному управлінні ризиками та дотриманням законодавчих вимог, швидкий розвиток технологій та постійну потребу в пошуку найкращих рішень для захисту інформації (рис. 2.1) .

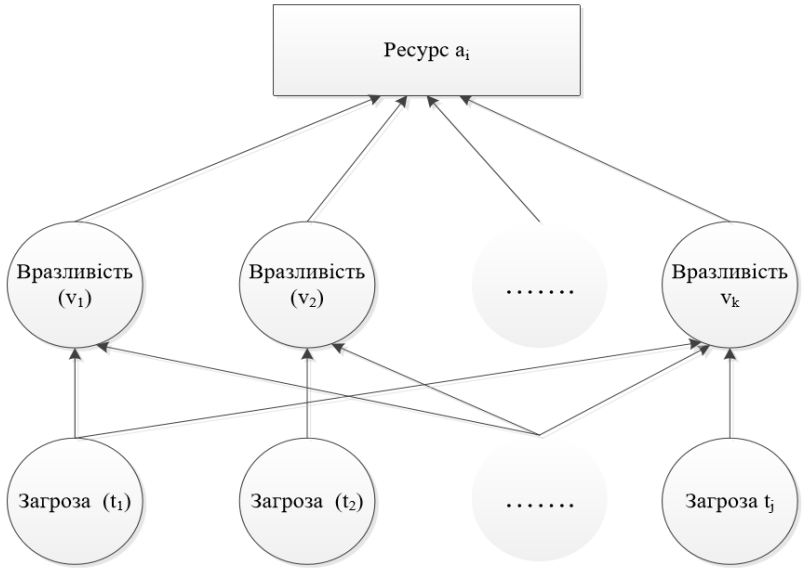

Рисунок 2.1 – Загальна ієрархічна модель загроз та вразливостей

Загрози інформаційній безпеці є різноманітними і можуть виникати з різних джерел. Основні типи загроз інформаційній безпеці включають :

1. Шкідливе програмне забезпечення (Malware): Це віруси, черв'яки, троянські програми та інші шкідливі програми, які можуть виконувати різні деструктивні або шпигунські дії на комп'ютері або в мережі. Вони можуть пошкоджувати або крадти дані, перешкоджати нормальному функціонуванню системи або навіть контролювати її.
2. Фішинг (Fishing): Це метод соціально-інженерної атаки, коли зловмисники намагаються шахрайським шляхом отримати конфіденційну інформацію, таку як паролі, номери кредитних карток, особисті дані тощо. Зазвичай, зловмисники відправляють підозрілі електронні листи або підроблені веб-сайти, що належать до легітимних організацій, з метою введення жертви в оману.
3. Деніал-сервіс (Denial-of-Service, DoS): Це атака, коли зловмисники переповнюють мережу або систему запитами, що призводить до перевантаження і зниження доступності для легітимних користувачів. Це може призвести до значних втрат у роботі бізнесу або порушення нормального функціонування організації.
4. Соціальний інжиніринг: Це метод, коли зловмисники використовують маніпуляцію та обман, щоб отримати невідповідну інформацію або змусити користувачів зробити небезпечні дії. Вони можуть надаватися під зарядкою представників технічної підтримки, просити паролі або інші конфіденційні дані, або використовувати інші способи маніпуляції.
5. Несанкціонований доступ (Unauthorized Access): Це коли зловмисники намагаються отримати доступ до комп'ютерної системи, мережі або облікових записів без дозволу. Вони можуть використовувати слабкі паролі, вразливості систем або техніки злому, щоб отримати контроль над системою та отримати конфіденційну інформацію.

	Вразливість	Загроза, яка використовує вразливість
РЕСУРСИ КОНТРОЛЮ ДОСТУПУ		
1	Неправильне розмежування доступу в мережах	Обхід механізмів контролю системи або додатки
2	Відсутня або некоректна політика контролю доступу	Несанкціоновані підключення до мереж
3	Відсутність механізмів ідентифікації і автентифікації	Втрата або пошкодження інформації
4	Відсутність захисту мобільного ком. обладнання	Привласнення чужого призначеного для користувача ідентифікатора
5	Відсутність політик чистих столів і чистих екранів	Використання програмного забезпечення неавторизованими користувачами
6	Відсутність “виходу з системи”, коли покидається робоча станція	Несанкціонований доступ до інформації

Рисунок 2.2 – Приклад загроз і вразливостей

Аналіз системи підтримки прийняття рішень допомагає в боротьбі з цими загрозами шляхом:

1. Виявлення загроз: Аналізуючи систему інформаційної безпеки, можна ідентифікувати потенційні загрози та ризики, зокрема за допомогою моніторингу мережі, аудиту системи та виявлення несправностей.
2. Оцінка ризиків: Аналіз допомагає визначити потенційні наслідки загроз та оцінити ймовірність їхнього виникнення. Це дозволяє приділити пріоритетну увагу найбільш значущим загрозам та розробити відповідні стратегії захисту.
3. Розробка заходів безпеки: Аналіз системи підтримки прийняття рішень допомагає ідентифікувати слабкі місця і розробляти ефективні заходи безпеки для запобігання атакам та захисту інформації.
4. Моніторинг та виявлення вторгнень: Аналіз системи підтримки прийняття рішень дозволяє встановити механізми моніторингу та

виявлення незвичних або підозрілих дій, які можуть свідчити про вторгнення або атаку. Це допомагає вчасно реагувати на загрози та вживати необхідні заходи для їхнього усунення.

5. Навчання та свідомість користувачів: Аналіз системи підтримки прийняття рішень допомагає розробити програму навчання та підвищення свідомості користувачів щодо безпеки інформації. Це включає навчання щодо фішингу, використання складних паролів, оновлення програмного забезпечення тощо.

Аналіз системи підтримки прийняття рішень є важливим інструментом для виявлення, оцінки та управління загрозами інформаційній безпеці, допомагаючи забезпечити безпеку даних та систем в організаціях. Порушення інформаційної безпеки можуть мати серйозні наслідки для організацій. Деякі з найпоширеніших наслідків порушень інформаційної безпеки включають [10]:

1. Втрата конфіденційності даних: Несанкціонований доступ до конфіденційної інформації може призвести до витоку цінної інформації, такої як особисті дані клієнтів, комерційні та фінансові відомості. Це може порушити довіру клієнтів та спричинити фінансові втрати або правові наслідки для організації.
2. Порушення цілісності даних: Несанкціонований доступ або модифікація даних можуть призвести до порушення цілісності даних. Це означає, що дані можуть бути змінені, видалені або пошкоджені без дозволу, що може спричинити серйозні наслідки для точності та надійності даних, наприклад, помилкові рішення, втрата довіри клієнтів або неправильні фінансові розрахунки.
3. Втрата доступності системи: Деніал-сервіс атаки або інші форми вторгнень можуть призвести до недоступності комп'ютерних систем або мережі. Це може призвести до перебоїв у роботі бізнесу, втрати продуктивності, втрати доходу та негативного впливу на репутацію організації.

4. Фінансові втрати: Порушення інформаційної безпеки можуть призвести до значних фінансових втрат для організації. Це може включати витрати на відновлення систем, компенсацію клієнтам, штрафи за порушення законодавства, втрату бізнесу через зниження довіри клієнтів, втрату ринкової позиції тощо.
5. Порушення вимог законодавства: Некоректна обробка, зберігання або передача конфіденційної інформації може призвести до порушення вимог законодавства щодо захисту даних. Це може призвести до серйозних правових наслідків, включаючи штрафи, судові позови, втрату довіри та негативний вплив на репутацію організації.
6. Аналіз системи підтримки прийняття рішень допомагає зменшити ризики та мінімізувати наслідки порушень інформаційної безпеки шляхом виявлення потенційних загроз, оцінки ризиків, розробки стратегій захисту, моніторингу та виявлення вторгнень, а також навчання та свідомості користувачів. Це дозволяє реагувати на загрози вчасно, приймати обґрунтовані рішення щодо захисту інформації та запобігати серйозним наслідкам порушень інформаційної безпеки. На сьогоднішній день існує кілька ефективних систем підтримки прийняття рішень для оцінки загроз інформаційної безпеки. Ось деякі з них:
7. Системи управління подіями та інформаційною безпекою (SIEM): Ці системи збирають, агрегують та аналізують дані з різних джерел, таких як журнали подій, системи виявлення вторгнень (IDS), файрволи тощо. Вони дозволяють виявляти аномалії, вторгнення та інші загрози інформаційній безпеці.
8. Аналітичні платформи з використанням штучного інтелекту (AI): Ці платформи використовують алгоритми машинного навчання та штучного інтелекту для аналізу великих обсягів даних і виявлення складних загроз. Вони можуть виявляти незвичайні зміни, аномалії та нові типи атак.

