МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА

РОБОТА 15.03 — КМР. 1939–“С” 2022.12.30. 015

ЛАХНА МИРОСЛАВА ВАЛЕРІЙОВИЧА

2023 р.

НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет інформаційних технологій

УДК 004.9-049.5

«ПОГОДЖЕНО»	**«ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ»**
Декан факультету	Завідувач кафедри
інформаційних технологій	комп'ютерних наук
Глазунова О.Г., д.п.н., професор	Голуб Б.Л., к.т.н., доцент
____ _____ 2023 р.	**____ _____ 2023 р.**

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему **«Програмне забезпечення системи підтримки прийняття рішень з інвестування у кібербезпеку об'єктів інформатизації»**

Спеціальність **121 «Інженерія програмного забезпечення»**

Освітня програма **«Програмне забезпечення інформаційних систем»**

Орієнтація освітньої програми **освітньо-професійна**

Гарант освітньої програми

к.т.н., доцент _____ Голуб Белла Львівна
(підпис)

Керівник магістерської кваліфікаційної роботи

ст. викладач _____ Міловідов Ю. О
(підпис)

Виконав _____ Лахно М.В
(підпис)

КИЇВ-2023

НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) Інформаційних технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних наук

к.т.н., доцент _____ Голуб Б. Л.
(науковий ступінь, вчене звання) (підпис) (ПІБ)

"____" _____ 2023 року

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТУ
Лахну Мирославу Валерійовичу

Спеціальність **121 «Інженерія програмного забезпечення»**

Освітня програма **«Програмне забезпечення інформаційних систем»**

Орієнтація освітньої програми **освітньо-професійна**

Тема магістерської кваліфікаційної роботи **«Програмне забезпечення системи підтримки прийняття рішень з інвестування у кібербезпеку об'єктів інформатизації»**

затверджена наказом ректора НУБіП України від **"30" грудня 2022р. №1939 – "С"**

Термін подання завершеної роботи на кафедру **"03" листопада 2023 р.**

Перелік питань, що підлягають дослідженню:

1. Дослідження процесів пошуку оптимальних стратегій за допомогою системи підтримки прийняття рішень.
2. Дослідження та аналіз існуючих математичних моделей, які використовуються для вибору стратегії інвестування у системи кібернетичної безпеки різних об'єктів інформатизації.
3. Проектування сучасної СППР для вибору оптимальних стратегій інвестування у засоби захисту інформації та системи кібернетичної безпеки об'єктів інформатизації.

Дата видачі завдання "_____"_____20___ р.

Керівник магістерської кваліфікаційної роботи _____ Міловідов Ю. О.
(підпис)

Завдання прийняв до виконання _____ Лахно М. В.
(підпис)

Зміст

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ - Інформаційна безпека;

ІР - Інформаційні ресурси ;

РОС - Розподілені обчислювальні системи;

ОПР - Особи, які приймають рішення;

ОБІ - Об’єкт інформатизації ;

СППР - Система підтримки прийняття рішень;

ФР - Фінансові ресурси ;

ЕС - Експертна система;

КБ - Кібербезпека;

ІІС - Інтелектуальні інформаційні системи;

ДС - Динамічна система;

ЗЗІ - Засоби захисту інформації;

ІнП - Інтегральний показник;

ІКС - Інформаційно-комунікаційна система;

УЗІБ – Удосконалення засобів інформаційної безпеки;

СЗІ – Система захисту інформації;

ЗІ – Захист інформації;

ООП – Об’єктно-орієнтоване програмування;

КВКС – Критично важливі комп’ютерні системи;

ІТ – Інформаційні технології;

ПЗ – Програмне забезпечення;

БД – База даних;

УЗІБ – Удосконалення засобів інформаційної безпеки;

ІС - Інформаційна система.

ВСТУП

Актуальність теми дослідження. На даний час інформація є найціннішим суспільним активом, як для будь-якої конкретної особи, так і для компаній різної форми власності. Інформація є найціннішим суспільним активом з декількох причин:

Роль в прийнятті рішень: Інформація є основою для прийняття рішень на всіх рівнях - від особистого життя до бізнесу та уряду. Якщо ми маємо доступ до відповідної, точної та зрозумілої інформації, ми можемо робити кращі розрахунки та виробляти обґрунтовані рішення.

Вартість інформації: Інформація може мати велику комерційну та стратегічну вартість. Вона може допомогти утримати конкурентну перевагу, забезпечити нові можливості для розвитку бізнесу та зробити організацію більш ефективною. Втрата важливої інформації може призвести до фінансових втрат, погіршення репутації і навіть занепаду організації.

Захист від загроз: Інформація може бути цілью кібератак, шпигунства, крадіжок та інших загроз. Важливо дбати про безпеку інформації, забезпечувати конфіденційність, цілісність та доступність даних. Захист інформації є критичним для збереження довіри та забезпечення стабільності суспільства.

Інновації та розвиток: Інформація є джерелом нових ідей, інновацій та технологічного прогресу. Вона допомагає виконувати дослідження, розробляти нові продукти, покращувати процеси та розвивати суспільство в цілому. Відкритий доступ до інформації сприяє швидкому поширенню знань та сприяє прогресу.

Вплив на громадське життя: Інформація впливає на громадське життя, політику, культуру, освіту та інші сфери. Вона допомагає формувати світогляд, підтримувати демократію, забезпечувати прозорість та взаєморозуміння між людьми.

Оскільки інформація є найціннішим суспільним активом, важливо дбати про її захист, доступність та якість. Це передбачає встановлення ефективних механізмів захисту, збереження та обміну інформацією, а також розвиток навичок критичного мислення та медійної грамотності у суспільстві..

З огляду на науковий та економічний аспекти тема магістерської роботи є, безумовно, актуальною, а здобутки можуть стати в нагоді широкому колу фахівців.

Мета і завдання дослідження. Розробка системи підтримки рішень для вибору оптимальних стратегій інвестування у засоби захисту інформації та системи кібернетичної безпеки різних об’єктів інформатизації.

Відповідно до зазначеної мети в магістерської роботи для її досягнення поставлені такі завдання:

- здійснити огляд попередніх досліджень та аналіз існуючих математичних моделей, які використовуються для вибору стратегії інвестування у системи кібернетичної безпеки різних об’єктів інформатизації;

- спроектувати та реалізувати сучасну СППР для вибору оптимальних стратегій інвестування у засоби захисту інформації та системи кібернетичної безпеки різних об’єктів інформатизації.

Об’єкт дослідження – це визначені процеси пошуку за допомогою системи підтримки прийняття рішень оптимальних стратегій інвестування у системи кібернетичної безпеки різних об’єктів інформатизації.

Предмет дослідження. Предметом дослідження магістерської роботи є методи та моделі для системи підтримки прийняття рішень для вибору стратегії інвестування у системи кібернетичної безпеки різних об’єктів інформатизації.

Методи дослідження. Для досягнення мети, поставленої в роботі, використовувалися; методи теорії ігор для розвитку моделей обчислювального ядра для системи підтримки прийняття рішень на вибір раціональної стратегії інвестування в системи кібернетичної безпеки різних об’єктів інформатизації; методи об'єктно-орієнтованого програмування для реалізації системи підтримки прийняття рішень.

Цінність одержаних результатів. Розроблена система підтримки прийняття рішень «InvestSecurely». Вище зазначена система дозволяє експертам в режимі онлайн оцінювати стратегії інвестування в різні об'єкти інформатизації, зокрема, критично важливі комп'ютерні системи.

РОЗДІЛ 1
ОГЛЯД ПОПЕРЕДНІХ ДОСЛІДЖЕНЬ ТА АНАЛІЗ ВЖЕ ІСНУЮЧИХ МАТЕМАТИЧНИХ МОДЕЛЕЙ З ІНВЕСТУВАННЯ У КІБЕРБЕЗПЕКУ ОБ'ЄКТІВ ІНФОРМАТИЗАЦІЇ

1.1 Актуальність досліджень, пов’язаних із проблематикою інвестування у кібербезпеку об’єктів інформатизації

Безперечним є факт, що забезпечення інформаційної безпеки (ІБ) – це складне та витратне завдання. Інвестування у кібербезпеку та захист інформації є надзвичайно важливим з кількох причин [1-20]:

1. Захист від кібератак: У сучасному цифровому світі кібератаки стають все більш поширеними та складними. Хакери та зловмисники постійно шукають нові способи проникнення в системи та отримання доступу до конфіденційної інформації. Інвестування у кібербезпеку допомагає забезпечити захист від таких атак, запобігти витоку даних та захистити бізнес від фінансових втрат.

2. Захист особистих даних: Вкладання коштів у кібербезпеку є одним із способів захисту особистих даних. Усі ми зберігаємо важливу інформацію на своїх комп'ютерах, смартфонах та в хмарних сховищах. Без належного захисту ці дані можуть стати жертвами кіберзлочинців. Інвестування у кібербезпеку допомагає підтримувати конфіденційність та цілісність особистої інформації.

3. Захист бізнесу: Успішне функціонування бізнесу в сучасних умовах неможливе без належного захисту інформації. Компанії зберігають велику кількість конфіденційних даних про своїх клієнтів, партнерів та власну діяльність. Зламана система може призвести до значних фінансових втрат, втрати довіри клієнтів і пошкодження репутації компанії. Інвестування у кібербезпеку допомагає забезпечити надійний захист бізнес-інформації та зменшити ризики витоку даних.

4. Виконання регуляторних вимог: У багатьох країнах існують законодавчі норми та регуляції, що стосуються захисту інформації та кібербезпеки. Бізнеси зобов'язані дотримуватися цих вимог і забезпечувати належний рівень захисту.

Інвестування в кібербезпеку допомагає виконувати ці вимоги та уникнути штрафів та інших правових наслідків.

Захист інфраструктури: Кіберзагрози можуть націлитися не лише на інформацію, але й на критичну інфраструктуру, таку як електроенергетика, транспортна система, комунікаційні мережі тощо. Інвестування у кібербезпеку допомагає забезпечити надійний захист цих систем, що є критичним для функціонування суспільства.

Вкладання коштів у кібербезпеку та захист інформації є важливою інвестицією, яка допомагає забезпечити безпеку особистих даних, бізнесу та суспільства в цілому.

Зрозуміло, що за таких умов складність багатокритеріального оптимізаційного завдання управління ресурсами сторони забезпечення ІБ ОБІ визначається багатовимірністю складу засобів захисту інформації (ЗЗІ) та складністю розподілених обчислювальних структур ОБІ. Очевидно, що в процесі вирішення такого завдання необхідно залучити потенціал інтелектуалізованих систем підтримки прийняття рішень (далі СППР). Подібні модульні [20-40] або кластерні [6] СППР у завданнях управління ІБ ОБІ можна використовувати як комплекс взаємозалежних систем. Подібні СППР, як правило, базуються на синергетичних ансамблях методів та моделей. Один з таких ансамблів методів та моделей, виключно важливий у такій підзадачі управління ІБ ОБІ, як задача пошуку раціональної стратегії інвестування у засоби захисту інформації для розподіленої обчислювальної системи (РОС) ОБІ. Дійсно, ОПР, необхідно оцінювати пріоритетність вкладення своїх фінансових ресурсів (ФР) у такі напрями розвитку ІБ РОС як [40-60]:

– забезпечення кібернетичної стійкості ОБІ;

– інноваційні технології у завданнях контролю показників ризику реалізації інформаційних загроз та забезпечення необхідного рівня ІБ ОБІ;

– культура ІБ;

– ІБ інфраструктури РОС або в цілому ОБІ;

– безпека прикладного програмного забезпечення (ПЗ);

– безпека технологій обробки даних;

– інші.

Зауважимо, що як показано в [7-27], у спеціалізованому сегменті ринку продуктів та послуг ІБ нововведення не завжди корисні. Інновації у сфері ІБ найчастіше – це результат інвестицій у розробку та отримання нових знань, вироблення ідей щодо оновлення складу систем ІБ.

Слід зазначити, що інноваційний процес у сфері ІБ базується на складній системі взаємозумовлених та взаємопов'язаних заходів. Крім того, важливо, які ресурси є в наявності в інвесторів: фінансові, організаційні, наукові, технологічні, виробничі, організаційні.

Таким чином, усі інноваційні проєкти у сфері ІБ можна класифікувати, як комплекс взаємоузгоджених цілей та програм, спрямованих на підвищення ефективності системи ІБ конкретного ОБІ.

В [16-33] зауважується, що ймовірність втрат, які виникають при невірно обраній стратегії вкладення фінансових ресурсів компанії в ІБ, досить велика. Хоча залишається фактом те, що сфера ІБ за своїм характером зовсім не сприяє інноваційності.

Захисні контури кібербезпеки великих компаній побудовані на основі кількох основних принципів:

Принцип захисту від зовнішніх загроз: Компанії встановлюють захисні механізми для запобігання зовнішнім загрозам, таким як хакерські атаки, фішинг, віруси тощо. Це включає в себе використання мережевих брандмауерів, інтрузійних систем виявлення та запобігання, антивірусного програмного забезпечення та інших технологій для виявлення та блокування небажаних дій.

Принцип внутрішнього захисту: Компанії використовують заходи безпеки для захисту внутрішніх ресурсів та інформації від внутрішніх загроз. Це може включати в себе встановлення систем контролю доступу, шифрування даних, використання мультифакторної аутентифікації та моніторингу діяльності користувачів.

Принцип неперервності бізнесу: Компанії розробляють плани неперервності бізнесу, які передбачають відновлення роботи систем та процесів у разі виникнення інцидентів. Це включає в себе резервне копіювання даних,

розробку планів відновлення, тестування резервних систем та тренування персоналу.

Принцип моніторингу та виявлення загроз: Компанії використовують системи моніторингу та виявлення загроз для постійного контролю за інформаційною системою. Це допомагає виявляти незвичайну або підозрілу активність, а також своєчасно реагувати на потенційні загрози.

Принцип навчання та свідомості користувачів: Компанії надають навчання та підвищують свідомість свого персоналу про кібербезпеку. Це включає в себе проведення навчальних семінарів, надання рекомендацій щодо безпечних практик в роботі з інформацією та використанням технологій.

Принцип постійного оновлення: Компанії постійно оновлюють свої захисні механізми та технології, щоб залишатися попереду зловмисників. Це включає в себе встановлення оновлень програмного забезпечення, патчів безпеки та використання новітніх технологій захисту.

Ці принципи допомагають побудувати ефективні захисні контури кібербезпеки, які допомагають великим компаніям захистити свою інформацію, ресурси та бізнес від кіберзагроз, див. рис. 1.1.

Рисунок. 1.1. Основні аналітичні методи оцінки інформаційних загроз

Експертна оцінка загроз інформаційної безпеки - це процес аналізу та оцінки потенційних загроз, які можуть вплинути на безпеку інформаційних систем. Це важлива складова частина стратегії кібербезпеки, яка допомагає виявити і розуміти потенційні ризики, що дозволяє прийняти належні заходи для їх запобігання або зменшення впливу.

Експертна оцінка загроз інформаційної безпеки складається з кількох

етапів:

– Ідентифікація загроз: Перший етап полягає в ідентифікації потенційних загроз, які можуть вплинути на безпеку інформаційних систем. Це можуть бути такі загрози, як хакерські атаки, фішинг, зловмисні програми, витоки даних, недбалість персоналу тощо;

– Аналіз загроз: На другому етапі проводиться детальний аналіз кожної ідентифікованої загрози. Це включає в себе визначення їх потенційного впливу на інформаційні системи, виявлення вразливостей, які можуть бути використані загрозами, та оцінку ймовірності виникнення цих загроз;

– Оцінка ризику: На третьому етапі проводиться оцінка ризику, пов'язаного з кожною ідентифікованою загрозою. Це включає в себе визначення рівня впливу загрози на безпеку інформаційних систем та визначення ймовірності виникнення цих загроз;

– Визначення прийняття рішень: На цьому етапі аналізується отримана інформація про ризики та загрози, і приймаються рішення щодо того, які заходи безпеки потрібно вжити для запобігання або зменшення впливу цих загроз. Це може включати в себе впровадження технічних рішень (наприклад, встановлення брандмауерів, антивірусного програмного забезпечення), організаційних заходів (наприклад, політик інформаційної безпеки, навчання персоналу) та фізичних заходів (наприклад, контроль доступу до приміщень, захист фізичних носіїв даних);

– Моніторинг та оновлення: Останній етап полягає в постійному моніторингу загроз та оцінці ризиків, а також в оновленні заходів безпеки відповідно до змін у загрозах та технологіях. Це допомагає забезпечити актуальний рівень захисту інформаційних систем. [50-60].

Результати подібного аналізу наведені на рис. 1.2.

Рисунок 1.2. Діаграма відсоткового співвідношення основних кіберзагроз підприємств [50-60]

Оцінка загроз інформаційної безпеки проводиться компаніями з наступними цілями [50-60]:

Виявлення потенційних ризиків: Оцінка загроз допомагає компаніям виявити потенційні ризики, які можуть вплинути на безпеку їх інформаційних систем. Це дозволяє ідентифікувати потенційні слабкі місця та небезпеки, які можуть призвести до витоку даних, порушення нормативних вимог або зупинки бізнес-процесів.

Запобігання кібератакам: Оцінка загроз допомагає компаніям розуміти, які види кібератак можуть бути спрямовані на їх інформаційні системи, і дозволяє прийняти належні заходи для запобігання таким атакам. Це включає в себе встановлення захисних механізмів, розробку стратегії кібербезпеки та вдосконалення політик безпеки.

Захист конфіденційності та цілісності даних: Оцінка загроз допомагає компаніям виявити потенційні загрози безпеці даних, такі як витоки даних, несанкціонований доступ або зміна даних. Це дозволяє вжити відповідних заходів для забезпечення конфіденційності та цілісності даних.

Забезпечення неперервності бізнесу: Оцінка загроз допомагає компаніям ідентифікувати потенційні загрози, які можуть призвести до перерви в роботі бізнес-процесів. Це дозволяє розробити плани неперервності бізнесу та вжити заходів для забезпечення швидкого відновлення роботи в разі виникнення інциденту.

Забезпечення відповідності нормативним вимогам: Оцінка загроз допомагає компаніям переконатися, що вони відповідають нормативним

вимогам з питань кібербезпеки. Це включає в себе дотримання вимог законодавства, стандартів, регуляторних вимог та інших вимог, що стосуються безпеки інформації.

Оцінка загроз інформаційної безпеки є важливим інструментом для компаній, оскільки допомагає їм розуміти потенційні загрози та ризики, а також приймати належні заходи для забезпечення безпеки інформаційних систем та даних..

Отже, все це дає підстави говорити про те, що актуальність тематики дослідження обґрунтована. І в рамках цієї роботи пріоритетним завданням стане розвиток математичних моделей для обчислювального ядра СППР, призначений для ОПР, у завданнях управління ІБ ОБІ.

У роботі [30] автори відзначають, що на ринок інвестицій у розвиток апаратно-програмних засобів ІБ позитивно впливають не всі інновації. А це найчастіше призводить до розбіжностей думок експертів щодо їх доцільності, коли необхідно розглянути питання про нові інвестиції в ІБ ОБІ.

У роботі [24] зазначається, що інвестиційні проєкти у сфері ІБ можуть розглядатися як система взаємопов'язаних цілей і програм ІБ. Однак подальшого розвитку у вказаній роботі це твердження не отримало.

Як зазначають автори [14, 60], досягнення заданого рівня ІБ ОБІ залежить від успішного вирішення цілого комплексу завдань: фінансових, конструкторських, виробничих, організаційних, дослідницьких, комерційних та ін. Авторами даного дослідження не наводиться оцінка потенціалу використання СППР у подібних завданнях, пов'язаних зі сферою ІБ.

