

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ПЛИСКА ЛЮБОВ ДМИТРІВНА

УДК 004.942:004.056

ДИСЕРТАЦІЯ

**МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМАХ
ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ З ІНВЕСТИВАННЯ У
КІБЕРБЕЗПЕКУ ОБ'ЄКТІВ ІНФОРМАТИЗАЦІЇ**

122 «КОМП'ЮТЕРНІ НАУКИ»

(12 – «Інформаційні технології»)

Подається на здобуття наукового ступеня доктора філософії з технічних наук

Дисертація містить результати власних досліджень. Використання ідей,
результатів, текстів інших авторів мають посилання на відповідне джерело

Л.Д. Плиска

Науковий керівник **Ляхно Валерій Анатолійович** — доктор технічних наук,
професор

Київ 2022

АНОТАЦІЯ

Плиска Л.Д. Методи, моделі та інформаційні технології в системах підтримки прийняття рішень з інвестування у кібербезпеку об'єктів інформатизації.

Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з технічних наук за спеціальністю 122 «Комп'ютерні науки». Національний університет біоресурсів і природокористування України. Київ, 2023.

Дисертаційну роботу присвячено розвитку математичних методів та моделей для обчислювального ядра системи підтримки прийняття рішень, які використовуються для пошуку оптимальних стратегій інвестування в засоби захисту інформації та системи кібернетичної безпеки різних об'єктів інформатизації.

Об'єктивна необхідність вирішення багатокритеріального оптимізаційного завдання управління ресурсами, що виділяються на забезпечення інформаційної безпеки, така, що особи, які приймають рішення, змушені діяти в динамічно складних ситуаціях. Подібні ситуації обумовлені ландшафтом кібернетичних загроз, що постійно змінюється, збільшенням складності кібератак, варіативністю використовуваних атакувальною стороною сценаріїв для проведення атак і т.д.

Інвестиції в інноваційні проєкти, наприклад, у галузі інформаційних технологій та кібербезпеки, у багатьох випадках характеризуються надзвичайно великою ймовірністю неточності обчислень та ризику. Для підвищення ефективності та оптимізації процедур оцінки проєктів та підтримки прийняття рішень, пов'язаних із інвестуванням, часто використовують системи аналізу даних. Створені системи підтримки прийняття рішень отримали добрі відгуки, пов'язані з розв'язанням таких проблем.

Було проаналізовано існуючі математичні моделі, які використовуються для вибору стратегії інвестування в системи кібернетичної безпеки різних

об'єктів інформатизації. У ході роботи детально досліджено й опрацьовано переваги та недоліки цих моделей.

У результаті порівняльного аналізу наукових праць, доведено, що завдання ефективного використання фінансових ресурсів на захист інформації є одним із найголовніших завдань для організацій та компаній, які потребують захисту власної інформації. У нинішніх умовах нестійкої ринкової економіки процес інвестування потребує проведення значних робіт аналітиками та експертами, від збору та обробки інформації, і до розроблення стратегії інвестування, що відповідає зазначеним цілям і завданням. Питання ефективності фінансових інвестицій та контролю над цим процесом є одним із найважливіших у фінансовій сфері. Оптимальне значення ресурсів залежить не лише від уразливості системи, а й від вартості інформації, яка підлягає захисту. Проте, дослідження дуже часто мають лише економічний характер і майже зовсім не враховують тенденції щодо впровадження інформаційних технологій у процедури контролю та прийняття рішень для інвестиційних проєктів. Головним недоліком цих досліджень є відсутність необхідних конкретних рекомендацій щодо формування стратегій фінансових інвестицій.

Результати, отримані у ході написання дисертаційної роботи, дали можливість встановити, що питання ефективності фінансових інвестицій та контролю над цим процесом є одним із найважливіших у фінансовій сфері. Оптимальне значення ресурсів залежить не лише від уразливості системи, а й від вартості цієї інформації, яка підлягає захисту. Разом із тим, у процесі вивчення та дослідження існуючої теоретичної бази визначено проблему, пов'язану з необхідністю розробки нових моделей, заснованих на спільному (гібридному) використанні апарата білінійних диференціальних ігор якості та генетичного алгоритму. Така комбінація для ядра інтелектуальних інформаційних систем у завданнях визначення раціональних стратегій фінансового інвестування у проєкти кібербезпеки не лише має право на існування, а і здатна, на нашу думку, дати позитивний ефект.

Вперше описано метод вибору раціональної стратегії інвестування у проєкти із забезпечення кібербезпеки об'єкта інформатизації, основні комбінації теорії ігор та генетичного алгоритму, як методу багатфакторної оптимізації, оскільки вони є винятково актуальними на сьогоднішній день.

Показано, що використання на першому етапі даного методу лише апарату білінійних динамічних ігор якості, дає результат, у якому кожна точка, відповідна стратегії інвестора, буде набором певних компонентів інвестування. Ці компоненти відповідають фінансовим ресурсам. 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. Це, як результат, диктує необхідність витрат додаткового часу для аналізу цих точок та пошуку області переваги інвестора.

У ході роботи встановлено, що застосування генетичного алгоритму на другому етапі запропонованого методу вибору раціональної стратегії інвестування у проєкти із забезпечення кібербезпеки об'єктів інформатизації усуває зазначений вище недолік.

Окрім того, запропоновано застосовувати модифікований генетичний алгоритм для вирішення завдання, пов'язаного з отриманням прогнозованої оцінки віддачі від різних напрямків інвестування у проєкти кібербезпеки об'єктів інформатизації. Це дозволяє потенційним інвесторам на стадії оцінки привабливості окремих проєктів, пов'язаних із розвитком кібербезпеки об'єктів інформатизації, отримувати прогнозні оцінки перспективності обраних стратегій інвестування шляхом визначення значущих факторів зростання віддачі від інвестування в кібербезпеку об'єктів інформатизації, а також відстеження точок зростання та структурних змін.

При комбінованому підході на першому етапі за допомогою системи диференціальних рівнянь для білінійної динамічної гри якості з кількома

термінальними поверхнями збирається, фактично, лише статистика варіантів рішень. А безпосередньо обробка та пошук підсумкової раціональної стратегії інвестора знаходиться за допомогою генетичного алгоритму. Даний генетичний алгоритм було застосовано для реалізації комбінованої обчислювальної процедури як додатковий інструмент зменшення невизначеності множини стабільних узагальнених ϵ -рівноваг гри.

Показано, що запропонований метод може бути застосований для скорочення часу в ході вирішення задачі пошуку раціональних (оптимальних) стратегій інвесторів на основі ігрових моделей у поєднанні з генетичним алгоритмом, зокрема в умовах динамічного протистояння зі стороною, що атакує, коли оцінка раціональної стратегії інвестування виключно важлива для сторони захисту. Комбінований підхід показує коротший час для пошуку рішень у конкретній ситуації.

Отримала подальший розвиток методика проектування системи підтримки прийняття рішень, для розв'язання задач оцінки стратегій інвестування в кібербезпеку об'єктів інформатизації.

У дисертаційній роботі виконано комплекс досліджень та випробувань, у результаті яких науково обґрунтовано розробку системи підтримки прийняття рішень «DSS Protect&Invest» у процесі аналізу та вибору раціонального (оптимального) варіанта стратегії інвестування в системи кібербезпеки. Крім того, розглянуто ключові функціональні модулі подібної системи підтримки прийняття рішень, які сприяють забезпеченню безперервного та ефективного функціонування системи захисту інформаційних ресурсів об'єктів інформатизації будь-якого масштабу.

Реалізація системи підтримки прийняття рішень «DSS Protect&Invest» виконана за модульним принципом. Це дає можливість доповнювати систему підтримки прийняття рішень іншими модулями. Запропонована система підтримки прийняття рішень «DSS Protect&Invest» є досить універсальною і може бути розширена за рахунок функціоналу інших підзадач.

Показано, що ця система підтримки прийняття рішень дозволяє експертам у режимі онлайн оцінювати стратегії інвестування в різні об'єкти інформатизації, зокрема, критично важливі комп'ютерні системи. Запропонована система підтримки прийняття рішень «DSS Protect&Invest» дозволяє реалізовувати оцінку привабливості інвестиційних проєктів у сфері захисту інформації та кібербезпеки підприємств. Обчислювальне ядро системи підтримки прийняття рішень «DSS Protect&Invest» базується на методах теорії ігор, а також на вперше отриманому математичному рішенні, яке засноване на інструментарії багатогранних ігор якості з кількома термінальними поверхнями, причому пошук траєкторії на безлічі точок, що формують термінальну поверхню інвестора, вперше реалізований на основі генетичного алгоритму. Важливо, що система підтримки прийняття рішень «DSS Protect&Invest» дозволяє автоматизувати в режимі онлайн отримання прогнозованих оцінок для різних варіантів розподілу фінансових ресурсів інвестора (інвесторів), що витрачаються на фінансування різних об'єктів контурів захисту інформації критично важливих комп'ютерних систем.

Показано, що розроблена система підтримки прийняття рішень «DSS Protect& Invest» дозволить зменшити розбіжності даних прогнозування та реальної віддачі (результатів) від інвестування в контури захисту інформації, кібербезпеки підприємств та об'єктів інформатизації. Також можлива оптимізація стратегій вкладення коштів в об'єкти інформатизації різними сторонами інвестиційного процесу. Розбіжність у поглядах експертів, які використовували систему підтримки прийняття рішень «DSS Protect&Invest», на 13–16 % менше, ніж для варіанта оцінювання без використання даного ПЗ. У ході тестування системи підтримки прийняття рішень «DSS Protect&Invest» на 45–55 % скоротилися витрати часу на оцінювання стратегій інвестування в кібербезпеці об'єктів інформатизації.

Доведено, що застосування в системі підтримки прийняття рішень, запропонованих моделей, дозволяє прискорити пошук оптимальних варіантів розміщення засобів кібербезпеки та захисту інформації для об'єктів

інформатизації більш ніж у 15–20 разів. Ця перевага дозволяє виконати швидкий перебір різних варіантів апаратно-програмних засобів захисту інформації та їх комбінацій для об'єктів інформатизації, а також задіяти комбінацію апарату теорії ігор та генетичного адгоритму під час оптимізації пошуку стратегій відбору засобів захисту інформатизації для об'єктів інформатизації. Потенційно така інтеграція моделей і методів дає можливість швидко перебудовувати захист об'єктів інформатизації, адаптуючи їх до інформації про можливість реалізації нових кіберзагроз, зокрема, на основі даних, що динамічно змінюються, про стан захисту об'єктів інформатизації.

Ключові слова: система підтримки прийняття рішень; засоби захисту інформації; математична модель; кібербезпека; теорія ігор; генетичний алгоритм.

ABSTRACT

Plyska L.D. Methods, models and information technologies in decision-making support systems for investing in cyber security of informatization objects.

Qualified scientific work on manuscript rights.

Thesis for obtaining the scientific degree of Doctor of Philosophy in technical sciences in the specialty 122 - Computer science. National University of Life and Environmental Sciences of Ukraine. Kyiv. 2023.

The thesis is devoted to the development of mathematical methods and models for the computing core of the decision support system, which are used to find optimal strategies for investing in information protection and cyber security systems of various informatization objects.

The objective necessity of solving a multi-criteria optimization task of managing resources allocated to information security is such that decision-makers are forced to act in dynamically complex situations. Such situations are caused by the ever-changing landscape of cyber threats, the increasing complexity of cyber attacks, the variability of the scenarios used by the attacking party to carry out attacks, etc.

Investments in innovative projects, for example, in the field of information technology and cyber security, in many cases are characterized by an extremely high probability of calculation inaccuracy and risk. Data analysis systems are often used to improve the efficiency and optimization of project evaluation procedures and to support investment decision-making. The created decision support systems received good reviews related to the solution of such problems.

Existing mathematical models used to choose a strategy for investing in cyber security systems of various informatization objects were analyzed. In the course of the work, the advantages and disadvantages of these models were studied and worked out in detail.

As a result of the comparative analysis of scientific works, it has been proven that the task of effective use of financial resources for information protection is one of the most important tasks for organizations and companies that need to protect their own

information. In the current conditions of an unstable market economy, the investment process requires significant work by analysts and experts, from the collection and processing of information to the development of an investment strategy that meets the stated goals and objectives. The question of the effectiveness of financial investments and control over this process is one of the most important in the financial sphere. The optimal value of resources depends not only on the vulnerability of the system, but also on the value of the information to be protected. However, studies are very often only of an economic nature and almost do not take into account the trends in the implementation of information technologies in the control and decision-making procedures for investment projects. The main drawback of these studies is the lack of necessary specific recommendations for the formation of financial investment strategies.

The results obtained during the writing of the dissertation made it possible to establish that the question of the effectiveness of financial investments and control over this process is one of the most important in the financial sphere. The optimal value of resources depends not only on the vulnerability of the system, but also on the value of the information to be protected. At the same time, in the process of studying and researching the existing theoretical base, a problem related to the need to develop new models based on the joint (hybrid) use of the apparatus of bilinear differential games of quality and the genetic algorithm was identified. Such a combination for the core of intelligent information systems in the task of determining rational strategies for financial investment in cyber security projects not only has the right to exist, but is also capable, in our opinion, of giving a positive effect.

For the first time, the method of choosing a rational investment strategy in projects to ensure cyber security of the informatization object, the main combinations of game theory and genetic algorithm, as they are extremely relevant today, are described. This genetic algorithm was applied to implement a combined computational procedure as an additional tool for reducing the uncertainty of the set of stable generalized ε -equilibria of the game.

It is shown that the use of only the apparatus of bilinear dynamic quality games at the first stage of this method gives a result in which each point corresponding to the investor's strategy will be a set of certain investment components. These components correspond to financial resources. The sets of points that will be located on the terminal surface of each of the investors characterize specific investment programs. The solutions by themselves, taking into account the application of the system of differential equations for the bilinear dynamic game of quality with several terminal surfaces, give a rather large spread of options for points on the terminal surfaces of investors. This, as a result, dictates the need to spend additional time to analyze these points and find the area of investor's advantage.

In the course of the work, it was established that the application of the genetic algorithm at the second stage of the proposed method of choosing a rational investment strategy in projects to ensure the cyber security of informatization objects eliminates the above-mentioned shortcoming.

In addition, it is proposed to use a modified genetic algorithm to solve the problem of obtaining a forecasted estimate of return from various directions of investment in cyber security projects of informatization objects. This allows potential investors at the stage of assessing the attractiveness of individual projects related to the development of cyber security of informatization objects, to obtain predictive assessments of the prospects of selected investment strategies by determining significant factors for the growth of returns from investing in cyber security of informatization objects, as well as tracking growth points and structural changes.

In the combined approach, at the first stage, using a system of differential equations for a bilinear dynamic game of quality with several terminal surfaces, only the statistics of decision options are collected. And the processing and search of the final rational strategy of the investor is done directly with the help of a genetic algorithm.

It is shown that the proposed method can be applied to reduce the time in solving the problem of finding rational (optimal) strategies of investors based on game models in combination with a genetic algorithm, in particular in the conditions of dynamic

confrontation with the attacking side, when the evaluation of the rational investment strategy is extremely important for the defense side. The combined approach shows a shorter time for finding solutions in a specific situation.

The method of designing a decision-making support system for solving the problems of evaluating strategies for investing in the cyber security of informatization objects received further development.

In the dissertation work, a set of research and tests was carried out, as a result of which the development of the decision support system "DSS Protect&Invest" was scientifically substantiated in the process of analysis and selection of a rational (optimal) variant of the strategy for investing in cyber security systems. In addition, the key functional modules of a similar decision-making support system are considered, which contribute to ensuring the continuous and effective functioning of the information resource protection system of informatization objects of any scale. The implementation of the DSS Protect&Invest decision support system is based on a modular principle. This makes it possible to supplement the decision support system with other modules. The proposed decision support system "DSS Protect&Invest" is quite universal and can be expanded due to the functionality of other subtasks.

It is shown that this decision support system allows experts to evaluate online investment strategies in various informatization objects, in particular, critical computer systems. The proposed decision support system "DSS Protect&Invest" allows to evaluate the attractiveness of investment projects in the field of information protection and cyber security of enterprises. The computing core of the decision support system "DSS Protect&Invest" is based on game theory methods, as well as on a mathematical solution obtained for the first time, which is based on the toolkit of multifaceted quality games with several terminal surfaces, and the search for a trajectory on a set of points forming the investor's terminal surface is for the first time implemented on the basis of a genetic algorithm. It is important that the decision support system "DSS Protect&Invest" allows you to automate online the receipt of forecasted estimates for various options for the distribution of financial resources of the investor (investors),

which are spent on financing various objects of information protection contours of critical computer systems.

It is shown that the developed decision support system "DSS Protect&Invest" will allow to reduce discrepancies between forecast data and real returns (results) from investing in the contours of information protection, cyber security of enterprises and informatization objects. At the same time, it is possible to optimize strategies for investing funds in informatization objects by various parties of the investment process. The difference in opinions of experts who used the decision support system "DSS Protect&Invest" is 13-16% less than for the evaluation option without using this software. During testing of the DSS Protect&Invest decision support system, 45–55% of the time spent on evaluating investment strategies in the cyber security of informatization objects has decreased. At the same time, it is possible to optimize investment strategies in informatization objects by various parties of the investment process.

It is proven that the application of the proposed models in the decision support system allows to accelerate the search for optimal options for placing cyber security and information protection tools for informatization objects by more than 15-20 times. This advantage allows you to perform a quick review of various options for hardware and software information protection tools and their combinations for informatization objects, as well as to use a combination of the game theory apparatus and a genetic algorithm during the optimization of the search for strategies for the selection of information protection tools for informatization objects. Potentially, such an integration of models and methods makes it possible to quickly rebuild the protection of informatization objects, adapting them to information about the possibility of new cyber threats, in particular, based on dynamically changing data about the state of protection of informatization objects.

Keywords: decision support system; means of information protection; mathematical model; cyber security; game theory; genetic algorithm.

СПИСОК ОПУБЛІКОВАНИХ НАУКОВИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Стаття у науковому виданні іншої держави, яке включено до міжнародної наукометричної бази даних Web of Science

1. B. B. Akhmetov, V. A. Lakhno, A. B. Adranova, L. M. Kydyralina, **L. D. Plyska**. Analysis of mathematical models of investment strategies in the university on cyber security systems. *Bulletin of national academy of sciences of the republic of Kazakhstan*, 2020. Volume 1, Number 383 (2020), 128 – 139.

Стаття у науковому фаховому виданні України, яке включено до міжнародної наукометричної бази даних Scopus

1. Lakhno, V., Malyukov, V., Akhmetov, B., Kasatkin, D., **Plyska, L.** Development of a model for choosing strategies for investing in information security. *Eastern-European Journal of Enterprise Technologies*, 2021. 2(3 (110)), 43–51.

Стаття у науковому фаховому виданні України

1. **Plyska L.**, Maliukov V. Optimization of the method of choosing the investment strategy of information security equipment based on the combination of game theory and the genetic algorithm. *Cybersecurity: education, science, technique*. 2022. №4 (16). P. 172 – 184.

Стаття в наукових виданнях України

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

Тези наукових доповідей

1. Методи, моделі та інформаційні технології в системах підтримки прийняття рішень (СППР) по інвестуванню у кібербезпеку об'єктів інформатизації / **Л.Д. Плиска**, В.А. Лахно. *Інформаційні технології: Економіка, техніка, освіта 2018*: зб. матеріалів IX міжнародної науково-практичної конференції (м. Київ, 14-15 листопада 2018 р.). Київ. С. 199-200.
2. Інвестування у кібербезпеку з використанням систем підтримки прийняття рішень (СППР) / **Л.Д. Плиска**. *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.
3. Перспективи розвитку кібербезпеки / **Л.Д. Плиска**. *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.
4. Основні загрози кібербезпеки / **Л.Д. Плиска**, В.А. Лахно. *Інформаційні технології: Економіка, техніка, освіта 2019*: зб. матеріалів X міжнародної науково-практичної конференції (м. Київ, 13-14 листопада 2019 р.). Київ. С. 252-253.
5. Ключові фактори необхідності інвестування у кібербезпеку / **Л.Д. Плиска**, В.А. Лахно. *Прикладні системи та технології в інформаційному суспільстві*: зб. матеріалів III міжнародної науково-практичної конференції (м. Київ, 30 вересня 2019 р.). Київ. С. 139-140.
6. Модель для опису процесу інвестування у кібербезпеку / **Л.Д. Плиска**, В.А. Лахно. *Комплексне забезпечення якості технологічних процесів та систем*: зб. матеріалів IX міжнародної науково-практичної конференції (м. Чернігів, 14-16 травня 2019 р.). Чернігів. С. 198.
7. Розвиток методів і моделей для оцінювання стратегій інвестування в системи кібербезпеки / **Л.Д. Плиска**, В.А. Лахно. *Інформаційна*

безпека та інформаційні технології: зб. матеріалів міжнародної науково-практичної конференції (м. Харків, 24-25 квітня 2019 р.). Харків. С. 198.

8. Analysis of models for selection of investment strategies / **L. Plyska**, V.Lakhno. *Problems of Infocommunications. Science and Technology PIC S&T'2020*: collection of materials international Scientific-Practical conference (Kharkiv, October 6-9 2020 Ukraine). Kharkiv, 2020. P. 43 – 46 (Scopus).

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

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

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	17
ВСТУП.....	19
РОЗДІЛ 1. ОГЛЯД ПОПЕРЕДНІХ ДОСЛІДЖЕНЬ ТА АНАЛІЗ ВЖЕ ІСНУЮЧИХ МАТЕМАТИЧНИХ МОДЕЛЕЙ.....	25
1.1 Актуальність досліджень, пов'язаних із проблематикою інвестування в кібербезпеку об'єктів інформатизації.....	25
1.2 Аналіз моделей інвестування в кібербезпеку об'єктів інформатизації	32
ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ	56
РОЗДІЛ 2. ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ НА ОСНОВІ КОМБІНАЦІЇ ТЕОРІЇ ІГОР ТА ГЕНЕТИЧНОГО АЛГОРИТМУ	57
2.1 Задача пошуку раціональних стратегій інвестування в кібербезпеку об'єкта інформатизації.....	57
2.2 Забезпечення кібербезпеки об'єкта інформатизації за допомогою генетичного алгоритму	83
ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ	99
РОЗДІЛ 3. РОЗРОБКА ПРОГРАМНОГО ПРОДУКТУ СППР У ПРОЦЕСІ ІНВЕСТИВАННЯ В КІБЕРБЕЗПЕКУ ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ....	101
3.1 Обґрунтування архітектури СППР у процесі прийняття рішень щодо вибору раціональної стратегії інвестування в КБ ОБІ.....	101
3.2 Реалізація СППР у процесі прийняття рішень щодо вибору раціональної стратегії інвестування в КБ ОБІ.....	109
ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ.....	133
ВИСНОВКИ.....	136
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	139
ДОДАТКИ	156

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;

ГА - Генетичний алгоритм;

КБ - Кібербезпека;

ПС - 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, а основою всіх бізнес-процесів є інформаційні технології. Головною умовою конкурентоспроможності та розвитку для організацій, компаній служить грамотно побудований захист інформації. Слабка захищеність даних може призвести до серйозних проблем для бізнесу, які здатні спричинити його повну зупинку.

Сьогодні існує тенденція збільшення фінансових надходжень від злочинних організацій та збільшення атак на інформаційні системи. Сучасні кібератаки сприяли розвитку досліджень, які пов'язані з інтелектуалізацією обчислень у сфері підтримки прийняття рішень захисту інформації та кібербезпеки для різних інформаційних систем та технологій. Водночас розробляються нові методи та моделі для підтримки прийняття рішень щодо вибору стратегій фінансування.

Інвестиції в інноваційні проєкти, наприклад, у галузі інформаційних технологій та кібербезпеки, у багатьох випадках характеризуються надзвичайно великою ймовірністю неточності обчислень та ризику. Для підвищення ефективності та оптимізації процедур оцінки проєктів та підтримки прийняття рішень, пов'язаних із інвестуванням, часто використовують системи аналізу даних. Створені системи підтримки прийняття рішень отримали добрі відгуки, пов'язані з розв'язанням таких проблем.

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

Мета і завдання дослідження. Метою дисертаційної роботи є розвиток математичних методів та моделей для обчислювального ядра системи підтримки прийняття рішень, які використовуються для пошуку оптимальних стратегій

інвестування у засоби захисту інформації та системи кібернетичної безпеки різних об'єктів інформатизації.

Відповідно до зазначеної мети в дисертаційній роботі для її досягнення поставлені такі завдання:

- здійснити огляд попередніх досліджень та аналіз існуючих математичних моделей, які використовуються для вибору стратегії інвестування в системи кібернетичної безпеки різних об'єктів інформатизації;
- розробити метод вибору раціональної стратегії інвестування в проєкти із забезпечення кібербезпеки об'єкта інформатизації на основі комбінації теорії ігор та генетичного алгоритму, як методу багатофакторної оптимізації;
- доповнити методику проєктування системи підтримки прийняття рішень, для розв'язання завдань оцінки стратегій інвестування в кібербезпеку об'єктів інформатизації, розробити та реалізувати систему підтримки прийняття рішень на основі комбінації теорії ігор та генетичного алгоритму для вибору стратегії інвестування в системи кібернетичної безпеки різних об'єктів інформатизації.

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

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

Методи дослідження. Для досягнення мети, поставленої в роботі, використовувалися такі методи дослідження: методи системного аналізу для опису концептуальної моделі системи підтримки прийняття рішень у процесі пошуку оптимальних стратегій інвестування в системи кібернетичної безпеки для системи підтримки прийняття рішень; 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; генетичний алгоритм для пошуку оптимальної стратегії інвестора у сфері переваги сторони захисту різних об'єктів інформатизації; методи об'єктно-орієнтованого програмування для реалізації системи підтримки прийняття рішень, комп'ютерного та імітаційного моделювання з метою оцінки ефективності запропонованих у дисертації рішень.

Наукова новизна одержаних результатів:

- вперше запропоновано метод вибору раціональної стратегії інвестування в проєкти із забезпечення кібербезпеки об'єкта інформатизації на основі комбінації теорії ігор та генетичного алгоритму, як методу багатофакторної оптимізації, який, на відміну від існуючих, дозволяє спочатку знаходити стратегію інвестування шляхом розв'язання системи диференціальних рівнянь для білінійної динамічної гри якості з кількома термінальними поверхнями, а потім - задіяти генетичний алгоритм для пошуку рішення переваги інвестора;

- отримав подальший розвиток метод розв'язання багатокритеріальних задач по вибору методів та засобів забезпечення кібербезпеки на базі використання модифікованого генетичного алгоритму та відповідна інформаційна технологія опрацювання даних для розв'язання завдання, пов'язаного з отриманням прогностичної оцінки віддачі від різних напрямків інвестування у проєкти кібернетичної безпеки різних об'єктів інформатизації, який, на відміну від існуючих, дозволяє, отримувати прогнозовані оцінки перспективності обраних стратегій інвестування шляхом визначення значущих факторів зростання віддачі від інвестування в кібернетичну безпеку різних об'єктів інформатизації;

- подальший розвиток отримала методика проєктування системи підтримки прийняття рішень, для розв'язання завдань оцінки стратегій інвестування у кібербезпеку об'єктів інформатизації, що дозволяє експертам за допомогою інформаційних технологій у режимі онлайн оцінювати стратегії інвестування в різні об'єкти інформатизації.

Практична цінність одержаних результатів. Розроблена система підтримки прийняття рішень «DSS Protect&Invest» у процесі аналізу та вибору стратегії інвестування в системи кібербезпеки. Вище зазначена система дозволяє експертам у режимі онлайн оцінювати стратегії інвестування в різні об'єкти інформатизації, зокрема, критично важливі комп'ютерні системи. Система підтримки прийняття рішень «DSS Protect&Invest» дозволяє реалізовувати оцінку привабливості інвестиційних проєктів у сфері захисту інформації та кібербезпеки підприємств. Це дозволить, що важливо, автоматизувати в режимі онлайн отримання прогнозованих оцінок для різних варіантів розподілу фінансових ресурсів інвестора (інвесторів), що витрачаються на фінансування різних об'єктів контурів захисту інформації критично важливих комп'ютерних систем.

Слід зазначити, що реалізація системи підтримки прийняття рішень «DSS Protect&Invest» виконана за модульним принципом. А це дає можливість доповнювати дану систему іншими модулями. Запропонована система підтримки прийняття рішень «DSS Protect&Invest» є досить універсальною і, при необхідності, може бути розширена за рахунок функціоналу інших підзадач.

У результаті роботи, доведено, що система підтримки прийняття рішень «DSS Protect& Invest» дозволить зменшити розбіжності даних прогнозування та реальної віддачі від інвестування в контури захисту інформації, кібербезпеки підприємств та об'єктів інформатизації. Крім того, можлива оптимізація стратегій вкладення коштів у об'єкти інформатизації різними сторонами інвестиційного процесу.

У межах проведеного дослідження показано, що застосування в системі підтримки прийняття рішень, запропонованих моделей, дозволяє прискорити пошук оптимальних варіантів розміщення засобів кібербезпеки та захисту інформації для об'єктів інформатизації більш ніж у 15–20 разів. Ця перевага дозволяє виконати швидкий перебір різних варіантів апаратно-програмних засобів захисту інформації та їх комбінацій для об'єктів інформатизації, а також задіяти комбінацію апарату теорії ігор та генетичного алгоритму під час

оптимізації пошуку стратегій відбору засобів захисту інформації для різних об'єктів інформатизації. Отримані результати свідчать, що потенційно така інтеграція моделей і методів дає можливість швидко перебудовувати захист об'єктів інформатизації, адаптуючи їх до інформації про можливість реалізації нових кіберзагроз, зокрема, на основі даних, що динамічно змінюються, про стан захисту об'єктів інформатизації.

Систему було впроваджено у Товаристві з обмеженою відповідальністю «Євро-Сервіс ЛТД», про що свідчить акт про впровадження результатів дисертації (додаток 3).

Основні положення, що виносяться на захист:

1. Метод вибору раціональної стратегії інвестування в проєкти із забезпечення кібербезпеки об'єкта інформатизації на основі комбінації теорії ігор та генетичного алгоритму, як методу багатфакторної оптимізації.

2. Модифікований генетичний алгоритм для розв'язання завдань, пов'язаних із отриманням прогнозової оцінки віддачі від різних напрямків інвестування у проєкти кібернетичної безпеки для об'єктів інформатизації.

3. Методика проєктування системи підтримки прийняття рішень, для розв'язання задач оцінки стратегій інвестування в кібербезпеку об'єктів інформатизації.