9. Системи інтелектуального аналізу загроз (Threat Intelligence): Ці системи збирають інформацію про нові загрози та вразливості з різних джерел, включаючи власні дослідження, публічні бази даних та спільноти. Вони надають цінну інформацію про потенційні загрози, їхні характеристики та способи протидії.

Щодо оновлень та покращень систем підтримки прийняття рішень, ця галузь постійно розвивається, оскільки з'являються нові загрози та вразливості. Деякі з оновлень та покращень включають:

Використання штучного інтелекту та машинного навчання для покращення аналітики та виявлення аномалій.

Розвиток систем автоматизації та інтеграції, які дозволяють швидше виявляти, відстежувати та реагувати на загрози.

Використання блокчейн-технологій для забезпечення безпеки даних та прозорості в процесі прийняття рішень.

Розширення можливостей аналізу та виявлення загроз на різних рівнях, включаючи мережевий рівень, рівень додатків та рівень користувача.

У цій області проводиться значна кількість досліджень з метою виявлення найкращих рішень та розробки нових методик інтелектуального аналізу загроз. Дослідження зосереджуються на вдосконаленні алгоритмів аналізу даних, розробці нових моделей машинного навчання та використанні нових джерел інформації для виявлення загроз. Такі дослідження сприяють розвитку ефективних систем підтримки прийняття рішень для оцінки загроз інформаційної безпеки і надають організаціям можливість вибрати найефективніші засоби для захисту своєї інформації.

2.2 Наукова новизна та практична цінність СППР

Аналіз системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки має як наукову новизну, так і практичну цінність. Є декілька аспектів, що підкреслюють їх важливість.

Наукова новизна: інноваційні методи аналізу даних, такі як машинне навчання, штучний інтелект та аналітика великих даних, внесли значний внесок у наукову новизну аналізу системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки. Деякі конкретні приклади включають:

Машинне навчання: Застосування алгоритмів машинного навчання дозволяє системам аналізувати великі обсяги даних та виявляти складні зв'язки, які можуть бути непомітними для людського аналізу. Моделі машинного навчання можуть виявляти зміну патернів поведінки, виявляти аномалії та надавати прогнози стосовно майбутніх загроз.

Штучний інтелект: Використання методів штучного інтелекту, таких як нейромережі та експертні системи, дозволяє системам аналізувати, інтерпретувати та використовувати складні дані для виявлення загроз. Штучний інтелект може самостійно навчатися на основі великого обсягу історичних даних та робити прогнози стосовно майбутніх ризиків.

Аналітика великих даних: Системи підтримки прийняття рішень використовують аналітику великих даних для обробки, інтеграції та аналізу даних з різних джерел. Це дозволяє отримати повну картину стосовно загроз та вразливостей, а також виявити складні залежності та тенденції, що допомагають прийняти обґрунтовані рішення з питань безпеки.

Такі інноваційні методи аналізу даних вносять новизну в систему підтримки прийняття рішень для оцінки загроз інформаційної безпеки, роблять її більш точною, ефективною та здатною передбачати майбутні ризики.

Аналіз системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки дійсно сприяє розширенню знань про загрози і відкриває нові аспекти в цій галузі. Деякі з аспектів наукової новизни включають:

Виявлення нових видів атак: Аналіз системи підтримки прийняття рішень дозволяє виявляти нові, раніше невідомі види атак, які можуть бути більш складними та витонченими. Це допомагає оновлювати знання про

загрози та розробляти нові методи для їх виявлення та протидії.

Вдосконалення методів виявлення і реагування на загрози: Аналіз системи підтримки прийняття рішень сприяє вдосконаленню методів виявлення та реагування на загрози. Він допомагає виявляти нові підходи та техніки, які використовуються зловмисниками, та розробляти ефективні стратегії для їх виявлення та протидії.

Удосконалення процесів управління ризиками: Аналіз системи підтримки прийняття рішень дозволяє розширити розуміння загроз та вразливостей і покращити процеси управління ризиками. Він надає можливість оцінити ризики, пріоритизувати заходи безпеки та розробити стратегії для зниження ризиків та збільшення стійкості інформаційної системи.

Таким чином, аналіз системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки вносить наукову новизну, розширюючи знання про загрози, удосконалюючи методи виявлення і реагування на них та поліпшуючи процеси управління ризиками.

Аналіз системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки має значну практичну цінність. Деякі з його практичних переваг включають [11] :

1. Розуміння загрозового ландшафту: Аналіз системи підтримки прийняття рішень дозволяє організаціям отримувати глибоке розуміння їхнього загрозового ландшафту. Це означає, що організації можуть ідентифікувати потенційні загрози та вразливості, що ставить під загрозу їхню інформацію та ресурси. Це забезпечує підвищену свідомість про потенційні ризики та дозволяє організаціям ухвалювати обґрунтовані рішення щодо заходів безпеки.
2. Ідентифікація вразливостей: Аналіз системи підтримки прийняття рішень допомагає ідентифікувати вразливості в інформаційних системах. Це дозволяє організаціям виявляти слабкі місця та потенційні маршрути атаки. Ідентифікація вразливостей дозволяє

вживати належні заходи безпеки та усувати вразливості, зменшуючи ризик компрометації інформації.

3. Прийняття обґрунтованих рішень: Аналіз системи підтримки прийняття рішень надає організаціям контекстну інформацію та рекомендації, необхідні для прийняття обґрунтованих рішень щодо безпеки. Враховуючи дані аналізу загроз та оцінки ризиків, організації можуть визначити пріоритети, визначити необхідні заходи безпеки та розробити стратегії управління ризиками.
4. Підвищення ефективності захисту: Аналіз системи підтримки прийняття рішень сприяє підвищенню ефективності захисту інформації. Шляхом ідентифікації загроз, визначення ризиків та вживання належних заходів безпеки організації можуть зменшити вразливість своїх систем та мінімізувати можливість виникнення інцидентів безпеки. Це сприяє забезпеченню безпеки даних, дотриманню регуляторних вимог та підвищенню довіри до організації з боку клієнтів та партнерів.

Практична цінність систем підтримки прийняття рішень для оцінки загроз інформаційної безпеки полягає в їхній здатності до автоматизації та прискорення процесів. Основні переваги включають:

1. Автоматизований аналіз даних: Системи підтримки прийняття рішень використовують передові методи аналізу даних, такі як машинне навчання та штучний інтелект, щоб автоматично обробляти великі обсяги інформації про загрози. Це дозволяє здійснювати швидкий та точний аналіз, виявляти аномалії та ідентифікувати потенційні загрози безпеки.
2. Моніторинг у реальному часі: Системи можуть забезпечувати постійний моніторинг подій та активності, що відбуваються в мережі або системі. Це дозволяє виявляти небажану активність або незвичну поведінку користувачів у реальному часі, що сприяє швидкій реакції на загрози та вчасному прийняттю заходів безпеки.

3. Швидка реакція на загрози: Завдяки автоматизованому аналізу та моніторингу, системи підтримки прийняття рішень дозволяють виявляти загрози швидше і ефективніше. Це дозволяє організаціям реагувати на інциденти безпеки негайно і зменшує час, необхідний для розслідування та вирішення проблем.
4. Підвищення ефективності ресурсів: Автоматизація процесів аналізу та виявлення загроз дозволяє зменшити навантаження на аналітиків безпеки та звільнити їх від рутинних та монотонних завдань. Це дозволяє спрямувати їхні зусилля на більш складні та стратегічні завдання, такі як розробка нових методів виявлення загроз та вдосконалення заходів безпеки.
5. Практична цінність систем підтримки прийняття рішень для оцінки загроз інформаційної безпеки також включає покращення стратегічного планування. Основні аспекти цієї практичної цінності включають:
6. Виявлення слабких місць: Аналіз системи підтримки прийняття рішень допомагає організаціям виявити свої слабкі місця в галузі інформаційної безпеки. Це може включати виявлення вразливостей, неефективних процесів або недостатньої освіченості персоналу. Ці дані надають основу для подальшого планування та прийняття заходів для забезпечення безпеки.
7. Визначення пріоритетів: Аналіз системи дозволяє організаціям визначити пріоритети щодо заходів безпеки. Враховуючи потенційні загрози та ризики, система надає інформацію про найбільш критичні аспекти безпеки, які вимагають негайної уваги. Це допомагає організації виконати ресурси та зусилля в першу чергу для захисту найважливіших активів.
8. Розробка довгострокової стратегії: Аналіз системи підтримки прийняття рішень надає дані та контекст для розробки довгострокової стратегії забезпечення безпеки інформації. Організації можуть

використовувати ці дані для формулювання цілей, визначення кроків для забезпечення безпеки та планування ресурсів на майбутнє. Це допомагає організації стати більш проривною та стратегічною в галузі інформаційної безпеки.