1.2 Аналіз моделей інвестування у кібербезпеку об’єктів інформатизації

Найпоширеніша у практичному застосуванні економічна модель (далі – модель ГЛ) була запропонована у 2002 році відомими американськими дослідниками з університету Меріленд Lawrence A. Gordon та Martin P. Loeb [58]. Їх робота представляє економічну модель, що визначає оптимальну суму

інвестицій захисту заданого набору інформації. Модель ГЛ враховує вразливість інформації для злому безпеки та потенційну втрату у разі такого злому. Показано, що для цієї потенційної втрати компанія не обов'язково має зосереджувати свої інвестиції на інформаційних наборах із найвищою вразливістю [1-40]. Оскільки надзвичайно вразливі набори інформації можуть бути надто коштовними, затратними для захисту, то компанії краще зосередити свої зусилля на інформаційних наборах із вразливістю середнього рівня. Аналіз також передбачає, що з максимізації очікуваної вигоди від інвестицій захисту інформації фірма має витратити лише невелику допустиму частину очікуваних збитків через порушення безпеки [59].

Структура моделі статична. А це означає, що рішення і результат настають одночасно, а динамічні ефекти, зокрема, залежність грошей від часу, не враховується. Інформаційний набір може набувати різних форм, таких як список клієнтів, бухгалтерська книга кредиторської заборгованості,

Якщо λ - грошовий збиток, спричинений порушенням безпеки інформаційного набору; t – імовірність нападу, $t \in [0,1]$; ν - вразливість інформації, під якою розуміють імовірність того, що за відсутності інвестицій атака буде успішною, що завдають шкоди λ; $0 \le \nu \le 1$; z - витрати на захист інформації.

Тоді для моделі $\lambda = const$, хоча практично $\lambda = \lambda(t)$ λ. Величина t належить до одиночного нападу (одночасне настання декількох нападів не розглядається).

Також розглядають й інші величини: νt - імовірність збитків внаслідок атаки; $L = t\lambda$ - потенційні збитки, пов'язані з інформаційним активом; $S(z,\nu)$ – імовірність порушення безпеки.

Слід зазначити, природа інформаційної вразливості та інформаційної безпеки призводить до розгляду наступних припущень щодо $S(z,\nu)$:

– $S(z,0) = 0$ для всіх z. Тобто, якщо набір інформації повністю невразливий, він залишиться ідеально захищеним для будь-якого обсягу інвестицій, що вкладаються в безпеку, включаючи нульові інвестиції.

– Для всіх ν, $S(0,\nu)=\nu$. Тобто, якщо взагалі немає інвестицій в інформаційну безпеку, то ймовірність порушення безпеки, зумовлена реалізацією загрози, залишиться незмінною.

– Для всіх $\nu \in (0,1)$ та всіх $z, S_z(z,\nu)<0$ і $S_{zz}(z,\nu)>0$, де S_z позначає часткову похідну по z і S_{zz} позначає часткову похідну з S_z до z. Таким чином, чим більше інвестицій в інформаційну безпеку, тим інформація стає більш захищеною. Крім того, існує припущення, що для всіх $\nu \in (0,1)$, $\lim S(z,\nu) \to 0$, як $z \to \infty$. Тому, на думку дослідників, чим значніші засоби вкладаються в безпеку, ймовірність порушення безпеки t разів $S(z,\nu)$, тобто може наблизитися до нуля [58, 60].

Очікувані вигоди від інвестицій у інформаційну безпеку, що позначаються як EBIS (Expected Benefits of an Investment in Information Security), дорівнюють скороченню очікуваних збитків фірми, пов'язаних із додатковою безпекою:

$$EBIS(z) = [v - S(z,v)]L. \tag{1.1}$$

Очікуваний чистий прибуток від вкладення інвестицій у інформаційну безпеку (Expected Net Benefits from an Investment in Information Security, ENBIS) дорівнює різниці EBIS та вартості інвестицій:

$$ENBIS(z) = [\nu - S(z,\nu)]L - z. \tag{1.2}$$

Оптимальним розміром інвестицій вважають $z^*(v)$, при якому $ENBIS(z)$ досягає максимального значення.

В [58, 60] запропоновано два класи функцій вразливості, що відповідають умовам 1.3.

Автори визначили клас показових функцій:

$$S^I(z,\nu) = \frac{\nu}{(\alpha z+1)^\beta}, \tag{1.3}$$

де параметри $\alpha > 0$, $\beta \geq 1$ є заходами продуктивності інформаційної безпеки (при заданих ν та z ймовірність порушення безпеки зменшується як для α, так і для β). З умови $ENBIS_z'(z^*) = 0$ випливає, що оптимальний розмір інвестицій у кібербезпеку.

Ймовірність порушення безпеки відноситься до ймовірності того, що стан безпеки буде порушений або виникнуть негативні події, пов'язані з безпекою. Це

можуть бути кібератаки, фізичні вторгнення, витоки інформації, крадіжки даних та інші загрози безпеці.

Для зменшення ймовірності порушення безпеки можна вжити наступні заходи [58, 60].:

Оцінка ризиків: Першим кроком є оцінка ризиків, пов'язаних з безпекою. Це включає ідентифікацію потенційних загроз, вразливостей та потенційних наслідків порушення безпеки. Оцінка ризиків допомагає визначити найбільш критичні області та встановити пріоритети для заходів з підвищення безпеки.

Розробка стратегії безпеки: На основі оцінки ризиків розробляється стратегія безпеки, яка включає в себе встановлення політик, процедур, технічних засобів та навчання персоналу. Стратегія безпеки повинна враховувати специфіку організації та її інформаційних потреб.

Технічні заходи безпеки: Використання технічних заходів безпеки, таких як файрволи, антивірусне програмне забезпечення, системи виявлення вторгнень та шифрування даних, може значно зменшити ризик порушення безпеки. Важливо регулярно оновлювати та підтримувати ці заходи [58, 60].

Організаційні заходи безпеки: Організаційні заходи безпеки включають в себе встановлення політик безпеки, контроль доступу, навчання персоналу та забезпечення свідомості щодо безпеки. Регулярне навчання персоналу про потенційні загрози та процедури безпеки може знизити ризик людського фактору [58, 60].

Моніторинг та аналіз: Систематичний моніторинг безпеки та аналіз потенційних загроз допомагають виявляти вразливості та реагувати на них вчасно. Це може включати моніторинг мережі, журналів подій, аудитів безпеки та проведення випробувань на проникнення.

Свідомість та культура безпеки: Важливо створити свідомість та культуру безпеки серед всього персоналу. Це може включати навчання про загрози безпеці, практикування безпечних поведінко для створення середовища, де безпека є пріоритетом.

Попри те, що модель Gordon–Loeb після опублікування була визнана в науковому середовищі та доповнена як іншими авторами [40-60], так і самими Lawrence A. Gordon і Martin P. Loeb [60], багато питань все ще потребують доопрацювання та вирішення. Беззаперечним фактом є те, що автори моделі вперше ґрунтовно розглянули вказану проблему та чітко визначили функцію вразливості, яка є ключовим показником інформаційної безпеки.

Модель, запропонована у роботах [58, 60], наразі стала однією з основних, які використовуються для оцінки інвестицій в ІБ ОБІ. Слід відзначити, що як для самої моделі, так і для її численних модифікацій, наприклад, [58, 60], притаманні певні недоліки. Зокрема, у [40-60] показано, що формально апроксимативний спосіб побудови моделі виключає можливість обліку при формуванні структури системи ІБ реальні механізми врахування та обліку інтересів інвесторів. А це призводить до суттєвого обмеження практичних аспектів застосування зазначеної моделі та об'єктивності отриманих висновків.

Автори [58, 60] вважають, що розвиток такого напряму прикладних досліджень, як математична підтримка прийняття рішення під час вибору раціональної стратегії інвестування в ІБ, має супроводжуватися синтезом нових моделей та методів. Програмна реалізація наведених у роботах моделей не описана. В [40-60] автори відзначають, що стосовно даного класу завдань, найбільш адекватним підходом у процесі пошуку рішення буде застосування теорії ігор.

Автори [57] зазначають, що категорія програмних продуктів типу СППР та експертних систем (ЕС) сприяє спрощенню завдання пошуку раціональних стратегій для інвесторів у сфері ІБ.

В роботі [58, 60] досить детально розглянуті різні підходи з погляду використовуваного в таких моделях математичного апарату. Однак програмна реалізація запропонованої моделі не наведена.

Автори [60] детально описують застосування класичних економіко-математичних моделей. Однак ці моделі в більшості ситуацій, пов'язаних з оцінкою вкладень, не враховують багато параметрів інвестування у складні проєкти у сфері ІБ ОБІ. Як показав аналіз подібних досліджень, більшість

моделей та алгоритмів, наведених у проаналізованих вище роботах, все ж не містять реальних рекомендацій та прогнозованих оцінок для інвесторів у сфері ІБ. СППР, що пропонують сьогодні на ринку програмного забезпечення, складно адаптувати до завдань ІБ. Це стосується й підтримки рішень під час вибору стратегій інвесторів для побудови ефективної системи ІБ для конкретного ОБІ. Основний недолік подібних програмних продуктів, описаних у роботах [58, 60] – це невисока інформативність отриманих результатів. Зокрема, на думку дослідників, досить складно оцінити перспективність інвестиційних проєктів та варіанти дій інвесторів у сфері ІБ ОБІ.

З огляду на все викладене вище, робимо висновок, що успішне розв’язання завдань вибору раціональної стратегії інвестування в інформаційну безпеку ОБІ, стало основою успішного ведення бізнесу [50-60]. Це особливо помітно з досвіду реалізації успішних проєктів розгортання систем ІБ для тих компаній, що займаються інноваційними розробками. Проте, мало мати достатні фінансові ресурси (ФР), спрямовані на реалізацію проєктів у сфері ІБ ОБІ. Необхідно також мати інструментарій для прогнозування та оцінювання варіантів стратегій вкладення ФР у відповідний проєкт. Як зазначалося вище, ефективна підтримка рішень у подібних проєктах не відбувається без застосування ІТ, і, зокрема, СППР. У багатокритеріальних оптимізаційних задачах, що стосуються пошуку аналітичних рішень, основні завдання виконує обчислювальне ядро аналогічних СППР. Наприклад, у контексті вирішуваної проблеми, з'являється можливість конструктивно визначати раціональні стратегії розподілу ФР на реалізацію складних проєктів у галузі ІБ ОБІ.

В [40-60] показано, що універсальний метод багатокритеріальної оптимізації розподілу ФР, що виділяються на побудову контурів ІБ розподілених обчислювальних систем для ОБІ, є поки що відсутнім. Це, безперечно, означає, що рішення, позначеного завдання, і обчислювальне ядро СППР, повинні включати до свого складу ансамбль моделей.

В [58, 60] обґрунтовано структуру системи захисту інформаційних джерел організації, яка дасть змогу визначити його потенційні збитки від витоку інформації, впровадження якої забезпечить компроміс між конфіденційністю,

доступністю та упущеною вигодою від обмеженого користування інформаційними джерелами організації та необхідними витратами на надійний її захист.

Визначення засобів захисту інформації включає наступні кроки:

Ідентифікація активів: Спочатку необхідно ідентифікувати всі активи, які потребують захисту. Це можуть бути фізичні активи (комп'ютери, сервери, мережеве обладнання), програмне забезпечення, дані, інформаційні системи, інтелектуальна власність та інше.

Оцінка ризиків: Наступним кроком є оцінка ризиків, пов'язаних з цими активами. Ризик оцінюється шляхом виявлення потенційних загроз, вразливостей та імовірності виникнення негативних подій. Це допомагає визначити, які активи потребують найбільшого захисту і які загрози потребують пріоритетного усунення.

Вибір захисних заходів: На основі оцінки ризиків визначаються захисні заходи, які можуть бути використані для зменшення ризиків і забезпечення безпеки інформації. Це можуть бути технічні засоби (файрволи, антивірусне програмне забезпечення, шифрування даних), організаційні заходи (політики безпеки, навчання персоналу), фізичні заходи (контроль доступу, відеоспостереження) та інші.

Розробка стратегії захисту: На основі вибраних захисних заходів розробляється стратегія захисту інформації. Це включає визначення послідовності та пріоритету застосування заходів, а також встановлення вимог щодо безпеки для всіх сторін, які займаються обробкою та зберіганням інформації.

Впровадження та оцінка ефективності: Після розробки стратегії захисту, засоби захисту інформації впроваджуються в організацію. Після впровадження проводиться оцінка ефективності захисних заходів, щоб переконатися, що вони діють належним чином та відповідають вимогам безпеки.

Постійна підтримка і оновлення: Захисні заходи повинні бути постійно підтримувані і оновлювані, оскільки загрози кібербезпеки постійно змінюються. Це включає регулярне встановлення оновлень програмного забезпечення,

моніторинг системи безпеки та аналіз нових загроз.

Визначення засобів захисту інформації є складним процесом, який вимагає комплексного підходу та врахування специфіки організації та її інформаційних потреб.

Особливо це стає помітним, якщо представити ліву частину рисунка в тривимірних координатах, а саме *PT0U*. На рис. 1.4 показано деякі результати моделювання параметрів системи захисту інформаційних ресурсів організації.

Для протидії одній і тій самій загрозі зазвичай існує декілька засобів захисту, що випускаються різними виробниками, розрізняються за вартістю реалізації та забезпечують різну можливість запобігання загрозам. У найпростішому випадку можна припустити, що кожен засіб захищає від однієї загрози. На жаль, вказане припущення не відповідає реальним умовам, за якими розвивається ринок засобів інформаційної безпеки, тому необхідно створення нових моделей підтримки прийняття рішень у області кібербезпеки, що відповідають реальному стану справ, тобто, коли кожен засіб захисту протидіє довільній кількості загроз, причому можливість запобігання кожній загрозі різна.

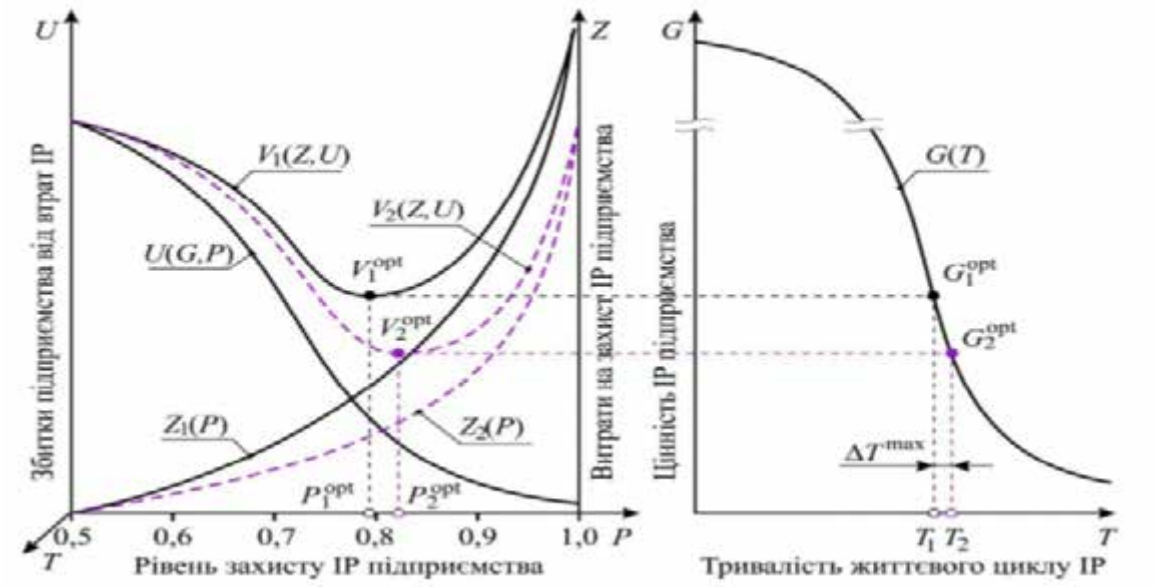


Рисунок 1.3. Модель оцінювання параметрів системи захисту інформаційних даних підприємства [50]

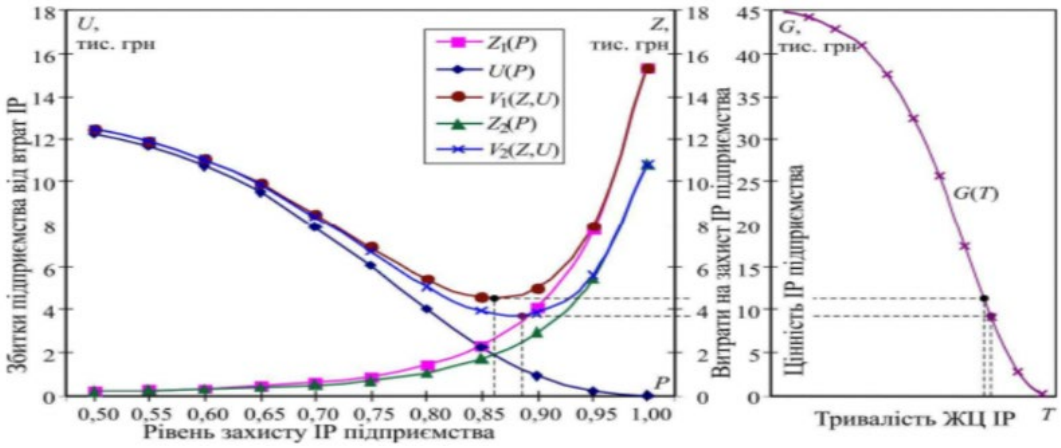


Рисунок 1.4. Результати моделювання параметрів системи захисту інформаційного ресурсу організації[60]

У роботах [60] показано, що досить ефективним підходом у вирішенні подібного класу оптимізаційних завдань є використання теорії ігор. Насамперед йдеться про такий розділ теорії ігор, як багатокрокові ігри якості з декількома термінальними поверхнями [60, 61]. Проте, слід зазначити, що для складних прикладних ігрових моделей властива висока розмірність, як для простору керівних параметрів, так і для критерійного простору. А крім того, якщо розглядати групу інвесторів у проєкти розвитку кібербезпеки та захисту інформації як коаліцію, то для компонентів векторних показників ефективності оцінювання такої коаліції, характерними будуть гладкість та наявність розривів. Розглядаючи складні інвестиційні проєкти, ігрова модель у чистому вигляді робить досить складним або неможливим застосування класичних ігрових моделей, а також відомих оптимізаційних методів. Це й актуалізує необхідність формування нових підходів до вирішення такого класу завдань. Наприклад, з урахуванням застосування генетичних алгоритмів.

У роботах [60] розглядаються можливості щодо застосування генетичних алгоритмів (ГА) для вирішення завдань, пов'язаних із вибором стратегії інвестора. У зазначених публікаціях доведено, що ГА підтримує популяцію (група хромосом), яка є претендентом на оптимальне рішення. Використавши ймовірні оператори, як кандидатури претендентів, автори наведених досліджень, прагнули отримати популяції, найбільш придатні до умов, поставлених для конкретного завдання. Проте дані ГА, фактично, являли собою прості операції з

обміну та копіювання частин хромосом. Цей підхід не завжди спрацьовує для такої предметної області, як процедура інвестування у складні проєкти.

У багатьох дослідженнях [50-60] автори показують, що передумова ефективної реалізації механізмів управління інвестиціями у складні проєкти у сфері ІТ, у тому числі пов'язані з КБ, - це завдання отримання якісних прогнозованих оцінок віддачі від інвестицій у розвиток кібербезпеки ОБІ та зменшення ризиків для відповідних бізнес-процесів. Така прогнозована інформація може надати менеджменту підприємств дані для більш детального визначення точок зростання економічних показників компаній шляхом мінімізації ризиків, пов'язаних із втратою інформаційних активів, наприклад, через несанкціонований доступ до них з боку комп'ютерних зловмисників.