Особистий внесок здобувача. Основні положення та результати досліджень дисертаційної роботи, висновки та пропозиції одержані автором самостійно. У роботі зроблено огляд теоретичної та практичної бази попередніх досліджень проблеми та проаналізовано існуючі математичні моделі, які використовуються для вибору стратегії інвестування в системи кібернетичної безпеки різних об'єктів інформатизації. Запропоновано метод вибору раціональної стратегії інвестування в проєкти із забезпечення кібербезпеки об'єкта інформатизації на основі комбінації теорії ігор та генетичного алгоритму, як методу багатфакторної оптимізації, та модифікованого генетичного алгоритму для розв'язання завдання, пов'язаного з отриманням прогнозованої оцінки віддачі від різних напрямків інвестування у проєкти кібербезпеки для

різних об'єктів інформатизації, розроблено модифікований генетичний алгоритм для розв'язання завдань кібербезпеки та описано подальший розвиток методики проєктування системи підтримки прийняття рішень, для розв'язання задач оцінки стратегій інвестування для кібербезпеки.

Особистий внесок здобувача в наукових працях, опублікованих у співавторстві, такий: детально проведено відповідні обчислювальні експерименти для перевірки коректності роботи запропонованого алгоритму та системи підтримки прийняття рішень, які сприяють забезпеченню безперервного та ефективного функціонування системи захисту інформаційних ресурсів об'єкта інформатизації будь-якого масштабу; запропоновано модифікований генетичний алгоритм для вирішення завдання, пов'язаного з отриманням прогнозованої оцінки віддачі від різних напрямків інвестування у проєкти кібербезпеки об'єктів інформатизації; розроблено та представлено метод, що може бути застосований для скорочення часу в ході розв'язання важливих завдань пошуку раціональних (оптимальних) стратегій інвесторів на основі ігрових моделей у поєднанні з генетичним алгоритмом; проаналізовано та виокремлено існуючі математичні моделі, які використовуються для вибору стратегії інвестування у системи кібернетичної безпеки різних об'єктів інформатизації; апробовано отримані результати розрахунків щодо задач із залученням теорії ігор.

Публікації. Результати досліджень за темою дисертації опубліковані в 14 працях, зокрема: одна – у науковому періодичному виданні іншої держави, яке включено до міжнародної наукометричної бази Web of Science, одна – у науковому періодичному виданні, яке включено до міжнародної наукометричної бази Scopus, одна – у науковому фаховому виданні України, одна – у науковому виданні України та десять – у збірниках матеріалів конференцій.

Обсяг і структура дисертації. Дисертація складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел (148 найменувань) та додатків. Загальний обсяг дисертації становить 161 сторінку, ілюстрації складають: 45 рисунків, 11 таблиць.

РОЗДІЛ 1

ОГЛЯД ПОПЕРЕДНІХ ДОСЛІДЖЕНЬ ТА АНАЛІЗ ВЖЕ ІСНУЮЧИХ МАТЕМАТИЧНИХ МОДЕЛЕЙ ІЗ ІНВЕСТИВАННЯ В КІБЕРБЕЗПЕКУ ОБ'ЄКТІВ ІНФОРМАТИЗАЦІЇ

1.1 Актуальність досліджень, пов'язаних із проблематикою інвестування в кібербезпеку об'єктів інформатизації

Безперечним є факт, що забезпечення інформаційної безпеки (ІБ) – це складне та витратне завдання. Варто зазначити, що крім витратних інвестицій, необхідно вирішувати певні розбіжності. По-перше, це розбіжності між доступністю інформаційних ресурсів (ІР) та необхідним ступенем захисту. Особливо це актуально для розподілених обчислювальних систем (РОС). По-друге, надмірне нарощування складу засобів захисту інформації веде до зниження зручності використання ІР. По-третє, це розбіжності інтересів сторони, що експлуатує засоби ІБ, орієнтованих на передбачувані параметри ефективності систем ІБ, та компаній-розробників апаратно-програмних рішень для ІБ [92].

Не секрет, що ряд виробників у сфері ІБ активно рекламують інноваційність своїх рішень. У результаті цього користувач, гарантовано переплачує за зайвий функціонал або змушений постійно нарощувати продуктивність своїх систем, адаптуючи їх до вимог розробників. Збільшення масштабів та кількості успішних кібератак [69, 118], розвиток темпів комп'ютерної злочинності стали глобальним трендом. Тому об'єктивна необхідність вирішення багатокритеріального оптимізаційного завдання управління ресурсами, що виділяються на забезпечення інформаційної безпеки (ІБ), така, що особи, які приймають рішення (ОПР), змушені діяти в динамічно складних ситуаціях. Подібні ситуації обумовлені ландшафтом кібернетичних загроз, що постійно змінюється, збільшенням складності кібератак, варіативністю використовуваних атакуювальною стороною сценаріїв для проведення атак і т.д.

У ситуації, що динамічно змінюється, стороні захисту різних об'єктів інформатизації (ОБІ) доводиться приймати непрості рішення, які можна схарактеризувати такими особливостями:

- для досягнення цілей, пов'язаних із забезпеченням ІБ, стороні захисту доводиться приймати безліч рішень (наприклад, технічних, організаційних, фінансових та ін.); причому кожне з цих рішень доводиться розглядати, беручи до уваги інші рішення;
- прийняті рішення в завданнях забезпечення ІБ ОБІ, практично завжди, залежні один від одного [70]; подібні рішення взаємопов'язані (наприклад, зв'язок може бути прямим, стохастичним, непрямим тощо).;
- зовнішнє середовище ОБІ може змінюватися під впливом як зовнішніх факторів, наприклад, при загальному зниженні ступеня захисту внаслідок цільових атак, так і внаслідок прийнятих рішень.

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 [53, 145] або кластерні [55] СППР у завданнях управління ІБ ОБІ можна використовувати як комплекс взаємозалежних систем. Зазначені вище СППР, як правило, базуються на синергетичних ансамблях методів та моделей. Один із цих ансамблів методів та моделей, виключно важливий у такій підзадачі управління ІБ ОБІ, як задача пошуку раціональної стратегії інвестування в засоби захисту інформації для розподіленої обчислювальної системи (РОС) ОБІ. Дійсно, що ОПР, необхідно оцінювати пріоритетність вкладення своїх фінансових ресурсів (ФР) у такі напрями розвитку ІБ РОС як [73, 93]:

- забезпечення кібернетичної стійкості ОБІ;
- інноваційні технології в 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 [73, 91], 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 проекти у сфері ІБ можна класифікувати, як комплекс взаємоузгоджених цілей та програм, спрямованих на підвищення ефективності системи ІБ конкретного ОБІ.

У [62] 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.

Інформацію можна вважати захищеною, якщо вона відповідає трьом основним принципам: конфіденційність, цілісність, доступність.

Принцип конфіденційності - забезпечення можливості отримання інформації лише користувачам (процесам), що відповідають встановленим вимогам організації.

Принцип цілісності - інформація в системі має бути актуальною, правильною та повною.

Принцип доступності - інформація має бути доступною лише для користувачів (процесів), що відповідають встановленим вимогам організації у встановлений час.

Якщо всі умови (принципи) дотримуються, систему можна вважати захищеною. Слід зазначити, що повністю захищеної інформації не існує. Чим цінніші дані, тим більше ресурсів витрачають на їх захист, звичайно до того часу, поки це доцільно, передусім економічно чи з погляду збереження таємниці.

До загроз інформаційної безпеки належать будь-які атаки, спрямовані на незаконний доступ до даних. До загроз також можна віднести порушення цифрових операцій або пошкодження інформації. Загрози можуть походити від різних суб'єктів, включаючи конкурентів, хакерів, злочинні організації і навіть співробітників організації.

Аналіз загроз інформаційної безпеки дозволяє виділити складові сучасних комп'ютерних загроз – їх джерела та рушійні сили, способи та наслідки реалізації. При аналізі загроз інформаційної безпеки використовуються три основні методи: експертна оцінка, статистичний аналіз і факторний аналіз (Рис.1.1).



Рисунок. 1.1. Основні аналітичні методи оцінки інформаційних загроз

Експертна оцінка загроз безпеки інформації необхідна для розробки відповідної моделі загроз. Також результати оцінки загроз застосовують для вибору та обґрунтування необхідних заходів при побудові системи захисту інформації. Експертна оцінка загроз безпеки інформації повинна мати систематичний характер і здійснюватися як на етапі створення систем та мереж, так і під час їх експлуатації, зокрема під час розвитку (модернізації) систем та

мереж.

Статистичний аналіз – це аналіз інформаційних загроз, в основу якого покладено на основі збирання відомостей про випадки порушення кібербезпеки, особливо про періодичність появи загроз певного типу, їх походження та підстави досягнення успіху чи зазнавання невдачі. Наприклад, дані про періодичність виникнення загрози дають можливість встановити ймовірність подібної атаки з певним інтервалом. Використання статистичного методу буде більш ефективним, якщо сукупність інформації про випадки атак буде досить великою. Звичайно, необхідна перевірка на унікальність даних, що вже занесені до бази даних, аби уникнути повторів інформації.

Для факторного аналізу необхідно визначати фактори, що можуть виявити підстави досягнення успіху чи зазнавання невдачі.

Для аналізу загроз інформаційної безпеки найкраще використовувати декілька аналітичних методів одночасно. Це посприє точності результатів.

Аналіз загроз безпеки інформації включає [36, 37, 40, 31, 27]:

- виявлення джерел загроз безпеці інформації та оцінку можливостей (потенціалу) зовнішніх та внутрішніх порушників;
- аналіз можливих уразливостей програмних, програмно-апаратних засобів;
- визначення можливих сценаріїв виникнення загроз безпеці інформації;
- оцінку можливих наслідків виникнення загроз безпеки інформації.

Модель загроз безпеки інформації включає короткий опис архітектури інформаційної системи, характеристику джерел загроз безпеки інформації, у тому числі модель порушника, та опис усіх загроз безпеці інформації, актуальних для конкретного випадку [19, 43].

Найважливішим завданням у розвитку та захисті бізнесу є підтримка в актуальному стані інформації про загрози. Сучасні загрози характеризуються високою динамікою та фахівці пропонують послуги з аналізу, класифікації, моделювання та ранжирування загроз різного характеру, включаючи [4, 5, 12, 25, 26,]:

– загрози вчинення щодо об'єктів, активів та персоналу замовника протиправних дій (розкрадання, саботаж, тероризм та ін.);

– загрози інформаційної безпеки та збереження інформаційних ресурсів організації (кіберзлочини, конкурентна розвідка, соціальна інженерія, несанкціонований доступ до інформації, порушення вимог регуляторів на предметній сфері тощо);

– загрози техногенного характеру (порушення режимів роботи обладнання, порушення ланцюжків поставок, надзвичайні ситуації, пов'язані з небезпечними речовинами та матеріалами тощо);

– загрози природного характеру (стихійні лиха);

– зовнішні загрози (висока соціальна напруженість у регіоні, розташування поруч із об'єктами замовника небезпечних виробництв, репутаційні ризики внаслідок розміщення хибної інформації про діяльність організації у соціальних мережах та ЗМІ тощо);

– внутрішні загрози;

– ризики країни (ризики зміни законодавства та вимог регуляторів, ризики зовнішньоекономічної діяльності тощо) [38, 42, 44, 46, 47, 49, 51, 66].

Результати подібного аналізу наведені на рис. 1.2.



Рисунок 1.2. Діаграма відсоткового співвідношення основних кіберзагроз підприємств [28, 30]

Оцінка загроз інформаційної безпеки проводиться з метою визначення загроз безпеки інформації, реалізація (виникнення) яких можлива в системах та мережах із заданою архітектурою та в умовах їх функціонування – актуальних загроз безпеці інформації [14, 15, 16, 9, 13, 80, 83].

Основними завданнями, які вирішуються в ході оцінки загроз безпеці інформації, є:

- визначення негативних наслідків, які можуть виникнути від реалізації (виникнення) загроз безпеці інформації;
- інвентаризація систем та мереж та визначення можливих об'єктів впливу загроз безпеці інформації;
- визначення джерел загроз безпеці інформації та оцінка можливостей порушників щодо реалізації загроз безпеці інформації;
- оцінка способів реалізації (виникнення) загроз безпеці інформації;
- оцінка можливості реалізації (виникнення) загроз безпеці інформації та визначення актуальності загроз безпеці інформації;
- оцінка сценаріїв реалізації загроз безпеці інформації в системах та мережах [17, 18, 41, 50, 138, 124, 125, 127, 115].

За допомогою інтелектуалізованих СППР ОПР, у ході прогнозованої оцінки, легше визначитися з тим, який саме із зазначених чи інших напрямів [62, 65] ІБ є більш пріоритетним у певний період для вкладення своїх ФР. Зауважимо, що насправді в подібних ситуаціях темпи повернення вкладених ФР для сторони захисту будуть різними. Тому все вище сказане, диктує необхідність інтелектуалізації пошуку раціональних стратегій інвестування в такі складні проєкти, як забезпечення інформаційної безпеки кожного об'єкта інформатизації. І без належної комп'ютерної підтримки для ухвалення подібних ризикованих рішень ОПР впоратися важко [29, 33].

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. Зокрема, у ході дисертаційних

досліджень детально розглядається завдання розробки нових моделей для вирішення завдань можливого безперервного інвестування групою інвесторів у складні інфраструктурні проєкти в галузі забезпечення інформаційної безпеки розподілених обчислювальних систем.

У роботі [135] 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 [128] 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 [74], 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 [78]. 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 в разі такого злому. Показано, що для цієї потенційної втрати компанія не обов'язково має зосереджувати свої інвестиції на інформаційних наборах із найвищою вразливістю. 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 [78].

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 завдасть шкоди λ ; $0 \leq \nu \leq 1$;

z - витрати на захист інформації.

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

Також розглядають й інші величини:

μ - імовірність збитків внаслідок атаки;

$L = t\lambda$ - потенційні збитки, пов'язані з інформаційним активом;

$S(z, \nu)$ - імовірність порушення безпеки.

Слід зазначити, що 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 $\nu \in (0,1)$, $\lim_{z \rightarrow \infty} S(z, \nu) \rightarrow 0$, як $z \rightarrow \infty$. Тому, на думку дослідників, чим значніші засоби вкладаються в безпеку, ймовірність порушення безпеки t разів $S(z, \nu)$, тобто може наблизитися до нуля [78].

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:

$$EBIS(z) = [\nu - S(z, \nu)]L. \quad (1.1)$$

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:

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

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

У [78] запропоновано два класи функцій вразливості, що відповідають умовам 1–3.

Перший клас показових функцій:

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

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 можна розрахувати так:

$$z^{I*}(\nu) = \frac{(\nu\beta\alpha L) \frac{1}{\beta+1}}{\alpha}. \quad (1.4)$$

Тобто, з (1.4) випливає, що $z^{I*}(\nu)=0$ для $0 \leq \nu \leq 1/\alpha\beta L$. Це означає, що оптимальні інвестиції для безпеки першого класу дорівнюють нулю до того моменту, поки величина ν не збільшиться до $\nu = \frac{1}{\alpha\beta L}$. А з цього слідує, що при подальшому збільшенні ймовірності реалізації загроз ν , величина $z^{I*}(\nu)$, відповідно до (1.3), збільшується зі швидкістю, що зменшується.

Другий клас показових функцій:

$$S^{II}(z, \nu) = \nu^{\alpha z+1}, \quad (1.5)$$

де параметр $\alpha > 0$ - міра продуктивності інформаційної безпеки. З умови $ENBIS'_z(z^*)=0$ отримуємо:

$$z^{II*}(\nu) = \frac{\ln\left(\frac{1}{-\alpha\nu L(\ln \nu)}\right)}{\alpha \ln \nu}. \quad (1.6)$$

З (1.6) випливає, що для II класу функцій $S(z, \nu)$, функція z^{II*} спочатку зростає, а потім зменшується зі збільшенням ν .

Попри те, що модель Gordon–Loeb після опублікування була визнана в науковому середовищі та доповнена як іншими авторами [86, 140, 144], так і самими Lawrence A. Gordon і Martin P. Loeb [79], 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.

Детально вивчивши проблему, можемо виділити такі недоліки моделі:

- Залежачи від постійного темпу зростання грошових надходжень, модель є однофазною. Тому її не варто застосовувати для оцінки компаній, чії грошові надходження можуть значно змінюватись. Для таких компаній краще використати багатофазну модель. На підставі вище сказаного, можна дійти невтїшного висновку, що ця модель більше підходить для оцінки великих компаній, які вже вичерпали всі можливості для зростання.

- Занадто сприйнятлива до вхідної інформації, не бере до уваги зміну дивідендної політики, зворотний викуп акцій та інше.

- Переважно орієнтується на дослідження оптимізаційних аспектів управління ризиками, що, нажаль, майже мінімізує можливість обліку реального об'єкта ризику.

- Дисконтована ставка більша за зростання виплат за дивідендами.

Модель, запропонована в роботах [76, 77], 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, [122], притаманні певні недоліки. Зокрема, у [106] 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 [56, 139] вважають, що розвиток такого напрямку прикладних досліджень, як математична підтримка прийняття рішення під час вибору раціональної стратегії інвестування в ІБ, має супроводжуватися синтезом нових моделей та методів. Однак, програмна реалізація наведених у роботах моделей не описана. У [56] автори відзначають, що стосовно даного класу завдань, найбільш адекватним підходом у процесі пошуку рішення буде застосування теорії ігор.

Автори [75] зазначають, що категорія програмних продуктів типу СППР та експертних систем (ЕС) сприяє спрощенню завдання пошуку раціональних стратегій для інвесторів у сфері ІБ.

У роботі [71] досить детально розглянуті різні підходи з погляду використовуваного в таких моделях математичного апарату. Однак програмна реалізація запропонованої моделі не наведена.

Автори [85] детально описують застосування класичних економіко-математичних моделей. Однак ці моделі в більшості ситуацій, пов'язаних із 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 [119, 134], – це невисока інформативність отриманих результатів. Зокрема, на думку дослідників, досить складно оцінити перспективність інвестиційних проєктів та варіанти дій інвесторів у сфері ІБ ОБІ.

Із 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 [2, 8, 10, 11, 39]. 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 [142, 84]. 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.

У [119] 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 [48, 6, 123] 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.

Ймовірні втрати (збитки) власника даних $U(G, P)$, понесені внаслідок недостатнього захисту даних, являють собою функцію від значущості інформації $G(T)$ та фактичного ступеня захисту даних P . У нульовому наближенні ці збитки апроксимуються добутком цінності інформації $G(T)$ на ймовірність її витоку H , інакше кажучи, $G(T) \cdot H$. Можливість витоку інформації знаходиться в зворотній залежності до досягнутого ступеню захисту, $H = (1 - P)$. При такому припущенні $U(G, P) = G(T) \cdot (1 - P)$. На рис. 1.3 показано, що збитки, пов'язані із забезпеченням конфіденційності інформації, можна представити у вигляді формули:

$$V^{opt}(Z, U) = Z_1(P) + U(G, P).$$

Водночас, оптимальний рівень захисту даних відповідає мінімуму суми видатків на захист $Z_1(P)$ і можливих збитків $U(G, P)$ через неповноту захисту даних, а саме:

$$V^{opt}(Z, U) = Z_1(P) + U(G, P) \rightarrow \min.$$

За такої умови, як зображено на рис. 1.3, величина витрат на захист інформації $Z_1(P)$ в сумі з можливими збитками від її втрати $U(G,P)$ менша від вартості самої інформації $G(T)$ з урахуванням її знецінення. Для спрощення викладення матеріалу, нехтуємо залежністю $Z(P,T)$, тобто зростанням сумарних витрат на захист інформаційних ресурсів підприємства з часом.

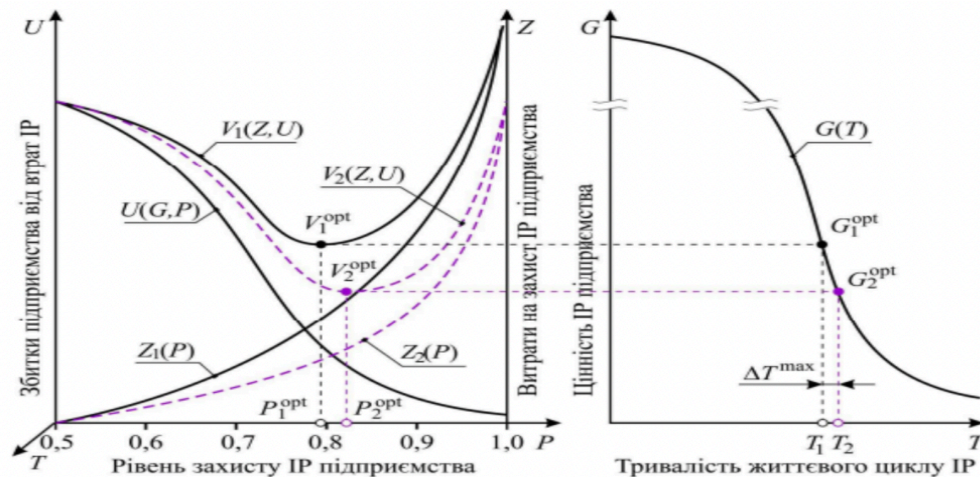


Рисунок 1.3. Модель оцінювання параметрів системи захисту інформаційних даних підприємства [48]

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

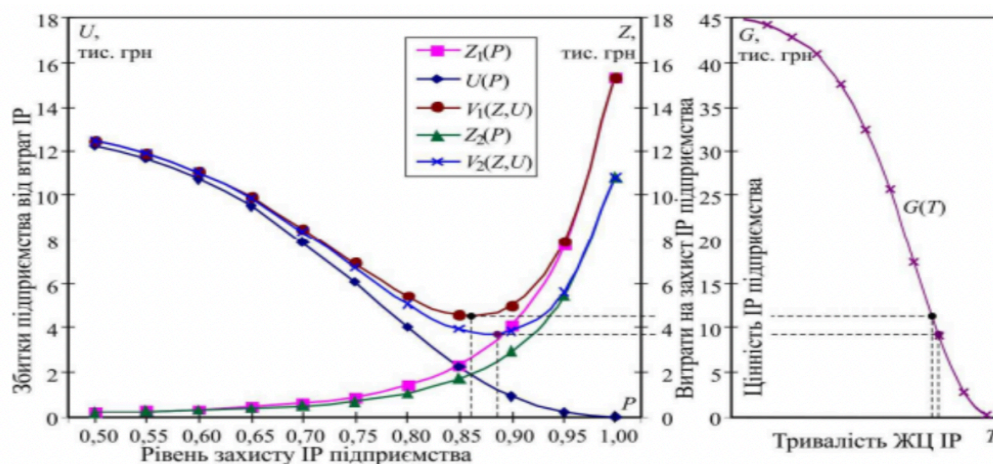


Рисунок 1.4. Результати моделювання параметрів системи захисту інформаційного ресурсу організації [48]

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 необхідне створення нових моделей підтримки прийняття рішень в області кібербезпеки, що відповідають реальному стану справ, тобто, коли кожен засіб захисту протидіє довільній кількості загроз, причому можливість запобігання кожній загрозі різна.

У роботах [72, 100] 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 [72, 99, 100]. 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, із урахуванням застосування генетичних алгоритмів.

У роботах [90, 99] розглядаються можливості щодо застосування генетичних алгоритмів (ГА) для вирішення завдань, пов'язаних із вибором стратегії інвестора. У зазначених роботах 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, що 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 проекти.

У багатьох дослідженнях [55, 62, 72, 74, 90, 100, 139] автори показують, що передумова ефективної реалізації механізмів управління інвестиціями у складні проекти 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 із боку комп'ютерних зловмисників.

У роботах [55, 62, 72, 74, 90, 100, 139] 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 проектів 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 проектів у систему кібербезпеки ОБІ. Звідси випливає потреба посилення потенціалу функції прогнозування, зокрема, із урахуванням застосування положень теорії ігор, наприклад, з урахуванням підключення генетичних алгоритмів (ГА).

Woohyun Shim, зважаючи на роботи Gordon-Loeb [78], розробив свою модель взаємозалежних ризиків для двох однакових підприємств [129, 130]. Автор продемонстрував, що оптимальна кількість вкладень у кібербезпеку при негативних зовнішніх ефектах буде більшою або дорівнює оптимальній кількості вкладень при незалежних ризиках, а область нульових вкладень буде меншою. Таким чином, якщо співпраця підприємств створює позитивні зовнішні ефекти, то оптимальна кількість вкладень у кібербезпеку буде більшою

або дорівнює оптимальній кількості вкладень при незалежних ризиках, а область нульових вкладень буде ідентичною моделі з незалежними ризиками.

Крім того, слід зазначити, що Woohyun Shim [129, 130] теоретично і емпірично довів, що фінансові вкладення, передбачені для опору нецільовим атакам, і спрямовані на завдання шкоди максимально можливій кількості сприйнятливих систем, викличуть позитивні зовнішні ефекти, оскільки збільшення фінансових вкладень організації знизить ризики інших компаній, сполучених із системою цієї фірми. У результаті проведеної роботи було вивчено та схематично зображено взаємозв'язок серед проблем зовнішніх ефектів та типами атак, як це показано на рис. 1.5.

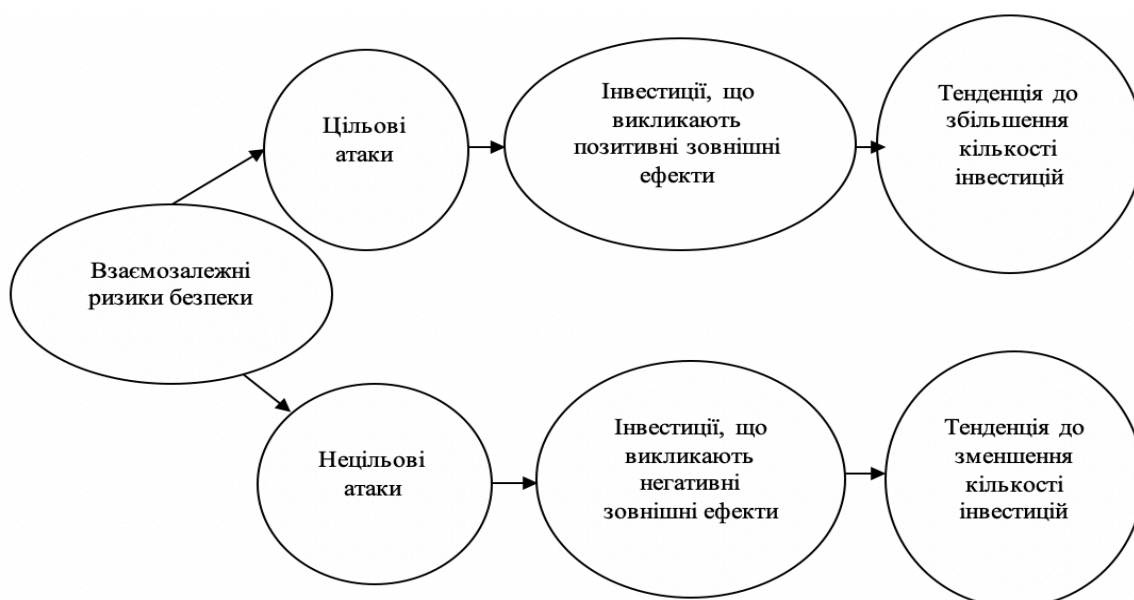


Рисунок 1.5. Зв'язки між зовнішніми ефектами та типами атак [129, 130]

Результати, отримані в ході досліджень, довели, що обидві з розглянутих вище моделей мають певні недоліки. Жодна з них не бере до уваги, розрахунок оптимального рішення у динамічному режимі, зокрема ефект фінансових вкладень. Наприклад, моделі не аналізують, яким чином правопорушник змінює стратегії своїх атак, після появи допоміжних фінансових вкладень у кібербезпеку. Для кожної з цих моделей є складним отримання конкретних даних, а саме таких, як кількісна оцінка збитків, оцінка ймовірності виникнення

загроз та оцінка сприйнятливості системи до атак правопорушників. Модель взаємопов'язаних ризиків підходить тільки для однакових підприємств, тому не підходить для роботи з усіма організаціями. Обидві моделі ґрунтуються на двох класах функцій вразливості інформаційної системи.

У роботі В.К. Задираки та співавторів [145] розглядається варіант моделі для визначення розміру витрат на захист інформації, який міг би бути корисним організаціям для побудови чи вдосконалення власної системи безпеки інформації.

Загальний очікуваний розмір втрат на безпеку інформації V можна виразити як суму витрат S та можливих втрат $b(S)$:

$$V = S + b(S). \quad (1.7)$$

Функцію (1.7) можна представляти як цільову, яку необхідно мінімізувати:

$$V(S) = S + b(S) \rightarrow \min. \quad (1.8)$$

Фінансування видатків S на гарантування безпеки даних має зменшити обсяг очікуваних витрат $b(S)$ у разі порушення безпеки. А це означає, що за цих умов більшим значенням S будуть відповідати менші значення $b(S)$:

$$0 < S_1 < S_2 \Rightarrow b(S_2) < b(S_1) < b(0) = B. \quad (1.9)$$

Тобто, формула (1.9) означає, що функція $b(S)$ монотонно спадає, а тому швидкість $b(S)$ зміни очікуваних втрат обсягу витрат – негативна:

$$b'(S) < 0. \quad (1.10)$$

Максимальне значення S – витрат отримуємо так:

$$S_{\max} = \frac{\nu B^{1-\nu} - B^{1-\nu}}{(\nu-1)(\nu B^{1-\nu}) \frac{\nu}{\nu-1}} = \frac{(B^{1-\nu})^{\frac{1}{\nu-1}}}{\nu \frac{\nu}{\nu-1}} = \frac{B}{\nu^{\frac{\nu}{\nu-1}}}. \quad (1.11)$$

У роботі Глушака-Новікова [87, 88] детально і чітко описано спосіб до розв'язання задачі створення системи захисту даних із умовою комплексного характеру атак нападника та обмеженості ресурсів захисника на побудову системи захисту.

Об'єктом вказаного дослідження є розподілена інформаційно-комунікаційна система (ІКС) з відкритою архітектурою, яка складається з S взаємодіючих компонентів, що беруть участь у обробці інформації. Кожен компонент описується набором характеристик, серед яких важливе місце посідають технологія обробки інформації, операційне середовище та інші. Зазначені параметри компонентів становлять їхню цінність для системи, яка буде позначатися через q_c .