Так, аналіз системи підтримки прийняття рішень для оцінки загроз інформаційної безпеки поєднує наукову новизну та практичну цінність. Використання передових методів аналізу даних, штучного інтелекту та машинного навчання сприяє виявленню складних зв'язків і передбаченню майбутніх загроз. Одночасно, системи підтримки прийняття рішень автоматизують та прискорюють процеси, полегшуючи роботу аналітиків та підвищуючи ефективність заходів безпеки. Крім того, вони надають цінні дані для стратегічного планування та управління ризиками, що сприяє покращенню безпеки та зменшенню ризиків для організацій. Отже, аналіз системи підтримки прийняття рішень має значний потенціал для покращення безпеки інформації та ефективності управління ризиками в організаціях.

2.3 Поняття СППР та аналіз систем підтримки прийняття рішень

Забезпечення необхідною інформацією та підтримка процесу прийняття управлінських рішень є завданням, яке має свої виклики. Основні типи інформаційних систем, які використовуються в цьому контексті, включають інформаційно-управлінські системи, системи підтримки прийняття рішень та виконавчі інформаційні системи. Люди повинні приймати рішення різної складності у своїй діяльності, такі як вибір стратегії розвитку компанії, автоматизації процесів, забезпечення інформаційної безпеки, вибір локації для зустрічей, обладнання, а також вибір кандидатів на вакантні посади. Врахування безпеки інформації на підприємстві вимагає уваги до економічних, соціальних, юридичних і моральних факторів, що ускладнює процес прийняття вірного рішення. При цьому потрібно враховувати взаємозв'язок між всіма факторами, які стосуються різних експертів. Однак,

керівнику, який приймає рішення, притаманні людські обмеження, пов'язані з психологією та фізіологією.

Один із способів вирішення цього протиріччя полягає в застосуванні математичних методів, які реалізовані у сучасних інформаційних системах підтримки прийняття рішень. СППР є комп'ютерними автоматизованими системами, які допомагають людям приймати рішення в складних умовах, забезпечуючи повний та об'єктивний аналіз предметної діяльності. Хоча точне визначення СППР з'явилося не одразу, ранні визначення СППР включали наступні характеристики: можливість опрацьовувати задачі, які мають нечітку або слабку структуру; використання методів дослідження операцій; взаємодія з інтерактивними автоматизованими системами; розподіл даних та моделей.

Сучасні системи підтримки прийняття рішень є спеціально адаптованими інструментами для ефективного вирішення управлінських завдань на щодень. Вони надають допомогу особам, які приймають рішення (ОПР). СППР використовують бази даних, включаючи як "сирі" дані, так і передоброблені матеріали. Мета цієї обробки полягає в зробленні даних зручними та інформативними для аналітичного використання різними групами користувачів. Існують певні елементи і характеристики, які загалом визнані як складові частини СППР.

Turban запропонував список характеристик ідеальної СППР, який включає наступне [12]:

1. Здатність працювати з рішеннями, які мають слабку структуру.
2. Придатність для ОПР різного рівня.
3. Адаптованість для групового та індивідуального використання.
4. Підтримка як взаємозалежних, так і послідовних рішень.
5. Підтримка трьох фаз процесу рішення: інтелектуальна частина, проектування та вибір.
6. Підтримка різних стилів та методів рішення, корисних при груповому прийнятті рішень.

7. Гнучкість та здатність адаптуватися до змін у підприємстві та його оточенні.
8. Простота використання та модифікації.
9. Підвищення ефективності процесу прийняття рішень.
10. Забезпечення можливості людині управляти процесом.
11. Легка побудова СППР, якщо логіка конструкції визначена.
12. Підтримка моделювання.
13. Використання знань.

Враховуючи принципи підтримки прийняття рішень, можна виділити три класи СППР в залежності від складності задач і областей застосування. Системи підтримки прийняття рішень першого класу, які володіють найбільш широким функціоналом, призначені для використання в органах державного управління на вищому рівні та великих компаніях.

СППР другого класу є системами для індивідуального використання, і бази знань цих систем формуються самим користувачем. Ці системи призначені для державних службовців середнього рівня та керівників малих і середніх підприємств для вирішення оперативних управлінських завдань.

СППР третього класу також є системами для індивідуального використання, але вони адаптуються до досвіду конкретного користувача. Ці системи призначені для розв'язання конкретних задач системного аналізу та управління, які часто зустрічаються, наприклад, вибір суб'єкта кредитування або призначення на посаду.

Окрім того, існують чотири типи СППР, які відрізняються архітектурою та способом зберігання даних. Функціональні СППР є найпростішими за архітектурою і поширені в організаціях з невеликими інформаційними потребами. Вони аналізують дані, що знаходяться в операційних системах. Перевагами таких систем є компактність та швидкість завдяки відсутності потреби переносити дані до спеціалізованих систем. Але недоліками є обмежений спектр питань, які можуть бути вирішені системою, а також збільшення навантаження на операційну систему.

Системи підтримки прийняття рішень , які використовують незалежні вітрини даних, активно застосовуються великими організаціями, що мають кілька підрозділів, включаючи відділи інформаційних технологій. Кожна вітрина даних створюється для вирішення конкретних завдань та спрямована на певну групу користувачів, що суттєво підвищує продуктивність системи. Проте, негативним аспектом є потреба повторного введення даних у різні вітрини, що може призвести до дублювання інформації. Заповнення вітрин даних є складним завданням, оскільки потрібно користуватися численними джерелами. Крім того, відсутня єдина цілісна картина бізнесу організації через відсутність остаточної консолідації даних. СППР, що базуються на дворівневому сховищі даних, використовуються великими компаніями, де дані консолідовані в єдину систему. Визначення та обробка інформації у цьому випадку є уніфікованими. Для забезпечення нормальної роботи такої СППР необхідно мати спеціалізовану команду, яка відповідатиме за її обслуговування. Така архітектура СППР не дозволяє структурувати дані для окремих груп користувачів і може обмежувати доступ до інформації. Також можуть виникати проблеми з продуктивністю системи.

СППР на основі трьохрівневого сховища даних використовують сховище даних, з якого формуються вітрини даних для різних груп користувачів з подібними завданнями. Такий підхід забезпечує доступ до конкретних структурованих даних, а також до єдиної консолідованої інформації. Ці СППР характеризуються гарантованою продуктивністю, але в них може бути надмірність даних, що призводить до збільшених вимог до зберігання інформації. Крім того, потрібно узгодити таку архітектуру з різними областями, що можуть мати різні потреби. Зазначено, що для СППР відсутня загальноприйнята класифікація. Проте існують різні варіанти та класифікації систем підтримки прийняття рішень , які можна зведені до єдиної. На рівні користувача, СППР можна поділити на три типи. Пасивні СППР допомагають у процесі прийняття рішень, але не можуть самостійно запропонувати конкретне рішення. Активні СППР мають можливість надати

пропозиції щодо прийняття рішень. Кооперативні СППР дозволяють користувачам змінювати або поліпшувати рішення, запропоновані системою, і відправляти їх назад для перевірки та узгодження, процес повторюється до досягнення консенсусу.

На концептуальному рівні можна виділити кілька типів СППР. СППР, керовані повідомленнями, зосереджуються на обміні інформацією між користувачами. СППР, керовані даними, використовують інформацію з різних джерел для прийняття рішень. СППР, керовані документами, забезпечують доступ до документів та інформації, пов'язаної з ними. СППР, керовані знаннями, базуються на знаннях та експертизі для прийняття рішень. СППР, керовані моделями, використовують математичні моделі та аналітичні методи для прийняття рішень.

На технічному рівні можна виділити два типи СППР. СППР усього підприємства підключаються до великих сховищ даних та обслуговують багатьох менеджерів. Настільні СППР, натомість, обслуговують лише один комп'ютер користувача.

Залежно від типу даних, які використовуються, СППР можна умовно розділити на оперативні та стратегічні. Оперативні СППР призначені для негайної реакції на зміни в поточній ситуації управління фінансово-господарськими процесами компанії. Вони базуються на інформації з транзакційних систем підприємства та надають звіти для керівництва. Стратегічні СППР орієнтовані на аналіз великого обсягу різноманітної інформації з різних джерел. Вони використовують спеціально підготовлені дані для прийняття стратегічних рішень, що спираються на правила та агреговані дані для підтримки прийняття рішень та зменшення ризиків, включаючи інформаційну безпеку. СППР цього типу активно розвиваються останнім часом.