У роботах [50-60] автори показали, що більшість запропонованих моделей ґрунтуються на короткостроковому прогнозуванні інвестицій у кібербезпеку ОБІ. Відсутність прогнозованих оцінок динаміки та перспективи розвитку різних інвестиційних проектів КБ, раціональних чи оптимальних варіантів розвитку різних проєктів з імплементації апаратно-програмних комплексів ЗЗІ, організаційних та інших заходів щодо ЗІ, загалом може призвести до невірного вибору пріоритетних напрямів розвитку системи управління інформаційною безпекою ОБІ, або ж породити складнощі, пов'язані з неправильною стратегією розміщення коштів інвестиційних проєктів у систему кібербезпеки ОБІ. Звідси випливає потреба посилення потенціалу функції прогнозування, зокрема, з урахуванням застосуванням положень теорії ігор.

Woohyun Shim, зважаючи на роботи Gordon-Loeb [50-60], розробив свою модель взаємозалежних ризиків для двох однакових підприємств [59, 60].

В результаті проведеної роботи було вивчено та схематично зображено взаємозв'язок серед проблем зовнішніх ефектів та типами атак, як показано на рис. 1.5.

Рисунок 1.5. Зв'язки між зовнішніми ефектами та типами атак [60]

У [50-60] описано модель Малюкова-Ахметова-Лахно стратегій інвестування у системи кібербезпеки.

Порівнявши різні наукові роботи [1-60], можна визначити, що ефективне управління фінансовими ресурсами для захисту інформації є надзвичайно важливим завданням для організацій. Процес інвестування вимагає великих зусиль, від збору і обробки інформації до розробки відповідних інвестиційних стратегій. Ефективність фінансових інвестицій та контроль над цим процесом важливі як для фінансової сфери, так і для захисту інформації.

Проте багато досліджень, хоч і мають економічний характер, ігнорують тенденції використання інформаційних технологій у контролі та прийнятті рішень для інвестиційних проєктів, див. табл. 1.1.

Головним недоліком таких досліджень є відсутність конкретних рекомендацій щодо формування фінансових інвестиційних стратегій.

У роботах [55, 60] для програмної реалізації СППР та вибору раціональної стратегії інвестування у проєкти із забезпечення кібербезпеки об'єкта інформатизації можна пропонується використовувати математичний апарат білінійних динамічних ігор якості. Це дає результати, відповідно до яких кожна точка у 3-х мірному просторі [60], характеризує відповідну стратегію інвестора, див. рис. 1.6. Тобто кожна точка буде набором певних компонентів інвестування. Ці компоненти відповідають фінансові ресурсам інвестора які від вкладає у КБ. Набори точок, що розташовуватимуться на термінальній поверхні кожного з інвесторів, характеризують конкретні інвестиційні програми. Самі собою рішення з урахуванням застосування системи диференціальних рівнянь для

білінійної динамічної гри якості з кількома термінальними поверхнями дають досить великий розкид варіантів точок на термінальних поверхнях інвесторів. А це, як показали проведені дослідження, диктує необхідність витрат додаткового часу для аналізу цих точок та пошуку області переваги інвестора. [60].

Таблиця 1.1 – Результати аналізу математичних моделей стратегій інвестування для систем кібербезпеки

(на основі аналізу робот [35, 56, 60])

	Математичні моделі стратегій інвестування для інформаційної безпеки					
Критерії порівняння	Модель Gordon–Loeb	Модель Woohyun Shim	Модель Архіпова	Модель Лев-ченко-Прус	Моде-ль Зади-раки	Модель Малюкова - Аметова-Лахно
Розрахунок оптимального рішення в динамічному режимі	-	-	+	+	-	+
Врахування вразливості об'єктів	-	-	+	+	-	-
Оптимізація розподілу ресурсів	+	+	-	+	-	+
Облік засобів захисту	+	+	+	+	+	-

В результаті розв'язання системи рівнянь авторами отримано таку сукупність точок у багатовимірному просторі рішення, як це показано на рис. 1.7 [50-60].

Обчислення проводилися з урахуванням множинності факторів, що

характеризують багатовимірність процесу інвестування в КБ ОБІ.

Це означатиме, що в СППР, що розробляється, буде запущено в дію інструментарій для графічного представлення в просторах розмірності навіть більше ніж три.

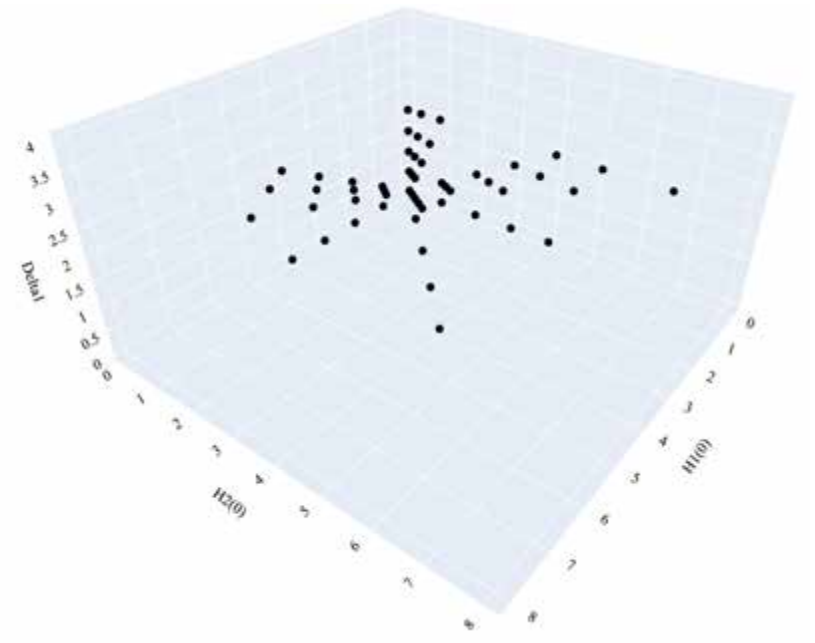


Рисунок 1.6. Залежність переваги множин W_1 для першого інвестора в КБ ОБІ для 3-х змінних [35, 56, 60]

Змінюючи параметри інвестування для гравців у завданнях забезпечення інформаційної безпеки, можна домогтися того, щоб рівновага Неша забезпечувала саме ті стратегії гравців, які необхідні для досягнення потрібного рівня інформаційної безпеки об'єкта моделювання. Більше того, навіть якщо раніше гравці обирали "непотрібні" (з точки зору управління інвестиціями щодо забезпечення стратегії ІБ, то вони (після відповідної зміни параметрів) обов'язково самі будуть виконувати "потрібну" діяльність щодо її забезпечення. Таким чином, створюються умови для самоорганізації суб'єктів в системі управління інформаційною безпекою, що дозволить значно скоротити сумарні необхідні фінансові ресурси для забезпечення заходів ІБ.

Як бачимо, частина цих наборів, разом із наборами компонентів ФР першого інвестора належить множині, що гарантує продовження процедури інвестування у проєкти ІБ. Інша частина належить множині, у якій другий

інвестор неспроможний продовжити інвестування. Тоді, вибираючи із цих значень мінімальні (по кожному компоненту), отримаємо для кожного ФР множину першого інвестора, яка буде належати перевазі множин першого інвестора [50-60].

Отже, вибираючи з наявних значень мінімальні за кожною компонентою, ми можемо отримати безліч переваг для першого гравця. Зазначимо, що внаслідок білінійності системи диференціальних рівнянь і багатовимірності розглянутого завдання, знаходження множини переваг інвесторів за допомогою інших підходів неможливо.

В контексті магістерської роботи Білінійна система диференціальних рівнянь - це система диференціальних рівнянь, в якій кожне рівняння містить добуток функцій та їх похідних. Така система може бути представлена у вигляді:

[\sum_{i=1}^{n} a_i(x) \frac{d^n y_i}{dx^n} + \sum_{i=1}^{m} b_i(x) y_i = f(x)]

де (y_i) - невідомі функції, (a_i(x)) і (b_i(x)) - відомі функції, (f(x)) - функція, а (n) і (m) - цілі невід'ємні числа.

У білінійних системах диференціальних рівнянь функції (a_i(x)) та (b_i(x)) можуть залежати від змінної (x), що призводить до зміни коефіцієнтів рівнянь залежно від точки. Це дає можливість моделювати різні фізичні явища, де параметри залежать від змінної (x) або від значень інших функцій.

Білінійні системи диференціальних рівнянь використовуються у багатьох галузях науки і техніки, зокрема в математичній фізиці, електротехніці, механіці, керуванні та інших. Вони дозволяють моделювати складні процеси з неоднорідними параметрами та взаємодіючими функціями, що робить їх потужним інструментом для вивчення та аналізу різних систем.

РОЗДІЛ 2
ПРОЕКТУВАННЯ ТА РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ З ІНВЕСТУВАННЯ У КІБЕРБЕЗПЕКУ ОБ'ЄКТІВ ІНФОРМАТИЗАЦІЇ

2.1. Обґрунтування архітектури СППР

У сучасному світі процеси протікають швидко в багатьох сферах життя суспільства, і люди прагнуть якомога ефективніше керувати процесами, вдосконалюючи та пристосовуючи їх до мінливих умов навколишнього середовища. Необхідною умовою розвитку будь-якої галузі є виконання не тільки вимог щодо якості обслуговування та прагнення до економії матеріальних ресурсів, але й уміле використання найважливішого ресурсу — часу.

Для діяльності будь-якої організації необхідно приймання рішень, виробництво та координування. Те, який конкретний вибір координується у виробничому середовищі, має значний вплив на ефективність діяльності та здатність організації конкурувати. Ця реальність зумовлює необхідність серйозного підходу до питань забезпечення якості при формуванні управлінських рішень, що свідчить про ефективність управління.

При виборі одного з різних варіантів управління враховується значна кількість суперечливих і неоднозначних аспектів. Загалом, існує три категорії невизначеності: невизначеність (1) належить до неповного знання питання, щодо якого слід прийняти рішення; невизначеність (2) належить нездатності повністю врахувати те, як середовище відреагує на прийняті рішення; невизначеність (3) належить до нечіткого розуміння особи, що приймає рішення (ОПР), своїх цілей.

Передусім, непослідовність є результатом суперечливої оцінки обставин і неправильного визначення пріоритетів, що, зі свого боку, надзвичайно ускладнює прийняття рішень. Відомо, що люди, які ухвалюють рішення без додаткової аналітичної підтримки, використовують спрощені, а іноді спірні шляхи вибору рішення. Процес прийняття рішень можна розділити на дві основні категорії: формально-евристичний та інтуїтивно-емпіричний.

Інформаційне забезпечення управління обома схемами процесу прийняття рішень є одним із вирішальних елементів у синтезі ефективних рішень. Успішно реалізовувати процес управління допомагає комплекс інформаційних ресурсів, інструментів, технологій і процесів, відомих як «інформаційне забезпечення управління».

Структура процесу прийняття рішення, як правило, вивчається при синтезі моделі проблемної ситуації. Ця структура складається зі станів вихідних даних задачі, моделі ситуації прийняття рішення, обмежень, зовнішніх факторів об'єктивного суб'єктивного характеру, варіантів рішень та їх наслідків. Так звана система підтримки прийняття рішень (далі - СППР) позначає цю сукупність елементів як тип середовища прийняття рішень (системи). Таким чином, СППР — це тип технології, яка надає ОПР, інформацію: висновки та пропозиції, необхідні для прийняття рішень.

В основу СППР покладено структуру самого процесу синтезу рішень, а також механізми надання ОПР попередніх і проміжних оцінок. Інформаційні технології використовуються для прийняття рішень і координації в якісному підході до інтеграції між комп'ютером та людиною.

Допомога особам, які приймають рішення, з аналізом попередніх даних, оцінкою поточної ситуації та обмежень, що накладаються зовнішнім середовищем; визначення та встановлення пріоритетів з урахуванням невизначеності в оцінках осіб, які приймають рішення, та формування їхніх переваг; синтез потенційних рішень, формування списку альтернатив; і аналіз потенційних наслідків є основними цілями систем підтримки прийняття рішень є основними функціями систем підтримки прийняття рішень.

Зосередження уваги на комп'ютерних інформаційних технологіях дозволяє ідентифікувати окремий клас систем підтримки прийняття рішень - системи людина-машина. Ці системи призначені для підтримки ОПР у їхній професійній діяльності, допомагаючи їм використовувати знання, моделі та дані для підготовки до прийняття важливих рішень. Активний розвиток ринку, підвищення конкурентоспроможності та методичного адміністрування бізнес-процесів обумовлюють такі потреби системи підтримки прийняття рішень: -

підвищення ефективності аналізу ефективності бізнес-процесів та аналітики їх розвитку; - аналіз та інтеграція джерел маркетингової, виробничої та фінансової інформації; - розширення кола осіб, які беруть участь у підготовці та прийнятті управлінських рішень.

Активний розвиток ринку, посилення конкуренції та системне управління бізнес-процесами висувають такі вимоги до системи підтримки прийняття рішень [40-60]:

– аналіз та інтеграція маркетингових джерел, виробничої та фінансової інформації;

– підвищення ефективності аналізу бізнес-процесів та аналітики їх розвитку;

– розширення кола осіб, які беруть участь у формуванні та прийнятті управлінських рішень.

На основі вивчення теперішньої практики можна виділити такі сфери ефективного використання СППР: фінансова аналітика та прогнозування; закупівлі; аналіз клієнтської бази, її поведінки та виявлення прихованих законів; координація активів.

З точки зору обслуговування процесів, це дозволяє успішно виконувати загальні завдання інформаційного забезпечення бізнесу. Одним із них є: координація IT та стратегічних бізнес-обов'язків; регулювання проєктів, виробничих потужностей, змін, проблем, витрат, непередбачених обставин, служб підтримки, а також відносин із постачальниками та клієнтами.

Прийняття рішень у природних умовах, у яких діють елементи, є основою успішної роботи виробничого середовища. СППР – це інструмент, створений для допомоги менеджерам у виконанні їхніх завдань у динамічному сучасному світі. Вони поєднують складні методології науки управління, інформатики та математичного моделювання.

Відсутність стандартизації інформаційного поля та обмежений доступ до структурованої інформації щодо ступеня КБ конкретного ОБІ, є однією з головних проблем сфери захисту інформації та кібербезпеки багатьох держав. В результаті на сьогодні лише деякі державні установи, підприємства чи приватні

компанії, можуть з упевненістю говорити про те, що мають усю повноту інформації про стан справ у сфері КБ свого об'єкта інформатизації. Беручи це до уваги, можна з упевненістю сказати, що для більшості компаній та організацій, які не володіють власними висококваліфікованими кадрами в області КБ, або мають недостатні ресурси для залучення зовнішніх фахівців з кібербезпеки та захисту інформаційних активів своїх ОБІ, єдиним варіантом залишається залучення потенціалу СППР або ЕС для розв’язання задачі пошуку раціональної стратегії інвестування в КБ.

СППР у процесі інвестування у системи кібернетичної безпеки створюється з метою її використання будь-якими зацікавленими особами в усіх установах чи підприємствах, для яких актуальне завдання пошуку раціональної стратегії інвестування в системи КБ в умовах зростання кількості та складності деструктивних впливів на інформаційні ресурси з боку комп'ютерних зловмисників.

Системи підтримки прийняття рішень (СППР) в галузі кібербезпеки та захисту інформації виконують різноманітні завдання, що спрямовані на покращення безпеки інформаційних систем і захисту важливої інформації. Основні завдання СППР у цій галузі включають [40-60]:

– Виявлення загроз інформаційній безпеці: СППР допомагають виявити потенційні загрози, які можуть призвести до порушення безпеки інформаційних систем. Вони проводять аналіз вразливостей, перевіряють наявність відомих загроз та розробляють алгоритми для виявлення вторгнень і несанкціонованого доступу до системи.

– Оцінка ризиків: СППР допомагають оцінити ризики, пов’язані з безпекою інформаційних систем, і визначити ймовірність виникнення загроз і можливі наслідки. Це дозволяє компаніям приймати обґрунтовані рішення щодо вкладення ресурсів у заходи з кібербезпеки.

– Планування і розробка стратегій безпеки: СППР допомагають розробити стратегію безпеки інформаційних систем, включаючи політики, процедури та технологічні рішення. Вони допомагають встановити перелік заходів з

кібербезпеки, розробити плани відновлення після інцидентів та плани неперервності бізнесу.

– Моніторинг та виявлення інцидентів: СППР відіграють важливу роль у моніторингу і виявленні незвичайної активності, підозрілих подій та потенційних інцидентів в інформаційних системах. Вони використовують технології аналізу журналів подій, виявлення вторгнень, аналізу підписів вірусів та інші методи для виявлення аномалій і загроз.

– Аналіз інформаційної безпеки: СППР допомагають проводити аналіз і оцінку ефективності заходів безпеки, виявляти слабкі місця та розробляти пропозиції щодо вдосконалення системи захисту. Вони використовують методи аудиту безпеки, тестування на проникнення та інші методи для оцінки рівня безпеки інформаційних систем.

Загалом, СППР у галузі кібербезпеки та захисту інформації допомагають компаніям ефективно управляти ризиками, виявляти загрози, розробляти стратегії безпеки і реагувати на інциденти, забезпечуючи високий рівень захисту інформаційних систем..

З огляду на все вище сказане, приходимо до висновку, що СППР обов’язково має забезпечувати такі види підтримки прийняття рішень:

– експертна підтримка;

– автоматизоване виведення рішення;

– комбіноване рішення.

2.2. Моделювання та проектування

Для розуміння вимог користувачів та визначення точок взаємодії, корисно буде побудувати діаграму прецедентів. Діаграми прецедентів є важливим інструментом для моделювання функціональності системи та взаємодії користувачів з нею. Вони допомагають в зрозумінні та документуванні того, як система виконує свої завдання і як користувачі взаємодіють з нею, див. рис. 2.1.