Враховуючи особливості обчислювального середовища, можна зробити висновок, що кожен із компонентів є вразливим до певних загроз із A допустимих загроз. Припускають, що інформація про архітектуру ІКС є відкритою та відомою учасникам конфлікту. Крім того, задано можливість успішної реалізації загрози α проти компонента системи c , а також можливість нейтралізації загрози, встановленням механізмів захисту p . Таким чином, вивчення та проведені дослідження підтвердили, що на ефективність прийнятих зловмисником або захисником рішень впливають випадкові фактори, які необхідно обов'язково врахувати під час моделювання.

Припустимо, що відносини між захисником та зловмисником можуть бути формалізовані з використанням функції ризику. Тоді зловмисник, завдаючи шкоди системі, намагається максимізувати ризик. У той же час захисник, протидіючи нападнику, встановлює механізми захисту, прагнучи мінімізувати, зменшити передбачуваний ризик до нуля. В умовах обмеженості фінансових та технічних ресурсів, за заданою моделлю зловмисника, захиснику необхідно

розподілити засоби та заходи захисту, таким чином, щоб ризик в ІКС був мінімальним.

Відомо, що у термінах теорії ігор функція ризику є платіжною функцією. Кількісною величиною для оцінки ризиків є завдані збитки Q_c , що виражаються у вигляді витрат та неотриманої вигоди. Таким чином, значення збитку Q_c викликано певним компонентом c , еквівалентним цінності цього компонента q_c для функціонування системи в цілому. У загальному вигляді співвідношення для функції ризику інформаційної безпеки R_{ac} можна записати як добуток ймовірності P_{ac} реалізації загрози α та завданих збитків при реалізації цієї загрози Q_c . Змінна V_{ac} описує можливість нейтралізації загрози з використанням встановлених додаткових механізмів захисту [87]:

$$R_{ac} = P_{ac} * Q_c * (1 - V_{ac}). \quad (1.12)$$

Однією з особливостей протистояння між захисником та зловмисником є динамічний характер, тому що атаці зазвичай передують спостереження за системою та розвідка, які необхідно враховувати у моделі. Таким чином, стан конкретної конфліктної ситуації може змінюватися з часом.

Побудову системи захисту інформації (СЗІ), відповідно до розробленого підходу [88], можна поділити на такі два етапи:

- Збір та аналіз вихідної інформації з використанням методів експертної оцінки – аналіз структури, аналіз уразливостей, аналіз загроз.
- Синтез структури системи захисту. У цьому випадку підставляємо отримані на першому етапі вихідні дані в модель. У результаті розв'язання отриманої задачі з використанням симплекс-методу було отримано відносне значення ризику R , а також набір конкретних механізмів захисту, який буде оптимальним під час протистояння.

Модель протистояння двох сторін, розроблена корпорацією RAND - модель Гросса [102], призначена для імітації тактичних військових операцій.

Відповідно до цієї моделі, сторони, що конфліктують, мають ресурси X та Y , а результат їхнього протистояння визначається цільовою функцією, яка лінійно залежить від різниці вкладених ресурсів і призводить до завдання лінійного програмування:

$$i(x, y) = \sum_{k=1}^l i_k(x_k, y_k) = \sum_{k=1}^l g_k \max(x_k - y_k, 0), \quad (1.13)$$

де k – номер об'єкта, x_k та y_k – ресурси нападу та захисту на k -му об'єкті, g_k – ваговий коефіцієнт, який виражає важливість об'єктів або їх вразливість.

Величина $\max(x_k - y_k, 0)$, значенням якої є більше з двох чисел $x_k - y_k$ та 0, являє собою ту частину підрозділу x_k , яка здатна проникнути через оборону до об'єкта. Таким чином, величина $g_k \max(x_k - y_k, 0)$ кількісно характеризує успіх нападу на k -й об'єкт. У застосуванні до завдань інформаційної безпеки g_k висловлює відносну цінність інформації на k -му об'єкті, а $g_k \max(x_k - y_k, 0)$ – завдані збитки від витоку інформації. Оскільки заподіяна шкода не може бути більшою від відносної вартості інформації, то слід покласти $i(x, y) = 1$, при $x - y \geq 1$. Відповідно, функція $i(x, y)$ має кусково-лінійний характер. Весь інтервал змінної x при постійному значенні y можна розділити на три зони, обмежені двома граничними значеннями x_1 та x_2 , при $x < x_1$ маємо $i(x, y) = 0$, при $x > x_1 - i(x, y) = 1$, при $x_1 < x < x_2$ – функція $i(x, y)$ зростає лінійно з кутовим коефіцієнтом g . Із урахуванням наведених міркувань, цільова функція, яка виражає заподіяну шкоду від витоку інформації, набуває вигляду [102]:

$$i(x, y) = \sum_{k=1}^l g_k (x_k - y_k), \quad (1.14)$$

$$\text{де } x_k - y_k = \begin{cases} 0 & \text{при } x_k - y_k \leq 0 \\ x_k - y_k & \text{при } 0 < x_k - y_k \leq 1 \\ 1 & \text{при } x_k - y_k > 1 \end{cases}$$

Задача Гросса, що виникла під час планування військових операцій, має низку значних відмінностей від розглянутих завдань. По-перше, цільова функція має дискретний характер, оскільки визначає кількість одиниць, які прорвалися через оборону або знищили напад чи оборону. По-друге, ці одиниці у кожному епізоді протистояння однакові для нападу і, відповідно, для оборони. Отримані результати свідчать, що однотипність об'єктів суттєво спрощує вирішення поставленого завдання, але обмежує умови протиборства. Проте, основний недолік моделі Гросса – кусково-лінійний характер її цільової функції, який, звісно, неспроможний відповідати реальним умовам. Отже, з цієї причини модель Гросса, враховуючи її простоту, використовується лише для апроксимації цільової функції та отримання результатів у першому наближенні [102].

Juniper Networks разом із корпорацією RAND створили інноваційне рішення для розв'язання економічних питань із якими стикаються фірми, що намагаються чинити опір кіберзагрозам, кількість яких збільшується щодня. На рис. 1.6 показано аналіз втрат та витрат, що передбачаються на інструментарій моделі [32].

У моделі RAND встановлено, що загрози будуть зростати на 38% упродовж наступних років. Це зростання обумовлено не збільшенням втрат від кібератак, а витратами на посилення заходів для запобігання збитків від нападів кіберзлочинців. Наприклад, інструменти, навчання та інше, як це показано на рис. 1.5.

Оскільки розробка методів для вирішення завдань, що розглядаються, є складною задачею, можна також використовувати оптимізаційно-імітаційний підхід. Суть цього підходу полягає в тому, що якщо обмеження чи показник не можуть бути явно обчислені (задані у вигляді деякої формули), то для їх розрахунку існує деяка процедура, яка, можливо, приводить до імітаційного моделювання. У рамках цього підходу можуть бути використані модифікації деяких класичних методів дискретної оптимізації. Наприклад, деякі модифікації методу вектора спаду дозволяють вирішувати завдання, для яких неможливо

знайти явно задані обмеження. У цьому випадку відбувається перехід від одного рішення до іншого для покращення значення цільової функції, при цьому допустимість рішення перевіряється за допомогою окремої процедури.

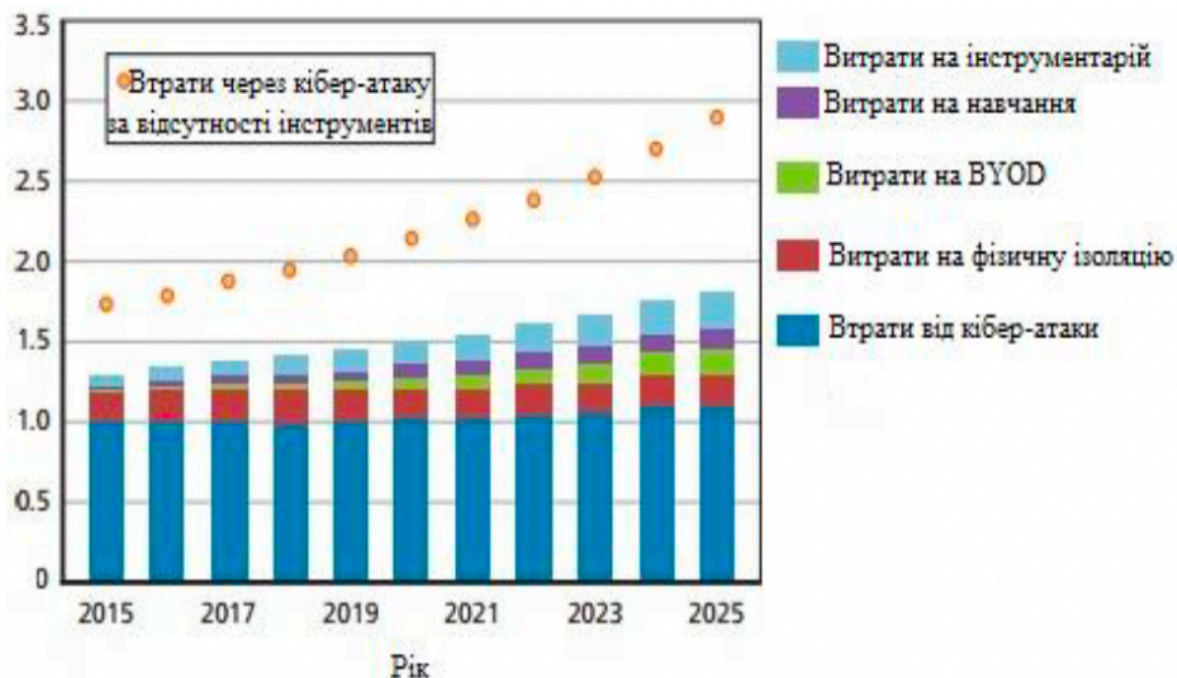


Рис 1.6. Аналіз базових втрат та витрат для роботи моделі [32]

У [82] детально описано Грищуком Р. В. дослідження кібератак на інформаційну сферу. У вище зазначеній роботі оцінка можливостей зловмисника при кібератаках проводиться за допомогою ігрових методів аналізу кібератак.

Автором була розглянута безкоаліційна кібератака A n гравців кібератак на інформаційні системи:

$$A = \left\langle N, \{x_i\}_{i \in N}, \{f_i(x)\}_{i \in N} \right\rangle, \quad (1.15)$$

де n – кількість гравців кібератак, яка визначена на безлічі N , $n \in \{N\}$, $N = \{1, 2, \dots, n\}$; i – номер гравця кібератаки, $i \in \{N\}$; x_i – стратегія i -го гравця кібератаки, $x_i \in \{X_i\}$; $f_i(x)$ – плата i -го гравця кібератаки A при виборі n гравцями власних стратегій x кібератаки, $x \in \{X\}$.

Плата за успішну кібератаку i -го гравця кібератак має вигляд квадратичної функції:

$$f_i(x) = xM^{(i)}x^T, \quad (1.16)$$

де $M^{(i)}$ – симетрична скалярна квадратична матриця, x^T – вектор-стовпчик.

Метою кібератаки для i -го гравця в кібератаці є вибір такої стратегії $x_i \in X_i$, щоб у ситуації x , що склалася, успіх від реалізації був найбільшим, тобто:

$$f_i(x) \rightarrow \max. \quad (1.17)$$

Розглянувши дану модель, робимо висновок, що в ній не враховано вплив інвестицій на вибір оптимального рішення, однак дослідники демонструють, як розроблені ігрові методи аналізу дозволяють оцінювати як одиничні, так і групові кібератаки. Це дає можливість отримати гарантовані та вірогідні оцінки рівня захищеності інформації від кібератак на інформаційну сферу.

У роботах О.Є. Архіпова [59, 60] детально вивчено та проаналізовано питання застосування економіко-вартісних моделей «атака-захист» для оцінки ризиків та дослідження ефективності інвестицій в інформаційну безпеку.

Зокрема, розглянуто ситуацію, що виникає при реалізації A загрози T щодо деякого інформаційного ресурсу I , який належить стороні B . Вважають, що D - загальна вартість витрат зловмисника A на реалізацію загрози T , g - отриманий ним у результаті «виграш», величина якого обумовлюється цінністю ресурсу I для нападника. Збитки, завдані у цій ситуації для сторони B (власника ресурсу I), тобто вартість ресурсу з погляду його власника, оцінюється ним як q , а загальна вартість реалізованого комплексу захисних заходів дорівнює c .

З огляду на все це, можна створити схему експертного оцінювання ймовірнісних характеристик, що застосовуються для розрахунку інформаційних ризиків. Приріст правопорушника в разі успішної реалізації загрози T становить $Q = g - D$. Якщо цінність g ресурсу I для атакуючої сторони A значна, зокрема,

якщо $g \gg D$, то можна припустити, що зловмисник буде намагатися скористатися різними можливостями для реалізації цієї загрози. Навпаки, для невеликих значень g економічні мотиви виникнення загрози T практично відсутні. Це дає підстави вважати, що при $Q = 0$ (або $g = D$) атака ресурсу i стає повністю недоцільною, у разі $P_i = 0$ для $g < D$ спроба реалізації загрози T втрачає будь-який економічний сенс. Виходячи з цих міркувань, у [60] запропоновано співвідношення:

$$P_i = \frac{Q}{g} = 1 - \frac{D}{g}, \quad (1.18)$$

яке може бути використане для оцінки приблизних (орієнтовних) значень ймовірності активації (виникнення) загрози T . Тоді, як наслідок, у випадку ймовірності реалізації загрози T — це похідне від:

$$P_T = P_i P_v, \quad (1.19)$$

де P_v - ймовірність вдалого використання зловмисником уразливостей інформаційної системи (ІС), що містить інформаційний ресурс I . Значення ймовірності P_v залежить від ступеня захищеності ІС, що, зі свого боку, обумовлено обсягом інвестицій c у систему захисту інформації (ЗЗІ), що з певним наближенням обраховується співвідношенням [59]:

$$P_v = \frac{q}{q + sc}, \quad (1.20)$$

де s - коефіцієнт, яким визначається рівень ефективності інвестицій c у систему захисту інформації, а саме: чим більше значення s , тим нижче, за умови одного і того ж обсягу інвестицій c , величина ймовірності P_v . Як наслідок, із

формули (1.20) зрозуміло, що за відсутності критичної інформації в ІС (тобто $q = 0$) ймовірність $P_v = 0$. Коли вартість q ресурсу I буде висока або дуже висока, проте витрати на створення та функціонування ЗЗІ низькі, тобто $q \gg sc$, ймовірність $P_v \rightarrow 1$. Отже, якщо власник ресурсу I приділяє його захисту достатньо уваги, значення q та sc пропорційні, $P_v < 1$. Загалом, за таких умов, значення ймовірності P_v при $q = \text{const}$ зростають зі спадом рівня інвестицій c у ЗЗІ та навпаки, збільшуються зі зростанням їх обсягу.

Формули (1.18) - (1.20) дозволяють побудувати оптимізаційну схему, за якою можна буде зробити висновки щодо ефективності та доцільності інвестицій у ЗЗІ організації. Тому в [59] розраховано припущення, яке доводить, що при нульових інвестуваннях у ЗЗІ організації $P_v = 1$, тоді вихідний інформаційний ризик становить $R_1 = P_t q$. Інвестування у ЗЗІ коштів у розмірі c приводить (за умови раціональних витрат цих коштів на потреби захисту) до того, що ймовірність успішного виконання вразливості стає менше одиниці, тобто $P_v < 1$. І, як результат, залишковий ризик у цьому випадку дорівнюватиме $R_t = P_t P_v q$, величина втрат, яким вдалося запобігти - $R_1 - R_t = P_t q - P_t P_v q = (1 - P_v) P_t q$, а відповідний «прибуток» фактично становитиме $\Delta_R = R_1 - R_t - c = (1 - P_v) P_t q - c$.

Економіко-вартісна модель ґрунтується на результатах аналізу реальних показників рівня захищеності інформаційної системи організації, потреб інформаційної безпеки, що вимагають використання реальних механізмів управління інформаційними ризиками, з урахуванням економічних тенденцій та дозволяє сподіватися на досягнення більш об'єктивних результатів при проведенні оцінки оптимального обсягу інвестицій у систему захисту інформації.

Слід зазначити, що економіко-вартісні моделі «атака – захист» також дають можливість на основі конкретної інформації про реальну організацію перевірити, чи достатні за обсягом кошти, інвестовані в інформаційну безпеку цієї організації.

В [121] запропоновано два можливі види залежностей $q(x)$ у вигляді $q(x) = Nx^n e^{-h^2 x^2}$: розподіл Максвелла $q_M(x) = Nx^2 e^{-h^2 x^2}$ та розподіл Релея $q_p(x) = Nx e^{-h^2 x^2}$, де N - нормувальний коефіцієнт, а константи n, h визначають положення максимуму залежності та ступінь її асиметрії. У зіставленні цих розподілів істотна їх відмінність полягає в тому, що $q_M(x)$ для початкової області $x \gtrsim 0$ опуклість спрямовано вниз, а для $q_p(x)$ - вгору.

Отже, наведені значення та висновки дозволяють керівникам підприємства зробити висновок про достатність виділених коштів чи доцільність їхнього збільшення. Це залежить, звичайно, від допустимих величин $i(x, y)$, які, у свою чергу, визначаються зі суб'єктивної оцінки керівника та його схильності до ризику.

Слід зазначити, що зараз для інвестування в кібербезпеку створюють нові моделі на основі теорії ігор. Одна з таких моделей – модель Ахметова-Малюкова.

У праці [54] описана модель Малюкова-Ахметова-Лакно стратегій інвестування в системи кібербезпеки. У зазначеній моделі підхід першого гравця-союзника $u: T \cdot [0,1] \cdot [0,1] \rightarrow [0,1]$ - це функція, що задає стан початкових даних (позицій) $(t, (z_1(0), z_2(0)))$ значення $u(t, (z_1(0), z_2(0)))$: $0 \leq u(t, (z_1(0), z_2(0))) \leq 1$, де u - параметр управління першого інвестора; t - часовий параметр; z_1 - величина матеріального ресурсу першого інвестора; z_2 - величина матеріального ресурсу другого інвестора. У відношенні поінформованості гравця-противника (у межах схеми позиційної гри) жодних припущень не робиться, що еквівалентно тому, що гравець-противник обирає сам свій керівний вплив $u(t)$, виходячи з будь-якої інформації.

Отже, у процесі аналізу описаної моделі доведено, що для будь-якого моменту часу t , виконуються такі умови: $\alpha_1(t) = \alpha_1$; $\alpha_2(t) = \alpha_2$; $\beta_1(t) = \beta_1$; $\beta_2(t) = \beta_2$; $r_1(t) = r_1$; $r_2(t) = r_2$.

Приймаємо: $q_1 = (1 - \beta_1) \cdot (a_1 + r_1) - 1$; $q_2 = (1 - \beta_2) \cdot (a_2 + r_2) - 1$,

де α_1 - коефіцієнт, що визначає відсоткову плату за фінансовий ресурс другого інвестора першому інвестору;

α_2 - коефіцієнт, що визначає відсоткову плату за фінансовий ресурс першого інвестора другому інвестору;

β_1 - коефіцієнт, що визначає частку погашення заборгованості першого інвестора другому інвестору;

β_2 - коефіцієнт, що визначає частку погашення заборгованості другого інвестора першому інвестору;

r_1 - коефіцієнт, що визначає частку повернення фінансового ресурсу другого інвестора першому інвестору;

r_2 - коефіцієнт, що визначає частку повернення фінансового ресурсу першого інвестора другому інвестору;

q^* - коефіцієнт, що визначає промінь збалансованості.

У роботі [54] запропонована модель для модуля системи підтримки прийняття рішень щодо взаємного інвестування у транспортний ситуаційний центр, зокрема у його систему кібербезпеки. Зазначена модель дозволяє скласти прогноз можливих наслідків інвестування та виявити методи керування інвестиційним процесом. Якщо прогноз буде незадовільним, то можливе гнучке коригування параметрів процесу інвестування з метою досягнення сторонами прийняттого фінансового результату [54].

Левченко та співавтори у роботах [103, 104, 105, 121] запропонували математичну модель, яка передбачає використання цільової функції $i(x, y)$, де i - віднесена до загальної кількості вартості втраченої інформації, x та y - ресурси нападу i , відповідно, захисту. Ця функція у загальних ознаках має такий вигляд:

$$i(x, y) = \sum_{k=1}^l i_k(x, y) = \sum_{k=1}^l g_k p_k q_k(x, y) f_k(x, y), \quad (1.21)$$

де $k = \overline{1, l}$ – номер об'єкта; g_k – обсяг інформації на об'єкті; p_k – ймовірність нападу на об'єкт; $q_k(x; y)$ – щільність імовірності виділення нападом ресурсів x на k -й об'єкт; $f_k(x; y)$ – залежність частки втраченої інформації від співвідношення x та y , яку можна розглядати як імовірність втрати інформації при заданих значеннях x та y .

Як залежність $f_k(x, y)$ запропоновано два класи функцій:

$$\text{степеневі } f(x, y) = \frac{\alpha(x/y)^n}{b(x/y)^n + c} \text{ та} \quad (1.22)$$

$$\text{показові } f(x, y) = d(1 - e^{-m(x/y)^n}), \quad (1.23)$$

де параметри α, b, c, d, n, m приймають позитивні значення і, відповідно, визначають положення і нахил кривих. У результаті розв'язання задачі буде знайдено засоби забезпечення інформаційної безпеки, що дозволить оптимально захистити обчислювальну мережу організації.

Автори [147, 148, 146, 64, 143, 7] досліджували та застосовували метод нечіткого індуктивного моделювання, відомого як груповий метод обробки даних у задачах інтелектуального аналізу даних, зокрема його застосування в задачі прогнозування в макроекономічній та фінансовій сфері. Завдання полягало в побудові прогнозних моделей і знаходженні невідомої функціональної залежності між заданим набором макроекономічних показників і прогнозованою змінною за експериментальними даними. Здебільшого дослідження проводилися у медичній сфері.

Детальний аналіз математичних моделей стратегій інвестування для систем кібербезпеки показав, що основні засоби та сили застосовуються до питань визначення розміру інвестицій для захисту інформаційних систем (Таблиця 1.1) [61].

**Аналіз математичних моделей стратегій інвестування для систем
кібербезпеки**

	Математичні моделі стратегій інвестування для інформаційної безпеки					
Критерії порівняння	Модель Gordon–Loeb	Модель Woohyun Shim	Модель Архіпова	Модель Левченко-Прус	Модель Задіраки	Модель Малюкова - Аметова-Ляхно
Розрахунок оптимального рішення в динамічному режимі	-	-	+	+	-	+
Врахування вразливості об'єктів	-	-	+	+	-	-
Оптимізація розподілу ресурсів	+	+	-	+	-	+
Облік засобів захисту	+	+	+	+	+	-
Облік засобів нападу	-	-	+	+	-	-
Відмінність позитивних та негативних ефектів	-	+	-	-	-	-
Облік вартості кожного засобу захисту	-	-	+	-	-	-

Крім того, варто зазначити, що усі наявні моделі рідко враховують, як правопорушник змінює тактику своїх кібератак, реагуючи на додаткові інвестиції в інформаційну безпеку [95]. І, що, в свою чергу, не менше важливо, також існують труднощі в отриманні даних для моделей, таких як числова оцінка збитків, ймовірності появи загроз і вразливості.

ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

У результаті порівняльного аналізу наукових праць, зазначених вище, доведено, що завдання ефективного використання фінансових ресурсів на захист інформації є одним із найголовніших завдань для організацій та компаній, які потребують захисту власної інформації. Для отримання повних об'єктивних результатів у нинішніх умовах нестійкої ринкової економіки процес інвестування потребує проведення значних робіт аналітиками та експертами, від збору та обробки інформації, і до розроблення стратегії інвестування, що відповідає зазначеним цілям і завданням. Питання ефективності фінансових інвестицій та контролю над цим процесом є одним із найважливіших у фінансовій сфері. Оптимальне значення ресурсів залежить не лише від уразливості системи, а й від вартості інформації, яка підлягає захисту. Проте, слід зазначити, що дослідження дуже часто мають лише економічний характер і майже зовсім не враховують тенденції щодо впровадження інформаційних технологій у процедури контролю та прийняття рішень для інвестиційних проєктів. Тож, у процесі проведення досліджень та порівнянь вище названих праць, зроблено висновок про те, що головним недоліком цих досліджень є відсутність необхідних конкретних рекомендацій щодо формування стратегій фінансових інвестицій.

Все вищезазначене і зумовило проблему, пов'язану з необхідністю розробки нових моделей, заснованих на спільному (гібридному) використанні апарату білінійних диференціальних ігор якості та ГА. Така комбінація для ядра інтелектуальних інформаційних систем (ІС) у завданнях визначення раціональних стратегій фінансового інвестування у проєкти кібербезпеки не лише має право на існування, а і здатна, на нашу думку, дати позитивний ефект.

РОЗДІЛ 2

МЕТОД ВИБОРУ РАЦІОНАЛЬНОЇ СТРАТЕГІЇ ІНВЕСТИВАННЯ У ПРОЄКТИ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ НА ОСНОВІ КОМБІНАЦІЇ ТЕОРІЇ ІГОР ТА ГЕНЕТИЧНОГО АЛГОРИТМУ

Для отримання об'єктивних результатів, розглянуте завдання щодо пошуку раціональної стратегії інвестування у проєкти кібербезпеки (КБ) для ОБІ пропонується вирішувати у два етапи.

На першому етапі залучено потенціал білінійних диференціальних ігор [109, 110] та опис взаємодії об'єктів у багатовимірних просторах [99]. Безперечно, у цьому напрямі величезний внесок у розвиток теорії білінійних диференціальних ігор для опису взаємодії об'єктів було внесено професором В.П. Малюковим [99, 109, 110].

На другому етапі пущено в дію модифікований ГА.

2.1. Задача пошуку раціональних стратегій інвестування в кібербезпеку об'єкта інформатизації

Розв'язання задачі з пошуку оптимальних стратегій формування кібербезпеки ОБІ та розміщення компонентів відповідних класів ЗЗІ та КБ по вузлах виконаємо виходячи, з необхідності визначити максимально ефективну архітектуру безпеки ОБІ [55, 56, 75, 77, 79, 86, 99, 101, 128, 138].

Тобто

$$Ef = \sum_{i=1}^{NU} \sum_{j=1}^N \sum_{d \in N_j} p_{ijd} \cdot x_{ijd} \rightarrow \max, \quad (2.1)$$

де NU – кількість класів вузлів ОБІ;

N – кількість класів ЗЗІ (або КБ);

d_j – ЗЗІ (або КБ) з класу j ;

i – клас вузла (точка), наприклад, серверна або робоча станція;

p_{ijd} – вихідна ефективність ЗЗІ (КБ), наприклад, відсоток виявлення вірусів для антивірусного ПЗ;

x_{ijd} – факт фіксації у СППР наявності ЗЗІ d , яке відноситься до класу j та, який належить батьківському класу i вузла, що аналізується;

N_j – кількість ЗЗІ в класі j .

У процесі вирішення завдання відстежується дотримання наступних умов та загальних обмежень.

Загальне обмеження:

$$\forall \psi_{l_1}^{\Psi_n}, \sum_{i=1}^{NU} \sum_{j \in N} \sum_{d \in N_j} cnd_{jdl} \cdot x_{ijd} \leq \psi_l, \quad (2.2)$$

де ψ_l – елементи множини загальних обмежень $\Psi = \{\psi_l, l = 1, \dots, \Psi_n\}$, де Ψ_n – кількість загальних обмежень;

cnd_{jdl} – показник ЗЗІ із загального обмеження l .

Прийнято, що загальні обмеження – це чинники, котрим важливо контролювати величину сумарного значення. Наприклад, до таких обмежень можна віднести вартість ЗЗІ в цілому для ОБІ, а не для окремого вузла.

Локальні обмеження:

$$\forall i_1^P, l_1^{LRN} \sum_{j=1}^N \sum_{d \in N_j} cnd_{ijdl} \cdot x_{ijd} \leq lr_{il}; j \in N, d \in j, \quad (2.3)$$

де $LR = \{lr_l, l = 1, \dots, LRN\}$, де LRN – кількість локальних обмежень;

lr_{li} – локальне обмеження lr_l на вузлі i ;

cnd_{ijl} – показник ЗЗІ з локального обмеження l .

На відміну від загальних, локальні обмеження немає сенсу розраховувати, як сукупний показник. Це пов'язано з тим, що локальні обмеження стосуються лише конкретного вузла ОБІ.

Прийнято, що один і той же самий ЗЗІ не може бути розміщено більш ніж один раз у точці одного класу. І справді немає сенсу розміщувати, наприклад, дві антивірусні програми на одній робочій станції. Це означає, що робоча станція при розглянутій постановці задачі, описана як точка ОБІ. Тобто, $\forall x_{ijd} \leq 1; i \in P; j \in N; d \in j$.

У процесі розробки СППР та пошуку конкретних алгоритмів для вирішення оптимізаційної задачі щодо вибору контрзаходів для захисту ОБІ не можна враховувати лише один критерій. Це пояснюється тим, що у ситуації, коли неможливо знайти компромісне рішення, розробники системи кібербезпеки ОБІ можуть дійти до умови, коли система кібербезпеки буде дешевою, але й ефективною. Або ж навпаки, система буде високоефективною, але дуже витратною, і, до того ж, дуже вимогливою до апаратних ресурсів ОБІ. Остання обставина зрештою веде до зниження продуктивності. Отже, повноцінне рішення сформульованого завдання може бути отримане тільки у разі використання багатокритеріальної оптимізації.

У рамках цього розділу дисертації ми обмежимося лише двома, на наш погляд, першорядними критеріями, якими повинні керуватися проектувальники системи КБ ОБІ: критерій 1 – мінімізація збитків від реалізації кіберзагроз для ОБІ; критерій 2 – мінімізація витрат на ЗЗІ для ОБІ в цілому.

Критерій 1 можна формалізувати так:

$$vc_1 = PD \rightarrow \min, \quad (2.4)$$

де vc_1 – векторний критерій 1;

PD – потенційні збитки ОБІ внаслідок кібератак.