3. ПОРІВНЯННЯ МЕТОДІВ БАГАТОКРИТЕРІАЛЬНОГО ПРИЙНЯТТЯ РІШЕНЬ

Процес прийняття рішень часто пов'язані з великою кількістю альтернативних рішень. Основною складністю у виборі одного з них є той факт, що критерії, які використовуються для оцінювання та порівняння альтернативних рішень найчастіше конфліктують так, що є неможливим вибір оптимального рішення, що перевершує всі інші за заданими критеріями. Інакше завдання багатокритеріального вибору має тривіальне рішення. Більше того, критерії або атрибути можуть бути як якісними, так і кількісними. Тому процес прийняття рішень називається багатокритеріальним (MCDM) [13].

Крім того, критерії можуть мати різні шкали та одиниці виміру. Зрештою, не останню роль відіграє важливість критеріїв щодо один одного. Від апріорної розстановки значимості критеріїв залежить результат прийняття рішення та вибір правильної стратегії визначення важливості критеріїв – окреме завдання, що вимагає експертизи та всебічної зануреності в контекст задачі, що вирішується.

У цьому розділі буде проведено порівняльний аналіз трьох методів багатокритерійного прийняття рішень: метод ELECTRE (ELimination and Choice Expressing Reality), просте адитивне зважування (Simple Additive Weighting), аналітичний ієрархічний процес (Analytic hierarchy process).

3.1 Аналітичний ієрархічний процес (AHP)

Метод аналізу ієрархій (AHP) є ефективним інструментом для вирішення складних проблем зі структурою ієрархії критеріїв, зацікавлених сторін, результатів та врахуванням міркувань для встановлення ваг або пріоритетів. Одна з основних переваг методу AHP полягає в тому, що він поєднує сильні сторони експертного бачення та логічного мислення, що дозволяє аналізувати та синтезувати різноманітні міркування з метою

отримання результатів, які відповідають нашим очікуванням.

Структура моделі AHP представляє собою ієрархічну структуру з оберненим деревом. У верхній частині дерева знаходиться єдина ціль, яка визначає мету прийняття рішень. На даному рівні встановлюється стовідсоткова вага цілі. Нижче цілі знаходяться критерії, які можуть бути як якісними, так і кількісними. Вага цілей розподіляється серед рейтингових балів відповідно до їхнього відносного значення.

Кроки виконання методу аналізу ієрархій можна розбити на такі кроки [14]:

1. Визначення ієрархічної структури: Спочатку потрібно визначити ієрархічну структуру проблеми, розбивши її на рівні цілей, критеріїв та альтернатив. Наприклад, якщо розглядається вибір автомобіля, то цілі можуть включати економічність, комфорт, безпеку тощо, критерії - витрати на паливо, якість салону, рівень безпеки, а альтернативи - різні моделі автомобілів.
2. Порівняння пар критеріїв або альтернатив: Для кожної пари критеріїв або альтернатив необхідно здійснити їх порівняння за важливістю або перевагою. Зазвичай використовується шкала відносних значень, де значення відображають ступінь переваги одного елемента над іншим. Наприклад, використовуючи шкалу від 1 до 9, ви оцінюєте, наскільки один критерій або альтернатива переважає над іншими.
3. Оцінювання ваг: Після порівняння пар критеріїв або альтернатив, вираховується вага для кожного критерію та альтернативи. Це робиться шляхом обчислення узагальнених вагових коефіцієнтів на основі парних порівнянь. Узагальнені вагові коефіцієнти відображають важливість кожного елемента в контексті всієї ієрархії.
4. Обчислення консистентності: Після введення парних порівнянь, проводиться перевірка консистентності цих порівнянь. Це допомагає переконатися в точності введених даних. Використовуються

математичні методи для обчислення індексу консистентності та визначення, чи відповідають введені дані логіці.

5. Обробка та аналіз результатів: Після отримання ваг кожного критерію та альтернативи, виконується обробка та аналіз цих результатів для прийняття рішення. Часто використовується сумування вагованих значень для кожної альтернативи для отримання загальної оцінки кожної альтернативи. Альтернативи з більшою загальною оцінкою вважаються більш привабливими або кращими.

Загалом, метод AHP надає систематичний підхід до вирішення складних мультикритеріальних задач. Він дозволяє структурувати проблему, враховувати вагомість кожного критерію та альтернативи, а також здійснювати аналіз результатів для прийняття обґрунтованих рішень.Недоліком методу AHP є можлива складність управління багатими наборами даних, а також вимога до експерта віддати перевагу парним порівнянням замість безпосередньої оцінки. Крім того, метод може бути вразливим до суб'єктивності та узагальнень експерта, які вводяться при визначенні ваг.

В цілому, метод аналізу ієрархій є потужним інструментом для прийняття рішень, здатним допомогти у структуруванні проблем та уточненні відносної важливості критеріїв і альтернатив, що допомагає зробити обґрунтовані та інформовані виробничі рішення.

3.2 Метод вагових коефіцієнтів (WSM)

Метод вагових коефіцієнтів є широко застосовуваним методом в області прийняття рішень та мультикритеріального аналізу. Його основна ідея полягає у призначенні вагових коефіцієнтів кожному критерію залежно від його важливості. Ці вагові коефіцієнти відображають ступінь впливу кожного критерію на загальний результат та дозволяють враховувати пріоритети та важливість кожного критерію в контексті прийняття рішень.

Після нормалізації значень кожного критерію, метод WSM обчислює вагову суму шляхом множення нормалізованих значень на відповідні вагові коефіцієнти та їх сумування. Цей підхід дозволяє зводити різні критерії до спільної шкали та отримувати числове значення, яке представляє кінцеву оцінку альтернативи. Перевагою методу WSM є його простота та зрозумілість, що дозволяє широко застосовувати його навіть користувачам без спеціалізованих знань. Також, завдяки можливості використання вагових коефіцієнтів, WSM дозволяє гнучко налаштувати врахування важливості кожного критерію залежно від конкретних потреб та умов прийняття рішень.

Проте, важливо враховувати деякі обмеження методу WSM. Він припускає незалежність критеріїв, що не завжди відповідає реальним умовам. Також, результати WSM можуть бути чутливими до вагових коефіцієнтів, тому необхідно обережно підходити до їх визначення та уникати суб'єктивних оцінок.

Кроки виконання методу вагових коефіцієнтів можна розбити на наступні етапи [15]:

1. Визначення критеріїв: Ідентифікуйте всі релевантні критерії, які необхідно врахувати при прийнятті рішень. Наприклад, у випадку вибору інформаційної системи можуть бути такі критерії, як вартість, функціональні можливості, надійність тощо.
2. Вагові коефіцієнти: Визначте вагові коефіцієнти для кожного критерію, що відображають їх відносну важливість. Вагові коефіцієнти можуть бути визначені на основі експертної оцінки, аналізу даних або застосування інших методів, таких як аналітична ієрархія процесів .
3. Нормалізація критеріїв: Нормалізуйте значення кожного критерію, щоб привести їх до спільної шкали. Це можна зробити шляхом масштабування значень критеріїв на відрізок [0, 1] або використання інших методів нормалізації, таких як мінімаксний метод.
4. Вагова сума: Обчисліть вагову суму для кожної альтернативи шляхом

множення нормалізованих значень критеріїв на відповідні вагові коефіцієнти та їх сумування. Це дає числову оцінку кожної альтернативи з урахуванням їх важливості.

5. Ранжування альтернатив: Ранжуйте альтернативи за значенням вагової суми. Чим вище значення вагової суми, тим краща альтернатива з перспективи заданих критеріїв.
6. Аналіз результатів: Проаналізуйте отримані результати та зробіть висновки. Перевірте чутливість рішення до зміни вагових коефіцієнтів та різних сценаріїв значень критеріїв.

Важливо зауважити, що метод вагових коефіцієнтів (WSM) базується на припущенні лінійної адитивності критеріїв та вагових коефіцієнтів. Це може бути перевагою у деяких ситуаціях, але також може викликати обмеження, оскільки не враховує можливого взаємодії між критеріями.

3.3 Метод ELECTRE

Метод ELECTRE є одним з методів багатокритеріального аналізу, використовуваних для прийняття рішень. Він був розроблений з метою вирішення проблем, пов'язаних з великою кількістю альтернатив та критеріїв. Основна ідея методу ELECTRE полягає в послідовному виключенні та відборі альтернатив на основі їхнього порівняння за різними критеріями. Спочатку проводиться елімінація альтернатив, які не задовольняють задані критерії, за допомогою встановленого порогу. Далі застосовуються різні правила, які враховують значущість кожного критерію та відстань між альтернативами, для вибору оптимального рішення.

Однією з переваг методу ELECTRE є його здатність працювати зі слабоструктурованими проблемами, де кількість альтернатив і критеріїв може бути дуже великою. Він дозволяє враховувати різні рівні значущості критеріїв та проводити детальний аналіз взаємозв'язків між ними.