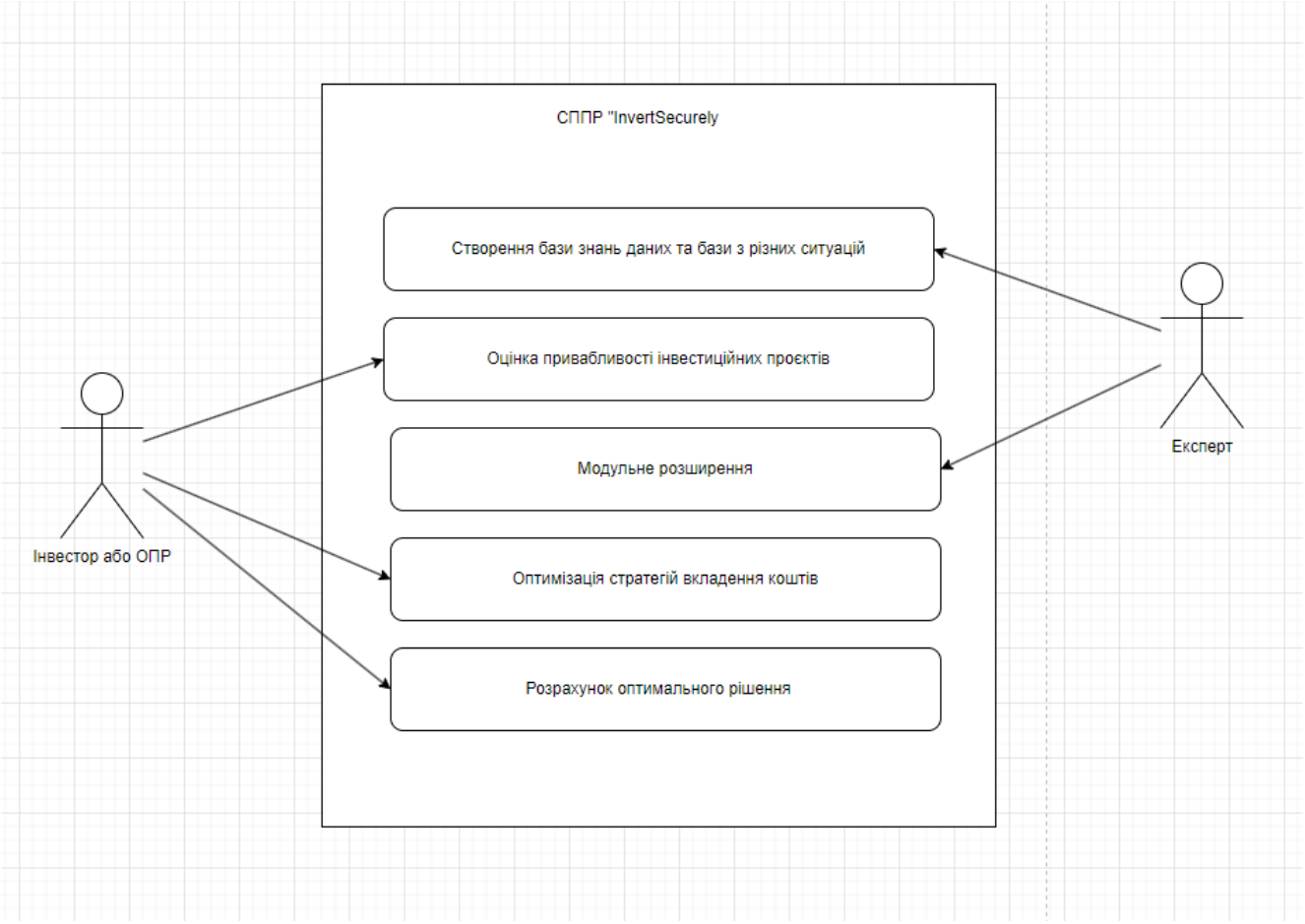


Рисунок 2.1– Діаграма прецедентів

Побудована діаграма прецедентів побудували для системи "InvestSecurely", виконує декілька важливих цілей:

– Діаграма допомагає уточнити та узгодити деталі взаємодії акторів (експертів) і прецедентів (функціональних можливостей). Вона служить як основа для подальшого розроблення системи та її функціональності.

– Діаграма надає візуальне уявлення про різні можливості та функціональність системи. Вона допомагає розробникам, експертам і іншим зацікавленим сторонам краще розуміти, як система функціонує та які завдання вона виконує.

– Діаграма допомагає уточнити та узгодити деталі взаємодії акторів (експертів) і прецедентів (функціональних можливостей). Вона служить як основа для подальшого розроблення системи та її функціональності.

– Діаграма допомагає взаємодіяти зі зацікавленими сторонами, такими як замовники проекту або користувачі системи, і пояснювати їм, як система працює і які переваги вона надає

– Вона дозволяє розробникам оцінити, наскільки великим і складним буде проект, який передбачає розробку системи "InvestSecurely", і прийняти рішення щодо ресурсів, необхідних для його реалізації.

– Діаграма є важливою частиною документації проекту, що зберігається і використовується під час розробки, тестування та підтримки системи.

Отже, діаграма прецедентів вирішує різні завдання, включаючи спрощення розуміння системи, уточнення її функціональності, зв'язок з зацікавленими сторонами та оцінку проекту. Вона є потужним інструментом для успішної розробки та впровадження системи прийняття рішень в галузі кібербезпеки і захисту інформації.

Розглянемо схему взаємодії модулів з базою даних. В контексті розробки СППР за модульним принципом раціонально буде створити єдиний простір для збереження даних всіх моделей. Це дозволить забезпечити ведення єдиного електронного архіву стратегій інвестування в галузі кібербезпеки та захисту інформації. Архітектурно це передбачає створення однієї централізованої бази даних з багатьма таблицями. Наприклад, сутності для моделі А та моделі Б зберігаються в одній базі даних, але розділені відокремленими таблицями без прямих зв'язків. Цей підхід дозволяє зберігати дані для кожної моделі окремо, уникаючи складних асоціацій і зв'язків між таблицями, що можуть бути важкими для управління та розуміння. В такому випадку, кожна модель має свою власну таблицю або групу таблиць, в яких зберігаються відповідні дані. Ця структура дозволяє керувати даними для кожної моделі ізольовано, спрощує операції додавання, видалення та зміни даних, і уникнути змішування даних між моделями. Такий підхід особливо корисний, коли моделі А та Б не взаємодіють напряму між собою та не потребують обміну даними. Він також допомагає зберегти чистоту та організацію бази даних, а також спрощує управління і підтримку системи, оскільки зміни в одній моделі не впливають на інші, див. рис. 2.2.

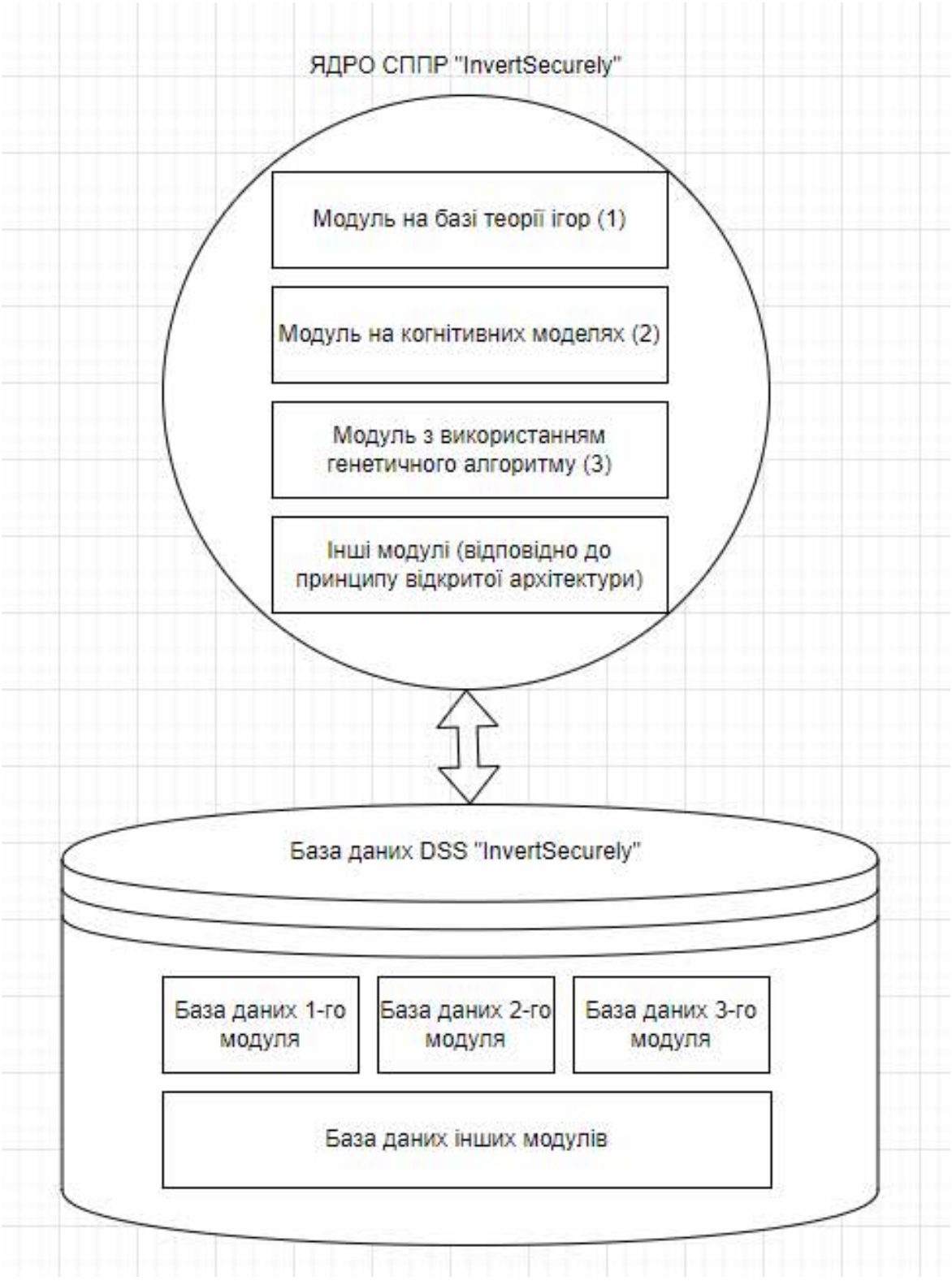


Рисунок 2.2 – Взаємодія модулів з БД

Одним із важливих аспектів перевірки запропонованої архітектури та алгоритму є аналіз сценаріїв поведінки користувача та взаємодії системи, які входять у роботу програми. Для цього дослідження була використана діаграма послідовностей, що є складовою частиною універсальної мови моделювання.

Дана діаграма дозволяє розглянути принципи взаємодії між акторами та програмною системою при виникненні різних ситуацій під час вирішення визначених завдань. Цей аналіз сценаріїв взаємодії користувача і системи є особливо корисним у контексті СППР, де правильне розуміння взаємодії акторів та системи є ключовим фактором успіху в оцінці інвестиційних проєктів в сфері кібербезпеки та захисту інформації.

Розглянемо детальніше механізм роботи модуля СППР, див. рис. 2.3.

Зауважимо, що в модулях міститься основний функціонал СППР. При взаємодії з цими модулями, користувач отримує можливість візуального відображення результатів своєї роботи. Крім того, існує можливість збереження результатів у базі знань за бажанням.

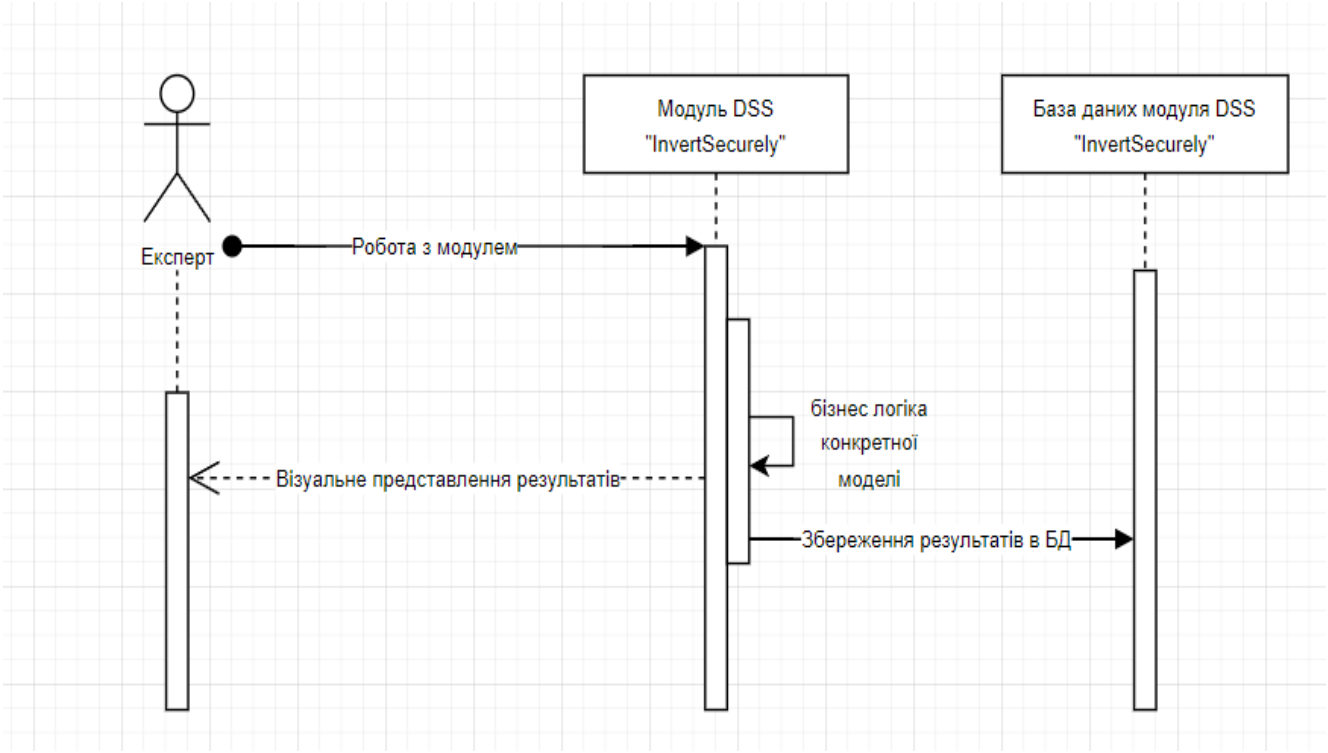


Рисунок 2.3– Діаграма послідовностей модуля СППР

Взаємодію з базою знань можна побачити на подальшій діаграмі, див. рис. 2.4.

На діаграмі можемо побачити, що кожен збережений сценарій взаємодії з модулем можна легко та повторно відтворити. Це надає значний комфорт та ефективність при роботі з системою підтримки прийняття рішень.

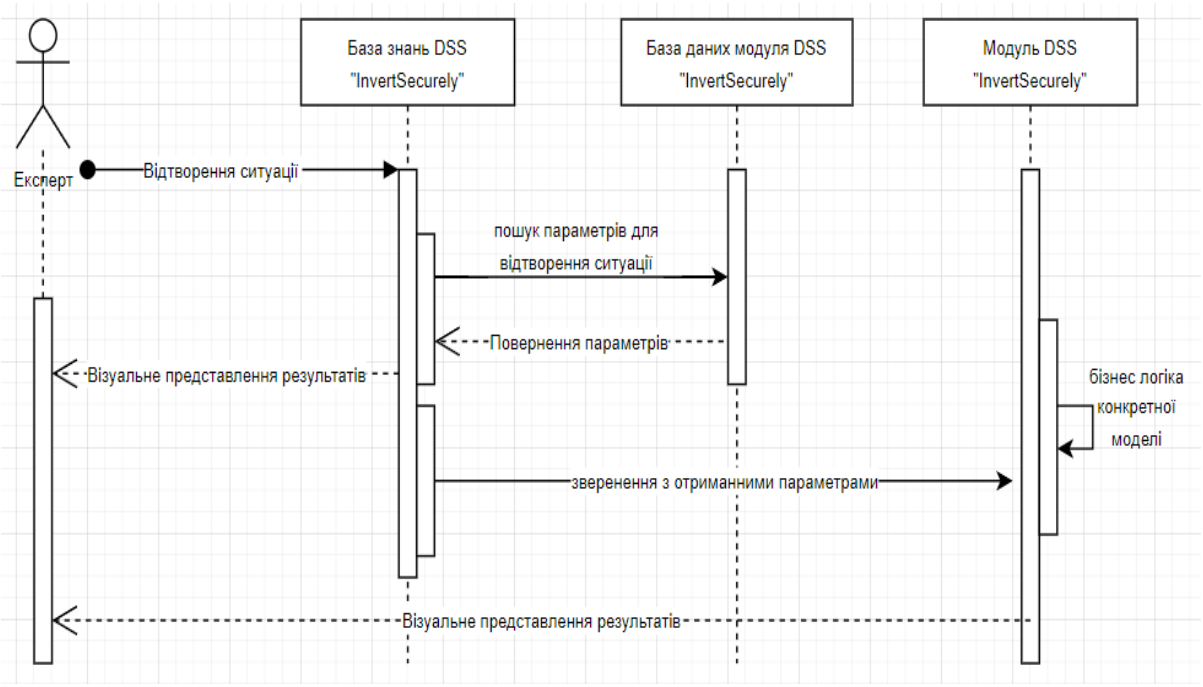


Рисунок 2.4 – Діаграма послідовностей бази знань СППР

Насамперед, ця можливість дозволяє економити час, оскільки користувачам не доводиться повторно вводити всі параметри для налаштування моделей і виконувати одні й ті ж кроки кожного разу. Використання збережених сценаріїв стає особливо корисним під час обробки великої кількості даних або вирішення рутинних завдань.

Крім того, ця можливість сприяє уникненню помилок та забезпечує послідовність у виконанні завдань. Користувачі можуть переконатися, що кожен етап роботи відбувається ідентично до попереднього разу, що важливо при важливих рішеннях та аналітичних процедурах.

Така можливість також сприяє збереженню інформації та досліджень. Користувачі можуть легко отримати доступ до попередніх результатів та аналізувати їх. Це допомагає створювати накопичену базу знань та робити більш обґрунтовані рішення у майбутньому.

Вивчені всі основні функціональні частини, що дозволяє перейти до наступного етапу - етапу розробки.

2.3. Розробка СППР

Вивчені всі основні функціональні частини, що дозволяє перейти до наступного етапу - етапу розробки.

Реалізація системи підтримки прийняття рішень (СППР) в сучасних умовах вимагає високої технічної компетентності та вибору передових технологій. З цією метою була обрана технологія ASP.NET Core для створення програмного забезпечення, яке дозволяє імплементувати СППР в реальному середовищі.

ASP.NET Core відома своєю продуктивністю та можливістю роботи на різних платформах. Ця технологія забезпечує доступ до СППР з будь-якого пристрою та операційної системи, дозволяючи операторам прийняття рішень працювати з системою в зручний для них час. ASP.NET Core також сприяє створенню безпечної та надійної системи, яка відповідає вимогам інформаційної безпеки. Використані інструменти ASP.NET Core гарантують захист конфіденційності та цілісності даних, а також відстежують та аудитують доступ до системи.

Також, використання ASP.NET Core сприяє легкій розширюваності функціоналу СППР, що дозволяє додавати нові моделі та аналітичні інструменти для розв'язання різних завдань управління інформаційною безпекою. Ця технологія дозволяє створювати додатки з відкритою архітектурою, спрощуючи інтеграцію нових модулів та розширень.

Обираючи архітектурний підхід для реалізації системи підтримки прийняття рішень (СППР), було прийнято рішення використовувати модель-представлення-контролер (MVC).

Побудуємо діаграму для візуалізації загальної архітектури системи. Така діаграма допоможе краще розуміти структуру та взаємозв'язки між компонентами СППР, див. рис. 2.5.

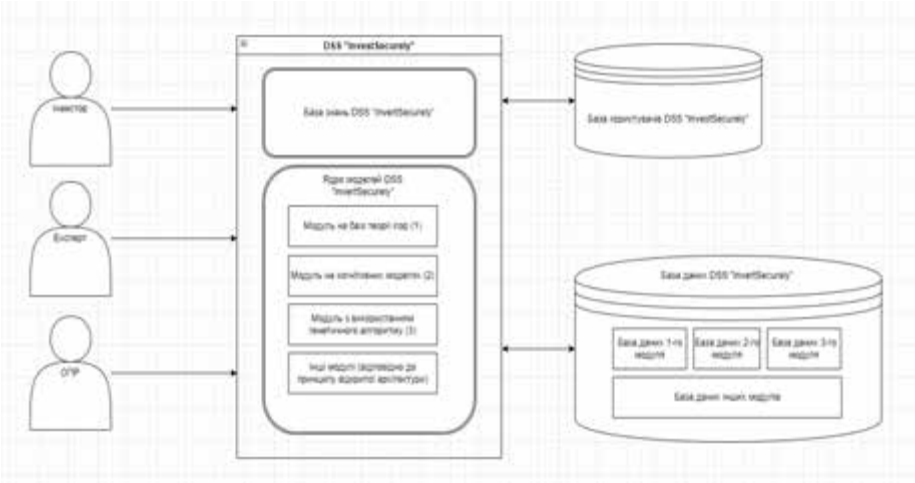


Рисунок 2.5– Загальна архітектура СППР

Для збереження бази даних була використана система керування базами даних Microsoft SQL Server (MS SQL Server). Використання MS SQL Server надає надійність та ефективність для зберігання даних у системі підтримки прийняття рішень.