Критерій 2 ($vc_2 = vc_{21} + vc_{22}$) включає два підкритерії, які формалізовані так:

$$vC_{21} = \sum_{i=1}^{NS} \sum_{j=1}^N \sum_{d=1}^{D_{cl}} IM_{ijd} \rightarrow \min, \quad (2.5)$$

$$vC_{22} = \sum_{i=1}^{NS} \sum_{j=1}^N \sum_{d=1}^{D_{cl}} UM_{ijd} \rightarrow \min, \quad (2.6)$$

де vC_{21}, vC_{22} – векторні підкритерії;

NS – кількість вузлів ОБІ;

N – кількість класів ЗЗІ або КБ;

D_{cl} – кількість ресурсів ЗЗІ або КБ, котрі належать одному класу, наприклад, кількість програм антивірусів, що розглядаються. і т.д.;

IM_{ijd} – показник d із класу j щодо витрачання локального ресурсу на вузлі i ;

UM_{ijd} – показник ЗЗІ d із класу j щодо витрачання загального ресурсу (наприклад, фінансового, оперативна пам'ять та ін.) на вузлі i .

Зазначимо, що збільшення обсягу інвестицій у ЗЗІ не завжди найкраще рішення в питаннях ІБ. У питанні визначення стратегій інвестування в ІБ ОБІ зазвичай виникають труднощі. Основною причиною цих проблем є складність моделей і супутніх алгоритмів, які використовуються для опису планів інвестування в ІБ. На нашу думку, цей недолік можна виправити, використовуючи можливості СППР. Більшість обчислень у таких системах виконується обчислювальним ядром. Тому СППР можуть бути використані для визначення найкращого курсу дій щодо інвестицій в ІБ організації (або ОБІ).

Пошук найкращого інвестиційного плану в ЗЗІ ОБІ можна порівняти з грою двох гравців. Тоді перший гравець відповідає за ІБ ОБІ. Вони прагнуть виявити та усунути будь-які вразливості системи, а також забезпечити найвищий рівень захисту ОБІ від атак і кіберзагроз. Другий гравець може взяти будь-що, що протистоїть стороні захисту, якщо це підходить для використання теорії ігор. Порушники ІБ як зсередини, так і ззовні можуть становити цю протилежну

сторону. Це включає в себе елементи, пов'язані з еволюцією природи загроз ІБ, а також еволюцію методів і стратегій зломисників. Не можна забувати про нові небезпеки для ІБ, поява яких є результатом розвитку тенденцій ринку інформаційних технологій. Наприклад, на ситуацію у сфері ІБ вплинуло широке використання інтернету речей [94], [67].

Втім, другий гравець не завжди є ворогом. Другим учасником можна вважати тих, хто бере участь у ринку венчурних інвестицій в ІБ. Наприклад, лише у 2021 році обсяг венчурних інвестицій у кібербезпеку в усьому світі сягнув 21,8 мільярдів доларів США та встановив новий інвестиційний рекорд, повідомляє Forbes [63]. Величезну частину цих грошей залучили стартапи в США та Ізраїлі. Атаки на API (тобто інтерфейси прикладного програмного забезпечення) – це головна кібернебезпека в 2022 році, вважають [1, 63].

Існують й інші інноваційні розробки. Технологія Priori від компанії BreachQuest використовується для реагування на проблеми кібербезпеки шляхом постійного спостереження за шкідливою діяльністю [1].

Програмне забезпечення від Cyilentium призначене для того, щоб сторонні особи не могли бачити мережу або будь-які підключені пристрої.

Зважаючи на все викладене вище, можна стверджувати, що формування системи фінансових заходів для досягнення довгострокових стратегічних цілей щодо рішень у сфері ІБ становить значну частину інвестиційної стратегії на ринку рішень у сфері ІБ. Такі цілі, як стабільне забезпечення високого рівня ІБ ОБІ, вирішуються шляхом інтеграції фіксованих і змінних характеристик інвестиційного проєкту.

Проєкти у сфері ІБ часто характеризуються високим рівнем ризику та непередбачуваністю. Багатогранний і диверсифікований характер потенційних стратегій інвестування в ІБ пов'язаний саме з цим. Ринок рішень для захисту інформації постійно розвивається. Небезпеки, з якими доводиться боротися обороні, з кожним роком зростають як кількісно, так і якісно. Наприклад, ризики ІБ відразу зросли, коли на ринку медичних послуг вперше з'явилися кібернетичні імпланти. Крім того, розробка різноманітних дронів і автономних

роботів викликала занепокоєння, що злочинці можуть взяти їх під контроль [89], [117].

Через це найкраща стратегія – розглядати інвестиції в інформаційну безпеку як постійний процес. Як і основний гравець, друга сторона також зацікавлена в надійному збереженні інформаційних активів ОБІ, але, оскільки у нього є власні фінансові інтереси, він працюватиме на ринку (брати участь у грі) насамперед відповідно до цих інтересів і прибутковості діяльності у швидко зростаючому секторі ІБ.

ІБ давно перетворилася з «нішевої» сфери, яка цікавила лише невелику групу професіоналів у цьому секторі, до того, щоб стати пріоритетом у порядку денному багатьох державних установ і приватних компаній. Постачальникам рішень для захисту інформації на сьогоднішній день не потрібно витрачати багато часу на пояснення потенційним клієнтам "чому ці рішення важливі?", оскільки кількість загроз для ІБ зростає. У той же час сторона захисту більше стурбована питаннями «як реалізувати рішення» і «скільки коштує рішення», ключові питання виникають під час обговорення.

Зважаючи на все викладене вище, у статті запропоновано модель, засновану на теорії диференціальних ігор якості з декількома термінальними поверхнями, для вирішення задачі вибору оптимальних стратегій безперервного спільного інвестування в ІБ з урахуванням багатфакторності цього процесу і для нечіткого оператора.

Тому наукове завдання зі створення ансамблю моделей на основі теорії ігор для обчислювального ядра СППР є актуальним при оцінці стратегій поточних інвестицій у СЗІ ОБІ.

Виходячи з досліджень авторів у роботах [94], [67], можна зробити висновок, що решта методологій і моделей, крім традиційних [58], можуть бути використані для оцінки інвестицій в інформаційну безпеку, оскільки вони також ефективно можуть охопити суть проблеми. Наприклад, у [57] зазначено, що широко розповсюджені методології СППР нечасто придатні для синтезу

прогнозних оцінок щодо доцільності вибору інвестором оптимальної стратегії інвестування в проекти, пов'язані з ІБ ОБІ.

Ігровий підхід також враховується в роботах [96], [133], [58] при виборі оптимальних стратегій інвестування.

Однак розглянуті вище моделі, засновані на теорії ігор [133], [58], [137], насправді не пропонують інвестиційних порад. Це справедливо і в тому випадку, коли вибір найкращого способу безперервного взаємного фінансового інвестування в проекти ІБ вимагає математичного обґрунтування.

Слід підкреслити, що оптимальну стратегію інвестування в ІБ ОБІ неможливо повністю визначити за допомогою методів [137], [126], або [115]. Завдання ускладнюється багатофакторним характером ринку продуктів ІБ. Як наслідок, інвесторам може бути складно визначитися відразу, на чому вони мають зосередитися. Сюди входять, серед багатьох інших, рішення в області управління ідентифікацією, контролю доступу до приватних даних, моніторингу активів і мережі, захисту хмарної інфраструктури ОБІ та багато іншого про що йшлося вище.

Значення безперервних інвестицій у рішення з ІБ полягає в тому, що вони пов'язані з постійним впровадженням досягнень у сфері ІБ цифрових об'єктів. Одним із основних методів забезпечення найвищого рівня захисту інформаційних активів для ОБІ є інноваційні рішення захисту інформації. Важливо зауважити, що час є одним із ключових факторів, що визначають інновації та інвестиції у створення ЗЗІ для цифрових об'єктів. У цих інвестиційних починаннях час є більш адаптивним інструментом, ніж готівка [141, 52].

Ці обставини обумовили необхідність створення нових моделей, призначених для контролю поточного процесу інвестування в ІБ ОБІ.

Сформулюємо модель першого етапу методу.

Повне рішення для цього етапу, методу, що пропонується для розгляду, описано в роботі [99].

Дві групи інвесторів (гравців) управляють динамічною системою у

багатовимірних просторах. Групи гравців дотримуються різних стратегій у підходах до інвестування ІБ ОБІ. Наприклад, одна група діє, виходячи з пріоритетності парадигми інноваційності систем ІБ для ОБІ, але для своїх дій кожного разу потребує все новіше «залізо». Друга група дотримується більш прагматичних підходів. Вважаючи, що за нинішніх умов клієнти дедалі менше реагують на «революційні продукти» у сфері ІБ. Як наслідок, такий підхід інвесторів, припускає, вкладення нового фінансового ресурсу в такі системи ІБ, які не висувають надмірних вимог до системних ресурсів. Крім того, частина подібних апаратно-програмних рішень вже встановлена на ОБІ.

У рамках статті [99] було описано розв'язання задачі з погляду першого гравця-союзника. Слід зазначити, що задачі ці симетричні, тому не потрібно детально розглядати розв'язання задачі з погляду другого гравця-союзника.

Динаміка зміни $FinR$ для гравців описана наступною системою рівнянь [99]:

$$\begin{aligned}
 dg_1(t)/dt &= -g_1(t) + \Delta_1^1 \times g_1(t) + [(\Psi_1^1 + Z_1^1) - E] \times \\
 &\times U_1(t) \times \Delta_1^1 \times g_1(t) - [(\Psi_2^1 + Z_2^1) - E] \times V_1(t) \times \Delta_2^1 \times p_1(t) \\
 &\dots \\
 dg_M(t)/dt &= -g_M(t) + \Delta_1^M \times g_M(t) + [(\Psi_1^M + Z_1^M) - E] \times \\
 &\times U_M(t) \times \Delta_1^M \times g_M(t) - [(\Psi_2^M + Z_2^M) - E] \times V_M(t) \times \Delta_2^M \times p_M(t); \\
 dp_1(t)/dt &= -p_1(t) + \Delta_2^1 \times p_1(t) + [(\Psi_2^1 + Z_2^1) - E] \times \\
 &\times V_1(t) \times \Delta_2^1 \times p_1(t) - [(\Psi_1^1 + Z_1^1) - E] \times U_1(t) \times \Delta_1^1 \times g_1(t); \\
 &\dots \\
 dp_M(t)/dt &= -p_M(t) + \Delta_2^M \times p_M(t) + [(\Psi_2^M + Z_2^M) - E] \times \\
 &\times V_M(t) \times \Delta_2^M \times p_M(t) - [(\Psi_1^M + Z_1^M) - E] \times U_M(t) \times \Delta_1^M \times g_M(t); \\
 &\dots
 \end{aligned} \tag{2.7}$$

де

$$\begin{aligned}
\Delta_1^* &= \begin{pmatrix} \Delta_1^1 0 \dots\dots 0 \\ 0 \Delta_1^2 \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots \Delta_1^M \end{pmatrix}; \Delta_2^* = \begin{pmatrix} \Delta_2^1 0 \dots\dots 0 \\ 0 \Delta_2^2 \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots \Delta_2^M \end{pmatrix}; U = \begin{pmatrix} U_1 0 \dots\dots 0 \\ 0 U_2 \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots U_M \end{pmatrix}; V = \begin{pmatrix} V_1 0 \dots\dots 0 \\ 0 V_2 \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots V_M \end{pmatrix}; \\
\Psi_1^* &= \begin{pmatrix} \Psi_1^1 0 \dots\dots 0 \\ 0 \Psi_1^2 \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots \Psi_1^M \end{pmatrix}; \Psi_2^* = \begin{pmatrix} \Psi_2^1 0 \dots\dots 0 \\ 0 \Psi_2^2 \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots \Psi_2^M \end{pmatrix}; Z_1^* = \begin{pmatrix} Z_1^1 0 \dots\dots 0 \\ 0 Z_1^2 \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots Z_1^M \end{pmatrix}; Z_2^* = \begin{pmatrix} Z_2^1 0 \dots\dots 0 \\ 0 Z_2^2 \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots Z_2^M \end{pmatrix}; \\
E^* &= \begin{pmatrix} E 0 \dots\dots 0 \\ 0 E \dots\dots 0 \\ \dots\dots\dots \\ 0 \dots\dots\dots E \end{pmatrix}; g = \begin{pmatrix} g_1 \\ g_2 \\ \cdot \\ \cdot \\ \cdot \\ g_M \end{pmatrix}; p = \begin{pmatrix} p_1 \\ p_2 \\ \cdot \\ \cdot \\ \cdot \\ p_M \end{pmatrix};
\end{aligned}$$

Динамічна система (ДС) задана сукупністю білінійних диференціальних рівнянь із залежними рухами. Для ДС визначено множину стратегій (U) та (V) груп гравців. Також для ДС визначено термінальні поверхні S_0, F_0 . Мета першої групи гравців (далі за текстом прийнято позначення $Inv1$) - привести ДС за допомогою своїх стратегій керування на термінальну поверхню S_0 . Важливо, що це необхідно зробити незалежно від дій другої групи гравців (далі прийнято $Inv2$). Ціль $Inv2$ привести ДС за допомогою своїх стратегій керування на термінальну поверхню F_0 , незалежно від дій $Inv1$. Отже, сформульована постановка проблеми генерує два завдання. Це, відповідно, конкретні завдання з боку першого гравця-союзника та другого гравця-союзника [107, 108, 109, 110, 111, 112, 113, 114].

Важливим є те, що рішення полягає у знаходженні множини початкових станів гравців. Також необхідно визначити їх стратегії. І, як результат, визначені стратегії дозволять усім гравцям привести ДС на ту чи іншу термінальну поверхню.

Одна з умов - гравці мають певні фінансові ресурси (ФР) для інвестування у проєкти ІБ ОБІ. Наприклад, побудова багатоконтурного захисту розподіленої

обчислювальної системи.

Тоді система диференціальних рівнянь у моделі виглядатиме так [99]:

$$\begin{aligned} dg(t)/dt &= -g(t) + \Delta_1^* \times g(t) + [(\Psi_1^* + Z_1^*) - E^*] \times \\ &\times U(t) \times \Delta_1^* \times g(t) - [(\Psi_2^* + \Delta_2^*) - E^*] \times V(t) \times \Delta_2^* \times p(t); \\ dp(t)/dt &= -p(t) + \Delta_2^* \times p(t) - [(\Psi_2^* + Z_2^*) - E^*] \times \\ &\times V(t) \times \Delta_2^* \times p(t) - [(\Psi_1^* + Z_1^*) - E^*] \times U(t) \times \Delta_1^* \times g(t), \end{aligned}$$

тут $g(t)$, $p(t)$ – вектори Mn мірного простору, $U(t)$, $V(t)$ – одиничні матриці порядку Mn з позитивними елементами $u_i(t), v_i(t)$ із сегмента $[0,1]$ на діагоналях матриць $U(t), V(t)$ відповідно [99, 107, 108, 109, 110, 111, 112, 113, 114];

Δ_1^*, Δ_2^* – матриці перетворення ФР $Inv1$ та $Inv2$, за умови, що ФР успішно реалізовані у відповідні проекти розвитку ІБ ОБІ. Матриці Δ_1^*, Δ_2^* – це квадратні матриці порядку Mn з позитивними елементами $\delta_1^{*ij}, \delta_2^{*ij}$, відповідно;

Ψ_1^*, Z_1^* – діагональні матриці із позитивними елементами. Дані матриці, що характеризують відсоткову плату $Inv2$ за фінансові інвестиції та частки повернення інвестицій $Inv2$ щодо інвестицій $Inv1$ у проекти ІБ ОБІ;

Ψ_2^*, Z_2^* – діагональні матриці із позитивними елементами. Дані матриці характеризують відсоткову плату $Inv1$ за фінансові інвестиції та частки повернення інвестицій $Inv1$ щодо інвестицій $Inv2$ в проекти ІБ ОБІ;

E^* – одинична матриця порядку Mn .

Матриці $\Delta_1^*, \Delta_2^*, \Psi_1^*, Z_1^*, \Psi_2^*, Z_2^*, E$ при даній постановці завдання, у тому числі враховують і техніко-економічні параметри окремих засобів захисту інформації за класами. Відповідно, інвестору буде легше в такому досить компактному вигляді, керуючись, наприклад, думкою експертів та, наприклад, використовуючи метод аналізу ієрархій Т. Сааті, з технічних аспектів того чи іншого класу засобів захисту, усвідомлено вибирати сумісні набори ЗЗІ.

Вважаємо, що у $Inv1$ є набір $g(0) = (g_1(0), \dots, g_n(0))$ ФР ($g_i(0)$ – ФР для

розвитку i -ої системи ІБ для ОБІ. Прийнемо, що $g_i(0)$ – вектор n -мірного простору з позитивними елементами. Навпаки, у $Inv2 - p(0) = (p_1(0), \dots, p_n(0))$, $(p_i(0))$ – ФР для розвитку i -ої системи ІБ для ОБІ, $p_i(0)$ – вектор n -мірного простору з позитивними елементами. Ці набори визначають прогнозовані, у момент $t=0$, величини ФР (далі по тексту – $FinR$) гравців для кожної нової системи інформаційної безпеки ОБІ.

На думку дослідників, взаємодія гравців (інвесторів у проєкти ІБ ОБІ), як результат, закінчується при виконанні наступних умов [99, 107, 108, 109, 110, 111, 112, 113, 114]:

$$(g(t), p(t)) \in S_0, \quad (2.8)$$

$$(g(t), p(t)) \in F_0. \quad (2.9)$$

Вважаємо, що

$$S_0 = \bigcup_{i=1}^{Mn} \{(g, p) : (g, p) \in R^{2M \cdot n}, g \succ 0, p_i = 0\},$$

$$F_0 = \bigcup_{i=1}^{Mn} \{(g, p) : (g, p) \in R^{2M \cdot n}, p \succ 0, g_i = 0\}.$$

Отже, якщо повністю виконано умову (2.8), то вважаємо, що процедура фінансування аналізованого проєкту ІБ ОБІ закінчена. У цьому випадку у $Inv2$ не вистачило ФР для продовження безперервної процедури інвестування. Це, принаймні, справедливо для одного з проєктів ІБ.

Якщо виконано умову (2.9), то вважаємо, що безперервна процедура інвестування у проєкти ІБ також закінчена. І, як результат, у цьому випадку в $Inv1$ не вистачило ФР для продовження безперервної процедури інвестування. Це, принаймні, теж справедливо для одного з проєктів ІБ ОБІ.

Якщо обидві умови (2.8) та (2.9) не виконуються, то вважаємо, що безперервна процедура інвестування для проєктів ІБ об'єкта інформатизації продовжується.

Процес безперервної процедури інвестування у межах схеми позиційної диференціальної гри з повною інформацією було раніше розглянуто на прикладі робіт [55, 100]. Це дослідження продовжує розгляд та вивчення проблем, що опрацьовані у вищевказаних публікаціях.

Як вище зазначалося, внаслідок симетричності обмежимося розглядом завданн я з позиції *Inv1*. Друга може бути вирішена аналогічно. Визначення чистої стратегії та безлічі переваги *Inv1* було наведено у роботах [55, 100].

Вирішення першого завдання полягає в знаходженні множин «переваги» *Inv1*. Також визначаються оптимальні стратегії *Inv1*. Аналогічно ставиться і вирішується завдання з погляду *Inv2*.

Наведемо умови, за яких перебуває рішення гри. Тобто в процесі рішення необхідно знайти множини «переваги» W_1 та оптимальні стратегії *Inv1*. Ці умови будуть задані такими матричними нерівностями (Випадки 1–5).

Випадок 1 – $(\Psi_1^* + Z_1^*) - E^* > 0, (\Psi_2^* + Z_2^*) - E^* > 0;$

Випадок 2 – $(\Psi_1^* + Z_1^*) - E^* > 0, (\Psi_2^* + Z_2^*) - E^* \leq 0;$

Випадок 3 – $(\Psi_1^* + Z_1^*) - E^* \leq 0, (\Psi_2^* + Z_2^*) - E^* > 0;$

Випадок 4 – $(\Psi_1^* + Z_1^*) - E^* \leq 0, (\Psi_2^* + Z_2^*) - E^* \leq 0;$

Випадок 5 – Решта варіантів співвідношень елементів даних матриць.

Введемо додаткові позначення:

$$A^i = \sum_{j=1}^n [(\Psi_2^* + Z_2^*) \times \Delta_2^*]_{ij};$$

$$B^i = \sum_{\theta=1}^n \{[(\Psi_1^* + Z_1^*) - E^*] \times \Delta_1^*\}_{i\theta} / \left\{ \sum_{j=1}^n \{[(\Psi_1^* + Z_1^*) - E^*]\}_{ij} \times \sum_{j=1}^n [(\Psi_2^* + Z_2^*) - E^*] \times \Delta_2^* \right\}_{\theta};$$

$$A_1^i = \sum_{\theta=1}^n \{[(\Psi_1^* + Z_1^*) - E^*] \times \Delta_1^*\}_{i\theta} / \left\{ \sum_{j=1}^n \{[(\Psi_1^* + Z_1^*) - E^*]\}_{ij} \times \sum_{j=1}^n [(\Psi_1^* + Z_1^*)] \times \Delta_1^* \right\}_{\theta};$$

$$B_1^i = \sum_{j=1}^n [[(\Psi_1^* + Z_1^*) - E^*] \times \Delta_1^*]_{ij};$$

$$\Omega^i = \sum_{j=1}^n [(\Psi_1^* + Z_1^*) \times \Delta_1^*]_{ij};$$

$$\Gamma^i = \sum_{\theta=1}^n \{[(\Psi_2^* + Z_2^*) - E^*] \times \Delta_2^*\}_{i\theta} / \left\{ \sum_{j=1}^n \{[(\Psi_2^* + Z_2^*) - E^*]\}_{ij} \times \sum_{j=1}^n [(\Psi_1^* + Z_1^*) - E^*] \times \Delta_1^* \}_{\theta} \right\};$$

$$\Gamma_1^i = \sum_{j=1}^n [[(\Psi_2^* + Z_2^*) - E^*] \times \Delta_2^*]_{ij};$$

$$\Omega_1^i = \sum_{\theta=1}^n \{[(\Psi_2^* + Z_2^*) - E^*] \times \Delta_2^*\}_{i\theta} / \left\{ \sum_{j=1}^n \{[(\Psi_2^* + Z_2^*) - E^*]\}_{ij} \times \sum_{j=1}^n [(\Psi_2^* + Z_2^*) - E^*] \times \Delta_2^* \}_{\theta} \right\};$$

$$(q_*)_i = [A^i - A_1^i] / [2 \times B_1^i] + \sqrt{\{[A^i - A_1^i] / [2 \times B_1^i]\}^2 + [B^i / B_1^i]};$$

$$(\varphi_*)_i = [\Omega^i - \Omega_1^i] / [2 \times \Gamma_1^i] + \sqrt{\{[\Omega^i - \Omega_1^i] / [2 \times \Gamma_1^i]\}^2 + [\Gamma^i / \Gamma_1^i]};$$

В рамках цих позначень для випадку 1 безліч переваги W_I визначається так:

$$\begin{aligned} W_1^i = & \bigcup_{i=1}^n \{(g(0), p(0)) : (g(0), p(0)) \in R_+^{2Mn}, (q_*)_i \times p_i(0) \prec \sum_{\theta=1}^n \{[(\Psi_1^* + Z_1^*) - E^*]_{i\theta} \times \\ & \sum_{j=1}^n [(\Psi_1^* + Z_1^*) - E^*]_{ij}\} \times g_\theta(0), \forall i = 1, \dots, n; (\varphi_*)_i \times g_i(0) \geq \sum_{\theta=1}^n [[(\Psi_2^* + Z_2^*) - E^*] \times \Delta_2^*] / \\ & \sum_{j=1}^n [[(\Psi_2^* + Z_2^*) - E^*] \times \Delta_2^*]_{ij} \times p_\theta(0)\}; \end{aligned}$$

$$W_1 = \bigcup_{i=1}^n W_1^i;$$

Оптимальною стратегією першого гравця буде $U^*(t) = E^*$.

Для всіх випадків, крім першого, безлічі переваги першого гравця ($InvI$) та його оптимальні стратегії знаходяться аналогічно. Так само знаходиться рішення

завдання і з боку другого гравця-союзника.

У результаті розв'язання системи рівнянь (2.7) отримано таку сукупність точок у багатовимірному просторі рішення, як це показано на рис. 2.1-2.3 [99].

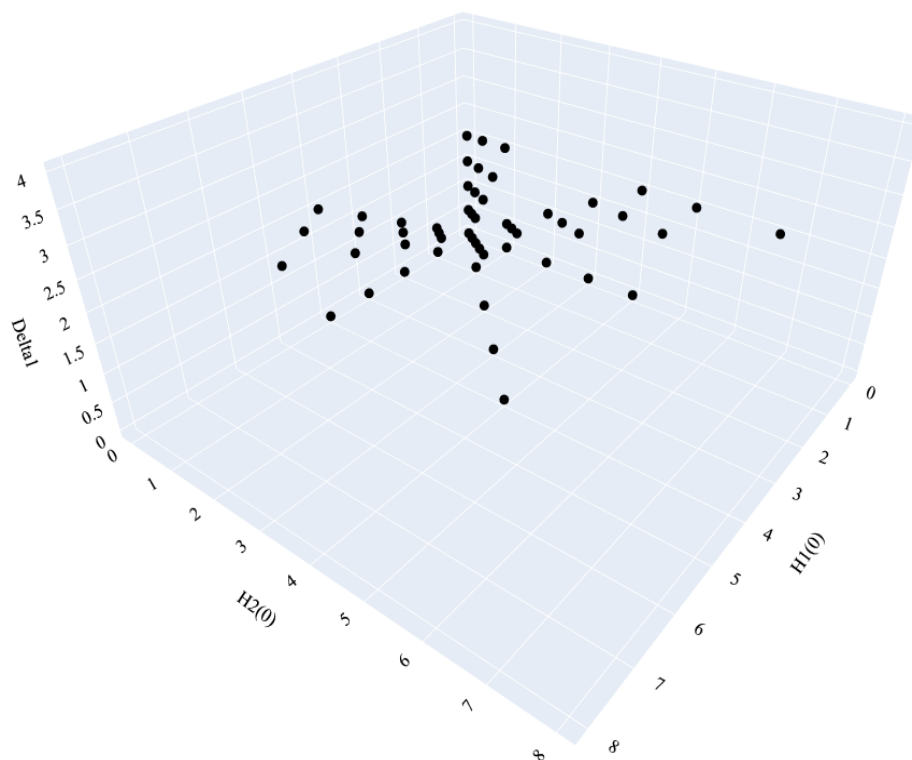


Рисунок 2.1. Залежність переваги множин W_1 для першого інвестора в КБ ОБІ для 3-х змінних

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.

Наприклад, для 4,5 та 6-ти мірних графіків за допомогою бібліотеки Plotly для мови Python можна емулювати глибину візуалізації, варіюючи кольорами, розміром або формою маркерів.

На рис. 2.2 та 2.3 наведено сукупність точок у тривимірному просторі. Осі відповідають наступним параметрам моделі: вісь $H1(0)$ – значення ФР першого гравця ($Inv1$); $H2(0)$ – значення ФР другого гравця ($Inv2$). Параметр $\Delta0(P0)$

характеризує величину ФР першого інвестора, витрачених на те, щоб вивести динамічну систему на свою термінальну поверхню.

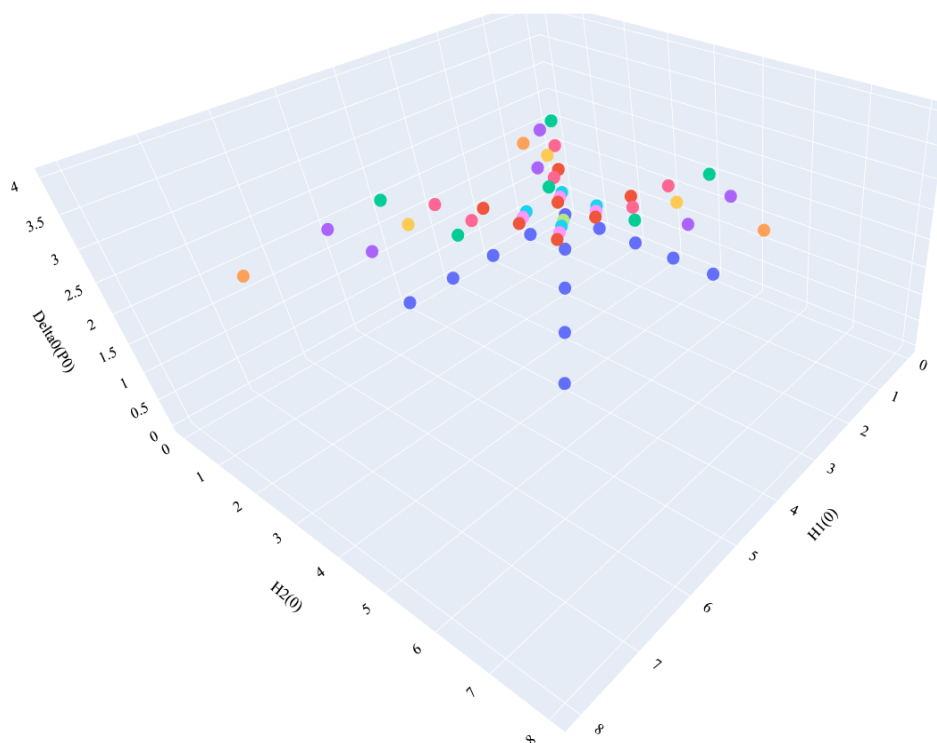


Рисунок 2.2. Залежність переваги множин W_1 для першого інвестора в КБ ОБІ для 4-х змінних

Точки дають можливість визначення переваги множин першого інвестора в КБ ОБІ. Відбувається це в такий спосіб. Як відомо, кожна точка є набором компонентів, що характеризують ФР інвесторів. Отже, набору компонентів, які є ФР першого інвестора, відповідає набір компонентів, що являє собою ФР другого інвестора. Таких наборів компонентів може бути кілька.

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.

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 [120].

Як зазначалося вище, для 4, 5 та 6-ти мірних графіків за допомогою бібліотеки Plotly для мови Python можна емулювати глибину візуалізації, варіюючи кольорами, розміром або формою маркерів. На рис. 2.2 світлий відтінок маркерів буде відповідати меншим значенням відсоткової плати $Inv2$ за фінансові інвестиції та частки повернення інвестицій $Inv2$ стосовно інвестицій $Inv1$ в проєкти ІБ ОБІ.