Ще однією перевагою методу ELECTRE є можливість застосування

гібридних оцінок, які поєднують якісні та кількісні критерії. Це дозволяє враховувати різні типи інформації та уникати втрати інформації при перетворенні критеріїв на числову шкалу. Проте, метод ELECTRE також має свої недоліки. Він може бути часо- та ресурсомістким, особливо при обробці великих обсягів даних. Крім того, він вимагає встановлення деяких порогових значень та параметрів, які можуть бути суб'єктивними і впливати на кінцеві результати.

Метод складається з 9 кроків виконання :

1. Визначення критеріїв: Визначте критерії, за якими будуть оцінюватися альтернативи.
2. Встановлення ваг критеріїв: Надайте вагу кожному критерію відповідно до його важливості.
3. Збір даних: Зіберіть дані про кожну альтернативу щодо їхньої відповідності критеріям.
4. Нормалізація даних: Нормалізуйте дані для забезпечення однакової шкали оцінок для всіх критеріїв.
5. Визначення матриці відповідності: Побудуйте матрицю відповідності, що відображає ступінь відповідності кожної альтернативи критеріям.
6. Визначення матриці невідповідності Побудуйте матрицю невідповідності, яка відображає ступінь невідповідності кожної альтернативи критеріям.
7. Використання порогових значень: Використовуйте порогові значення, щоб відфільтрувати альтернативи, які не задовольняють встановлені вимоги.
8. Побудова матриці переваг: Побудуйте матрицю переваг, що відображає перевагу однієї альтернативи над іншою на основі відповідності та невідповідності.

9. Ранжування альтернатив: Застосуйте методи ранжування, які використовуються в методі ELECTRE, щоб отримати ранжований список альтернатив.

У загальному, метод ELECTRE є потужним інструментом для багатокритеріального аналізу та прийняття рішень, але перед його використанням варто ретельно розглянути його переваги та недоліки, а також врахувати особливості конкретної проблеми та контексту застосування.

3.4 Порівняльний аналіз розгляданих методів

Для порівняльного аналізу методів AHP , WSM та ELECTRE в контексті мультикритеріального прийняття рішень, було визначено наступні критерії [16] :

1. Простота використання: Цей критерій відноситься до легкості та зручності використання методу прийняття рішень. Метод, який отримує високу оцінку за цей критерій, є простим у розумінні та застосуванні особою, яка приймає рішення.
2. Можливість гібридних оцінок: Цей критерій відображає можливість використання якісних та кількісних оцінок в методі прийняття рішень. Метод, який отримує високу оцінку за цей критерій, має гнучкість у використанні різних типів оцінок, що дозволяє враховувати різноманітність інформації.
3. Розширюваність до роботи з багатьма експертами: Цей критерій описує здатність методу працювати зі значною кількістю експертів, які надають свої оцінки та думки. Метод, який отримує високу оцінку за цей критерій, дозволяє ефективно зібрати та обробити думки різних стейкхолдерів.
4. Обмежена кількість параметрів моделі: Цей критерій вказує на кількість зовнішніх параметрів, які необхідно враховувати у моделі методу прийняття рішень. Метод, який отримує високу оцінку за цей

критерій, має меншу кількість параметрів, що дозволяє йому бути більш стійким та менш залежним від апріорного вибору значень параметрів.

5. Зрозумілість для користувача: Цей критерій відображає зрозумілість та доступність методу для особи, яка приймає рішення. Метод, який отримує високу оцінку за цей критерій, пропонує зрозумілі та зрілі результати, які допомагають користувачу легко оцінити та вибрати оптимальне рішення. Обчислювальна ефективність: Цей критерій відноситься до обчислювальної складності методу прийняття рішень. Метод, який отримує високу оцінку за цей критерій, вимагає менше обчислювальних ресурсів та часу для виконання, що робить його більш ефективним у застосуванні.
6. Урахування сутності критеріїв: Цей критерій відображає здатність методу враховувати взаємозв'язок та значущість критеріїв при прийнятті рішень. Метод, який отримує високу оцінку за цей критерій, дозволяє враховувати сутність кожного критерію та вагу, яку він має в розглянутій проблемі. Для оцінки порівнюваних методів було використано приклад, пов'язаний з вибором найбільш небезпечної загрози інформаційній безпеці, на яку потрібно зосередити найбільшу увагу та ресурси. У цьому прикладі розглядаються шість основних критеріїв: ймовірність виникнення, потенційний вплив, складність експлуатації, розповсюдженість, виявлення та потенційний збиток. З цих критеріїв обирається найбільш підходяща альтернатива з чотирьох основних загроз: вірусні атаки, фішингові атаки, кібершпигунство та ddos-атаки.

Після застосування всіх трьох методів для вирішення описаної проблеми була створена матриця оцінок (табл.3.1) та побудований порівняльний графік (рис.3.1). Оцінки були здійснені з використанням шкали, наведеної в таблиці 3.2.

Таблиця 3.1 – Матриця оцінок методів прийняття рішень

	Методи прийняття рішень		
Критерії	AHP	WSM	ELECTRE
Простота	4	3	3
Можливість гібридних оцінок	4	3	4
Розширюваність до роботи з кількома експертами	5	4	4
Число параметрів моделі	3	3	2
Зрозумілість для особи, яка приймає рішення	4	4	4
Обчислювальна складність	3	4	3
Облік сенсу критеріїв	5	4	4

Таблиця 3.2 – Шкала оцінювання методів прийняття рішення

Оцінка	Значення
1	Very poor
2	Poor
3	Satisfactory
4	Good
5	Excellent

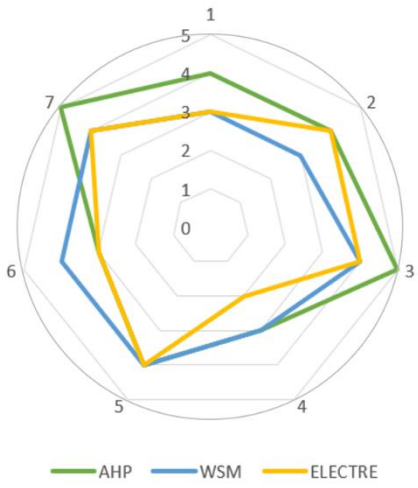

Рисунок 3.1 – Порівняльний аналіз методів прийняття рішення

З огляду на надані оцінки за різними критеріями, проведений порівняльний аналіз методів показав, що метод AHP є найбільш ефективним для вирішення проблеми загрози ІБ. AHP отримав високі оцінки за кілька важливих аспектів, що роблять його привабливим в контексті даної проблеми.

Перш за все, метод AHP відзначається простотою використання. Його структура і процес вирішення проблеми легкі для розуміння та реалізації. Це важливо, оскільки дозволяє швидко включити метод у роботу і виконати аналіз без великих зусиль і складнощів.

Крім того, AHP може працювати з гібридними оцінками, що дає можливість поєднати як кількісні, так і якісні фактори у вагових коефіцієнтах. Це дозволяє більш гнучко враховувати різноманітні аспекти проблеми та вагомість кожного з них у прийнятті рішення.

Також важливою перевагою AHP є його розширюваність до роботи з кількома експертами. Врахування думок та оцінок різних експертів може забезпечити більш об'єктивну оцінку проблеми та уникнути індивідуальних упереджень. AHP забезпечує систематичний підхід до узгодження та врахування різних точок зору. Не менш важливим аспектом AHP є його зрозумілість для особи, яка приймає рішення. Чіткість методу дозволяє розбиратися в процесі оцінювання та зробити обґрунтоване рішення на основі отриманих результатів.

Хоча WSM і ELECTRE також отримали позитивні оцінки у порівнянні, AHP має перевагу з точки зору простоти використання та гнучкості в оцінюванні. Його висока оцінка відображає його ефективність та придатність для вирішення проблеми загрози ІБ.

4 ПРАКТИЧНА РЕАЛІЗАЦІЯ СППР ДЛЯ АНАЛІЗУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Даний розділ пропонує опис процесу розробки та впровадження системи підтримки прийняття рішень для аналізу загроз інформаційної безпеки (ІБ). Ми використовуємо метод аналізу ієрархій, щоб ефективно виявляти та оцінювати загрози ІБ, оскільки цей метод дозволяє структурувати та систематизувати критерії та альтернативи для прийняття обґрунтованих рішень.

У розробці програмної системи СППР ми використовуємо мову програмування Python, яка є потужним та широко використовуваним інструментом для аналізу даних, розробки алгоритмів та реалізації різноманітних застосунків. Python має зручний синтаксис, широкий вибір бібліотек та інструментів для обробки даних, що робить його ідеальним вибором для розробки систем підтримки прийняття рішень.

Система складається з двох основних компонентів: архіву даних та програмної частини, що виконує розрахунки. Архів даних містить інформацію про різні загрози ІБ, їх характеристики, історичні дані та іншу важливу інформацію. Програмна частина відповідає за обробку цих даних та виконання аналізу.