На рис. 2.6 можна бачити схему бази даних СППР «InvestSecurely». Основна база даних використовується для збереження сценаріїв взаємодії з моделями та наповнення бази знань. Вона відіграє ключову роль у зберіганні та управлінні важливою інформацією, необхідною для подальшої роботи системи підтримки прийняття рішень.

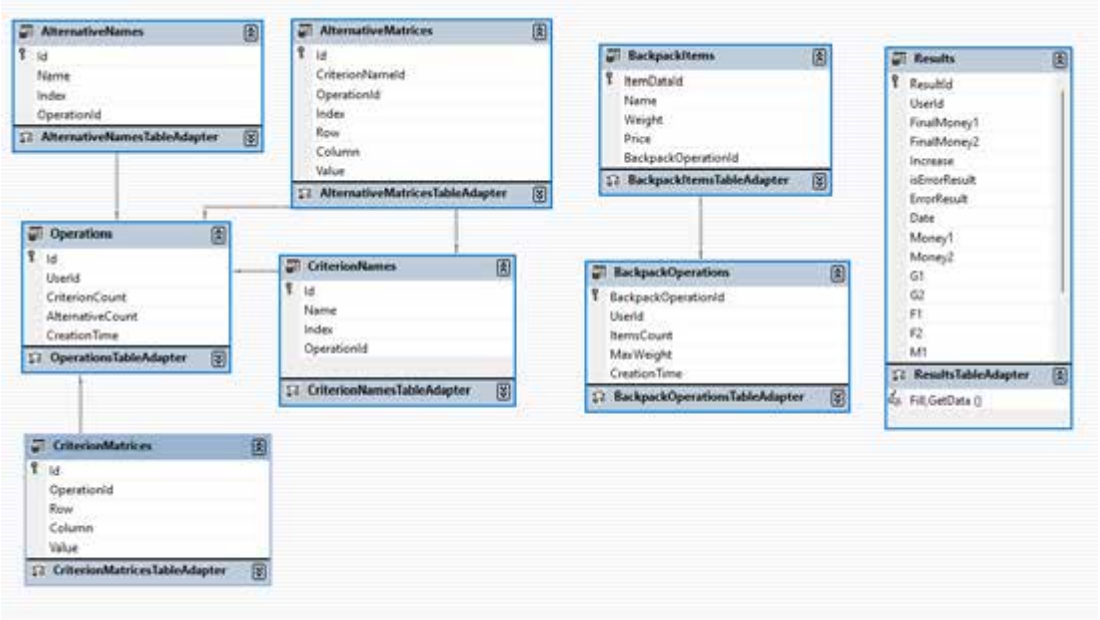


Рисунок 2.6– Схема бази знань СППР «InvestSecurely»

Побудуємо діаграму для візуалізації загальної архітектури системи. Така діаграма допоможе краще розуміти структуру та взаємозв'язки між компонентами СППР.

Для збереження та управління інформацією про користувачів СППР «InvestSecurely» використовує окрему базу даних. Її схему можна побачити на рис. 2.7.

Ця база даних забезпечує надійну систему авторизації та ідентифікації користувачів, зберігаючи їхні дані в безпеці. Механізм ASP.NET Identity використовується для створення та управління обліковими записами користувачів, а також для контролю доступу до різних функціональних частин системи. Цей підхід забезпечує конфіденційність та безпеку даних користувачів, а також дозволяє налагоджувати рівні доступу для різних користувачів та груп. Крім того, він спрощує процес реєстрації та авторизації, забезпечуючи користувачам комфортне використання системи.

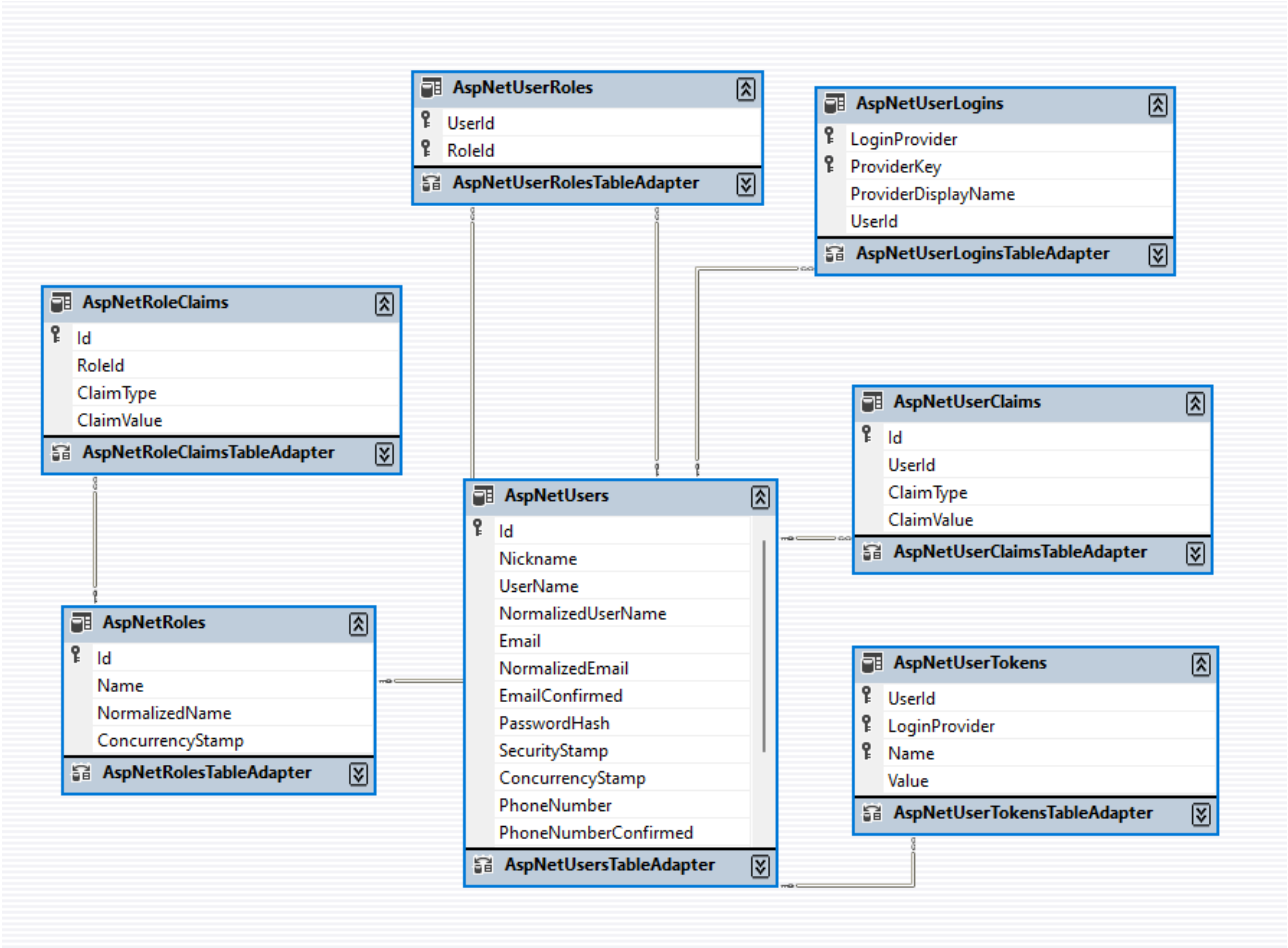


Рисунок 2.7– Схема бази користувачів СППР «InvestSecurely»

РОЗДІЛ 3
РЕЗУЛЬТАТИ РОЗРОБКИ ПРОГРАМНОГО ПРОДУКТУ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ПРОЦЕСІ ІНВЕСТУВАННЯ В КІБЕРБЕЗПЕКУ ОБ'ЄКТУ ІНФОРМАТИЗАЦІЇ

3.1. Опис СППР «InvestSecurely»

Загальний вид форми для завдання вихідних даних у СППР «InvestSecurely» наведено на рис. 3.1.

Реєстрація. Слід зазначити, що для того, щоб отримати доступ до функціоналу, наданого експертам на сайті «InvestSecurely», необхідно створити обліковий запис та авторизуватися, див. рис. 3.2.

Отже, механізм реєстрації дає можливість користувачам «СППР «InvestSecurely» отримувати доступ до нових функціональних можливостей у міру розширення переліку моделей, які можуть використовуватися в ході пошуку раціональної стратегії інвестування в КБ об'єкта інформатизації будь-якого масштабу.

Рисунок 3.1 – Загальний вигляд СППР «InvestSecurely»

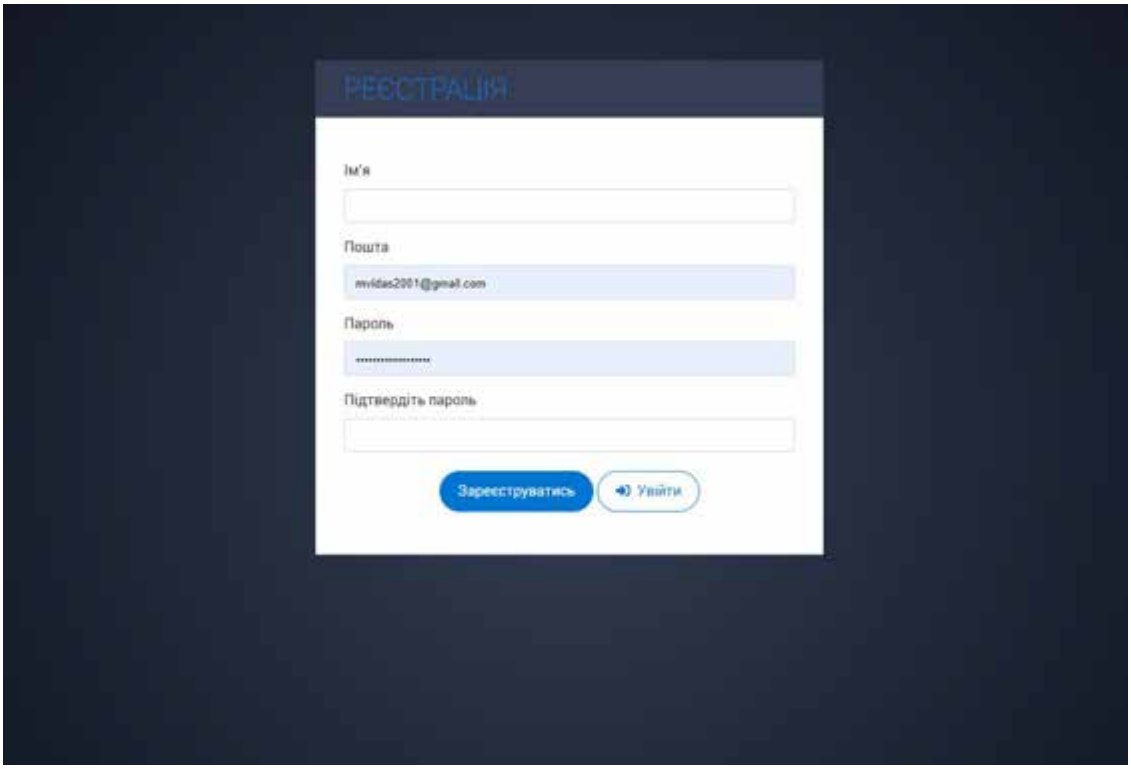


Рисунок 3.2 – Процедура реєстрації експертів на сайті СППР «InvestSecurely»

Після реєстрації на вказану електронну адресу прийде лист із посиланням на підтвердження. Для завершення реєстрації необхідно перейти за посиланням, вказаним у листі.

Далі, після створення облікового запису необхідно авторизуватись, див. рис. 3.3.

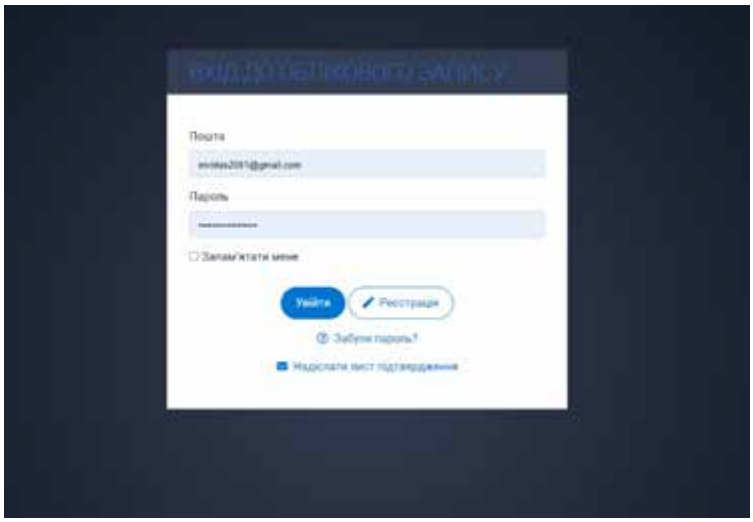


Рисунок 3.3 – Вхід експерта до облікового запису СППР «InvestSecurely»

Важливо те, що користувач може відновити доступ до облікового запису в разі втрати пароля.

СППР розробляється за модульним принципом для того, щоб при необхідності додавати нові функціональні завдання, див. рис. 3.4.

На прикладі модуля 1 розглянемо роботу з реалізованим інструментарієм, див. рис. 3.4. Зазначений модуль заснований на класичному методі аналізу ієрархій (далі MAI) Т. Сааті [50-60]. MAI використовується на першому етапі роботи СППР «InvestSecurely»для експертної оцінки конкретних систем захисту інформації за класами. Модуль створено на застосуванні методу Т. Сааті і може використовуватись експертами як самостійний програмний продукт, так і у складі СППР для вибору оптимальних варіантів ЗЗІ для вузлів РОС.

Важливою часткою перевірки запропонованих в роботі методів, моделей на взагалі інформаційних технологій, пов’язаних із СППР є методологія планування обчислювального експерименту.

Нижче показані приклади роботи даного модуля під час оцінювання альтернативних варіантів при виборі антивірусного ПЗ, див. рис. 3.4.

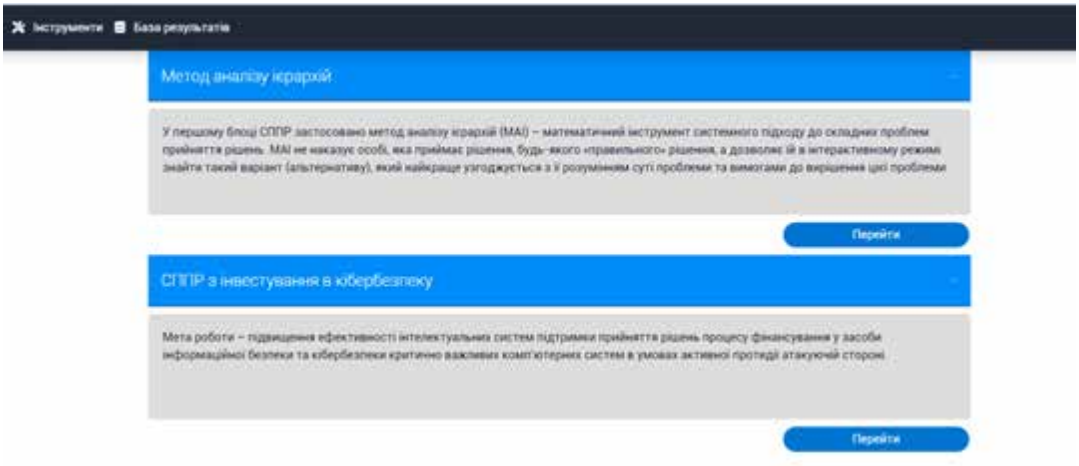


Рисунок 3.4 – Модулі СППР «InvestSecurely»

Виконаємо ряд обчислювальних тестів, щоб перевірити всі наші розрахунки. Важливо виконати кроки, включені до планування експерименту, щоб результати експерименту були репрезентативними. Для того, щоб дізнатися більше про характеристики інвестиційних процесів із системи захисту РОС, на етапі тестування функціональних можливостей програмних продуктів, описаних у роботі, необхідно провести обчислювальні експерименти з представленими в роботі моделями. Ці дані можуть знадобитися для аналізу об’єкта моделювання.

Ефективність обчислювального експерименту із застосуванням пропонованих моделей знаходиться у прямій залежності від того, як буде складено план експерименту. Зі свого боку, план експерименту визначає порядок і обсяг розрахунків, що проводяться на електронно-обчислювальних машинах. Крім того, план експерименту повинен охоплювати такі питання як прийоми обробки отриманих статистичних даних, процедури накопичення статистичних даних та інше. Таким чином у контексті проведених досліджень можна сформулювати завдання планування експерименту так: необхідно отримати інформацію про об'єкт моделювання, яка задана у вигляді математичних, що описують можливі ситуації із інвестуванням систем кібербезпеки РОС. При цьому необхідно мінімізувати витрати обчислювальних та часових ресурсів, які необхідні для проведення моделювання. Тому під час проведення обчислювальних експериментів доцільно планувати не лише які моделі братимуть до уваги під час експерименту, а й безпосередньо порядок їх проведення.

3.2. Обчислювальні експерименти

Безсумнівно очевидно, що, як і будь-які наукові чи технічні завдання, завдання експериментального та статистичного моделювання вирішуються відповідно до певного потоку подій, що дозволяє перейти від постановки цих завдань до пошуку рішень. Спробуймо розбити цей підхід на кілька логічно чітких кроків. Можна з упевненістю стверджувати, що при використанні запропонованих підходів для розв'язання практичної задачі ці етапи певною мірою будуть присутні.

Оптимальний вибір досліджуваних компонентів, фактичний вибір плану експерименту та методи аналізу експериментальних даних є першими етапами процесу, відомого як планування експерименту, який спрямований на раціональну організацію експериментального дослідження. Обсяг, параметри та методика експериментального дослідження встановлюються планом експерименту, який є сукупністю даних.

Розробка мети та завдань дослідження є першим етапом. На цьому етапі цілі та завдання чітко створюються та повинні бути вирішені з використанням результатів дослідження. Одним із прикладів цього є завдання оптимізації предмета дослідження. Тут вирішується, яке дослідження буде проводитися, хто його підтримуватиме, як воно буде реалізовуватися тощо.

Другим етапом необхідно буде вибрати функції зворотного зв'язку. На цьому етапі аналізуються всі змінні об’єкта та вибираються ті, які будуть використані в дослідженні як функції відповіді. У ролі функцій відповіді можна вибрати одну або кілька змінних. Очевидно, що ці змінні повинні, по-перше, задовольняти цілям і завданням дослідження, а по-друге, задовольняти стандарти, встановлені для функцій відповіді. У цей момент також вибирається або встановлюється шкала чисельних оцінок функцій відповіді, вибирається методика, і вирішується похибка вимірювання необхідних значень результату, а також реєстрація результатів цих вимірювань.

Третім етапом буде вибір факторів. Змінні, обрані для дослідження, суттєво впливатимуть на всі або більшість функцій відповіді. Звичайно, чинники також повинні відповідати висунутим до них вимогам. Щоб визначити релевантність впливу певних елементів, може знадобитися проаналізувати результати попередніх досліджень або провести невелику кількість, як правило, несуттєвих випробувань.