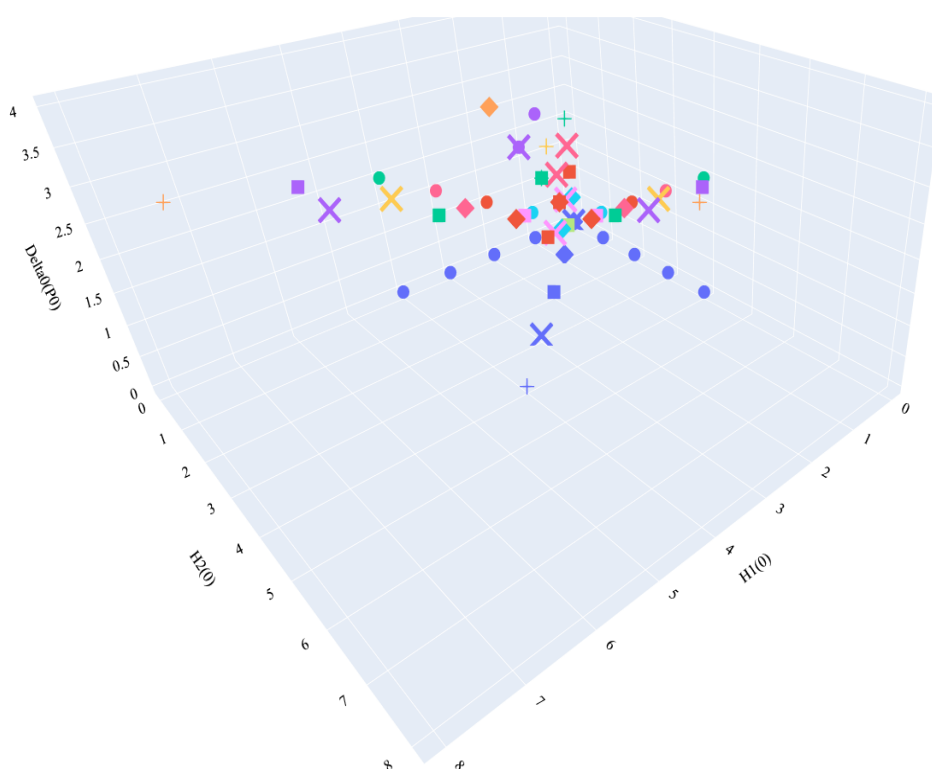


Рисунок 2.3. Залежність переваги множин W_1 для першого інвестора в КБ ОБІ для 5-х змінних

Слід зазначити, що у процесі дослідження зроблено висновок про те, що графічна інтерпретація із зображенням безлічі точок для онлайн графіків СППР

буде відповідати моделі інвестування, у якій передбачається, що перший інвестор може використовувати ФР, зумовлені заданими наборами цих ресурсів. Ці набори ФР можуть визначатися вибором конкретних інвестиційних програм [34]. Наприклад, це можуть бути програми розвитку нових технологій у завданнях контролю показників ризику реалізації інформаційних загроз та забезпечення необхідного рівня ІБ ОБІ і т.д.

Рисунок 2.3 служить додатковим підтвердженням можливості графічної інтерпретації у просторах більшої розмірності, ніж три й навіть чотири. Зазначимо, що суть інтерпретації така ж сама, як і для рисунка 2.2.

Розрахунки проведені для інвестиційних проектів у різні варіанти стратегій інвестування в ІБ товариства з обмеженою відповідальністю «Євро-Сервіс ЛТД». Вихідні дані для моделювання 3-х змінних показані в табл. 2.1., показані у табл. 2.1., для 4-х змінних у табл. 2.2.

Таблиця 2.1

Фрагмент таблиці вихідних даних для моделювання 3-х змінних

№	H1(0)	H2(0)	Delta0(P0)
1	2.5	3.2	0.7
2	3.1	1.3	2.2
3	2.4	3.7	1.9
4	1.9	5.0	1.3
5	2.4	3.8	2.1
6	1.4	4.2	2.0
7	3.6	1.8	1.2
8	3.4	5.3	2.7
9	2.0	3.9	3.0
10	3.1	6.0	2.4
11	3.8	7.6	1.0
12	2.4	6.9	0.8
13	1.0	5.6	2.9
14	3.7	6.0	1.8
15	2.1	4.3	1.1
16	1.2	5.5	2.7
17	3.3	2.9	0.9
18	2.6	3.4	1.2
19	3.5	4.7	1.5
20	1.8	5.2	2.4

Результати розрахунків представлені у табл. 2.3 та 2.4. Графічні залежності множини переваги W_I для першого інвестора в ІБ для випадків 3-х, 4-х і 5-ти

змінних, показані на рис. 2.1 – 2.3, відповідно.

T - час, за який перший гравець приведе стан системи на свою термінальну поверхню за даними з відповідним номером у таблиці.

$\Delta_0(P_0)$ - ступінь достовірності процедури інвестування в ІБ ОБІ (із заданим рівнем достовірності) за першою змінною.

$\Delta_1(P_0)$ - ступінь достовірності процедури інвестування в ІБ ОБІ (із заданим рівнем достовірності) за другою змінною.

Для кожної точки, яка відповідає ресурсам першого гравця, маємо значення змінних $\Delta_0(P_0)$, $\Delta_1(P_0)$. Цих значень може бути декілька. Частина цих значень буде відповідати множині, яка гарантує продовження процедур інвестування в ІБ. Інша частина відповідає ситуації, в якій другий гравець не може продовжити інвестування із заданим рівнем достовірності.

Таблиця 2.2

Фрагмент таблиці вихідних даних для моделювання 4-х змінних

№	H1(0)	H2(0)	$\Delta_0(P_0)$	$\Delta_1(P_0)$
1	2.5	3.2	0.7	3.8
2	3.1	1.3	2.2	8.1
3	2.4	3.7	1.9	4.5
4	1.9	5.0	1.3	8.7
5	2.4	3.8	2.1	1.6
6	1.4	4.2	2.0	4.9
7	3.6	1.8	1.2	3.9
8	3.4	5.3	2.7	6.7
9	2.0	3.9	3.0	1.6
10	3.1	6.0	2.4	7.1
11	3.8	7.6	1.0	3.3
12	2.4	6.9	0.8	4.9
13	1.0	5.6	2.9	2.8
14	3.7	6.0	1.8	4.4
15	2.1	4.3	1.1	6.9
16	1.2	5.5	2.7	2.4
17	3.3	2.9	0.9	5.9
18	2.6	3.4	1.2	7.6
19	3.5	4.7	1.5	3.8
20	1.8	5.2	2.4	4.5

Отже, вибираючи з наявних значень мінімальні за кожною компонентною, 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.

Таблиця 2.3

Фрагмент таблиці з результатами моделювання області переваги першого інвестора та його стратегії інвестування для 3-х змінних

№	W_1	T
1	$(2.5)H1(0)+(3.2)H2(0)>(0.7)\Delta(P0)$	5.2
2	$(3.1)H1(0)+(1.3)H2(0)>(2.2)\Delta(P0)$	4
3	$(2.4)H1(0)+(3.7)H2(0)>(1.9)\Delta(P0)$	3.7
4	$(1.9)H1(0)+(5.0)H2(0)>(1.3)\Delta(P0)$	2
5	$(2.4)H1(0)+(3.8)H2(0)>2.1\Delta(P0)$	9.1
6	$(1.4)H1(0)+(4.2)H2(0)>(2.0)\Delta(P0)$	15.3
7	$(3.6)H1(0)+(1.8)H2(0)>(1.2)\Delta(P0)$	22
8	$(3.4)H1(0)+(5.3)H2(0)>(2.7)\Delta(P0)$	2.9
9	$(2.0)H1(0)+(3.9)H2(0)>(7.7)\Delta(P0)$	8.9
10	$(3.1)H1(0)+(6.0)H2(0)>(2.4)\Delta(P0)$	13
11	$(3.8)H1(0)+(7.6)H2(0)>(1.0)\Delta(P0)$	24
12	$(2.4)H1(0)+(6.9)H2(0)>(0.8)\Delta(P0)$	12
13	$(1.0)H1(0)+(5.6)H2(0)>(2.9)\Delta(P0)$	3
14	$(3.7)H1(0)+(6.0)H2(0)>(1.8)\Delta(P0)$	33
15	$(2.1)H1(0)+(4.3)H2(0)>(1.1)\Delta(P0)$	15
16	$(1.2)H1(0)+(5.5)H2(0)>(2.7)\Delta(P0)$	6
17	$(3.3)H1(0)+(2.9)H2(0)>(0.9)\Delta(P0)$	12
18	$(2.6)H1(0)+(3.4)H2(0)>(1.2)\Delta(P0)$	7.5
19	$(3.5)H1(0)+(4.7)H2(0)>(1.5)\Delta(P0)$	19
20	$(1.8)H1(0)+(5.2)H2(0)>(2.4)\Delta(P0)$	28

Розмір маркера для рисунка 2.3 дозволяє використовувати візуалізацію п'ятого вимірювання. Тут використовувався параметр `markersize` функції `Scatter3D` для бібліотеки `Plotly`. Форми маркерів відмінно підійдуть для візуалізації категорій проєктів у рамках пошуку раціональної стратегії ІБ ОБІ. Наприклад, круглі маркери відповідають категорії проєктів із розвитку безпеки прикладного ПЗ. Тоді маркери у вигляді ромбів – інвестування в безпеку технологій обробки даних. А маркери у вигляді символу плюс (+) – інвестування в контроль показників ризику реалізації інформаційних загроз та забезпечення необхідного рівня ІБ ОБІ і т.д. Отже, бібліотека `Plotly` надає на вибір 10 різних фігур для 3D графіків. Таким чином, у якості форми маркерів для онлайн платформи СППР можна показати до 10 різних значень.

Але слід зазначити, що виявленим недоліком моделей на основі даного підходу є той факт, що отримані дані прогнозованої оцінки при виборі стратегій інвестування в КБ ОБІ, фактично, не завжди легко інтерпретувати, не будучи фахівцем у галузі теорії ігор або не володіючи інформацією про функціонал бібліотеки Plotly.

Таблиця 2.4

Фрагмент таблиці з результатами моделювання області переваги першого інвестора та його стратегії інвестування для 4-х змінних

№	W_1	T
1	$(2.5)H1(0)+(3.2)H2(0)>(0.7)\Delta(P0)>(0.75)\Delta(P1)$	5.6
2	$(3.1)H1(0)+(1.3)H2(0)>(2.2)\Delta(P0)>(0.68)\Delta(P1)$	4.4
3	$(2.4)H1(0)+(3.7)H2(0)>(1.9)\Delta(P0)>(0.53)\Delta(P1)$	6
4	$(1.9)H1(0)+(5.0)H2(0)>(1.3)\Delta(P0)>(0.8)\Delta(P1)$	4
5	$(2.4)H1(0)+(3.8)H2(0)>(2.1)\Delta(P0)>(0.64)\Delta(P1)$	12.1
6	$(1.4)H1(0)+(4.2)H2(0)>(2.0)\Delta(P0)>(0.77)\Delta(P1)$	9.3
7	$(3.6)H1(0)+(1.8)H2(0)>(1.2)\Delta(P0)>(0.5)\Delta(P1)$	16
8	$(3.4)H1(0)+(5.3)H2(0)>(2.7)\Delta(P0)>(0.82)\Delta(P1)$	4.7
9	$(2.0)H1(0)+(3.9)H2(0)>(7.7)\Delta(P0)>(0.9)\Delta(P1)$	6.9
10	$(3.1)H1(0)+(6.0)H2(0)>(2.4)\Delta(P0)>(0.74)\Delta(P1)$	2
11	$(3.8)H1(0)+(7.6)H2(0)>(1.0)\Delta(P0)>(0.62)\Delta(P1)$	29
12	$(2.4)H1(0)+(6.9)H2(0)>(0.8)\Delta(P0)>(0.56)\Delta(P1)$	8
13	$(1.0)H1(0)+(5.6)H2(0)>(2.9)\Delta(P0)>(0.7)\Delta(P1)$	14
14	$(3.7)H1(0)+(6.0)H2(0)>(1.8)\Delta(P0)>(0.61)\Delta(P1)$	15
15	$(2.1)H1(0)+(4.3)H2(0)>(1.1)\Delta(P0)>(0.8)\Delta(P1)$	33
16	$(1.2)H1(0)+(5.5)H2(0)>(2.7)\Delta(P0)>(0.79)\Delta(P1)$	2.7
17	$(3.3)H1(0)+(2.9)H2(0)>(0.9)\Delta(P0)>(0.63)\Delta(P1)$	7.3
18	$(2.6)H1(0)+(3.4)H2(0)>(1.2)\Delta(P0)>(0.55)\Delta(P1)$	5
19	$(3.5)H1(0)+(4.7)H2(0)>(1.5)\Delta(P0)>(0.81)\Delta(P1)$	22
20	$(1.8)H1(0)+(5.2)H2(0)>(2.4)\Delta(P0)>(0.52)\Delta(P1)$	30

Систему диференціальних рівнянь (2.1) можна вирішити, застосувавши один із математичних пакетів, наприклад MatLab або Maple.

Так, наприклад, на малюнку 2.4 наведено множину W_1 , отриману в результаті моделювання в пакеті MatLab.

Множина переваги першого гравця, що представляє бік захисту ОБІ, буде перебувати під цією поверхнею в тривимірному позитивному ортанті.

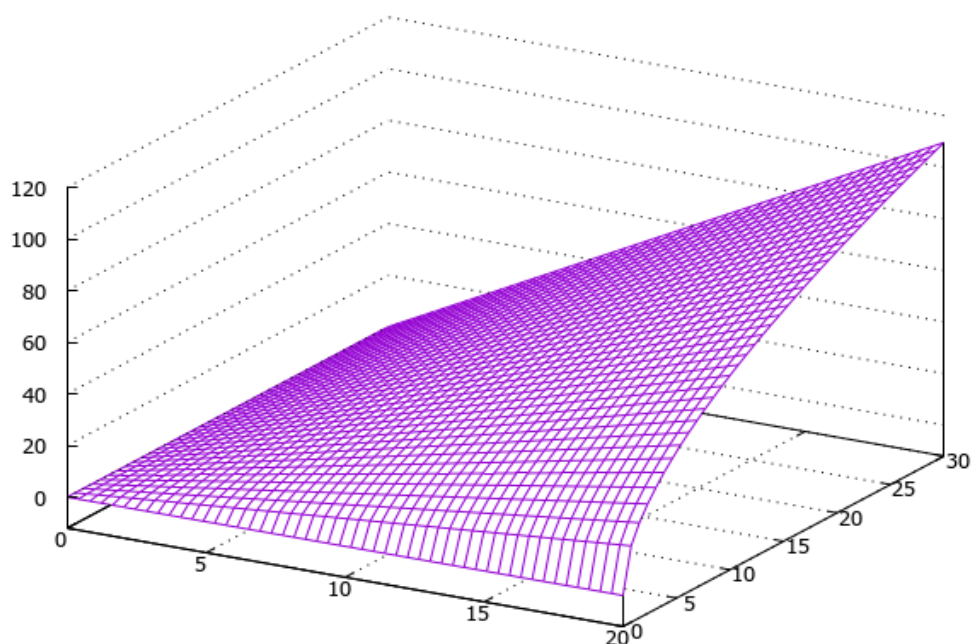


Рисунок 2.4. Результати моделювання множини W_1

На рис. 2.5–2.7 і показані результати для 3-х тестових розрахунків під час обчислювального експерименту.

Мета експерименту визначити безліч стратегій гравців U та V .

На рисунках лінії траєкторій зміни раціональних стратегій гравців, за відповідних інвестиційних ресурсів, зображені червоним кольором із маркерами у вигляді ромбів синього кольору).

Під час обчислювальних експериментів розглядаються випадки, коли стратегії гравців виводять їх на відповідні термінальні поверхні S_0 , F_0 .

У ході експерименту знаходяться безліч початкових станів об'єктів та їх стратегій, які дозволяють об'єктам привести систему на ту чи іншу термінальну поверхню.

На рис. 2.5–2.7 прийнято:

вісь h_1 – фінансові ресурси $Inv1$;

вісь h_2 – фінансові ресурси $Inv2$;

область під променем – \hat{W}_1 (область “переваги” $Inv1$);

область над променем – \hat{W}_2 (область “переваги” $Inv2$) [99, 101].

Промені збалансованості відображаються без маркерів. Крпки, що знаходяться на раціональній стратегії гравця 1 позначені круглими маркерами.

Рисунок 2.5 ілюструє ситуацію, коли $Inv1$ має перевагу у співвідношенні початкових ФР при інвестуванні на захист ОБІ. Тобто $FinR$ перебувають у множині переваги $Inv1$.

У цьому випадку 1-й гравець, застосовуючи свою оптимальну стратегію, досягне своєї мети, а саме приведення стану системи на «свою» термінальну поверхню.

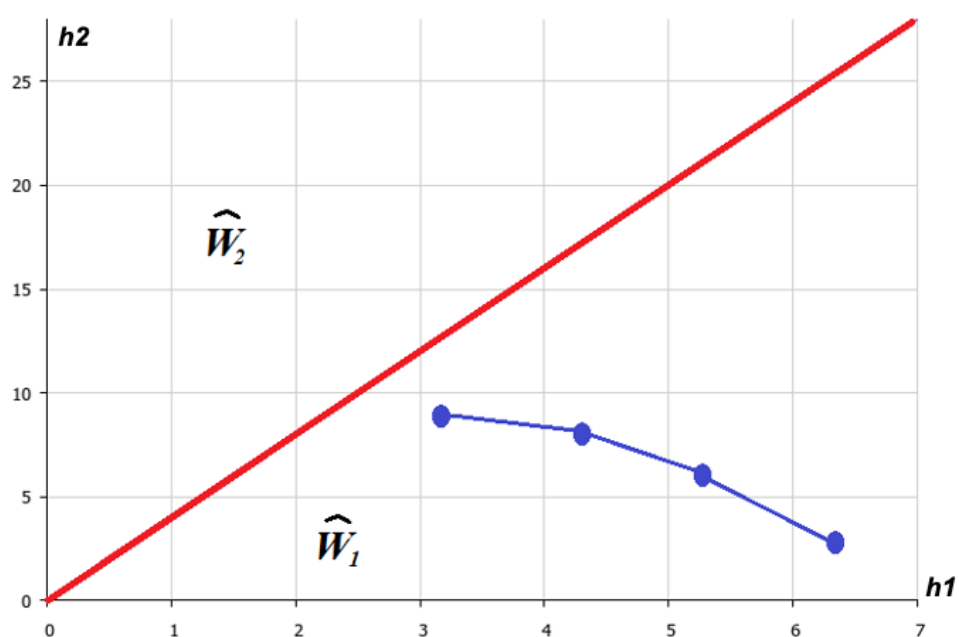


Рисунок 2.5. Результати обчислювального експерименту 1

Рисунок 2.6 демонструє ситуацію, в якій $Inv2$, використовує неоптимальну стратегію $Inv1$ у початковий час.

Гравець 2 домагається того, що «наводить» стан системи на «свою» термінальну поверхню.

Рисунок 2.7 відповідає випадку, коли початковий стан системи перебуває в промені збалансованості. Це «задовольняє» одночасно обох інвесторів $Inv1$ та $Inv2$. Ми отримуємо "стійку" систему.

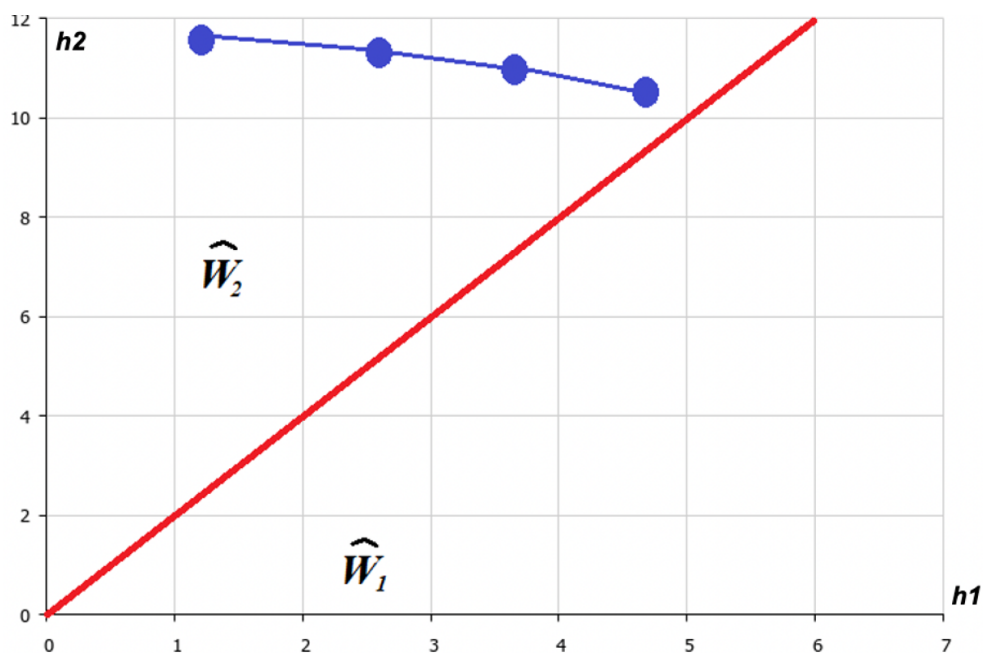


Рисунок 2.6. Результати обчислювального експерименту 2

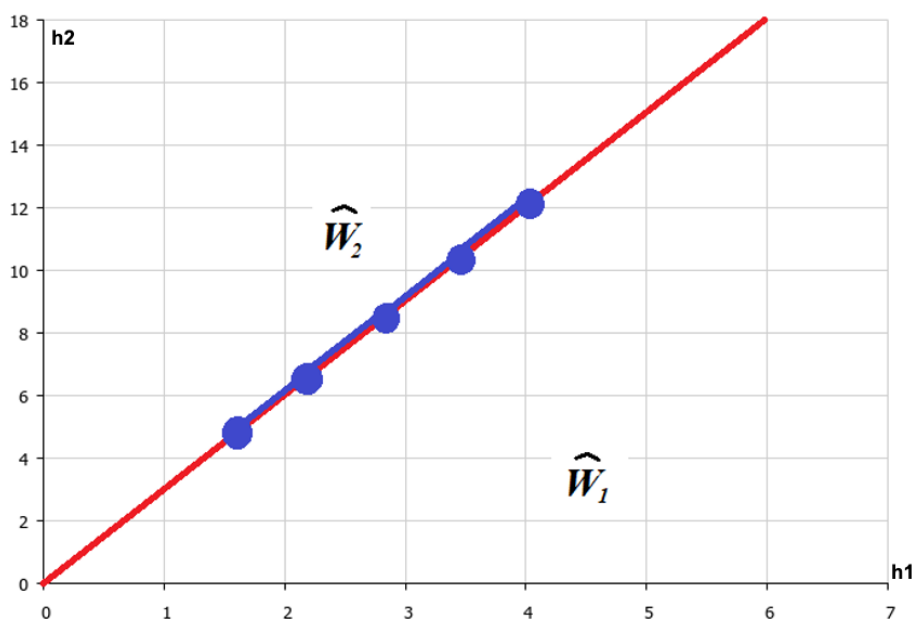


Рисунок 2.7. Результати обчислювального експерименту

Таким чином, отримані результати під час обчислювальних експериментів дали можливість продемонструвати коректність запропонованої моделі.

Зауважимо, що в реальних проектах інвестування в КБ ОБІ доводиться розглядати безліч інших параметрів, що впливають на успішність реалізації проекту зі створення ефективної системи захисту ОБІ.

Дійсно, ОПР, необхідно оцінювати пріоритетність вкладення своїх фінансових ресурсів (ФР) у такі напрями розвитку ІБ ОБІ як [99, 101]:

- забезпечення кібернетичної стійкості ОБІ;
- інноваційні технології в завданнях контролю показників ризику реалізації інформаційних загроз та забезпечення необхідного рівня ІБ ОБІ;
- культура ІБ;
- ІБ інфраструктури ОБІ;
- безпека прикладного програмного забезпечення (ПЗ);
- безпека технологій обробки даних;
- інше.

У міру зростання кількості напрямів інвестування в КБ ОБІ зростає і кількість варіантів рішення для системи диференціальних рівнянь.

Так нижче показані результати обчислювальних експериментів для пошуку прийнятної сторони захисту стратегії інвестування в КБ ОБІ.

У результаті експерименту перебувають безлічі початкових станів об'єктів та його стратегій. Саме ці стратегії дозволяють об'єктам привести систему на ту чи іншу термінальну поверхню.

На площині (рисунок 2.8) вертикальна вісь – фінансові ресурси $Inv2$. Дві горизонтальні осі (x, y) – фінансові ресурси $Inv1$. Область, що знаходиться під обома гіперплощинами одночасно («нижче» за них) – W_1 (область "переваги" $Inv1$).

На рис. 2.8 цифрою 1 позначена гіперплощина, що визначає область, розташовану нижче за гіперплощину, в якій $Inv1$ гарантує собі збереження своїх ФР з обох напрямів інвестування у КБ.

Цифрою 2 позначена гіперплощина, що визначає область, розташовану нижче цієї гіперплощини, в якій $Inv1$ має можливість забезпечити втрату ФР $Inv2$ (Тобто цілі атак за таких витрат ФР з боку $Inv2$ не будуть досягнуті).

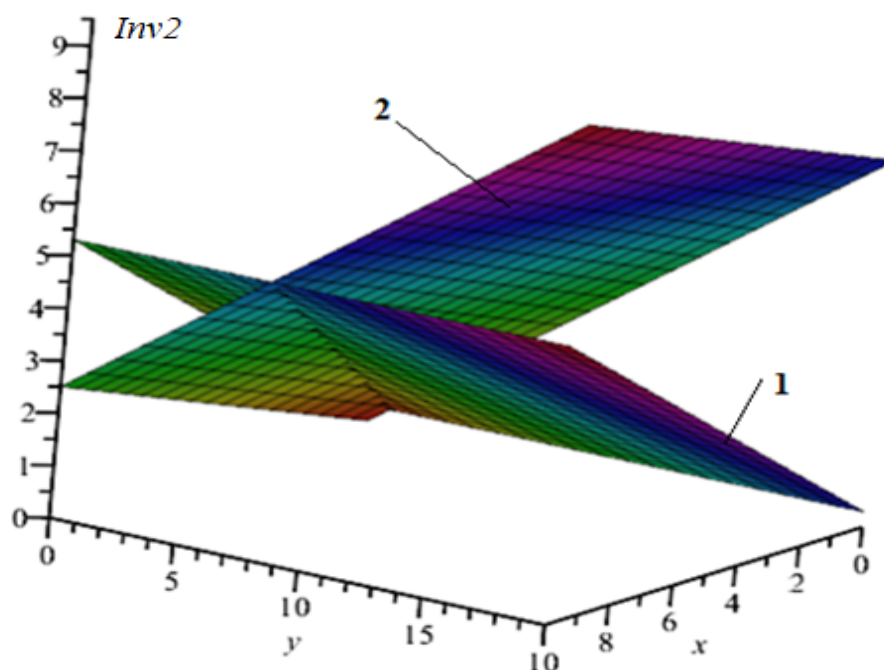


Рисунок 2.8. Результати обчислювального експерименту 1

На рис. 2.9 вертикальна вісь також позначає фінансові ресурси $Inv2$, а дві горизонтальні осі (x,y) – ФР $Inv1$. Область, що знаходиться під трьома гіперплощинами одночасно («нижче» за них)– W_1 (область "переваги" $Inv1$).

На рис. 2.9 розглянуто завдання пошуку раціональної стратегії інвестування для напрямів:

- забезпечення кібернетичної стійкості ОБІ;
- інноваційні технології в завданнях контролю показників ризику реалізації інформаційних загроз та забезпечення необхідного рівня ІБ ОБІ;
- культура ІБ.

На рис. 2.9 цифрами 1 і 2 позначені гіперплощини, що визначають область, розташовану нижче цих гіперплощин, в якій $Inv1$ гарантує собі збереження своїх ФР по обох компонентах, наприклад, 1) забезпечення кібернетичної стійкості ОБІ; 2) безпека прикладного ПЗ.

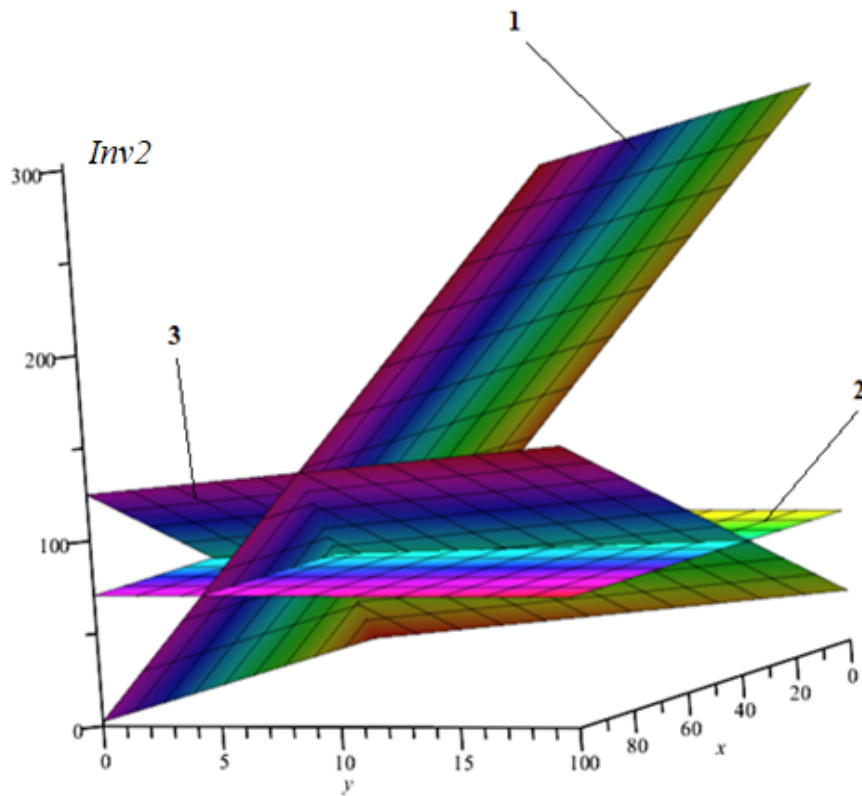


Рисунок 2.9. Результати обчислювального експерименту 2

Цифрою 3 позначена гіперплощина, що визначає область, розташовану нижче цієї гіперплощини, в якій *Inv1* має можливість забезпечити втрату ФР для *Inv2*.

Інвестиційний процес у КБ ОБІ характеризується безліччю факторів, наприклад, як розподілити ФР на пріоритетні чи не пріоритетні напрямки. Зазначена обставина призводить до того, що проблема не може бути описана будь-яким одним фактором, що призводить до багатовимірності. Вирішення багатовимірних завдань, як правило, вимагає розробки інструментарію, який не є ідентичним інструментарію, розробленому для одновимірного випадку.