4.1 Опис інтерфейсу програми

Однією з головних метою цієї системи є визначення пріоритету конкретної загрози інформаційній безпеці серед інших можливих загроз (рис. 3.1.).

В результаті аналізу виділимо наступні критерії, які найкраще описують будь-яку загрозу ІБ підприємства (табл.4.1) :

– вірогідність виникнення;

– потенційний вплив;

– складність експлуатації;

– розповсюдженість;

– виявлення;

– потенційний збиток.

Виділимо наступні загрози ІБ які можуть вплинути на будь-яке підприємство як альтернативи вибору(табл.4.2):

– вірусні атаки;

– фішингові атаки;

– кібершпигунство;

– ddos-атаки.

Таблиця 4.1 – Критерії

№	Критерії
К1	Вірогідність виникнення
К2	Потенційний вплив
К3	Складність експлуатації
К4	Розповсюдженість
К5	Виявлення
К6	Потенційний збиток

Таблиця 4.2 – Альтернативи

№	Альтернативи
А1	вірусні атаки
А2	фішингові атаки
А3	кібершпигунство
А4	ddos-атаки

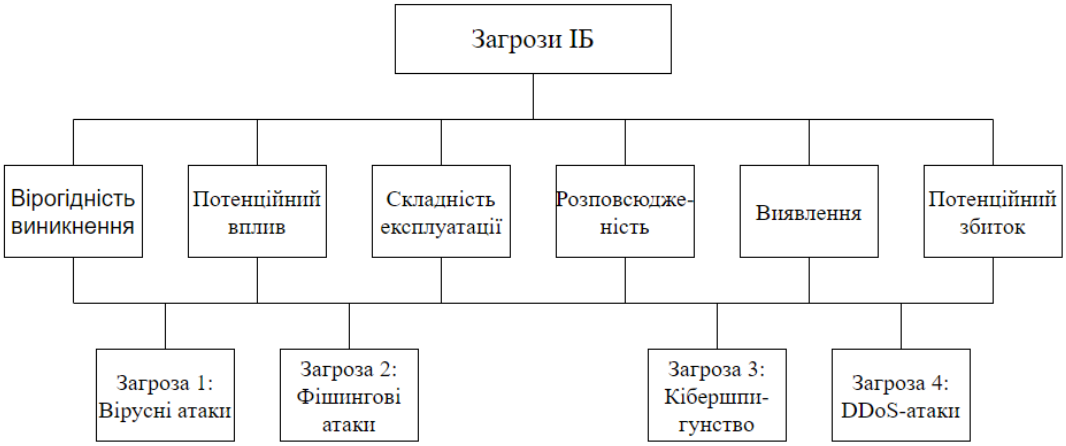

Рисунок 4.1 – Структуризація завдання у вигляді ієрархічної структури

На найвищому рівні ієрархії знаходиться загальна мета – «Загроза ІБ». На другому рівні розташовані фактори, які конкретизують цю мету, а на третьому (нижньому) рівні розташовані чотири конкретні загрози ІБ, які потрібно оцінити відносно факторів (критеріїв) другого рівня.

Програма має інтуїтивний та зрозумілий інтерфейс, який показаний на рисунку 4.2.

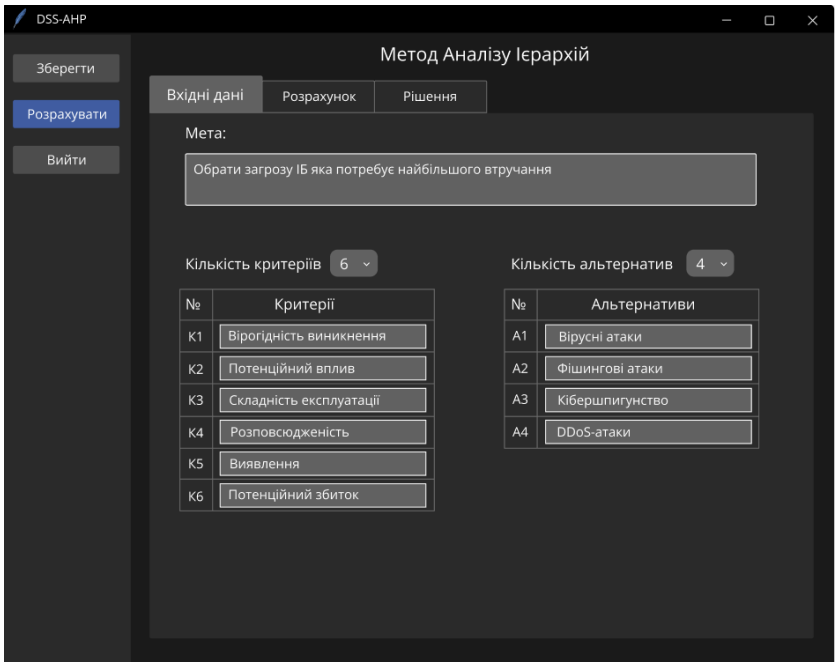

Рисунок 4.2 – Введення даних

Перш за все, користувачеві потрібно ввести необхідні дані для проведення розрахунків, такі як ціль проекту, критерії оцінювання та варіанти розглянутих альтернатив. Програма надасть можливість вибрати загрозу, якій необхідно приділити найбільшу увагу та пріоритетність. З цими даними програма зможе провести відповідні розрахунки та надати корисну інформацію щодо вибору найефективніших заходів для захисту від цієї загрози.

У розділі «Розрахунки» програми знаходяться всі розрахункові матриці для альтернатив та критеріїв. В цьому розділі можна переглянути кожну матрицю альтернатив окремо та ознайомитись з її значеннями та переглянути матрицю критеріїв, де представлені ваги або важливість кожного критерію в рамках аналізу користувача.

Це дозволить краще розуміти результати, отримані програмою, та здійснювати аналіз ефективності альтернатив відповідно до заданих критеріїв.

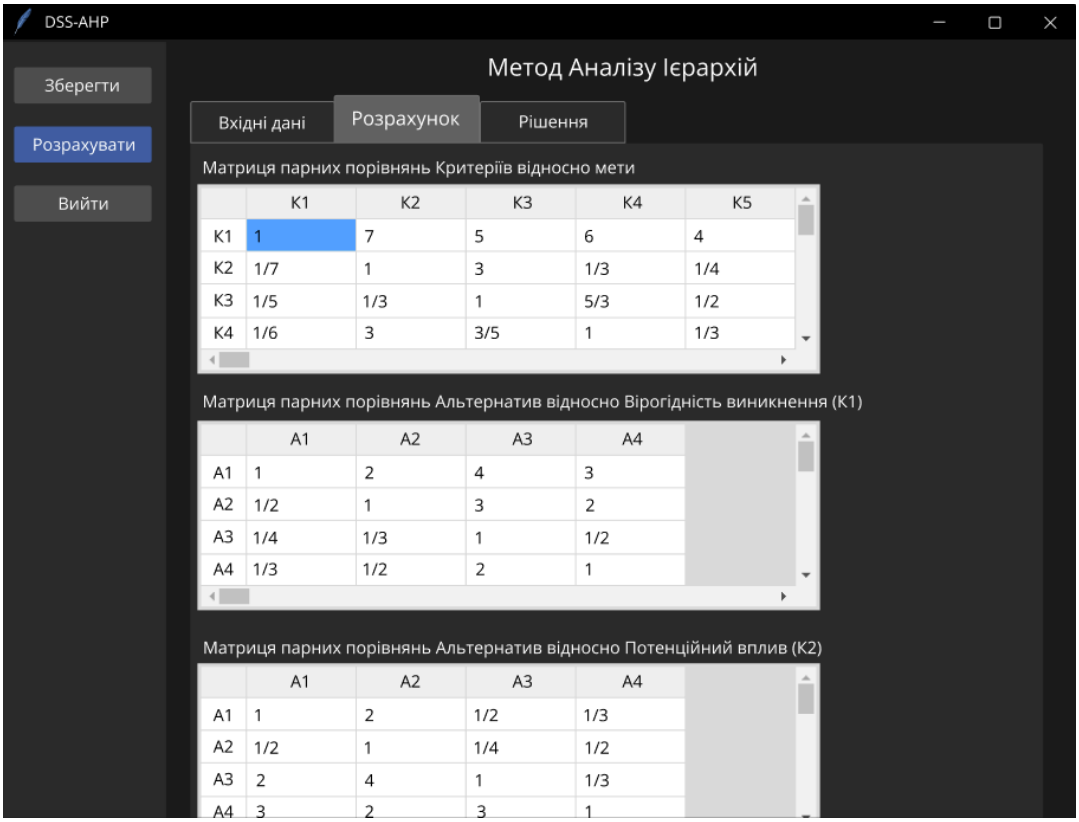

Рисунок 4.3 – Розрахунки

Після завершення розрахунків, остання частина програми надає користувачу можливість ознайомитися з результатами аналізу (рис. 4.4) . Тут він може переглянути значення глобальних пріоритетів для кожної альтернативи та оцінити їх за допомогою стовбчастої діаграми. Програма виділяє альтернативу з найвищим пріоритетом, яка є рішенням аналізу.