До вибору кількості елементів слід підходити дуже обережно. Непотрібні елементи можуть значно збільшити кількість експериментів, які проводяться в дослідженні, що неминуче призведе до необґрунтованого збільшення витрат. Дослідження в цілому буде поставлено під сумнів, якщо основні аспекти будуть виключені з дослідження, що призведе до неповних і неточних висновків. При цьому визначаються області визначення факторів разом з їх первинними рівнями та діапазонами варіації.

Розглянемо основоположні ідеї теорії планування експерименту. Основоположні ідеї теорії планування експерименту включають наступні принципи:

Вибір факторів: Теорія планування експерименту ставить перед собою завдання вибору релевантних факторів, які впливають на об'єкт дослідження. Це можуть бути різні змінні параметри або умови, які можуть вплинути на результати експерименту.

Визначення рівнів факторів: Для кожного вибраного фактора необхідно визначити рівні, на яких буде проводитись експеримент. Рівні можуть бути кількісними (наприклад, температура, час) або категоріальними (наприклад, тип матеріалу, метод обробки).

Розробка плану експерименту: Після визначення факторів і їх рівнів необхідно розробити план експерименту, який включає послідовність проведення експериментальних випробувань і встановлення відповідних комбінацій рівнів факторів.

Випадковість: Теорія планування експерименту підкреслює важливість випадковості у виборі комбінацій рівнів факторів. Це дозволяє забезпечити більш точні і об'єктивні результати експерименту, оскільки випадковість допомагає уникнути систематичних помилок і спотворень.

Реплікація: Для підтвердження достовірності результатів експерименту рекомендується проводити реплікацію, тобто повторення експерименту на кількох незалежних об'єктах чи у різних умовах.

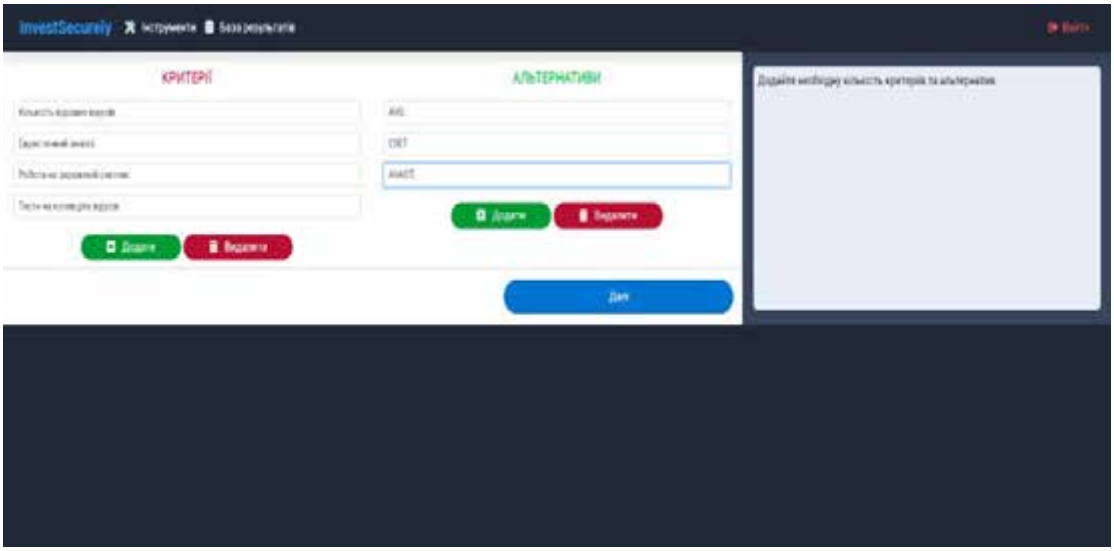
Аналіз результатів: Після проведення експерименту необхідно аналізувати отримані дані та встановлювати залежності між факторами і результатами. Це допомагає зрозуміти, як фактори впливають на об'єкт дослідження і як можна оптимізувати його характеристики.

Теорія планування експерименту дозволяє систематично вивчати вплив факторів на об'єкт дослідження, забезпечуючи об'єктивність, повноту та точність результатів. Вона знаходить широке застосування у наукових дослідженнях, промисловості, медицині та інших галузях, де необхідно проводити контрольовані експерименти для отримання достовірних висновків..

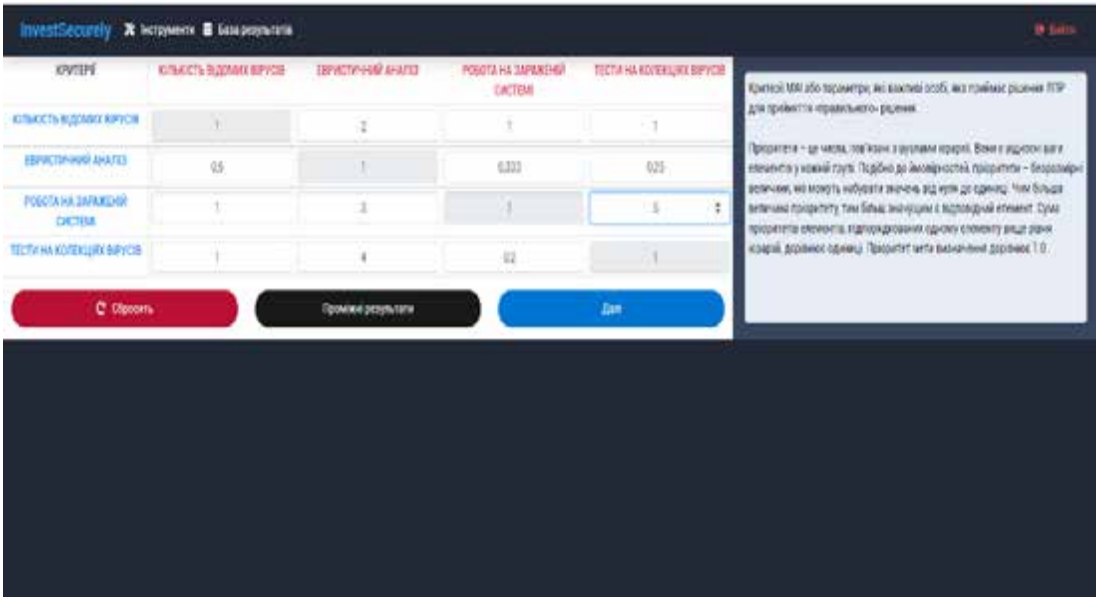
На рис. 3.5 схематично зображено описані вище етапи.

Усі реалізовані моделі дотримуються загальної концепції – поділ екрана на дві функціональні області, див. рис. 3.6. Отже, тоді ліва частина дозволяє експерту працювати з СППР, а права частина призначена для пояснення одержуваних результатів.

Рисунок 3.5 – План використання статистичного та експериментального моделювання для розв'язання проблеми.



а) – загальний вигляд модуля на основі застосування MAI;



б) – заповнення матриці порівняння альтернатив

Рисунок 3.6 – Приклад модуля СППР «InvestSecurely», використовуваного під час вибору антивірусного ПЗ

На кожному кроці можна побачити проміжні результати попарних порівнянь. Результати візуалізуються, як у вигляді матриці, так і у вигляді гістограми.

Нормалізована матриця

КРИТЕРІЇ	КІЛЬКІСТЬ ВІДОМИХ ВІРУСІВ	ЕВРИСТИЧНИЙ АНАЛІЗ	РОБОТА НА ЗАРАЖЕНІЙ СИСТЕМІ	ТЕСТИ НА КОЛЕКЦІЯХ ВІРУСІВ
КІЛЬКІСТЬ ВІДОМИХ ВІРУСІВ	0.286	0.2	0.395	0.138
ЕВРИСТИЧНИЙ АНАЛІЗ	0.143	0.1	0.132	0.034
РОБОТА НА ЗАРАЖЕНІЙ СИСТЕМІ	0.286	0.3	0.395	0.690
ТЕСТИ НА КОЛЕКЦІЯХ ВІРУСІВ	0.286	0.4	0.079	0.138

Вага критеріїв

КІЛЬКІСТЬ ВІДОМИХ ВІРУСІВ	25%	0.255
ЕВРИСТИЧНИЙ АНАЛІЗ	10%	0.102
РОБОТА НА ЗАРАЖЕНІЙ СИСТЕМІ	42%	0.418
ТЕСТИ НА КОЛЕКЦІЯХ ВІРУСІВ	23%	0.226

Рисунок 3.7 – Представлення у вигляді матриці

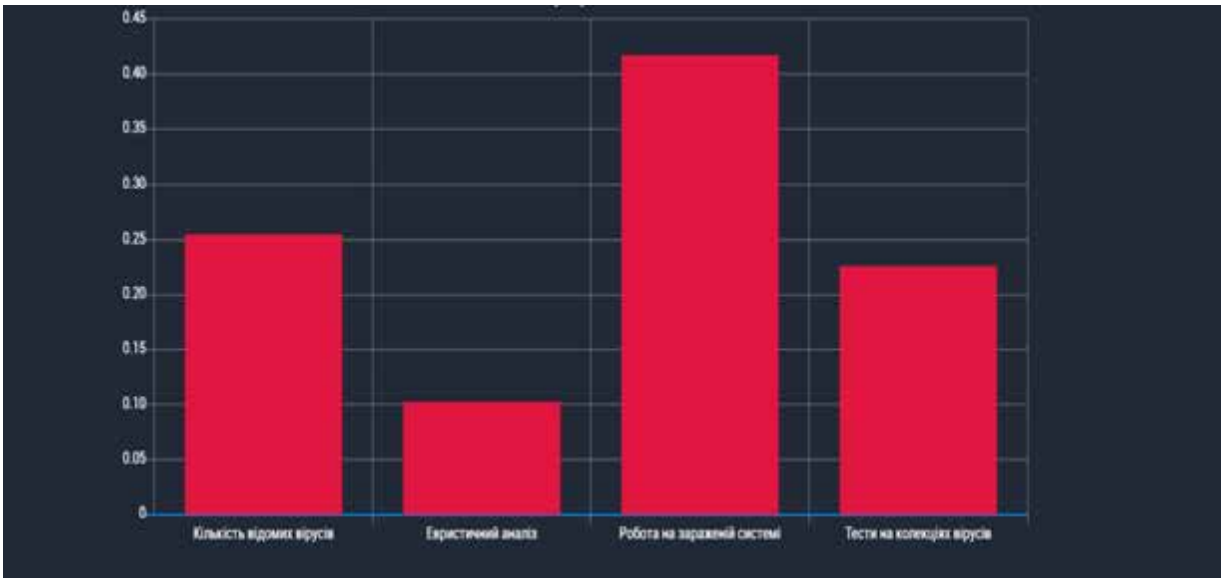


Рисунок 3.8 – Представлення у вигляді гістограми

Далі коротко опишемо другий модуль, який заснований на застосуванні апарату теорії ігор. Вважаємо, що є дві сторони – сторона захисту ОБІ – Гравець 1. І сторона атакуюча ОБІ – Гравець 2, див. рис. 3.9.

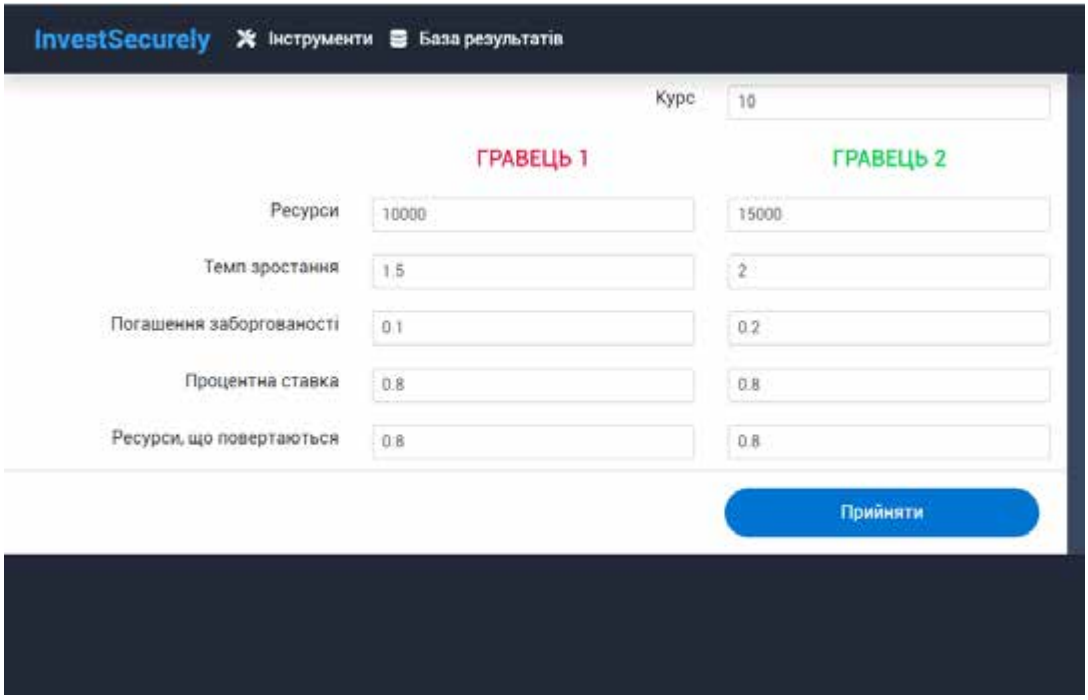


Рисунок 3.9 – Область для завдання вихідних даних експертами СППР «InvestSecurely»

У правій частині міститься текстове вікно з допоміжною інформацією, загальними відомостями про модель або підказками для роботи з інструментом, див. рис. 3.10.

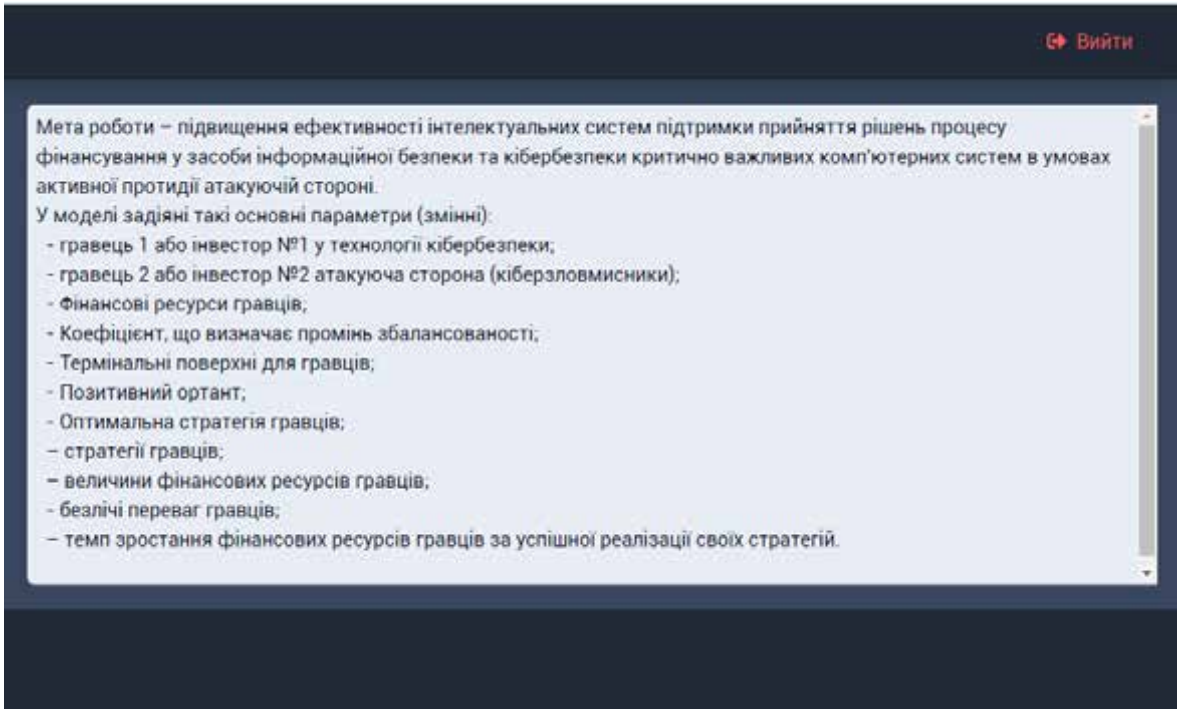


Рисунок 3.10 – Область підказок для роботи експертів з СППР «InvestSecurely»

Введемо тестові параметри та запустимо виконання, наприклад, для вихідних даних, показаних на рис. 3.11.

Результат успішного виконання - текстовий висновок та 3 графіка, див. рис. 3.12, 3.13.

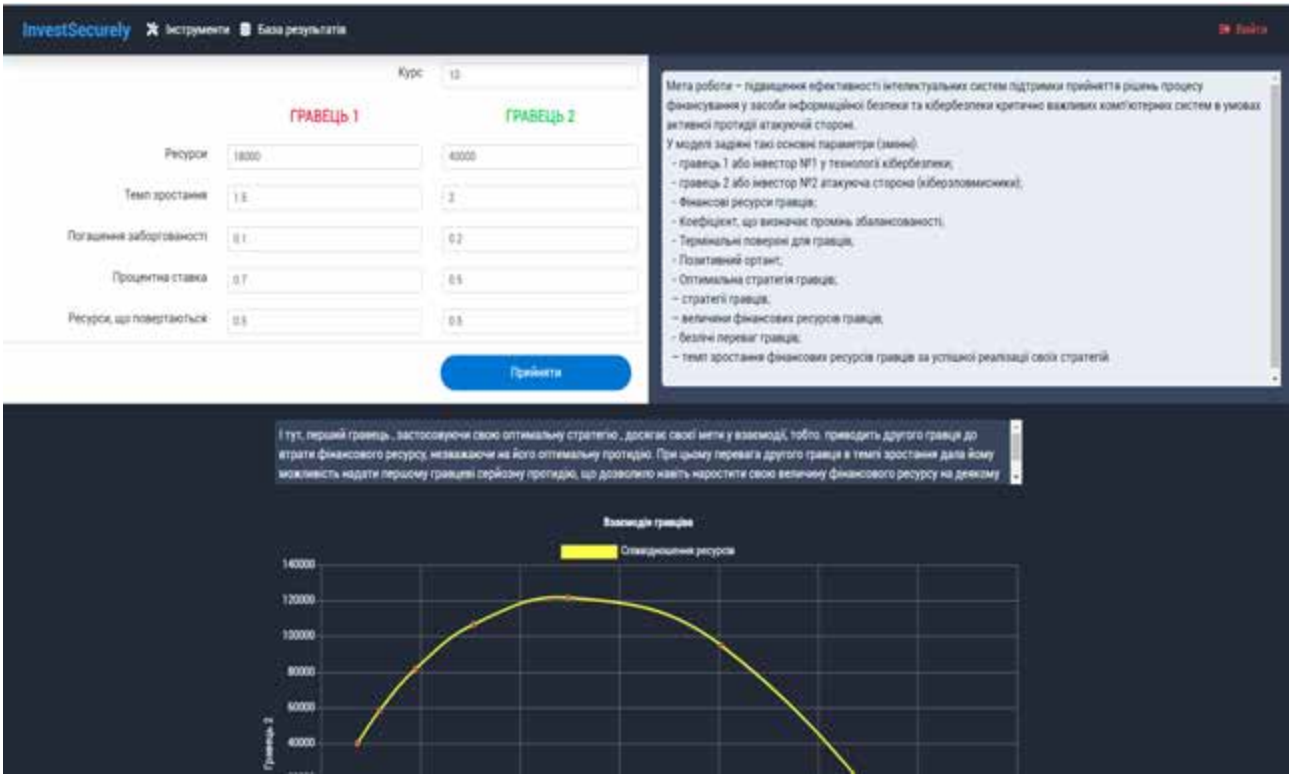


Рисунок 3.11 – Приклад тестування СППР «InvestSecurely»

Кожен із цих напрямків, так само може бути розділений на піднапрямки, наприклад, при виборі конкретних апаратно-програмних ЗЗІ. Все це диктує необхідність підключити більш швидкодійний алгоритм для перебору точок на термінальній поверхні для пошуку раціональної траєкторії, що відповідає стратегії інвестування в КБ ОБІ. Ітераційний процес застосування ГА для різної кількості поколінь хромосом ГА, що складає набори ЗЗІ, показано нижче на рис. 3.13.