В області W_1 1-й гравець (захисник ІС) може досягти мети:

а) за кінцеве число кроків, тобто $\widehat{W}_1 \subseteq \bigcup_{m=1}^{N_*} W_1^m, 0 < N_* < +\infty$,

якщо $\lim_{T \rightarrow \infty} \left(\left(\min_{1 \leq k \leq n} 1_k^{T,i} \right) \right) > 1$, при деякому $i: 1 \leq i \leq n$;

б) принаймні за злічене число кроків

якщо $\lim_{T \rightarrow \infty} \left(\left(\min_{1 \leq k \leq n} 1_k^{T,i} \right) \right) = 1$, при деякому $i: 1 \leq i \leq n$.

Можлива ситуація, за якої в області W_1 1-й гравець (захисник ІС) за будь-яке число кроків може не досягти мети:

$$\text{в) при } \sup_T \left(\max_{1 \leq i \leq n} \left(\min_{1 \leq k \leq +n} (1^{T,j}) \right) \right) < 1.$$

На думку дослідників, необхідність залучення генетичного алгоритму (далі ГА) на другому етапі методу вибору раціональної стратегії інвестування у проєкти із забезпечення кібербезпеки об'єкта інформатизації обумовлена наступним міркуванням. Термінальну поверхню, як це показано на рис. 2.1-2.3 або в роботі [101], утворює безліч точок, які відповідають перевазі множини інвестора. Ця множина утворена точками на термінальній поверхні. І для того, щоб знайти раціональну стратегію, необхідно додатково досліджувати інформацію, що стосується досить великої кількості можливих напрямів інвестування. Кожен із цих напрямів, так само, може бути розбитий на піднапрямки. Наприклад, при виборі конкретних апаратно-програмних засобів захисту інформації. Детально проаналізувавши дані опрацьованих робіт, можливі отримані результати та довготривалість процесу, робимо висновок, що все це диктує необхідність залучати більш швидкодіючий алгоритм для перебору точок на термінальній поверхні для пошуку раціональної траєкторії, що відповідає стратегії інвестування в КБ ОБІ.

2.2. Забезпечення кібербезпеки об'єкта інформатизації за допомогою генетичного алгоритму

Спираючись на дані робіт, проаналізованих у першому розділі дисертації, а також робіт [132, 68, 20, 21, 24, 3, 35, 68, 81, 116], визначимо можливі напрями інвестування (показники), що якісно впливають на зростання віддачі від інвестування у проєкти із забезпечення КБ ОБІ.

Найменування цих напрямів інвестування (показники), а також перелік змінних, які ставляться у відповідність до кожного з напрямків, до якого виявляють інтерес інвестори, приведені в таблиці 2.5.

Передбачається, що кожен напрямок інвестування може сприяти зростанню прибутковості чи ефективності для умовного ОБІ.

Таблиця 2.5

**Кодування змінних для завдання пошуку раціональної стратегії
інвестування у проєкти із забезпечення кібербезпеки об'єкта
інформатизації**

№	Параметри	Позначення
	Зростання віддачі від інвестування у проєкти із забезпечення КБ ОБІ	PrG
	Напрямки інвестування (показники)	X_i
1	Проєктування, розробка та розгортання комплексної ЗЗІ	X_1
2	Удосконалення системи забезпечення ІБ (УЗІБ)	X_2
3	Виявлення інцидентів ІБ, реагування на інциденти, прогнозування кібернетичних ризиків для ОБІ	X_3
4	Мінімізація зв'язків між окремими об'єктами захисту інформації та уніфікація компонентів контурів захисту інформації (ЗІ) для конкретного ОБІ	X_4
5	Розробка організаційних заходів щодо захисту інформації та КБ, яка відповідає специфіці бізнес-процесів ОБІ	X_5
6	Матеріальні та фінансові витрати на ЗІ (Програмне забезпечення для задач ЗІ)	X_6
7	Матеріальні та фінансові витрати на ЗІ (Апаратний захист ОБІ)	X_7
8	Матеріальні та фінансові витрати на ЗІ (Захист мережевої інфраструктури ОБІ)	X_8
9	Витрати на аудит інформаційної безпеки ОБІ в цілому та ІТ, які забезпечують ключові бізнес-процеси	X_9
10	Витрати на пошук вразливостей нового ПЗ для забезпечення бізнес-процесів на ОБІ	X_{10}
11	Людські ресурси залучені у проєктах із забезпечення ЗІ та КБ ОБІ	X_{11}
12	Витрати управління проєктами у сфері ЗІ та КБ ОБІ	X_{12}
13	Інші витрати на забезпечення ЗІ та КБ ОБІ	X_{13}
14	Підвищення рівня конкурентоспроможності та нові ринки	X_{14}
15	Розвиток інновацій та впровадження цифрових технологій у бізнес-процеси	X_{15}
16	Зниження витрат на ІТ	X_{16}

Зрозуміло, що перелік заходів та відповідних витрат, наведений у таблиці 2.5, далеко не повний. Він лише дозволяє продемонструвати загальний напрямок і суть запропонованого методу вибору раціональної стратегії інвестування в проєкти із забезпечення кібербезпеки об'єкта інформатизації на основі комбінації теорії ігор та генетичного алгоритму, як методу багатофакторної оптимізації.

Вважатимемо, що в таблиці 2.5 PrG – параметр, який характеризує зростання віддачі від інвестування у кібербезпеку ОБІ.

Параметр PrG прийнято у фінансових одиницях і розглядається він як залежна від x (напрями інвестування в технології захисту інформації та забезпечення кібербезпеки ОБІ) змінна.

Зазначимо, що генетичний алгоритм повинен дозволяти реалізовувати такі процедури у процесі обробки даних:

- розраховувати приріст PrG ;
- визначати порогові значення PrG ;
- перетворювати значення PrG до бінарного вигляду;
- перетворювати значення показників X_i до бінарного вигляду;
- визначати кількість помилок для класифікованої послідовності PrG ;
- визначати список пріоритетних напрямів інвестування в КБ ОБІ, які можуть забезпечити максимальне зростання його економічних показників; при цьому необхідно мінімізувати кількість помилок для PrG .

Крім того, слід зазначити, що величину параметра PrG – зростання віддачі від інвестування в забезпечення КБ та захисту інформаційних активів ОБІ у загальному вигляді можна визначити на підставі моделей, які були представлені в роботах [97, 98]. У зазначених роботах докладно розглядаються теоретичні аспекти застосування ГА для вирішення оптимізаційного завдання, пов'язаного з підбором оптимального складу апаратно-програмних комплексів захисту інформації.

Для того щоб представити прогнозовані оцінки, що отримуються для термінальних поверхонь або в багатовимірному просторі (для цієї мети й служить перший етап запропонованого методу) за певний часовий період, застосуємо бінарне кодування.

За умови, якщо результат вирішення білінійної динамічної гри якості з декількома термінальними поверхнями показує збільшення прибутків інвесторів у систему КБ ОБІ, то індикатор бінарного коду прийнято вважати рівним 1.

Якщо прогноз зростання нульовий чи негативний, то індикатор прийнято вважати рівним 0.

Фрагмент таблиці з прикладом результатів бінаризації показаний нижче.

Виконаємо кодування для змінних.

Як приклад, розглянемо хромосомну нитку, що включає два гени, X_1 та X_2 з таблиці 2.5.

Таблиця 2.6

Результати бінаризації показників зростання віддачі від інвестування в кібербезпеку об'єкта інформатизації

Напрямок (див. таблицю 2.1)	Прогнозована величина зростання віддачі від інвестування в кібербезпеку об'єкта інформатизації за окремими напрямками	Індикатор
1	+25 (приклад розрахункового значення на підставі моделей [9,10,21])	1
2	-10	0
...
16	+5	1

Це, відповідно, напрями інвестування в проекти з проектування, розробки та розгортання комплексного ЗЗІ та вдосконалення системи забезпечення ІБ (УЗІБ) для ОБІ.

Вважатимемо, що довжина кожного з генів становить 16 біт. Отже, хромосомна нитка буде включати 32 біти, див. рис. 2.10.

X_1															
1	0	0	0	1	0	1	1	0	1	1	1	0	1	1	0
X_2															
0	0	1	1	0	0	0	1	1	1	1	1	1	0	1	1

Рисунок 2.10. – Результат кодування хромосом

Як бачимо на рис. 2.10 двійковий код для хромосом X_1 та X_2 отримано на підставі перенесення даних прикладу прогнозованої оцінки зростання фінансового ресурсу інвестора в проекти забезпечення КБ ОБІ для випадку реалізації інвестиційних проектів за напрямками, пов'язаними з розробкою та

розгортанням комплексного ЗЗІ та вдосконалення системи забезпечення ІБ (УЗІБ). Розрахунок прогнозованої оцінки виконано на підставі моделей [97, 98].

ГА, що розробляється, повинен підтримувати N хромосомних ниток, які утворюють популяцію.

Отже, у ході кожної ітерації виконуватиметься відбір із популяції тих хромосом, які найбільше пристосовані до подальшого розвитку. Ці хромосоми утворюють пари батьків. Далі, відповідно до класичного оператора схрещування, відтворюється нове покоління нащадків. Як результат, бачимо, що нащадки успадкують найкращі з батьківських генів.

Різноманітність генів забезпечить оператор мутації. Його застосування дозволяє досліджувати нові області у просторі пошуку для поєднання напрямків інвестування у проекти КБ ОБІ.

Слід відзначити, що під час відбору виживуть ті екземпляри хромосом, які демонструють найбільшу придатність. Хромосоми, у яких менша придатність, не будуть враховані для процедур відтворення нащадків. Як результат, імовірність відбору може бути визначена так:

$$P_i^{sel} = \frac{F_i}{\sum_{j=1}^N F_j}, \quad (2.4)$$

де F – значення функції придатності під час аналізу i -го напрямку інвестування у проекти із забезпечення КБ ОБІ;

N – кількість хромосом.

Слід зазначити, що точка схрещування визначалася випадковим чином. Після цього виконувався обмін із іншою розділеною хромосомою вмісту відповідних бітів, що знаходяться праворуч або ліворуч від даної точки.

Приклад для батьківських хромосом $N1$, $N2$ показано на рис. 2.11.

Точка схрещування показана з жовтою заливкою.

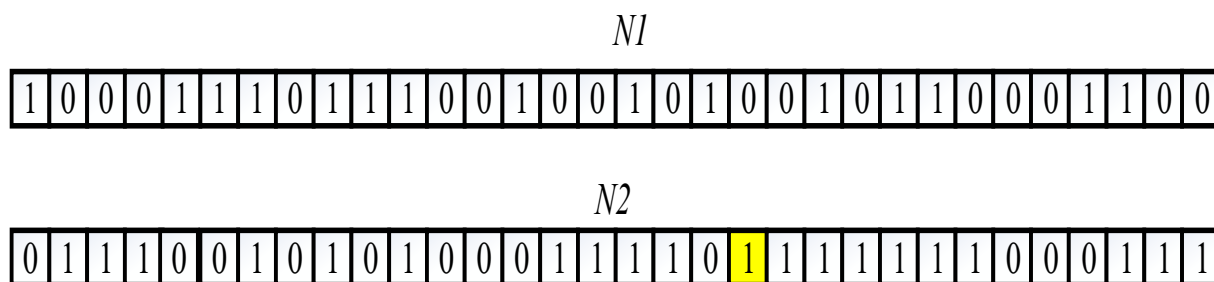


Рисунок 2.11 – Приклад для батьківських хромосом $N1$, $N2$
з точкою схрещування

Припустивши, що обмін бітів відбуватиметься праворуч від точки схрещування, отримаємо вигляд нащадків, представлений на рис. 2.12.

Замінені фрагменти хромосом показані заливкою. Відповідно для першого нащадка ($N1^p$) – світло-зеленою. Для другого нащадка ($N2^p$) - блакитною.

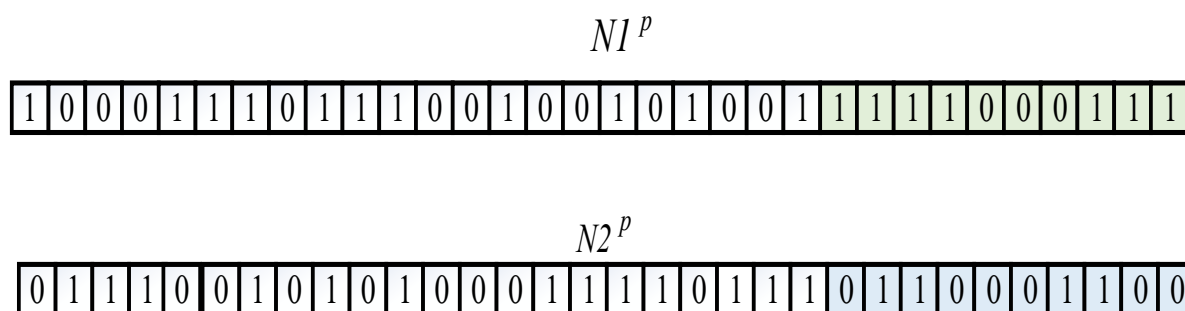


Рисунок 2.12 – Приклад формування нащадків

Далі реалізується мутація, тобто випадковий процес, який, на нашу думку, внесе в бінарний код хромосоми зміну значення в деякій позиції біта.

Наприклад, якщо припустити, що для хромосоми $N1^p$ внаслідок мутації зміниться 9 біт з 1 на 0, відповідно, вся хромосома нащадка буде виглядати, як показано на рис. 2.13.

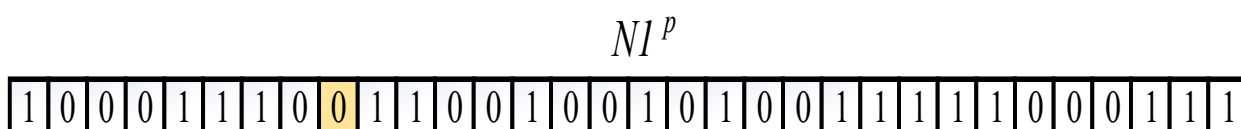


Рисунок 2.13– Вид хромосоми нащадка $N1^p$ після мутації гена

Після того, як реалізовані оператори з відбору, схрещування та мутації, необхідно здійснити спрямований пошук. Такий пошук реалізується на основі правила, що кожне з наступних поколінь успадковуватиме лише найкращі ознаки попередніх поколінь. Причому це правило має бути реалізовано, виходячи з необхідності руху в бік оптимального вибору для інвесторів. Таким чином, у результаті попередніх напрацювань буде сформовано підмножину точок, що містять розв'язання задачі. Для цих точок відхилення від цільової функції буде мінімальне.

Зауважимо, що за такого комбінованого підходу до розв'язання задачі з пошуку стратегій інвестування з максимізацією віддачі фінансового ресурсу для інвесторів, можна вирішувати високонелінійні завдання. Причому важливо, що при їх вирішенні ми не залежимо від виду цільової функції. Тому, як результат, знайдене рішення буде квазіоптимальним та близьким до глобального. Загальна схема реалізації запропонованого в дослідженні ГА показана на рис. 2.14.

Далі в роботі розглянуто основні етапи розв'язання задачі вибору раціональної стратегії інвестування у проекти КБ для ОБІ. Як було показано вище, пошук рішення виконується у два етапи. Зазначимо, що на першому етапі залучено потенціал апарату білінійних диференціальних ігор. Це дозволило отримати термінальну поверхню, де розташовані точки, що характеризують набори певних напрямів інвестування. А на другому етапі використано генетичний алгоритм, який внаслідок досить високої швидкодії забезпечує оперативний перебір різних варіантів заходів щодо забезпечення КБ ОБІ. Слід зауважити, що це особливо важливо в умовах динамічного протистояння зі стороною, що атакує, коли стороні захисту складно прогнозувати всі сценарії проведення атак на свої інформаційні системи.

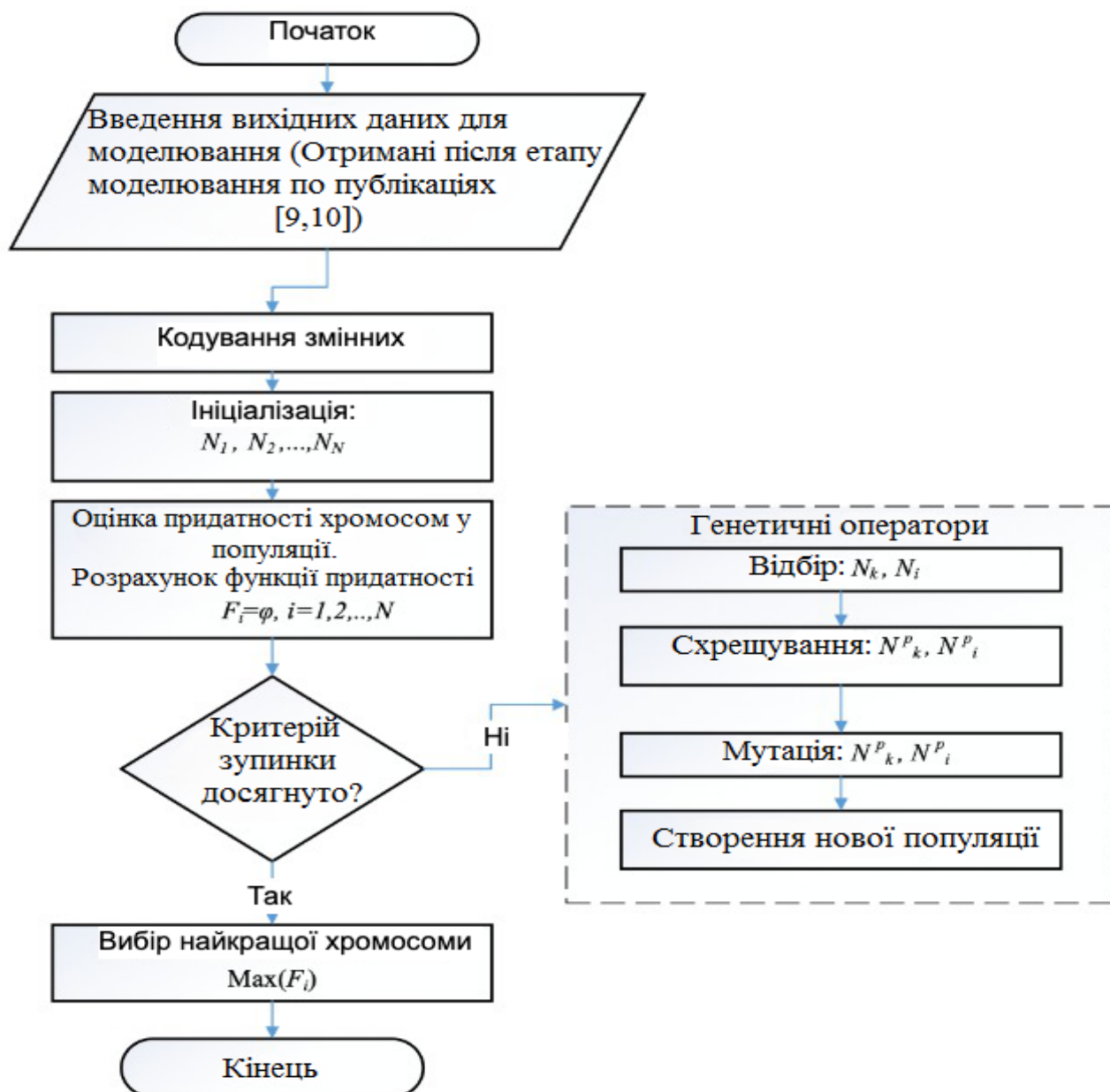


Рисунок 2.14 – Блок-схема генетичного алгоритму для розв’язання задачі вибору раціональної стратегії інвестування у технології КБ для ОБІ

Зокрема, варто наголосити, що зазначений метод включає такі кроки для частини застосування ГА.

1. Ініціалізація.

Генерується початкова популяція, що складається з N хромосом. Хромосоми представлені в бінарному коді. Вихідними даними для кодування є дані, які отримані в процесі вирішення багатокрокової гри якості з кількома термінальними поверхнями [76].

2. Виконується оцінка пристосованості хромосом у популяції.

Розраховується функція придатності (цільової функції в загальному випадку). У такому випадку в якості цільової функції прийняті прогнозовані значення віддачі від інвестування в ті чи інші напрями розвитку системи КБ для ОБІ. А тому цільова функція визначається для кожної з хромосом.

3. Відтворення.

Розглянемо наведені нижче кроки 3.1–3.4. Це реалізується до того моменту, поки не буде створено нову популяцію, що складається з N хромосом.

3.1. Відбір та селекція. Відбираємо з популяції дві батьківські хромосоми з ймовірністю P_i^{sel} .

3.2. Схрещування. Визначимо чи є необхідність виконання операції зі схрещування чи ні. Якщо така потреба є, то здійснимо обмін бітів у випадкових позиціях. Для будь-якого варіанта (реалізовано схрещування або воно відсутнє) хромосоми перейдуть у розряд нащадків.

3.3. Мутація. Для хромосом нащадків випадково замінимо відібраний біт.

3.4. Генерація нової популяції. Генерується нова популяція. При цьому застосуємо принцип «елітного» відбору.

4. Повторення.

Повторюємо процес відповідно до пункту 2 до того моменту, поки не буде досягнуто умови для припинення дії алгоритму.

5. Відбираємо «найкращу» хромосому.

Потрібно зазначити, що підбір кращої хромосоми характеризує пріоритетні напрямки інвестування проєктів у КБ ОБІ, з погляду інвестора, для яких віддача від інвестицій у КБ буде максимальною.

Інфраструктура ОБІ з погляду забезпечення КБ представлена на рис. 2.15.

За замовчуванням у вузлах інформаційно-комунікаційної системи (ІКС) ОБІ обов'язково мають бути встановлені стандартні ЗЗІ: антивіруси; брандмауер; засоби: 1) виявлення вторгнень; 2) криптографічного ЗІ; 3) розмежування доступу; 4) контролю цілісності; 5) автентифікації та ін.

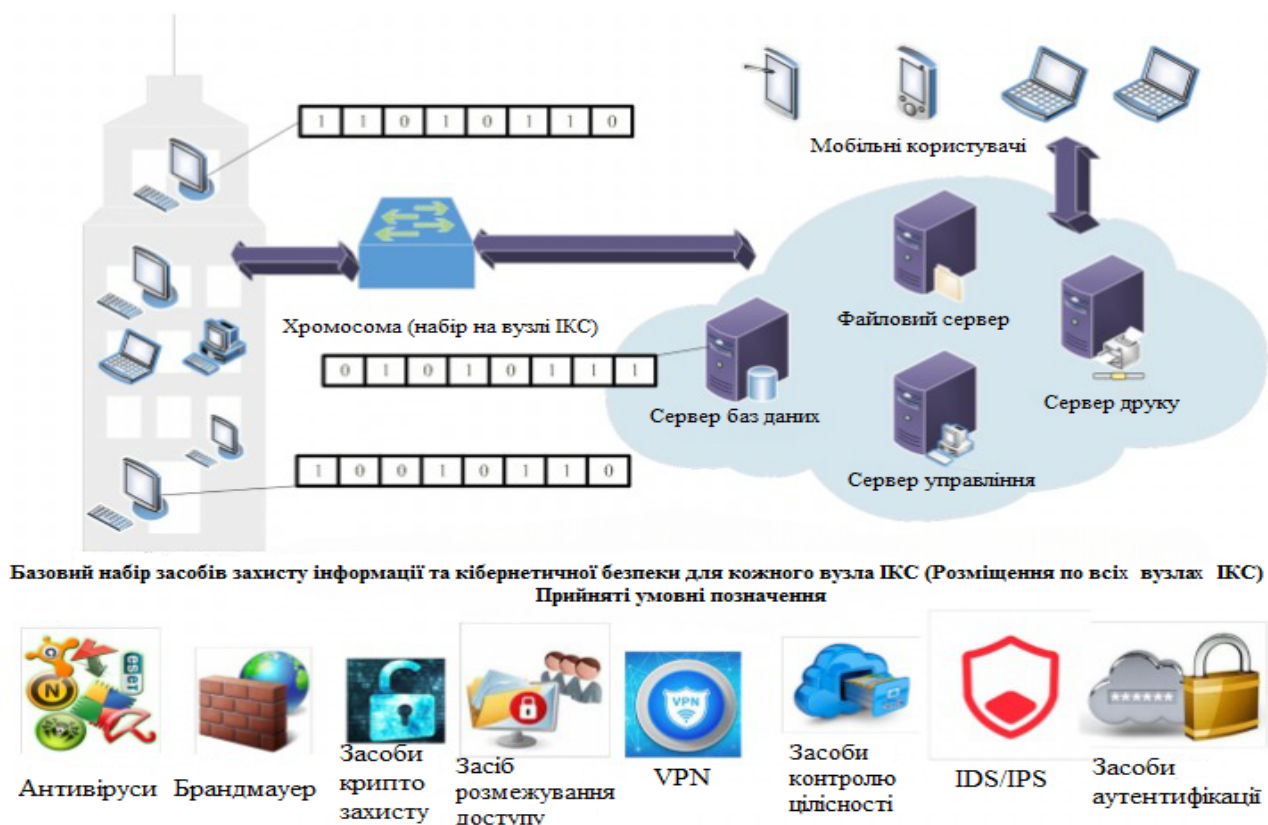


Рисунок 2.15 – Інфраструктура ІКС ОБІ з погляду забезпечення КБ

Зрозуміло, що для конкретної ІКС ОБІ список може бути доповнений через недостатність або скорочений через надмірність.

Залежно від специфіки бізнес-процесів, критичності інформаційних ресурсів на ОБІ, цей перелік може бути значно розширено, як внаслідок апаратно-програмних засобів захисту, наприклад, SIEM систем (що забезпечують процеси аналізу в реальному часі подій (тривог) ІБ і дозволяють реагувати на ці події до настання суттєвої шкоди), систем контролю роботи персоналу (що дозволяють відстежувати та аналізувати дії співробітників із метою запобігання витоку інсайдерської інформації) та ін., так і завдяки організаційним та іншим заходам, наприклад, проведення періодичних навчань із КБ.

Слід зазначити, що для багатьох компаній вартість вузла ІКС обмежена загальною вартістю ЗЗІ при максимізації їх ефективності (або для нашого випадку інтегральний показник (ІнП – *IND*) ЗЗІ).

Фітнес-функція в такій постановці задачі для кожної особи характеризуватиме ступінь «близькості» даної особи до вірогідного варіанту вирішення завдання. І, як результат цього, чим більше буде значення фітнес-функції, тим ближче рішення до максимуму.

Тоді фітнес-функцію для вузла (точка розміщення ЗЗІ для ІКС) можна подати так:

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^n w_i \cdot x_i, \quad (2.5)$$

де w_i – інтегральний показник (ІнП) конкретного ЗЗІ з класу, який характеризує так званий індекс якості або ступінь досяжності бажаних цілей для конкретного ЗЗІ [127].

Також ІнП можна трактувати як узагальнений показник якості найважливіших характеристик конкретного ЗЗІ.

У розробленому ГА в якості ІнП ЗЗІ прийнятий так званий індекс якості або ступінь досяжності бажаних цілей для конкретного ЗЗІ [127]. При цьому вважаємо, що ІнП обчислено як ступінь близькості параметрів ЗЗІ до ідеальних характеристик у просторі виділених приватних показників. Для розрахунку ІнП ЗЗІ, як правило, використовують таку залежність [127]:

$$IND_j = \sum_{i=1}^k \beta_i \cdot a_{ij}, \quad (2.6)$$

де β_i – вага критерію, що використовується для оцінки i -го ЗЗІ (наприклад, для фаєрволів можна використовувати такі критерії: тест фаєрволів на захист від внутрішніх атак; тест фаєрволів на захист від зовнішніх атак; тест персональних IDS/IPS на захист від атак на вразливі програми; наявність документації та ін.);

a_{ij} – ступінь досягнення заданого рівня захисту вузла для j -ого класу атак;

k – кількість класів ЗЗІ для конкретного типу вузла ІКС ОБІ.

Аналізуючи системи захисту інформації та окремі ЗЗІ, які розосереджені за відповідними контурами ОБІ, слід зазначити, що не всі об'єкти, що представляють для системи однакову цінність, і повинні підлягати однаконому ступеню захисту.

Тож робимо висновок, що ця обставина накладає свої особливості на розрахунок ІнП ЗЗІ в контексті застосування для частини розв'язання оптимізаційного завдання за допомогою ГА.

У процесі аналізу робимо висновок про те, що, дійсно, функціонування одних об'єктів, що розташовані в ІКС, дуже важливе для реалізації бізнес-процесів, наприклад, серверів БД, або сервера програм. Їх вихід із ладу негайно позначиться на всій ІКС ОБІ і, у крайньому разі, призведе до її відмови. Інші системи є менш важливими, їх ступінь впливу на працездатність усієї ІКС не такий великий. Наприклад, вихід з ладу звичайного ПК не призведе до повної зупинки бізнес-процесів. Хоча і для більш важливих, і для менш важливих вузлів ІКС необхідні свої засоби захисту, та їх перерозподіл, залежно від значущості та критичності розміщених на них інформаційних ресурсів, що теж грає не останню роль. У зв'язку з цим, розрахунок ІнП є складнішим завданням, ніж проста процедура узагальнення характеристик якості найважливіших параметрів конкретних ЗЗІ.

Отже, для того, щоб у межах нашого дослідження якісно описати ІнП, необхідно врахувати всі властивості вузла ОБІ, у якому цей засіб передбачається встановити, тобто проінвестувати фінансовий ресурс. Беззаперечно, у процесі вивчення мають бути враховані: критичність вузла; важливість даного вузла в ІКС; спосіб реалізації захисних заходів для вузла.

Підкреслюємо, що в цьому списку властивість «критичність» буде пріоритетною. Вона визначатиме ступінь впливу вузла на всю ІКС ОБІ.

Така властивість як «значущість» визначатиме ваги конкретних параметрів ЗЗІ на їх спільний ІнП. Відповідно до цього, властивість, поняття значимості у такому трактуванні якраз і визначає, які з функцій ЗЗІ є за спаданням більш значущими для вузла, а які менш значущими. Отже, згідно визначення

«значущості» ЗЗІ на вузлі слід розставляти їх функціональні характеристики за важливістю пріоритетів. Наприклад, у характеристиці ІнП для антивірусного ПЗ, найбільш значущим є показник виявлення шкідливого ПЗ, а періодичність оновлення антивірусних сигнатур 2 або 1 раз на день менш важлива.