У цьому розділі користувач може отримати чітку візуалізацію результатів, що допомагає зрозуміти, які альтернативи є найбільш пріоритетними згідно з проведеним аналізом. За допомогою стовбчастої діаграми він може порівняти значення глобальних пріоритетів і визначити альтернативу з найвищим значенням, яка рекомендується для прийняття рішення.

Цей розділ програми надає користувачеві зручну інтерфейсну можливість візуалізувати та оцінити результати аналізу, допомагаючи йому прийняти обґрунтоване рішення на основі пріоритетів, встановлених в процесі аналізу.

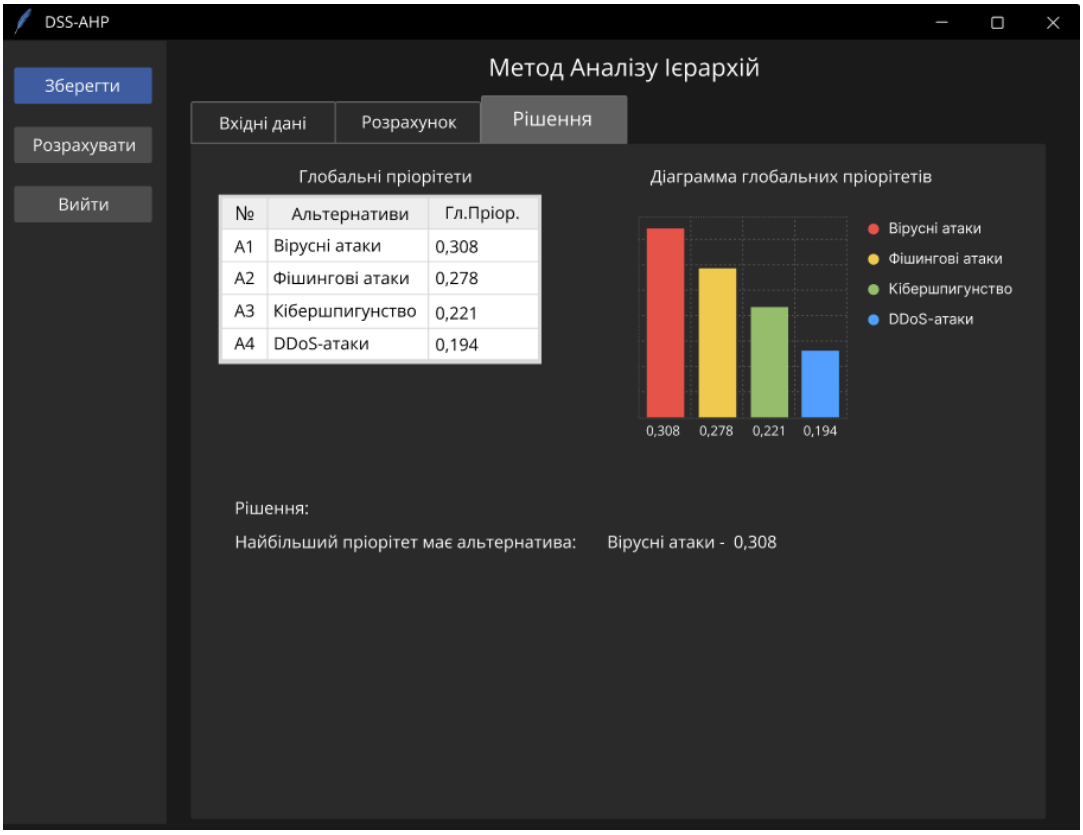

Рисунок 4.4 – Рішення

4.2 Математична частина. Заповнення матриць парних порівнянь для рівня 2

Далі будуть наведені розраховані матриці, що відображають вагові коефіцієнти та оцінки альтернатив для кожного критерію, які були отримані за допомогою методу аналізу ієрархій. Кожнен критерій буде оцінен , з використанням шкали Саати, де 1 – немає переваги, а 9 – велика перевага альтернативи.

Таблиця 4.3 – матриця порівнянь для значень пріоритетів критеріїв

	К1	К2	К3	К4	К5	К6
К1	1	7	5	6	4	8
К2	1/7	1	3	1/3	1/4	1/2
К3	1/5	1/3	1	5/3	1/2	2
К4	1/6	3	3/5	1	1/3	2/5
К5	1/4	4/3	2	3	1	3/2
К6	1/8	2	1/2	5/2	2/3	1

4.3 Математична частина .Заповнення матриць парних порівнянь для рівня 3

Аналіз загроз ІБ:

1 Вірусні атаки: Вірусні атаки полягають у використанні зловмисники спеціального програмного забезпечення, відомого як віруси, для пошкодження, злому або контролю над комп'ютерними системами. Ця загроза може мати серйозні наслідки для підприємств, включаючи втрату чутливої інформації, перерву в роботі, порушення конфіденційності даних та зниження продуктивності.

2 Фішингові атаки: Фішингові атаки є формою соціального інженерінгу, коли зловмисники намагаються отримати конфіденційну інформацію, таку як паролі, кредитні картки або особисті дані, шляхом використання підроблених електронних листів, веб-сайтів або повідомлень. Фішингові атаки можуть спричинити фінансові втрати, порушення репутації та виток конфіденційної інформації.

3 Кібершпигунство: Кібершпигунство означає незаконне отримання конфіденційної інформації шляхом вторгнення в комп'ютерні мережі чи системи. Зловмисники, які займаються кібершпигунством, можуть здійснювати шпигунські дії, зламувати паролі, викрасти корпоративні секрети, перехоплювати комунікації тощо. Це може призвести до втрати конкурентної переваги, порушення конфіденційності клієнтів та фінансових втрат.

4 DDoS-атаки: DDoS-атаки (розподілені атаки заперечення обслуговування) спрямовані на перевантаження комп'ютерних систем або мереж шляхом надсилання великого обсягу запитів з багатьох джерел. Це може призвести до відмови в обслуговуванні, перерви в роботі, фінансових втрат і порушення репутації. DDoS-атаки часто використовуються як засіб для вимагання викупу або здійснення вандалізму.

Всі ці загрози становлять серйозну небезпеку для інформаційної безпеки підприємств. Інциденти безпеки можуть мати негативний вплив на фінансовий стан, репутацію, довіру клієнтів і впливати на продуктивність підприємства. Підприємства можуть зазнавати фінансових втрат, втрати конфіденційної інформації, недоступність систем, зупинки бізнес-процесів та інших шкідливих наслідків. На основі вищепереліченого розрахуємо матриці парних порівнянь для альтернатив з використанням відносної важливості від 1 до 9.

Таблиця 4.4 – матриця оцінки альтернатив за критерієм «Вірогідність»

	A1	A2	A3	A4
A1	1	2	4	3
A2	1/2	1	3	2
A3	1/4	1/3	1	1/2
A4	1/3	1/2	2	1

Ця матриця відображає оцінки вірогідності виникнення кожної загрози ІБ в порівнянні з іншими загрозами. Значення в матриці вказують на те, наскільки вірогідно виникнення однієї загрози в порівнянні з іншими.

Таблиця 4.5 – матриця оцінки альтернатив за критерієм «Потенційний вплив»

	A1	A2	A3	A4
A1	1	2	1/2	1/3
A2	1/2	1	1/2	1/2
A3	2	4	1	1/3
A4	3	2	3	1

Ця матриця відображає оцінки потенційного впливу кожної загрози ІБ в порівнянні з іншими загрозами. Значення в матриці вказують на те, наскільки потенційно впливовою є одна загроза в порівнянні з іншими.

Таблиця 4.6 – матриця оцінки альтернатив за критерієм «Складність експлуатації»

	A1	A2	A3	A4
A1	1	1/2	1/5	3
A2	2	1	1/2	2
A3	5	2	1	4
A4	1/3	1/2	1/4	1

У цій матриці значення відображають складність експлуатації кожної загрози ІБ в порівнянні з іншими загрозами. Чим менше значення, тим менша

складність експлуатації.

Таблиця 4.7 – матриця оцінки альтернатив за критерієм «Розповсюдженість»

	A1	A2	A3	A4
A1	1	1/3	1/2	1/4
A2	3	1	1/2	1/3
A3	2	2	1	1/2
A4	4	3	2	1

У цій матриці значення відображають розповсюдженість кожної загрози ІБ в порівнянні з іншими загрозами. Чим більше значення, тим ширше розповсюдження.