Графіки є інтерактивними. При наведенні на точку або колонку відображаються її параметри, див. рис. 3.14.

При заданих у тестовому прикладі вихідних даних СППР видала таке рішення, що показане в області текстового висновку; «І тут, перший гравець, застосовуючи свою оптимальну стратегію, досягає своєї мети у взаємодії, тобто

призводить другого гравця до втрати фінансового ресурсу, незважаючи на його оптимальну протидію. При цьому перевага другого гравця в темпі зростання дозволила йому надати першому гравцеві серйозну протидію, що дозволило йому навіть наростити свою величину фінансового ресурсу на певному проміжку часу».

Рисунок 3.12 – Приклад візуалізації графіків після виконання розрахунків у СППР «InvestSecurely»

Так само графіки можна завантажити у форматі звичайного зображення, див. рис. 3.15.

Основні заходи та ЗЗІ для кожного ОБІ, можуть відрізнятися, в залежності від вартості інформаційних масивів, які має це підприємство.

Рисунок 3.13 – Приклад візуалізації графіків після виконання розрахунків у СППР «InvestSecurely» (гістограма).

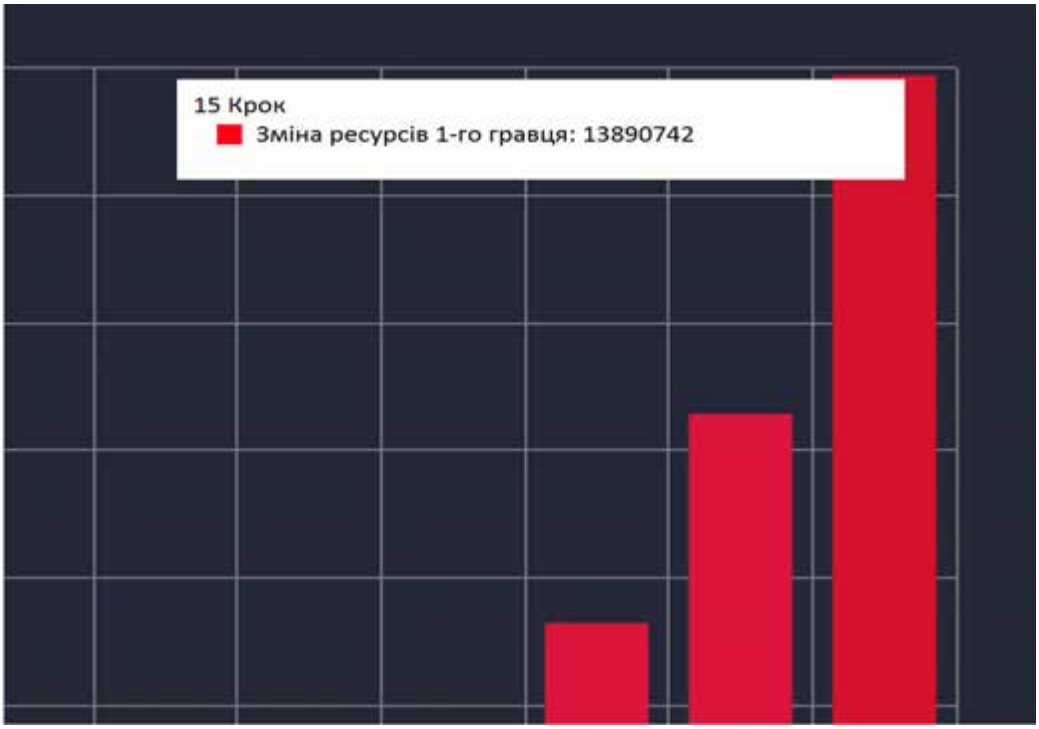


Рисунок 3.14 – Приклад візуалізації даних для розрахункової точки графіка в СППР «InvestSecurely» (гістограма)

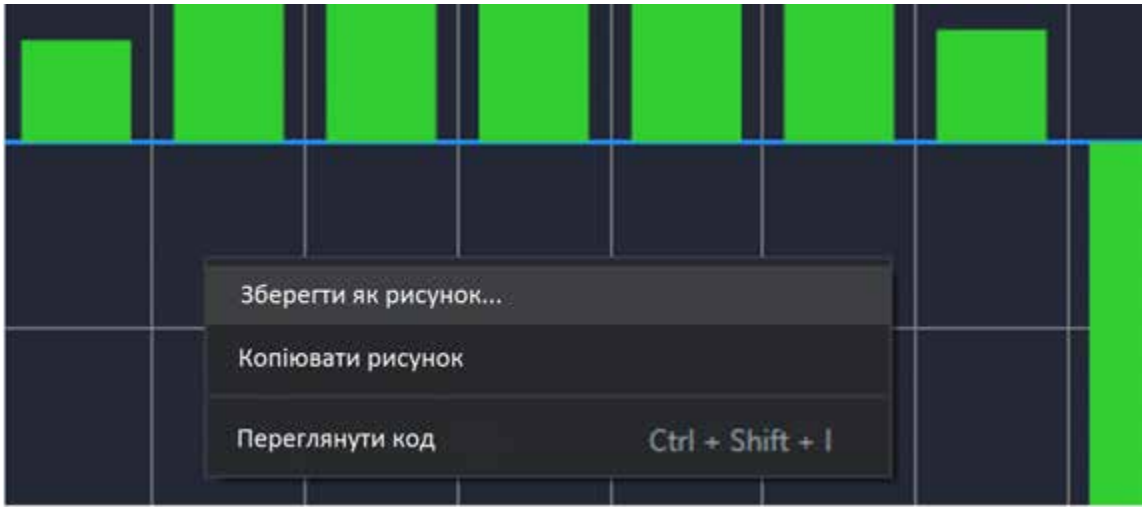


Рисунок 3.15 – Приклад збереження результатів графіка в СППР «InvestSecurely» (гістограма)

Нижче показаний інтерфейс модуля СППР «InvestSecurely» з результатами вибору рекомендованих заходів та засобів захисту інформації. При цьому можна на вибір використовувати два алгоритми - простий перебір (потрібний час близько 30 хвилин для процесора i7) або модифікований ГА (витрачений час не перевищував 1 хвилини для того ж процесора i7).

У даному модулі вирішується багатокритеріальне оптимізаційне завдання для вузлів ОБІ (які мають аналогію з «рюкзаками»). До таких вузлів ОБІ можна віднести сервери, робочі станції, комутатори, маршрутизатори та інше. В якості предметів, що знаходяться в «рюкзаках», виступають антивірусні ПЗ, міжмережеві екрани та ін. Тоді завдання з погляду на забезпечення КБ формулюється так: необхідно розмістити в «рюкзаку» якнайбільше ЗЗІ. Варто зазначити, що при цьому потрібно: 1) забезпечити кращу ефективність предметів; 2) не перевищити заданих обмежень, наприклад, на вартість «рюкзака».

У нижній частині інтерфейсу відображається результат рішення, див. рис. 3.17.

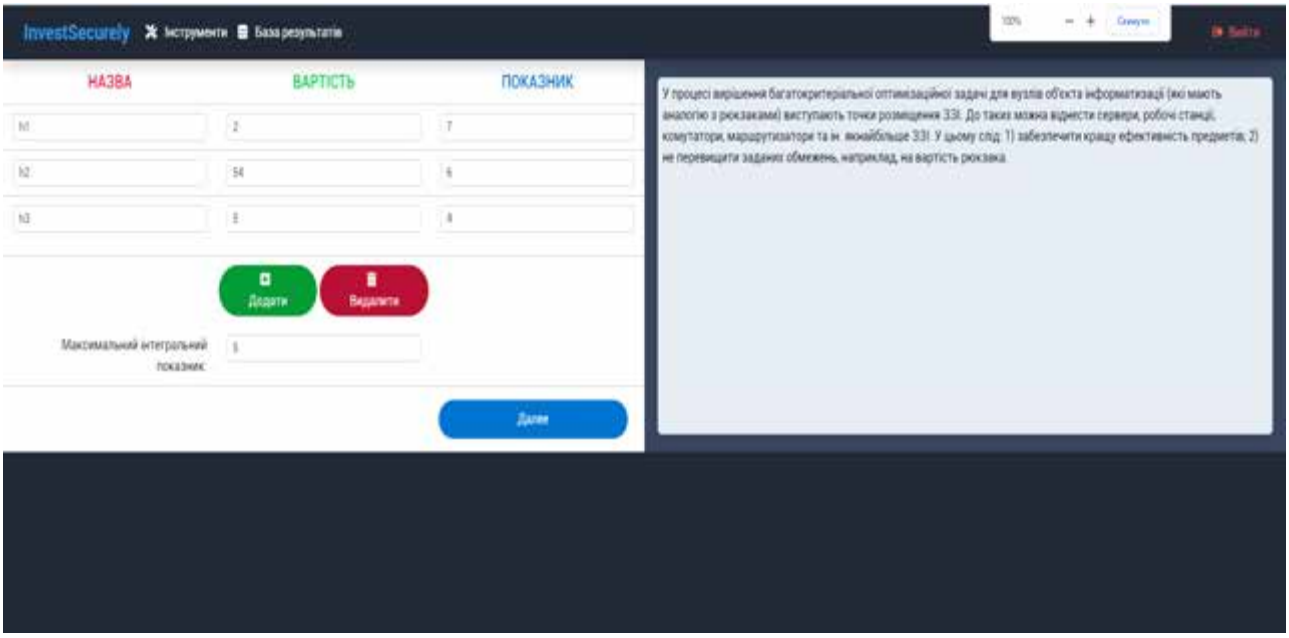
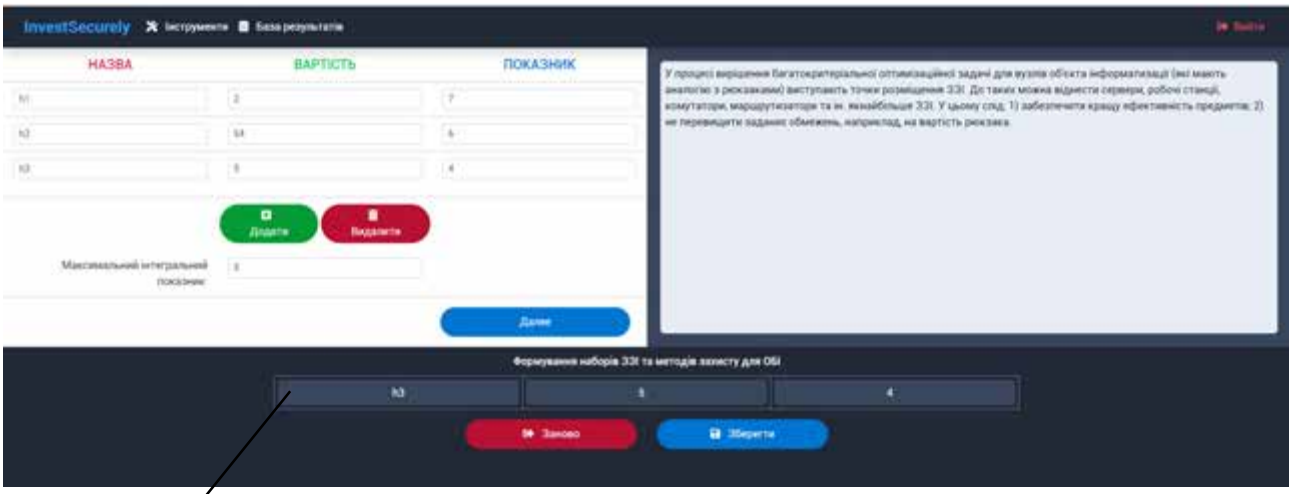


Рисунок 3.16 – Приклад модуля СППР для вирішення багатокритеріальної оптимізаційної задачі для вузлів ОБІ (на основі ГА)



Область формування набору ЗЗІ для вузла ОБІ на основі ГА

Рисунок 3.17 – Приклад модуля СППР для вирішення багатокритеріальної оптимізаційної задачі для вузлів ОБІ (на основі ГА)

Отримані у ході дослідження та вивчення результати свідчать про те, що після обчислень, що виробляються в модулях СППР всі параметри та результати заносяться до бази даних. А щоб уникнути дублювання записів, інформація

заноситься в БД, тільки тоді, якщо в ній немає запису з аналогічними параметрами, див. рис. 3.18.

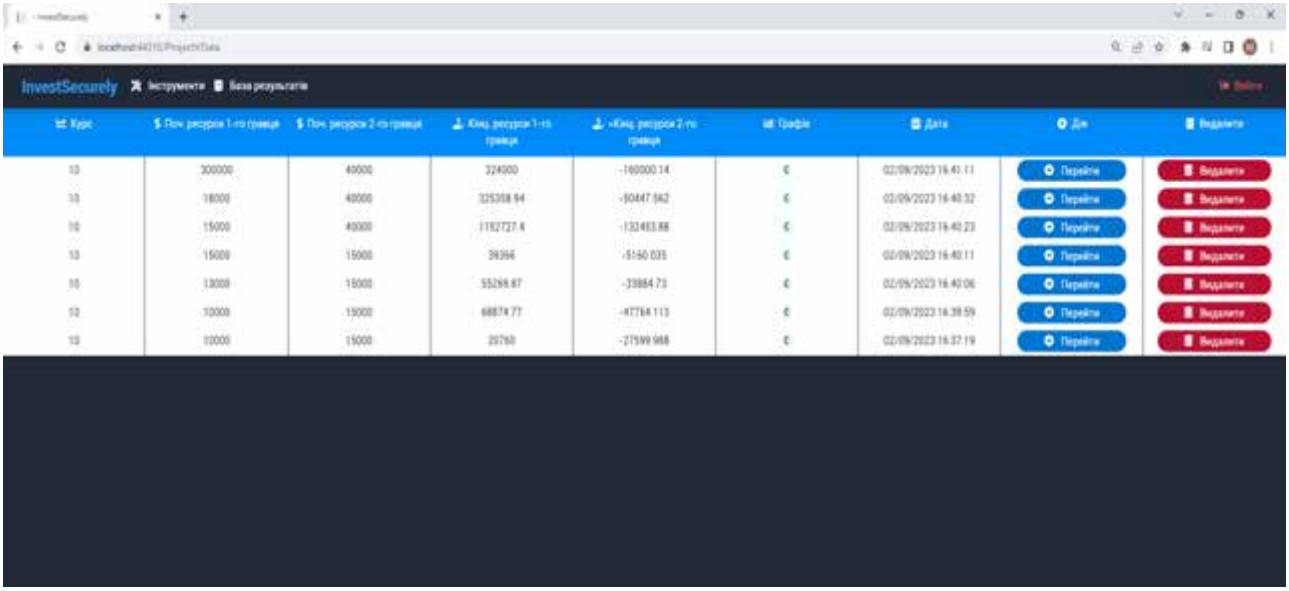


Рисунок 3.18 – Фрагменти бази даних графіка СППР

З таблиці можна одразу перейти до необхідного інструменту, натиснувши кнопку «Перейти». У такому разі, після вказаної дії відкриється вікно із заповненими вихідними даними тестового прикладу та коефіцієнтами.

Слід зазначити, що всі модулі СППР «InvestSecurely», крім табличного виведення результатів розрахунку, мають розвинену структуру візуалізації отриманих результатів у вигляді гістограм або графіків, що дає особі, що приймає рішення, найбільш наочно уявити, які зміни засобів і систем захисту інформації дозволять стороні захисту побудувати ефективну багатоконтурну систему інформаційних ресурсів ОБІ.

Наприклад, на наступному рисунку, див. рис. 3.19, показано приклад візуалізації результатів роботи СППР «InvestSecurely». Аналогічні засоби візуалізації результатів є і в інших модулях СППР «InvestSecurely».

Завдяки тому, що всі отримані результати можна зберегти під час роботи з СППР, то у такому разі вхідні дані збережуться в БД і процес обчислень можна буде відновити без ручного заповнення полів.

Рисунок 3.19 – Приклад візуалізації результатів вибору ЗЗІ для першого модуля СППР

На рис. 3.20 і 3.21 показані порівняльні результати, отримані в ході опитування експертів та висновків, зроблених ними самостійно, та за допомогою, запропонованої СППР «InvestSecurely».

У процесі перевірки СППР брали участь 7 експертів.

Відбір експертів у галузі кібербезпеки може базуватися на різних критеріях, що враховують їхні знання, навички, досвід та професійну експертизу. Основні критерії відбору експертів у галузі кібербезпеки включають наступні:

Знання та освіта: Експерти повинні мати глибокі знання і розуміння в галузі кібербезпеки. Вони повинні мати високий рівень освіти, такий як вища кваліфікація в області комп'ютерних наук, інформаційної безпеки або інших відповідних дисциплін.

Досвід роботи: Експерти повинні мати практичний досвід роботи в галузі кібербезпеки. Це може включати роботу в компаніях з інформаційною безпекою, урядових органах, дослідницьких лабораторіях або проведення проектів з кібербезпеки.

Сертифікація: Експерти можуть мати сертифікати, які підтверджують їхні навички і знання у галузі кібербезпеки. Наприклад, сертифікати CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CEH (Certified Ethical Hacker) є визнаними стандартами в галузі.

Професійна репутація: Важливим критерієм є репутація експерта в галузі кібербезпеки. Це може бути визнання від колег, публікації у наукових журналах, участь у конференціях та інші професійні досягнення.

Аналітичні навички: Експерти повинні мати сильні аналітичні навички для виявлення загроз, аналізу ризиків та розробки стратегій безпеки. Вони повинні бути здатні оцінювати складні проблеми та знаходити ефективні рішення.

Комунікаційні навички: Експерти повинні мати вміння чітко і зрозуміло комунікувати свої ідеї та рекомендації. Вони повинні бути здатні пояснити складні технічні концепції нерозуміючим людям та спілкуватися з різними зацікавленими сторонами.

Враховуючи ці критерії, компанії можуть вибрати кваліфікованих експертів у галузі кібербезпеки, які здатні забезпечити надійний захист інформаційних систем та виявляти потенційні загрози.

У таблиці 3.1 наведено отримані дані під час проведення експерименту роботи експертів без розробленої СППР та з нею.

Таблиця 3.1

Результати проведення експерименту роботи експертів самостійно та за допомогою інтерфейсу СППР «InvestSecurely»

СППР «InvestSecurely»	Експерти
0,6	0,58
0,78	0,59
0,78	0,57
0,79	0,67
0,73	0,68
0,77	0,73
0,76	0,68
0,77	0,69
0,72	0,71
0,68	0,63

Отже, на рис. 3.20 показані результати оцінювання експертами самостійно та за допомогою СППР «InvestSecurely» актуальності інвестування в ЗЗІ ОБІ. Як бачимо, при самостійній оцінці необхідності інвестування в КБ ОБІ розкид думок експертів був набагато ширшим, ніж при використанні СППР. Вісь ординат означає параметр (p), вісь абсциса – порівняння роботи еспертів самостійно (червоні стовпці) та за допомогою інтерфейсу СППР «InvestSecurely» (сині стовпці). Еталонне значення параметрів (p), що оцінюються прийнято рівним 1. Якщо оцінка параметра дорівнює 0 – захист відсутній.