Така властивість, як «реалізація захисних заходів для вузла» визначатиме наявність або відсутність поточних даних про стан відповідного параметра ЗЗІ.

Для того, щоб якісно оцінювати предмети (ЗЗІ) в наборі для вираження (2.6) неважливо, чи використовується точне значення β_i чи наближене. Це пов'язано з тим, що в параметрі β_i , насамперед, реалізується одностороння відповідність чисельної оцінки β_i та об'єкта. Беремо до уваги, що на практиці, у процесі оцінювання об'єктів часто роблять оцінку песимістичнішою, ніж у реальності. Таким чином, можна говорити, що при визначенні параметра β_i та значення інтегрального показника в цілому, краще застосовувати для оцінювання β_i інтервальні оцінки.

Вибираючи для ГА конкретні значення $\tau(\beta_i)$ (див. вираз 2.7), акцент робимо на формування вагових співвідношень між різними якісними оцінками предмета, що входить у набір. Зрозуміло, що зміна значень $\tau(\beta_i)$ у межах відповідного інтервалу посилить або навпаки послабить якісну оцінку предмета в наборі, а це буде означати, що і розмір інвестованих ФР у набір буде різним.

Із урахуванням вищесказаного, ІнП ЗЗІ можна розрахувати за допомогою наступних залежностей:

$$IND_j = \sum_{i=1}^k \tau(\beta_i) \cdot a_{ij}, \quad (2.7)$$

$$\text{де } \tau(\beta_i) = \begin{cases} \tau_1, \beta_i \in [b_{1_1}, b_{1_2}] \\ \tau_2, \beta_i \in [b_{2_1}, b_{2_2}] \\ \dots \\ \tau_j, \beta_i \in [b_{j_1}, b_{j_2}] \end{cases},$$

b_{j_l}, b_{j_n} – ліва та права межа шкали оцінювання предмета в наборі ЗЗІ на вузлі ІКС.

Таким чином, стало зрозумілим, що співвідношення (2.7) буде відповідати відтворенню множини чисельних еквівалентів, що характеризують якісні оцінки параметрів β_i на безлічі чисельних еквівалентів оцінок об'єкта.

Ця частина ГА була реалізована у вигляді консольної програми алгоритмічною мовою C#, див. рис. 2.16 та 2.17. Приклад коду наведено у додатку А.

Отже, основним завданням консольної програми була перевірка працездатності алгоритму.

ЗЗІ	ІнП	Вартість
Антивірус	15	10
ФВ	5	8
ЗКЗ	11	16
ЗРД	10	9
ЗА	10	4
ЗКЦ	9	9
ЗВВ	50	60
VPN	4	2

Задайте розмір популяції: █

Рисунок 2.16 – Вікно з переліком вихідних даних для відбору ЗЗІ та розміру інвестованих у КБ засобів для вузла ІКС за допомогою ГА

Повна програмна реалізація розробленого методу для вибору раціональної стратегії інвестування в проєкти із забезпечення кібербезпеки об'єкта інформатизації на основі комбінації теорії ігор та генетичного алгоритму буде описана у третій завершальній главі дисертаційної роботи.

```

d:\Programs\ConsoleApp1_GA_2020\ConsoleApp1_GA_2020\bin\Debug\netcoreapp3.1\ConsoleApp1_GA_2020.exe

---Хромосома 19 має 3,106508875739645 % шанс бути використаною
---Хромосома 20 має 2,0710059171597637 % шанс бути використаною
---Хромосома 21 має 10,798816568047338 % шанс бути використаною
---Хромосома 22 має 4,585798816568047 % шанс бути використаною
---Хромосома 23 має 0 % шанс бути використаною
---Хромосома 24 має 6,656804733727811 % шанс бути використаною
---Хромосома 25 має 7,2485207100591715 % шанс бути використаною

Хромосома 1 має найбільшу вірогідність
Selected Chromosomes / Parents

----- Покоління : 2-----

Хромосома 1:  1      0      0      0      0      1      1      1
Хромосома 21: 0      0      0      1      1      0      1      0

----- Покоління : 3-----

Батько 1:    1      0      0      0      0      1      1      1
Батько 2:    0      0      0      1      1      0      1      0
Нащадок 1:   1      0      0      0      0      1      1      1
Нащадок 2:   0      0      0      1      1      0      1      0

```

Рисунок 2.17 – Вікно з результатами моделювання процесу оптимізації відбору ЗЗІ та розміру інвестованих у КБ засобів для вузла ІКС за допомогою ГА

На рис. 2.18 показані витрати часу для вибору стратегій інвестування лише на підставі знаходження рішень за допомогою системи диференціальних рівнянь для білінійної динамічної гри якості з кількома термінальними поверхнями та для комбінованого підходу.

При комбінованому підході на першому етапі за допомогою системи диференціальних рівнянь для білінійної динамічної гри якості з кількома термінальними поверхнями збирається, фактично, лише статистика варіантів рішень. А безпосередньо обробка та пошук підсумкової раціональної стратегії інвестора знаходиться за допомогою ГА.

Комбінований підхід показує коротший час для пошуку рішень, зокрема, приблизно на 15-17%. Це пояснюється наступною обставиною.

Точки дають можливість визначення безлічі переваги першого інвестора в ІБ. Відбувається це в такий спосіб. Якщо використовувати тільки апарат білінійних динамічних ігор якості, то кожна точка, що відповідає стратегії інвестора, буде являти собою набори певних компонентів. Ці компоненти відповідають фінансовим ресурсам інвесторів. Набори точок, що

розташовуватимуться на термінальній поверхні кожного з інвесторів, характеризуватимуть вибір конкретних інвестиційних програм. Наприклад, це можуть бути програми з виявлення інцидентів ІБ, реагування на інциденти, прогнозування кібернетичних ризиків для ОБІ, мінімізації зв'язків між окремими об'єктами ЗІ та уніфікації компонентів контурів ЗІ для конкретного ОБІ, розробкою організаційних заходів щодо КБ ОБІ й т.д. Тобто, самі собі рішення на основі застосування системи диференціальних рівнянь для білінійної динамічної гри якості з декількома термінальними поверхнями дають досить великий розкид варіантів точок на термінальних поверхнях інвесторів. Але, слід зазначити, що потрібен додатковий час для аналізу цих точок та пошуку області переваги інвестора. На даному етапі застосування ГА істотно спрощує і мінімізує час пошуку таких точок, а значить і раціональної стратегії інвестора в цілому.

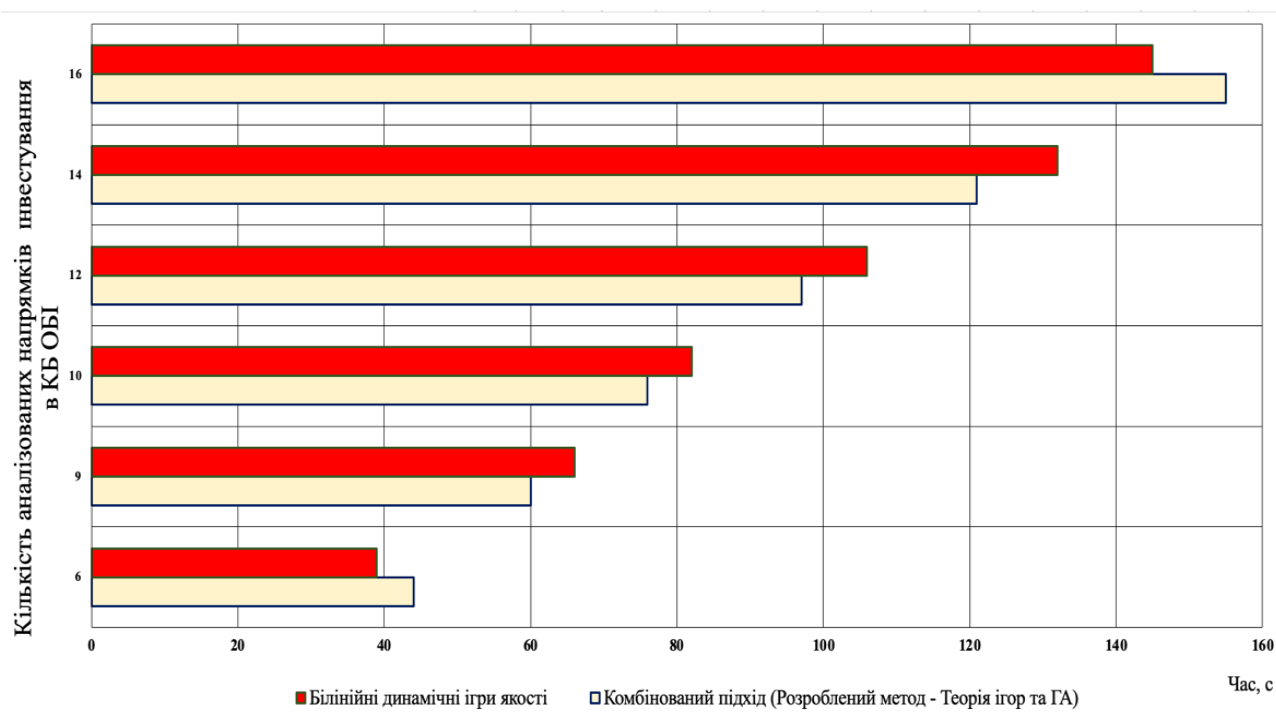


Рисунок 2.18 – Витрати часу на вибір стратегій інвестування

Отже, даний ГА застосовується для реалізації комбінованої обчислювальної процедури як додатковий інструмент зменшення невизначеності множини стабільних узагальнених ϵ - рівноваг гри.

ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ

У другому розділі дисертаційної роботи отримано такі основні результати.

Вперше описано метод вибору раціональної стратегії інвестування у проєкти із забезпечення кібербезпеки об'єкта інформатизації на основі комбінації теорії ігор та генетичного алгоритму, як методу багатофакторної оптимізації.

Показано, що використання на першому етапі даного методу лише апарату білінійних динамічних ігор якості, дає результат, у якому кожна точка, відповідна стратегії інвестора, буде набором певних компонентів інвестування. Ці компоненти відповідають ФР. 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.

Доведено, що застосування ГА на другому етапі запропонованого методу вибору раціональної стратегії інвестування у проєкти із забезпечення КБ ОБІ усуває зазначений вище недолік.

Запропоновано модифікований ГА та відповідна інформаційна технологія для опрацювання даних для вирішення завдання, пов'язаного з отриманням прогнозованої оцінки віддачі від різних напрямків інвестування у проєкти КБ ОБІ. Фактично доведено, що це дозволяє потенційним інвесторам на стадії оцінки привабливості окремих проєктів, пов'язаних із розвитком КБ ОБІ, отримувати прогнозовані оцінки перспективності обраних стратегій інвестування шляхом визначення значущих факторів зростання віддачі від інвестування в КБ ОБІ, а також відстеження точок зростання та структурних змін.

Виконана в другому розділі дисертації дослідницька робота та отримані результати дають можливість зробити висновок, що вивчений у цьому розділі метод може бути застосований для скорочення часу в ході розв'язання задачі пошуку раціональних (оптимальних) стратегій інвесторів на основі ігрових моделей у поєднанні з ГА, зокрема в умовах динамічного протистояння нападнику, коли оцінка раціональної стратегії інвестування виключно важлива для сторони захисту. Комбінований підхід показує коротший час для пошуку рішень. Приблизно на 15-17%.

РОЗДІЛ 3

РОЗРОБКА ПРОГРАМНОГО ПРОДУКТУ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ПРОЦЕСІ ІНВЕСТИВАННЯ В КІБЕРБЕЗПЕКУ ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ

3.1. Обґрунтування архітектури СППР у процесі прийняття рішень щодо вибору раціональної стратегії інвестування в КБ ОБІ

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 необхідні 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. 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 із урахуванням невизначеності в оцінках осіб, які приймають рішення, та формування їхніх переваг; синтез потенційних рішень, формування списку альтернатив; аналіз потенційних наслідків — все є основними цілями систем підтримки прийняття рішень та 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 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:

- 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.

Із точки зору обслуговування процесів, це дозволяє успішно виконувати загальні завдання інформаційного забезпечення бізнесу. Одними із них є:

- координація ІТ 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 є основою успішної роботи виробничого середовища. СППР – це інструмент, створений для допомоги менеджерам у виконанні їхніх завдань у динамічному сучасному світі. Вони (ці системи) 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. Як результат, на сьогодні лише деякі державні установи, підприємства чи приватні компанії, можуть із упевненістю говорити про те, що мають усю повноту інформації про стан справ у сфері КБ своїх об'єктів 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 із 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.

Зрозуміло, що аналіз і роз'яснення процесу прийняття рішень ОПР, ідентифікація обмежень, накладених на процес прийняття рішень, і вибір методів і обчислювальних процедур, які дозволять усунути такі обмеження, є основними

проблемами в проектування СППР. Зазвичай процес проектування СППР передбачає такі етапи:

- процес прийняття рішень розбивається на найпростіші етапи, а дії ОПР описуються під час їх виконання;
- вивчення окремої проблеми прийняття рішень і розробка ефективних систем підтримки прийняття рішень;
- явне визначення функцій системи, їх реалізація, перевірка (тестування) і забезпечення підтримки.

СППР покликана вирішити такі завдання [22]:

- створення бази знань даних та бази з різних ситуацій, пов'язаних із вибором стратегії інвестування в системи КБ, розробка програмного забезпечення ведення єдиного електронного архіву стратегій інвестування в КБ ОБІ з розмежуванням доступу користувачів;
- створення єдиного інформаційного простору у сфері обліку раціональних стратегій інвестування в системи КБ, забезпечення інформаційної взаємодії між підсистемами СППР шляхом внутрішньої стандартизації форматів даних та протоколів обміну;
- створення єдиної системи формування вихідної документації для вибору раціональних стратегій інвестування в системи КБ;
- ведення баз даних (БД) зразків та шаблонів документів, які необхідні ОПР;
- формування аналітичної інформації для прийняття рішень у графічному та друкованому вигляді;
- забезпечення системності, комплексності та узгодженості розвитку інформатизації інвестування в системи КБ з використанням традиційних форм та методів супроводу та контролю.

Основні функції СППР для програм інформаційної та кібернетичної безпеки зазвичай регламентують, виходячи з необхідності дотримання:

- принципів комплексного аналізу проблематики КБ;

- можливостей комбінування формальних та неформальних методів, що використовують у процесі підтримки прийняття рішень;
- принципів достовірності та актуальності інформації щодо поточного стану проблеми, при цьому зазвичай використовують різноманітні звіти, статистичні дані, аналітичні огляди, а також дані, що отримують від підсистем моніторингу.;
- принципів автоматизованого вибору методів та моделей для інтелектуалізації підтримки прийняття рішень;
- принципів подальшого розвитку станів СППР;
- принципів динамічного управління СППР із метою підвищення ефективності її функціонування та обґрунтованості одержуваних рекомендацій та висновків, які можуть бути використані особою, яка приймає рішення, у процесі вироблення керуючих впливів;
- потенціалу модулів аналізу, оперативного управління та контролю над вирішуванням завданням.

Слід зазначити, що для забезпечення повноцінного функціонування СППР повинна, як правило, містити наступні основні модулі і підсистеми, див. рис. 3.1:

- Модулі бази даних, бази знань, бази моделей та правил, що використовують для прийняття рішення.
- Систему управління інтерфейсом, що проєктується, зважаючи на архітектуру СППР – локальну або клієнт-серверну.
- Інші важливі модулі та підсистеми, необхідність яких обумовлена специфікою предметної області.

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

- експертна підтримка;
- автоматизоване виведення рішення;
- комбіноване рішення.

Зробити правильний вибір – це вибрати курс дій із доступних варіантів, який найбільш ефективно сприятиме досягненню мети.

Вибираючи альтернативи, потрібно зважити кілька конкурентних вимог, що вимагає їх оцінки за різними критеріями.

Під час використання СППР людина та комп'ютер залучаються до циклу під час процесу прийняття рішення людиною та машиною. Цикл складається з двох фаз: комп'ютерної фази аналізу та формулювання проблеми та комп'ютерної фази оптимізації (пошук рішення та застосування його якостей на практиці).

Системи підтримки рішень можуть бути розподілені та локальні. Система підтримки прийняття рішень, що розгорнута на одному комп'ютері, називається локальною. Ці системи менш складні, ніж розподілені, оскільки не виникає необхідність обміну інформацією.

Розподілені системи підтримки прийняття рішень можна розділити на основі функціональних можливостей або розташування. Локальні системи підтримки прийняття рішень розташовані у зв'язаних вузлах комп'ютерної мережі та здатні автономно вирішувати певні завдання. Ці системи і просторово, і функціонально розподілені. Лише шляхом об'єднання власних ресурсів і координації конкретних рішень вони можуть спільно розв'язати поставлену проблему.

Інструменти зберігання та аналізу даних складають два основних компоненти систем підтримки прийняття рішень. Сховище даних - це єдине середовище для зберігання даних. Кінцевий користувач, якому бракує спеціальних навичок інформаційних технологій, може переглядати та представляти дані за допомогою аналітичних інструментів.

При реалізації програмного коду моделей, описаних у другому розділі роботи, використана мова програмування C#. Тримання та налагодження виконуваного коду було реалізовано засобами MS Visual Studio 2022. Побудова графічного інтерфейсу користувача здійснювалася з використанням технології ADO.NET (ActiveX Data Object для NET).

У межах поточного розділу розглянемо детально лише блок-схему алгоритму функціонування експертної підсистеми для проектованої СППР, див. рис. 3.1

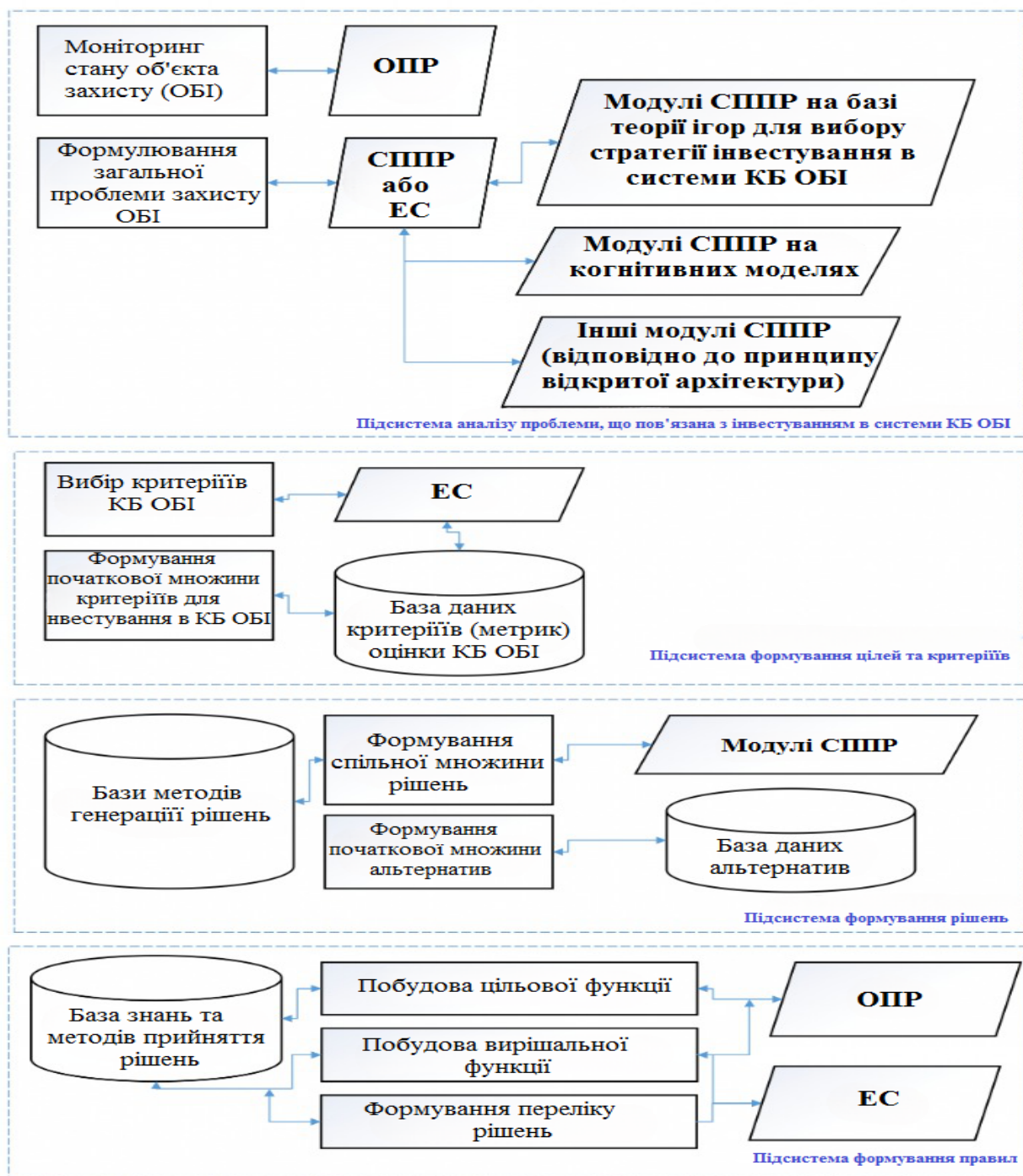


Рисунок 3.1 – Архітектура СППР в процесі прийняття рішень щодо вибору раціональної стратегії інвестування в КБ ОБІ

Взаємодія експертів із СППР реалізована через WEB інтерфейс, що дає можливість відразу кільком експертам працювати над пошуком розв'язання завдання. СППР, відповідно, розгорнуто на спеціальному сервері. Сайт для роботи експертів із СППР «DSS Protect&Invest» розроблено на ASP.NET Core MVC. Слід зазначити, що ASP.NET Core є кросплатформовим, високопродуктивним середовищем із відкритим вихідним кодом для створення сучасних хмарних додатків, підключених до Інтернету. Одним із відмінних моментів платформи ASP.NET Core є застосування патерну MVC. Фреймворк ASP.NET Core MVC працює поверх платформи ASP.NET Core, і призначений для того, щоб спростити створення програми.

3.2. Реалізація СППР у процесі прийняття рішень щодо вибору раціональної стратегії інвестування в КБ ОБІ

Важливо, що експертна підсистема забезпечує вироблення та оцінку можливих альтернатив інвестування в системи КБ ОБІ користувачем завдяки знанням, отриманим від фахівців-експертів.

Вказана розробка була виконана в IDE Visual Studio 2022 із встановленими компонентами, див. рис. 3.2:

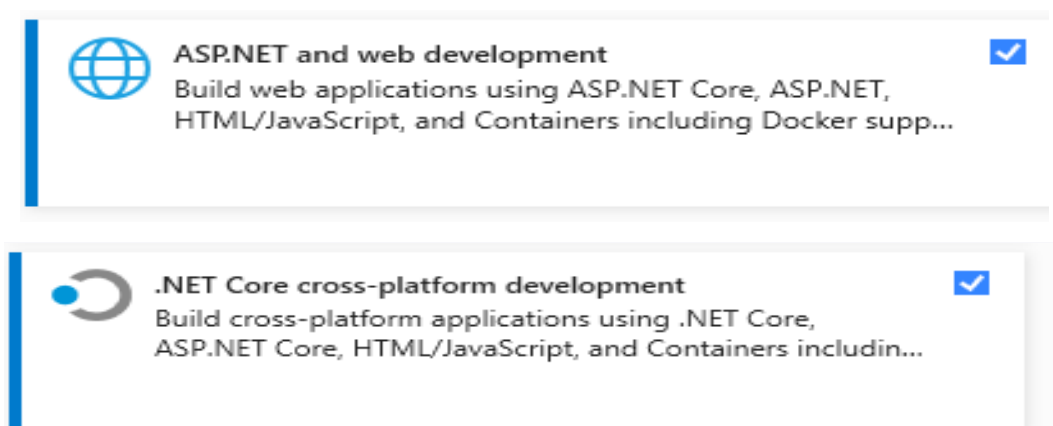


Рисунок 3.2 – Компоненти для роботи з СППР «DSS Protect&Invest»

Загальний вид форми для завдання вихідних даних у програмному продукті (ПП) «DSS Protect&Invest» наведено на рис. 3.3.

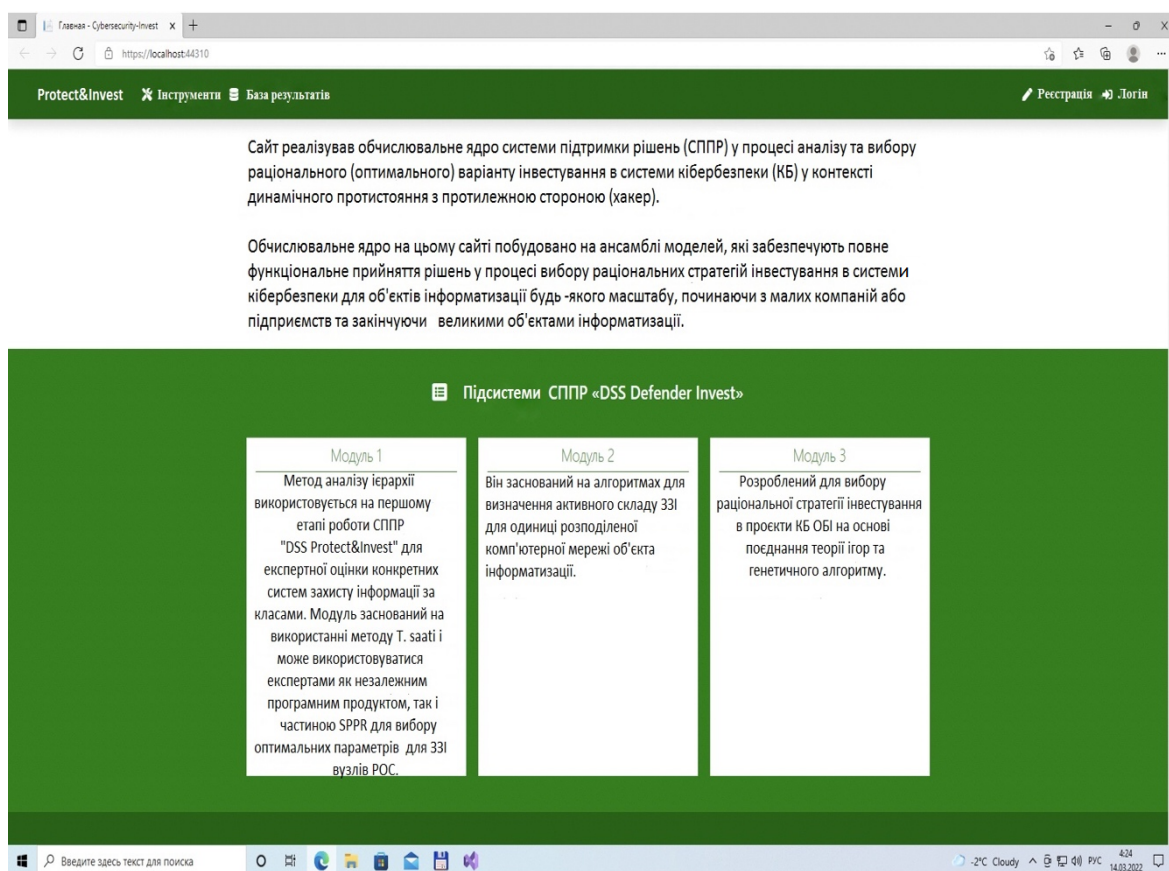
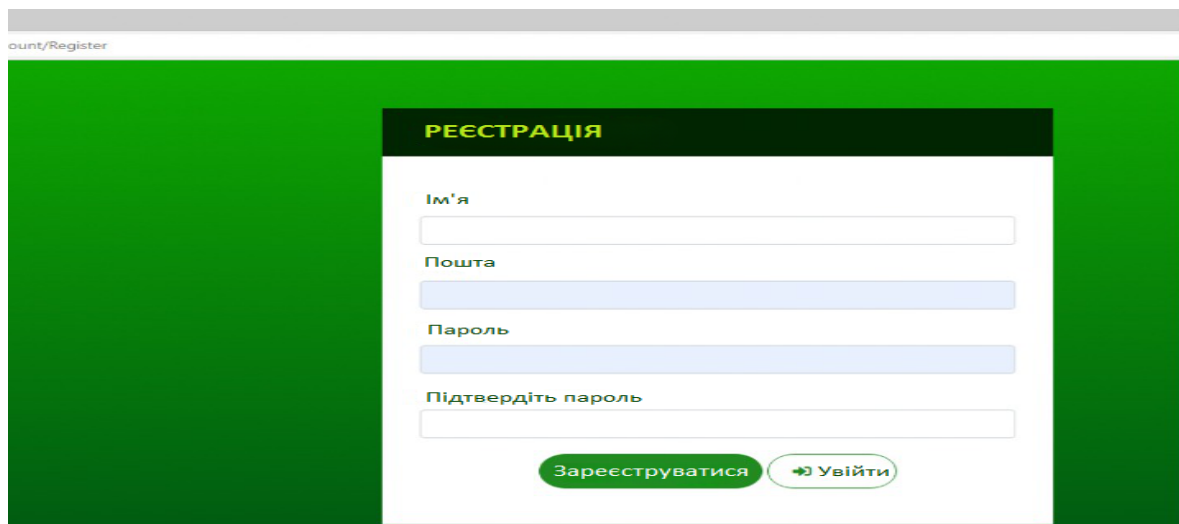


Рисунок 3.3 – Загальний вигляд «DSS Protect&Invest»

Реєстрація. Слід зазначити, що для того, щоб отримати доступ до функціоналу, наданого експертам на сайті «DSS Protect&Invest», необхідно створити обліковий запис та авторизуватися, див. рис. 3.4.