Таблиця 4.8 – матриця оцінки альтернатив за критерієм «Виявлення»

	A1	A2	A3	A4
A1	1	1/2	1/5	2
A2	2	1	1/3	3
A3	5	3	1	1/2
A4	1/2	1/3	2	1

У цій матриці значення відображають виявлення кожної загрози ІБ в порівнянні з іншими загрозами. Чим більше значення, тим легше виявити загрозу.

Таблиця 4.9 – матриця оцінки альтернатив за критерієм «Потенційний збиток»

	A1	A2	A3	A4
A1	1	1/2	2	4
A2	2	1	3	5
A3	1/2	1/3	1	2
A4	1/4	1/5	1/2	1

У цій матриці значення відображають потенційний збиток, який може бути спричинений кожною загрозою ІБ в порівнянні з іншими загрозами. Чим більше значення, тим більший потенційний збиток.

4.4 Оцінка векторів пріоритетів

Для визначення пріоритетів на останньому рівні ієрархії використовуються вектори. Для цього створюються матриці парних порівнянь, і обчислюються їх максимальні власні значення, які використовуються для оцінки однорідності суджень, а також основні власні вектори, що відображають пріоритети. Аналогічний підхід використовується для матриць парних порівнянь на вищих рівнях ієрархії. Ці матриці допомагають визначити перевагу елементів на певному рівні щодо вищестоящих елементів.

Для матриці порівнянь для значень приоритетів критеріїв (табл.4.3) був розрахований такий вектор пріоритетів:

W=(0.47; 0.0792; 0.0864; 0.0834; 0.178; 0.103).

Для матриці оцінки альтернатив за критерієм «Вірогідність» (табл.4.4) був розрахований такий вектор пріоритетів:

W1=(0.446; 0.29; 0.0929; 0.171).

Для матриці оцінки альтернатив за критерієм «Потенційний вплив» (табл.4.5) був розрахований такий вектор пріоритетів:

W2=(0.171; 0.1; 0.327; 0.401).

Для матриці оцінки альтернатив за критерієм «Складність експлуатації» (табл.4.6) був розрахований такий вектор пріоритетів:

W3=(0.194; 0.226; 0.494; 0.0858).

Для матриці оцінки альтернатив за критерієм «Розповсюдженість» (табл.4.7) був розрахований такий вектор пріоритетів:

W4=(0.0929; 0.216; 0.245; 0.446).

Для матриці оцінки альтернатив за критерієм «Виявлення» (табл.4.8) був розрахований такий вектор пріоритетів:

W5=(0.158; 0.271; 0.407; 0.164).

Для матриці оцінки альтернатив за критерієм «Потенційний збиток» (табл.4.9) був розрахований такий вектор пріоритетів:

W6=(0.309; 0.453; 0.158; 0.0803).

4.5 Обчислення глобальних пріоритетів

Для визначення глобальних пріоритетів ми складемо таблицю, в яку внесемо раніше розраховані вектори пріоритетів. Шляхом множення векторів пріоритетів другого рівня на вектори пріоритетів третього рівня, ми обчислимо глобальний пріоритет. Потім результати додаватимуться уздовж кожного рядка таблиці (табл.4.10) .

Таблиця 4.10 – Розрахунок глобальних пріоритетів

	К1	К2	К3	К4	К5	К6	Гл.Пріор.
А1	0,446	0,171	0,194	0,0929	0,158	0,309	0,30762366
А2	0,29	0,1	0,226	0,216	0,271	0,453	0,2766578
А3	0,0929	0,327	0,429	0,245	0,407	0,158	0,221396
А4	0,171	0,401	0,0858	0,446	0,164	0,0803	0,19420162

Таким чином, найбільший глобальний пріоритет отримала загроза для інформаційної безпеки - вірусна атаки, яка вимагає найбільшої уваги і заходів з протидії. Вірусні атаки можуть мати серйозні наслідки, такі як втрата конфіденційної інформації, зупинка роботи систем, порушення конфіденційності даних та низька продуктивність.

У цьому розділі було розроблено програму підтримки прийняття рішень для системи, яка зосереджується на аналізі загроз інформаційній безпеці підприємства. Для забезпечення ефективного аналізу загроз було використано

метод аналізу ієрархій, що дозволяє враховувати та порівнювати різні критерії та альтернативи. Реалізація програми була здійснена за допомогою мови програмування Python.

ВИСНОВКИ

У результаті виконання дипломного проектування було розроблено програму системи підтримки прийняття рішень , яка зосереджується на аналізі загроз інформаційній безпеці підприємства. Для ефективного аналізу загроз був обраний метод аналізу ієрархій, який дозволяє враховувати і порівнювати різні критерії та альтернативи.

Отримані результати можуть бути використані для прийняття обґрунтованих рішень з питань інформаційної безпеки в організації. Зокрема, вони допоможуть ідентифікувати найбільш значущі загрози та розробити ефективні заходи щодо їх запобігання та управління ризиками.

У даній дипломній роботі була проведена детальна аналітична робота та дослідження щодо систем підтримки прийняття рішень та методів прийняття рішень . Був проведений порівняльний аналіз трьох методів багатокритеріального прийняття рішень: Метод вагових коефіцієнтів , метод аналітичної ієрархії процесів та метод ELECTRE. Цей аналіз був спрямований на визначення найбільш ефективного методу для вирішення проблеми загрози інформаційної безпеки. Під час порівняння методів було враховано їхні переваги та недоліки з погляду простоти використання, гнучкості, обліку сенсу критеріїв та можливості гібридних оцінок.

Головна мета програми СППР полягає у наданні підтримки прийняття рішень щодо інформаційної безпеки підприємства. Вона спрямована на ідентифікацію, аналіз та оцінку загроз інформаційній безпеці, а також надає рекомендації щодо впровадження заходів для запобігання та управління ризиками. Програма СППР розроблена з урахуванням потреб та пріоритетів користувача, що дозволяє її легко адаптувати до їх вимог. Завдяки динамічній обчислювальній структурі програми, користувач може зручно змінювати її параметри та налаштування через інтуїтивний інтерфейс. Це надає гнучкість та можливість персоналізації програми під конкретні потреби та вимоги користувача.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. В.В.Остроухов, М.М.Присяжнюк, О.І.Фармагей, М.М.Чеховська. Інформаційна безпека : підручник. Київ : Видавництво Ліра-К, 2021. – 412 с.
2. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. – 2012. – № 2. – С. 162-169.
3. Розорінов Г.М., Єрмошин В.В. Проблемні питання в реалізації оцінки ризиків інформаційної. Київ: Науково-видавничий центр «Лабораторія думки», 2014. – С.7
4. А.В.Олійник, В.М.Шацька. Навчальний посібник. Львів: Видавництво «Новий Світ-2000» , 2006 – 436 с.
5. Джерела загроз інформаційній безпеці. URL: https://stud.com.ua/34559/informatika/dzherela_zagroz_informatsiyniy_bezpetsi (дата звернення: 20.05.2023).
6. Інформаційна безпека підприємства: ключові загрози та засоби захисту.URL:https://www.kp.ru/guide/informatsionnajabezopasnostpredprijatija.html (дата звернення: 1.06.2023).
7. Легомінова, С. В. Теоретичні засади інформаційної безпеки підприємства . Економіка. Менеджмент. Бізнес. 2015. – № 3. – С. 87–92.
8. Голубев В.О.. Гавловський ВД., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використаная комп'ютерних технологій . Запоріжжя: Просвіта, 2001. – 252 с.
9. Волошин, О. Ф. Моделі та методи прийняття рішень: навч. посіб. К.: Центр «Київський університет», 2010. – 336 с.
10. Архипов О.Є., Касперський І.П. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації. 2007. – Вип. 2(15). – С. 13-19.

11.Пушкар О.І. Системи підтримки прийняття рішень:навч.посіб. Харків: Інжек, 2006. – 304с.

12.Ситник В. Ф. Системи підтримки прийняття рішень: навч. посіб. К.: КНЕУ, 2009. – 614 с.

13. Тоценко В.Г. Методи та системи підтримки прийняття рішень. К.: Наукова думка, 2002. - 382с

14. Moghaddam N.B., Nasiri M., Mousavi S.M. An appropriate multiple criteria decision making method for solving electricity planning problems, addressing sustainability issue. Int. Journal Environ. Sci. Tech. 2011. Vol. 8, N 3. P. 605–620

15. Multiple Criteria Decision Analysis. State of the Art Surveys. Springer, 2016. – 1365 p.

16. Файнзільберг Л. С., Жуковська О. А., Якимчук В. С. Теорія прийняття рішень. Київ: Освіта України, 2018. – 246 с.