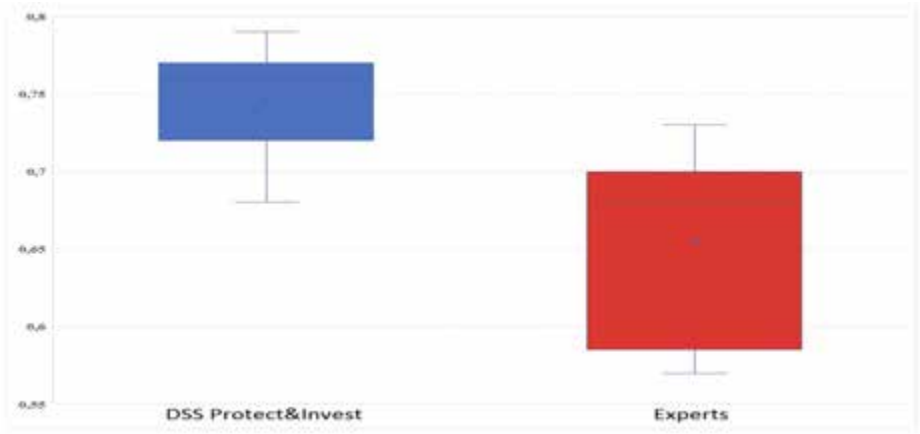


Рисунок 3.20 – Результати оцінювання експертами самостійно та за допомогою СППР ступеня захищеності ОБІ

У таблиці 3.2 наведено отримані дані під час проведення експерименту порівняння часу (у хвилинах) роботи експертів без розробленої СППР «InvestSecurely» та з нею.

Таблиця 3.2

Результати проведення експерименту порівняння часу (у хвилинах), що витрачається експертами самостійно та за допомогою інтерфейсу СППР

СППР «InvestSecurely»	Експерти
9	25
13	39
16	38
16	36
10	32
11	34
11	34

На рис. 3.21. показана гістограма порівняння часу (у хвилинах), що витрачається експертами самостійно (червоні стовпці) та за допомогою інтерфейсу СППР (сині стовпці), на вибір стратегії інвестування в КБ захисного вузла ОБІ. Вісь ордината означає кількість експертів, що приймали участь у дослідженні, вісь абсциса – час (у хвилинах), за який вони впоралися з роботою самостійно та за допомогою запропонованої СППР «InvestSecurely».

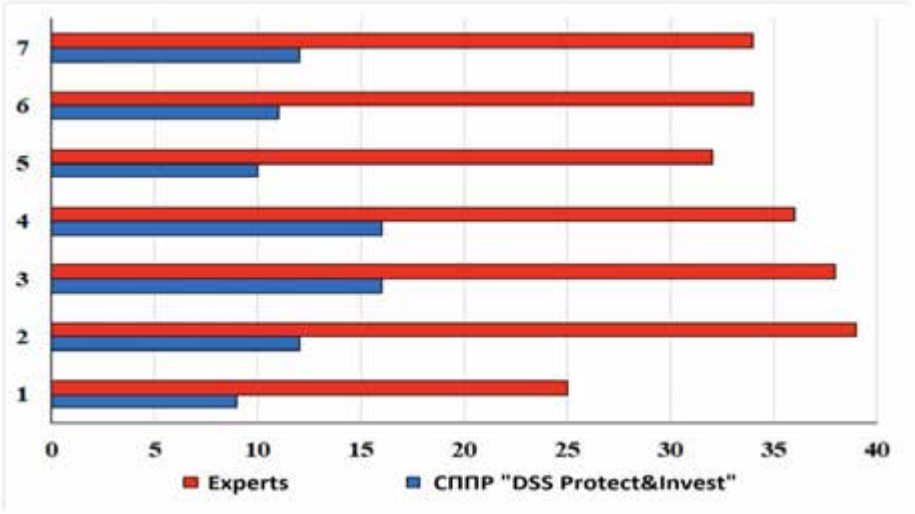


Рисунок 3.21 – Час, що витрачається експертами самостійно та за допомогою інтерфейсу СППР для вибору стратегії інвестування в КБ захисного вузла ОБІ

Беручи до уваги результати оцінювання експертами самостійно та за допомогою СППР ступеня захищеності ОБІ, зображеного на рис. 3.20, доведено, що розбіжність у поглядах експертів, які використовували СППР на 13–16 % менше, ніж для варіанта оцінювання без використання даного ПЗ.

І, що є дуже важливим, у ході тестування на СППР «InvestSecurely» 45–55 %. скоротилися витрати часу на оцінювання стратегій інвестування в КБ.

ВИСНОВКИ ПО РОБОТІ

У ході написання магістерської роботи було детально вивчено теоретичну базу досліджуваної проблеми, виконано комплекс важливих досліджень та випробувань, у результаті яких науково обґрунтовано створення системи підтримки прийняття рішень «InvestSecurely».

Показано, що в умовах нестійкої ринкової економіки процес інвестування з системи КБ ОБІ потребує проведення значних робіт аналітиками та експертами, від збору та обробки інформації, і до розроблення стратегії інвестування, що відповідає зазначеним цілям і завданням. Показано, що більшість попередніх досліджень часто мають лише економічний характер і не враховують тенденції щодо впровадження інформаційних технологій у процедури контролю та прийняття рішень для інвестиційних проектів у сфері захисту інформації та КБ.

Розроблено СППР «InvestSecurely» з інвестування у кібербезпеку об'єктів інформатизації. Показано, що ця СППР дозволяє експертам в режимі онлайн оцінювати стратегії інвестування в різні об'єкти інформатизації, зокрема, критично важливі комп'ютерні системи. СППР дозволяє реалізовувати оцінку привабливості інвестиційних проєктів у сфері захисту інформації та кібербезпеки підприємств. Обчислювальне ядро базується на методах теорії ігор.

СППР «InvestSecurely» дозволить зменшити розбіжності даних прогнозування та реальної віддачі від інвестування в контури захисту інформації, кібербезпеки підприємств та ОБІ. Розбіжність у поглядах експертів, які використовували СППР на $13-16$ % менше, ніж для варіанта оцінювання без використання даного СППР «InvestSecurely».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 18 стартапів у галузі кібербезпеки, які заслуговують на увагу. - Доступний з https://cisoclub.ru/18-startapov-v-oblasti-kiberbezopasnosti-kotoryе-zasluzhivayut-vnimaniya/.

2. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / Г.Я. Аніловська. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf

3. Безнікін, Дмитро Сергійович; Ремпель, Анастасія Віталіївна; Ожерельєва, Олександра Романівна. Інвестування над ринком інформаційних технологій. Синергія Наук, 2018, 25: 168-173..

4. Бікмаєва, Катерина Валеріївна, and Руслан Іванович Баженов. "Про оптимальний вибір системи захисту інформації від несанкціонованого доступу." APRIORI. Серія: Природні та технічні науки 6 – 2014-.Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ : НІСД, 2012. 96 с.

5. Бондар, І. В., et al. "Система підтримки прийняття рішень щодо захисту інформації "Оазис"." Програмні продукти та системи 3 - 2011 -: 177-180.Волошин О. Концепція аналізу та прийняття рішень при моделюванні сталого розвитку національної економіки. // О. Волошин, В. Кудін, В. Кулик // XX Міжнародна конференція «Знання – Діалог – Рішення» (“Knowledge – Dialogue - Solution”), С. 17–20., 2014.

6. Герасименко О.В. Інформаційна безпека підприємства: поняття та методи її забезпечен- ня / О.В. Герасименко, А.В. Козак. [Електронний ресурс]. – Доступний з http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-za- bezpechennya/

7. Глушаков С.В., Хачаров Т.С., Соболєв Р.О. Секрети хакера: захист та атака. Харків: Фоліо, 2008. 414 с.

8. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства/Г.С. Гриджук. [Електронний ресурс]. – Доступний з http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf

9. Грицюк Юрій. Обґрунтування потреби захисту інформаційних ресурсів підприємства / Юрій Грицюк, Ольга Сівець // Інформаційна безпека в сучасному суспільстві : матер. II Між- нар. наук.-техн. конф., 24-25 листопада 2016, м. Львів, Україна. – Львів : Вид-во ЛДУ БЖД, 2016. – С. 41-43.

10. Грищук Р., Охрімчук В., Ахтирцева В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак // Захист інформації. 2016. Т. 18, № 1. С. 21–29.

11. Давиденко А. М., Суліма О. А. Використання формальних засобів опису процесів надання повноважень // Захист інформації. 2016. Т. 18, № 2. С. 143–149.

12. Давиденко А.М., Головань С.М., Щербак Л.М. Аналіз дій загроз у автоматизованих системах обробки інформації // Моделювання та інформаційні технології. 2006. Вип. № 36. С. 3–8.

13. Давиденко А.М., Головань С.М., Щербак Л.М. Структурована база загроз для інформації в інформаційних системах // Моделювання та інформаційні технології. 2006. Вип. 32. С. 17–22.

14. Джеймс Л. Фішінг. Техніка комп'ютерних злочинів М.: НТ Прес, 2008. 320 с.

15. Довбиш А.С. Основи проектування інтелектуальних систем : Навч. посіб. / А.С. Довбиш. – Суми : СумДУ, 2009. – 170 с.

16. Жаринова, Світлана Сергіївна, та Олексій Олександрович Бабенко. "Оптимізація інвестицій в інформаційну безпеку підприємства." Інформаційні системи та технології 83.3 – 2014 -: 114.

17. Жук, Олександр Павлович, Дмитро Леонідович Осипов, і Олексій Андрійович Гавришев. "Оцінка фінансових витрат на побудову засобів захисту інформації за допомогою системи підтримки прийняття рішень." Інфокомунікаційні технології 13.4 – 2015: 451-457.

18. Журиленко, Б. – 2012. – Математична модель ймовірнісної надійності комплексу технічного захисту інформації. Безпека інформації (2), 61-65.

19. Журиленко, Б., Ніколаєва, Н., & Пєліх, Н. - 2011. - Оптимальні фінансові витрати та основні критерії побудови або модернізації комплексу технічного захисту інформації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 33-43.

20. Звєрєв, Ілля Миколайович. "Застосування методу аналізу ієрархій у порівнянні DLP-систем." Природні та математичні науки в сучасному світі 20 – 2014. – 1-11.

21. Зібін, С. В. – 2017. – Підсистеми та модулі системи підтримки прийняття рішень. Алгоритми функціонування. Телекомунікаційні та інформаційні технології, (4), 58-70.

22. Іванов, С. О., Ільїна, Л. А., Ільїн, Д. В. – 2019. - Формування системи захисту інформації організації, що відповідає актуальним вимогам. Інноваційний розвиток економіки (3), 171-181.

23. Карпінський Н.П., Корченко О.О., Ахметова С. Т. Метод формування базових детекційних правил для систем виявлення вторгнень // Захист інформації. 2015. Том 17, № 4. С. 312-324.

24. Козунова, С. С., & Бабенко, А. А. – 2016. – Система оптимізації ризиків інвестування інформаційної безпеки промислових підприємств. Вісник комп'ютерних та інформаційних технологій, (7), 22-29.Козунова, С. С., & Бабенко, А. А. - 2017. - Методика инвестирования информационной безопасности организации. NBI-technologies, 11(4). 42-51.

25. Корнієнко Б.Я., Щербак Л. Н. Аналіз дії та методів протидії інформаційним загрозам типу "Riskware" // Захист інформації. 2008. № 1. С. 54-59.

26. Л.Д. Плиска В.А. Лахно. Модель для опису процесу інвестування у кібербезпеку /Комплексне забезпечення якості технологічних процесів та систем: зб. матеріалів IX міжнародної науково-практичної конференції (м. Чернігів, 14-16 травня 2019 р.). Чернігів. С. 198.

27. Л.Д. Плиска, В.А. Лахно. "Основні загрози кібербезпеки" / Інформаційні технології: Економіка, техніка, освіта 2019: зб. матеріалів X міжнародної науково-практичної конференції (м. Київ, 13-14 листопада 2019 р.). Київ. С. 252-253.

28. Л.Д. Плиска, В.А. Лахно. / Прийняття інвестиційних рішень щодо кібербезпеки / Інформаційні технології: Економіка, техніка, освіта 2022: зб. матеріалів XIII міжнародної науково-практичної конференції (м. Київ, 26-27 жовтня 2022 р.). Київ. С. 116-117.

29. Л.Д. Плиска, В.А. Лахно. Ключові фактори необхідності інвестування у кібербезпеку / Прикладні системи та технології в інформаційному суспільстві: зб. матеріалів III міжнародної науково-практичної конференції (м. Київ, 30 вересня 2019 р.). Київ. С. 139-140.

30. Л.Д. Плиска, В.А. Лахно. Методи, моделі та інформаційні технології в спр по інвестуванню у кібербезпеку об’єктів інформатизації / Інформаційні технології: Економіка, техніка, освіта 2018: зб. матеріалів IX міжнародної науково-практичної конференції (м. Київ, 14-15 листопада 2018 р.). Київ. С. 199-200.

31. Л.Д. Плиска, В.А. Лахно. Основні тенденції кібербезпеки 2021 року / Інформаційні технології: Економіка, техніка, освіта 2021: зб. матеріалів XII міжнародної науково-практичної конференції (м. Київ, 11-12 листопада 2021 р.). Київ. С. 150-151.

32. Л.Д. Плиска, В.А. Лахно. Розвиток методів і моделей для оцінювання стратегій інвестування в системи кібербезпеки/ Інформаційна безпека та інформаційні технології: зб. матеріалів міжнародної науково-практичної конференції (м. Харків, 24-25 квітня 2019 р.). Харків. С. 198.

33. Л.Д. Плиска. "Перспективи розвитку кібербезпеки / Інформаційні технології в культурі, мистецтві, освіті, науці, економіці та бізнесі": зб. матеріалів міжнародної науково-практичної конференції (м. Київ, 18-19 квітня 2019 р.). Київ. С. 204-205.

34. Л.Д. Плиска. Інвестування у кібербезпеку з використанням систем підтримки прийняття рішень (СППР) / Сучасні інформаційні та комунікаційні

технології на транспорті, в промисловості та освіті 2018: зб. матеріалів XII міжнародної науково-практичної конференції (м. Дніпро, 12-13 грудня 2018 р.). Дніпро. С. 177.

35. Лахно В.А., Малюков В.П., Плиска Л.Д. Модель стратегій інвестування в системи кібербезпеки ситуаційних центрів транспорту. Кібербезпека: освіта, наука, техніка. 2018. №2 (2). С. 68 – 79

36. . Необоротний тектонічний зсув: де осідають інвестиції у кібербезпеку. https://www.forbes.ru/svoi-biznes/453055-neobratimyj-tektoniceskij-sdvig-gde-osedaut-investicii-v-kiberbezopasnost.

37. Нормативне забезпечення інформаційної безпеки / [за ред. проф. В.О. Хорошка]. Київ : ДУІКТ, 2008. 533 с.

38. Норткат С. Аналіз типових порушень безпеки у мережах. М.: "Вільямс", 2006. 424 с.

39. Поповський В.В., Перенков А.В. Захист інформації у телекомунікаційних системах. У 2-х т. Харків: ТОВ «Компанія ЗМІТ», 2006.

40. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/ Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

41. Стасюк А.И., Корченко А.А. Метод виявлення аномалій породжених кібератаками в комп'ютерних мережах // Захист інформації. 2012. Том 14, № 4. С. 127–132.

42. Стасюк А.И., Корченко А.А. Метод виявлення аномалій породжених кібератаками в комп'ютерних мережах // Захист інформації. 2012. Том 14, № 4. С. 127–132.

43. Хорошко В.А. [и др.]. Методи та засоби захисту інформації. Київ : Юніор, 2003. 504 с.

44. Шведун В. Організаційно-правове забезпечення державного регулювання інформаційної безпеки реклами // Безпека інформації. 2015. Т. 21, № 2. С. 174–178.

45. Шевченко А., Кокотов О. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових

інформаційно-телекомунікаційних систем під час інформаційних операцій // Безпека інформації. 2014. Т. 20, № 1. С. 7–11.

46. Ю.І. Грицюк, Обґрунтування розумної достатності структури системи захисту інформаційних ресурсів підприємства/ Ю.І. Грицюк, О.О. Сівець. [Електронний ресурс]. – Доступний з https://nv.nltu.edu.ua/index.php/journal/article/view/572

47. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення: підручник. Київ : НАУ, - 2011. - 640 с.

48. Юдін О. К., Бучик С. С. Правові аспекти формування системи державних інформаційних ресурсів // Безпека інформації. - 2014. - Т. 20 (1). С. 76–82.

49. Юдін О. К., Бучик С.С., Чунарьова А.В., Варченко О.І. Методологія побудови класифікатора загроз державним інформаційним ресурсам // Наукоємні технології. - 2014. - № 2. С. 200–210.

50. Akdeniz E., Bagriyanik M. A knowledge based decision support algorithm for power transmission system vulnerability impact reduction //International Journal of Electrical Power & Energy Systems. – 2016. – Т. 78. – С. 436-444. (2016) DOI https://doi.org/10.1016/j.ijepes.2015.11.041

51. Akhmetov B. B., Lakhno V. A., Malyukov V. P. “Model of investment strategies in cyber security systems of transport situational centers”, Scientific journal Radio Electronics, Computer Science, Control, 2(45), p. 83, 2018.

52. Akhmetov B. et al. Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity //Proceedings of the Computational Methods in Systems and Software. – Springer, Cham, 2018. – С. 162-171. (2018) DOI https://doi.org/10.1007/978-3-030-00184-1_15

53. Akhmetov B. et al. Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity //Proceedings of the Computational Methods in Systems and Software. – Springer, Cham, 2018. – С. 162-171. (2018) DOI: 10.1007 / 978-3-030-00184-1_15

54. Akhmetov, B. B., Lakhno, V. A., Akhmetov, B. S., & Malyukov, V. P. (2018). The Choice of Protection Strategies During the Bilinear Quality Game On

Cyber Security Financing. Bulletin of The National Academy of Sciences of the Republic of Kazakhstan, (3), pp. 6–14.

55. Arasteh, A. (2017). Considering the investment decisions with real options games approach. Renewable and Sustainable Energy Reviews, 72, pp. 1282-1294.

56. Ахметов Б.С., Ахметов Б.Б., Лахно В.А., Малюков В.П. Фінансові аспекти підтримки кібербезпеки ситуаційних центрів та інформаційних систем транспорту. Монографія. Алмати: вид-во університету "Туран", 2019.-196 с. Табл.6, іл. 50, бібліограф. назв. 81.

57. Lakhno, V., Akhmetov, B., Yagaliyeva, B., Kryvoruchko, O., Desiatko, A., Tsiutsiura, S., Tsiutsiura, M. The Model of Server Virtualization System Protection in the Educational Institution Local Network, (2023) Lecture Notes on Data Engineering and Communications Technologies, 166, pp. 461-475.

58. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., Turgynbayeva, A., Kryvoruchko, O., Chubaievskyi, V., Desiatko, A., Adaptive Monitoring of Companies' Information Security, (2023) International Journal of Electronics and Telecommunications, 69 (1), p. 75-82.

59. Lakhno, V., Malyukov, V., Kasatkin, D., Chubaieskyi, V., Rzaieva, S., Rzaiev, D., Continuous Investing in Advanced Fuzzy Technologies for Smart City, (2023) Lecture Notes on Data Engineering and Communications Technologies, 142, pp. 313-327.

60. Lakhno, V., Akhmetov, B., Smirnov, O., Chubaievskyi, V., Khorolska, K., Bebeshko, B., Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm, (2023) Lecture Notes on Data Engineering and Communications Technologies, 131, p. 21-34.