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

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



ount/Register

РЕЄСТРАЦІЯ

Ім'я

Пошта

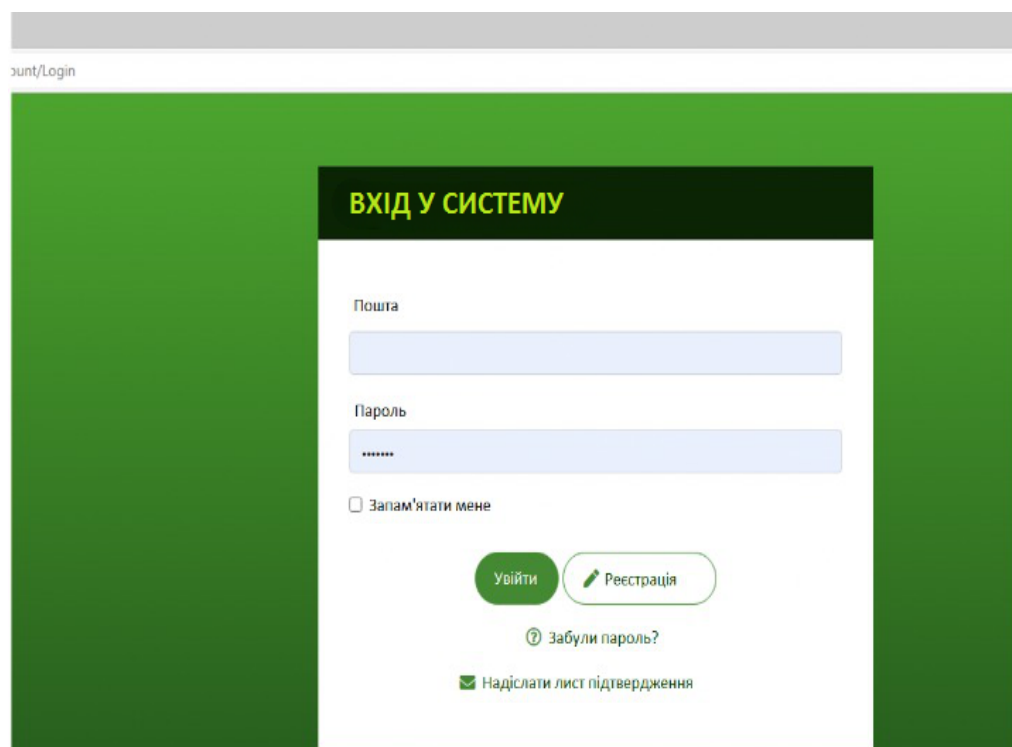
Пароль

Підтвердьте пароль

Зареєструватися Увійти

Рисунок 3.4 – Процедура реєстрації експертів на сайті СППР «DSS Protect&Invest»

Далі, після створення облікового запису необхідно авторизуватись, див. рис. 3.5.



ount/Login

ВХІД У СИСТЕМУ

Пошта

Пароль

☐ Запам'ятати мене

Увійти Реєстрація

Забули пароль?

☒ Надіслати лист підтвердження

Рисунок 3.5 – Вхід експерта до облікового запису СППР «DSS Protect&Invest»

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. 3.6.

На прикладі модуля 1 розглянемо роботу з реалізованим інструментарієм, див. рис. 3.6. Зазначений модуль заснований на класичному методі аналізу ієрархій (далі MAI) Т. Сааті [23, 131, 136]. MAI використовується на першому етапі роботи СППР «DSS Protect&Invest» для експертної оцінки конкретних систем захисту інформації за класами. Модуль створений 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 та 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. 3.6.

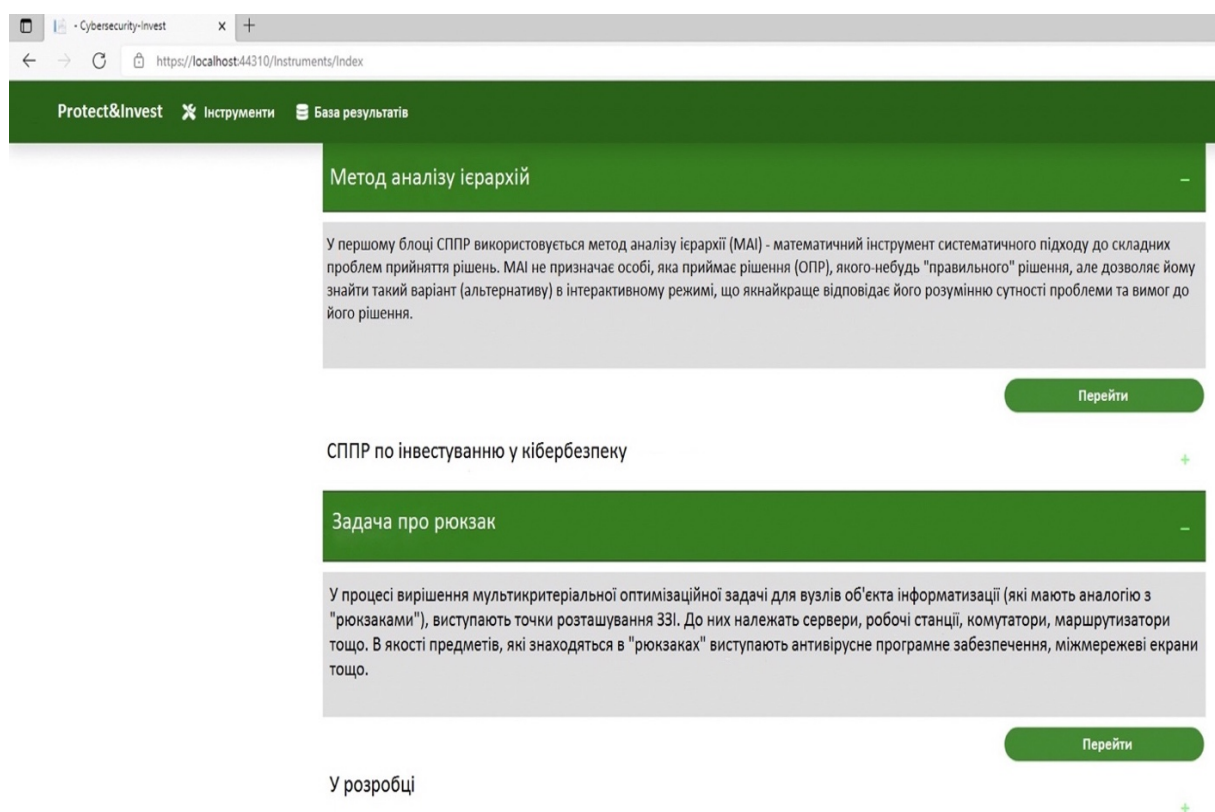


Рисунок 3.6 – Модулі СППР «DSS Protect&Invest»

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 дисертації, 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 моделей, 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 те, які моделі братимуть до уваги під час експерименту, а й безпосередньо порядок їх проведення.

Для планування обчислювальних експериментів першорядне значення приділяється:

- простоті повторення умов, за яких проводилися експерименти з запропонованими у роботі моделями;

- можливостям із управління експериментами з пропонованими математичними моделями, включаючи їх переривання та відновлення проведення;
- простоті при варіюванні умов проведення обчислювальних експериментів;
- наявності кореляцій між послідовностями точок під час моделювання;
- труднощам, які можуть супроводжувати визначення інтервалів моделювання.

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 їх 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 цілі і завдання 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 визначається 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 аналіз результатів попередніх досліджень або проведення невеликої кількості, як правило, несуттєвих випробувань.

До вибору кількості елементів слід підходити дуже обережно. Оскільки, 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 із їх первинними рівнями та діапазонами варіації.

Розглянемо основоположні ідеї теорії планування експерименту. Фактори - це змінні значення, які стосуються методів впливу на об'єкт дослідження і приймають певні значення в певний час. Нехай x та y — єдині дві змінні. Тоді x є фактором, а y є реакцією, при тому, що метою експерименту є дослідження впливу змінної x на змінну y . Екзогенні або контрольовані (вхідні) змінні використовуються для факторів у обчислювальних експериментах, тоді як ендегенні (вихідні) змінні використовуються для реакцій.

В експерименті кожен фактор x_i може мати одне з кількох значень, які називаються рівнями. Один із різних станів цієї системи визначається даним набором факторних рівнів. Цей набір також слугує представленням обставин, за яких може бути проведений один потенційний експеримент.

Кожна фіксована сукупність факторних рівнів відповідає певному положенню в багатовимірному (факторному) просторі. Для експериментів можна використовувати лише відповідну прийнятну область факторного простору.

Співвідношення, яке можна використати для демонстрації зв'язку між рівнями компонентів і реакцією системи, є чітко визначеним $y_l = \psi_l(x_1, x_2, \dots, x_k), l = \overline{1, m}$.

Поверхня реакції - це геометричне зображення, яке відповідає функції реакції, а функція реакції - це функція, яка зв'язує реакцію з факторами. Залежності, засновані на експериментальних даних, повинні бути налаштовані таким чином, щоб можна було побудувати математичну модель системи та оцінити її властивості з найменшими витратами обчислювального часу (наприклад, шляхом виконання найменшої кількості тестів).

Основні характеристики компонентів повинні бути встановлені перед проєктуванням випробувань. Під час проведення експериментів змінні можуть бути фіксованими та випадковими, спостережуваними та неспостережуваними, досліджуваними та невивченими.

Кожен компонент має діапазон значень, які він може приймати під час випробування, або рівні, і якщо рівні свідомо встановлюються експериментатором, фактор буде контрольованим. Необхідно вказати порядок дій, за допомогою яких встановлюються окремі рівні фактора, щоб його адекватно визначити. Це практичне визначення фактора гарантує чітке розуміння фактора.

Вибір експериментально-статистичної моделі та планування експерименту складають четвертий етап. На цьому етапі вибирається порядок майбутньої експериментально-статистичної моделі (лінійний, квадратичний тощо), виходячи з попередньої інформації про характер функцій відгуку та поставлене завдання. На основі кількості компонентів, які були обрані для перевірки, визначається категорія моделі. Кількість індивідуальних експериментів і рекомендації щодо їх проведення формуються на основі плану експерименту,

який вибирається залежно від обраного типу моделі. Існує також необхідність проведення такої ж кількості «паралельних експериментів».

Існує кілька способів опису машинного моделювання системи. Щоб вибрати певну модель, необхідно перерахувати такі якості, як достатність, значущість, простота тощо. Корисність моделі планування вимірюється її здатністю пояснювати широкий спектр уже встановлених фактів, відкривати нові та прогнозувати їх подальшу еволюцію. Однією з ключових переваг моделі планування є простота, яка проявляється в можливості проводити експеримент на ЕОМ, але, слід зазначити, що також існує конфлікт із вимогами достатності та значущості.

Виконання плану експерименту – п'ятий етап. На цьому етапі проводяться прямі експериментальні дослідження. Очевидно, що дослідження проводяться відповідно до вказівок, передбачених стратегією. Зі статистичної точки зору, під час проведення експериментів важливо дотримуватися принципу рандомізації. Ця теорія стверджує, що тести слід проводити не по порядку, зазначеному в плані, а скоріше у довільному порядку. Це особливо важливо для випадків одночасних експериментів. Принцип рандомізації допомагає запобігти систематичним помилкам під час проведення досліджень.

Шостим етапом є регресійний аналіз. Інша назва цього етапу – математична обробка результатів експерименту. Регресійний аналіз передбачає розв'язання наступних питань: визначення відтворюваності експериментів і виявлення серйозних помилок, допущених під час їх проведення, розрахунок числових оцінок коефіцієнтів експериментально-статистичної моделі, визначення значущості кожного компонента моделі — регресорів — і визначення придатності досліджуваної моделі для теми дослідження. Відповідні розділи цієї версії надають детальне пояснення кроків, пов'язаних із проведенням регресійного аналізу моделі, яка має специфічні характеристики на основі обраного плану експерименту.

Сьомий етап включає фактичну реалізацію мети дослідження, розв'язання питань, порушених на першому етапі, з використанням експериментальних статистичних моделей, які були побудовані.

На рис. 3.7 схематично зображено описані вище етапи.

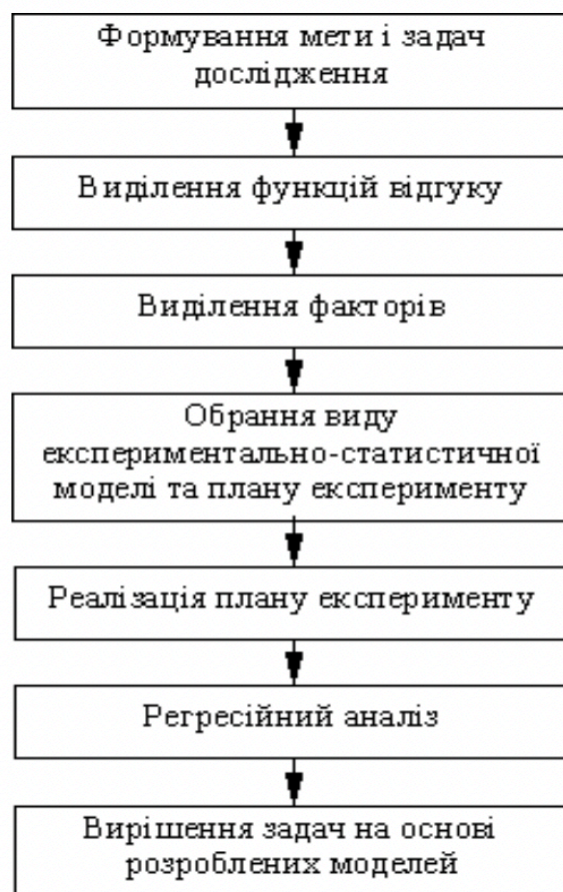


Рисунок 3.7 – План використання статистичного та експериментального моделювання для розв'язання проблеми.

Усі реалізовані моделі дотримуються загальної концепції – поділ екрана на дві функціональні області, див. рис. 3.8. Отже, тоді ліва частина дозволяє експерту працювати з СППР, а права частина призначена для пояснення одержуваних результатів.

Protect&Invest Інструменти База результатів Вийти

КРИТЕРІЇ

Кількість відомих вірусів

Евристичний аналіз

Робота на зараженій системі

Тести на колекціях вірусів

Додати Видалити

АЛЬТЕРНАТИВИ

AVG

ESET

Avast

Додати Видалити

Далі

Додайте необхідну кількість критеріїв та альтернатив.

2022 - Protect&Invest
Контакти: luba.pliska@gmail.com

а) – загальний вигляд модуля на основі застосування МАІ;

Protect&Invest Інструменти База результатів Вийти

КРИТЕРІЇ	КІЛЬКІСТЬ ВІДОМИХ ВІРУСІВ	ЕВРИСТИЧНИЙ АНАЛІЗ	РОБОТА НА ЗАРАЖЕНІЙ СИСТЕМІ	ТЕСТИ НА КОЛЕКЦІЯХ ВІРУСІВ
КІЛЬКІСТЬ ВІДОМИХ ВІРУСІВ	1	4	6	7
ЕВРИСТИЧНИЙ АНАЛІЗ	0,25	1	7	2
РОБОТА НА ЗАРАЖЕНІЙ СИСТЕМІ	0,167	0,143	1	4
ТЕСТИ НА КОЛЕКЦІЯХ ВІРУСІВ	0,143	0,5	0,25	1

Відмінити Проміжні результати Далі

Критерії МАІ або параметри, які важливі для особи, яка приймає рішення ОПР для прийняття "правильного" рішення.

Пріоритетами є числа, які пов'язані з вузлами ієрархії. Вони є відносними вагами елементів у кожній групі. Як і ймовірності, пріоритети - це безрозмірні значення, які можуть мати значення від нуля до одного. Чим більший пріоритет, тим важливішим є відповідний елемент. Сума пріоритетів елементів, підпорядкованих одному елементу, ієрархії вищого рівня, дорівнює одному. Пріоритет цілі за визначенням становить 1,0.

б) – заповнення матриці порівняння альтернатив

Рисунок 3.8 – Приклад модуля СППР «DSS Protect&Invest», використовуваного під час вибору антивірусного ПЗ

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.

Protect&Invest Інструменти База результатів

Курс 30

	ГРАВЕЦЬ 1	ГРАВЕЦЬ 2
Ресурси	25000	11000
Темп зростання	0.6	0.7
Погашення заборгованості	0.7	0.8
Відсоткова ставка	10	12
Ресурси, що повертаються	0.9	0.9

Прийняти

Рисунок 3.9 – Область для завдання вихідних даних експертами СППР «DSS Protect&Invest»

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

Вийти

Мета роботи - підвищити ефективність інтелектуальних систем підтримки прийняття рішень процесу фінансування у засоби інформаційної безпеки та кібербезпеки критично важливих комп'ютерних систем в умовах активної протидії атакуючій стороні.

Модель включає такі основні параметри (змінні):

- гравець 1 або інвестор №1 в технології кібербезпеки;
- гравець 2 або інвестор №2, що атакує (кіберзлочинці);
- фінансові ресурси гравців;
- коефіцієнт, який визначає промінь врівноваженості;
- термінальні поверхні для гравців;
- позитивний ортант;
- оптимальна стратегія гравців;
- стратегії гравців;
- величини фінансових ресурсів гравців;
- множини переважності гравців;
- темпи зростання фінансових ресурсів гравців при успішному впровадженні їх стратегій.

Рисунок 3.10 – Область підказок для роботи експертів із СППР «DSS Protect&Invest»

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

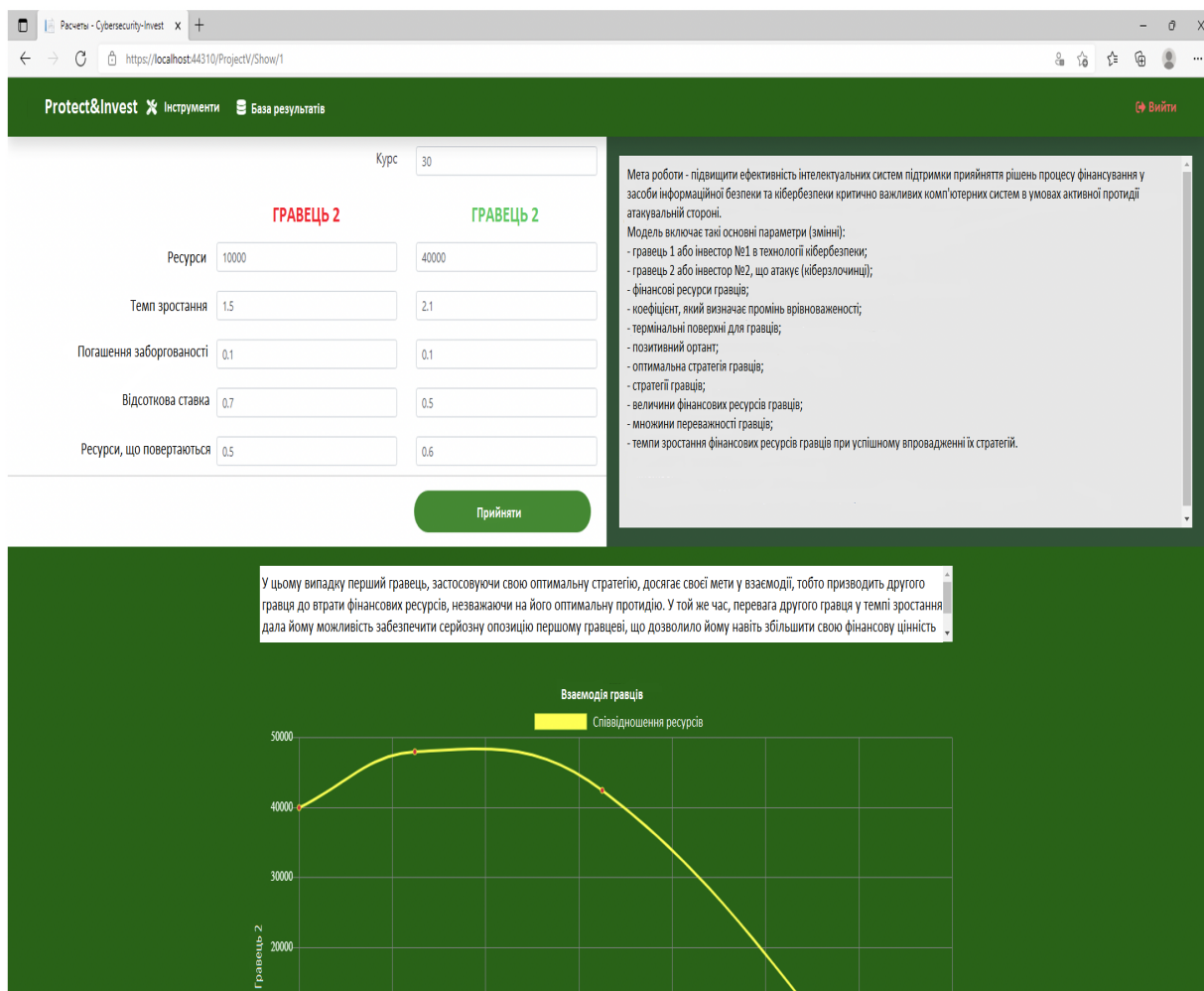


Рисунок 3.11 – Приклад тестування СППР «DSS Protect&Invest»

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

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

тому навіть наростити свою величину фінансового ресурсу на певному проміжку часу».

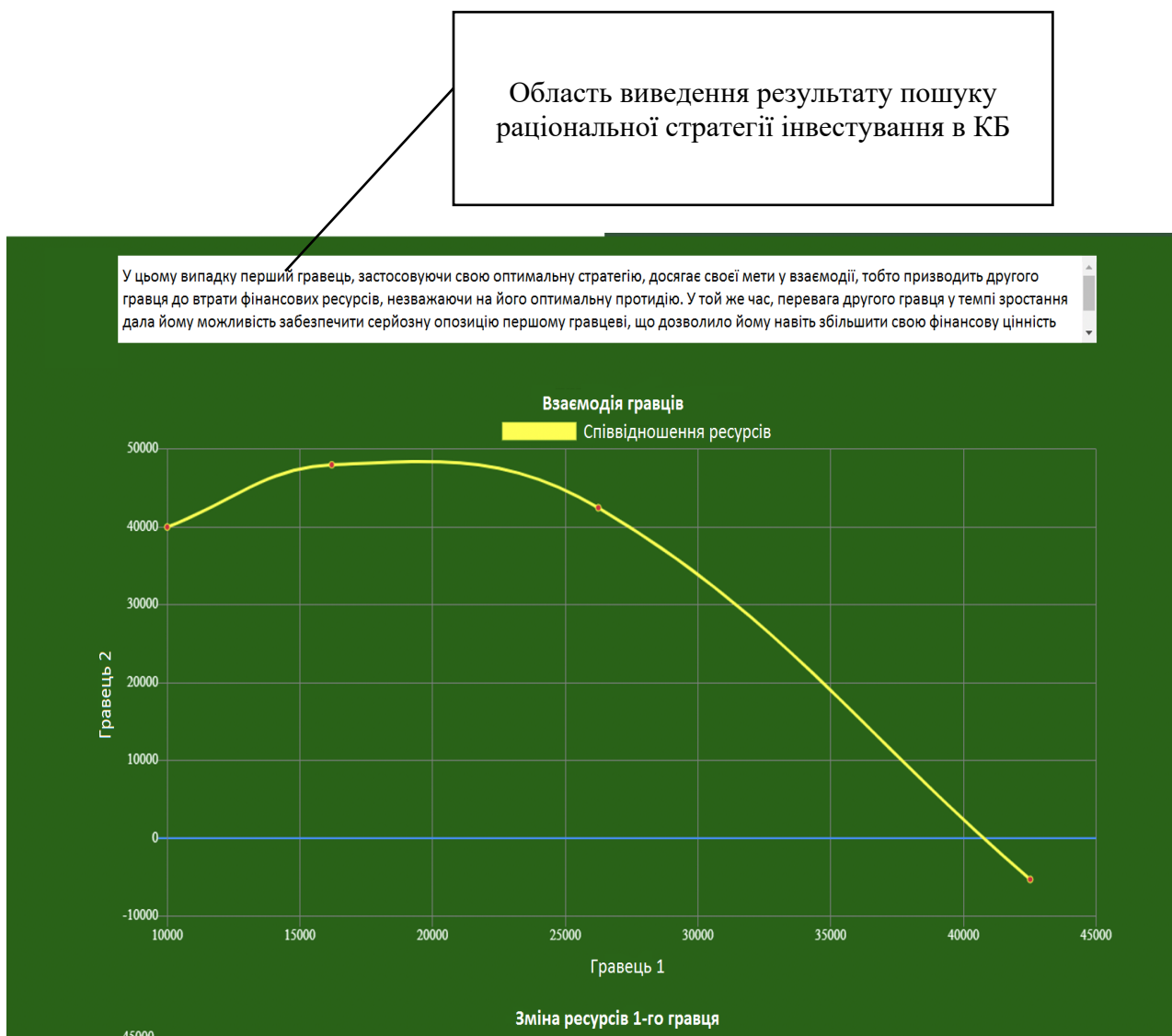


Рисунок 3.12 – Приклад візуалізації графіків після виконання розрахунків у
СППР «DSS Protect&Invest»

Як було зазначено в нашому дослідженні вище (див. розділ 2), необхідність залучення ГА на даному етапі методу вибору раціональної стратегії інвестування у проєкти із забезпечення КБ ОБІ обумовлена тим, що термінальну поверхню утворює безліч точок, відповідних до переваги інвестора. А це означає, що для того, щоб знайти раціональну стратегію, необхідно додатково досліджувати

інформацію, що стосується досить великої кількості можливих напрямів інвестування в засоби КБ ОБІ.

Кожен із цих напрямків, так само може бути розділений на піднапрямки, наприклад, при виборі конкретних апаратно-програмних ЗЗІ. Все це диктує необхідність підключити більш швидкодіючий 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.

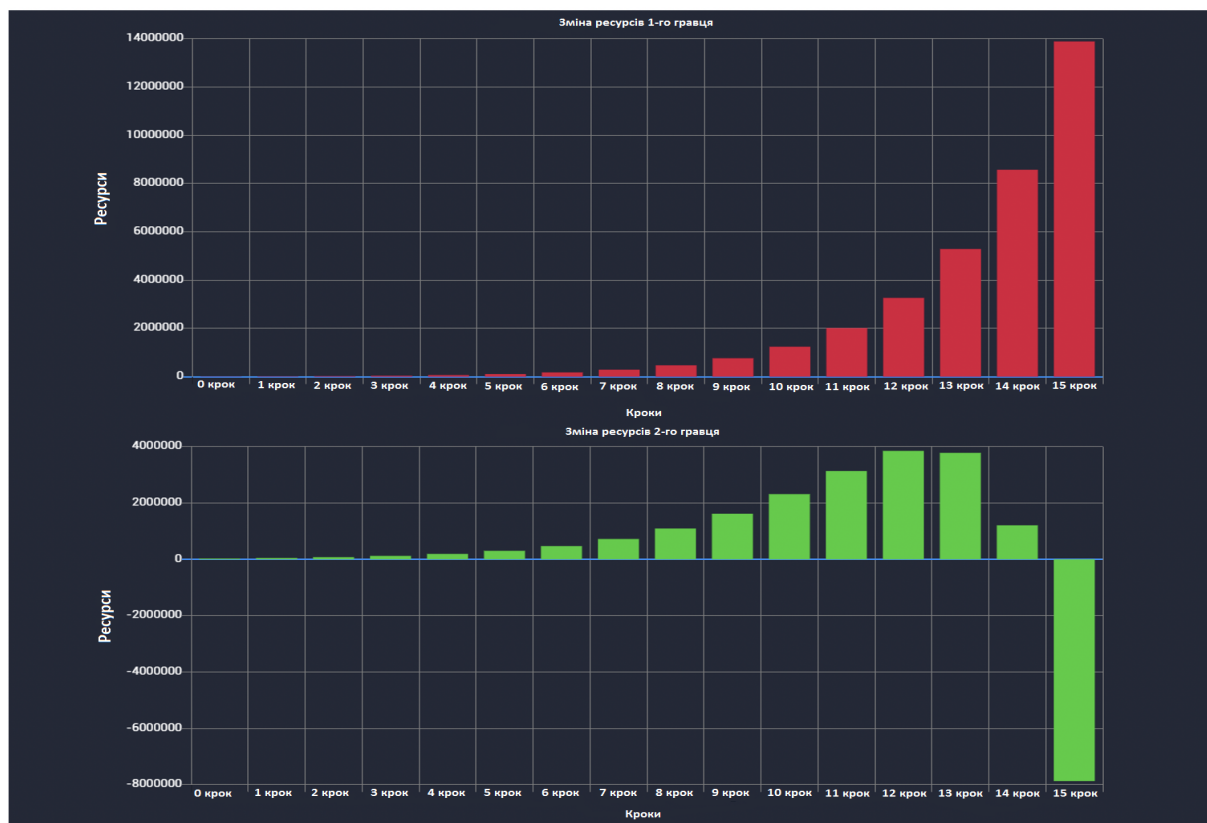


Рисунок 3.13 – Приклад візуалізації графіків після виконання розрахунків у СППР «DSS Protect&Invest» (гістограма).

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

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.

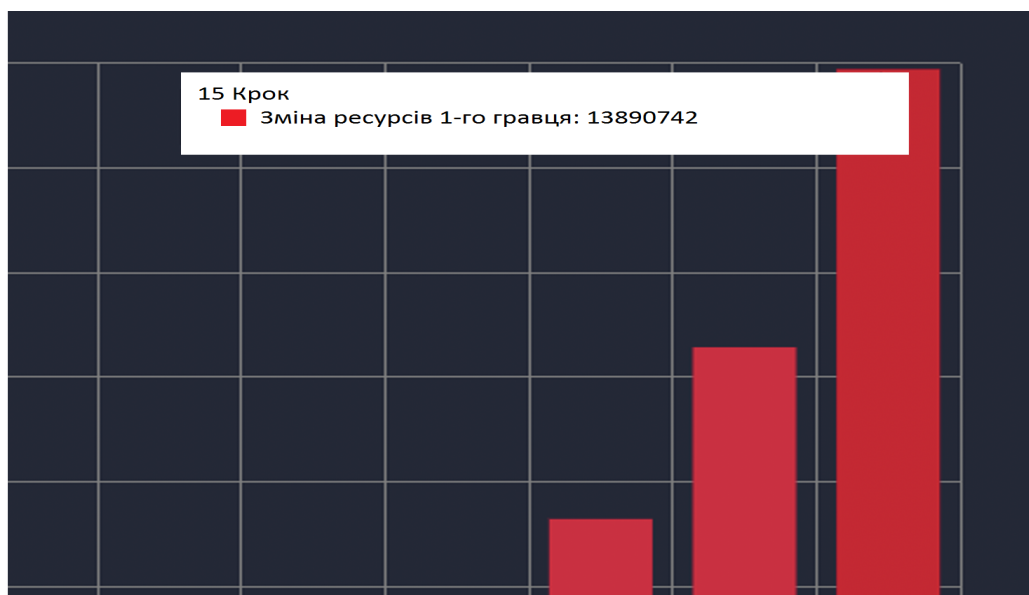


Рисунок 3.14 – Приклад візуалізації даних для розрахункової точки графіка в СППР «DSS Protect&Invest» (гістограма)

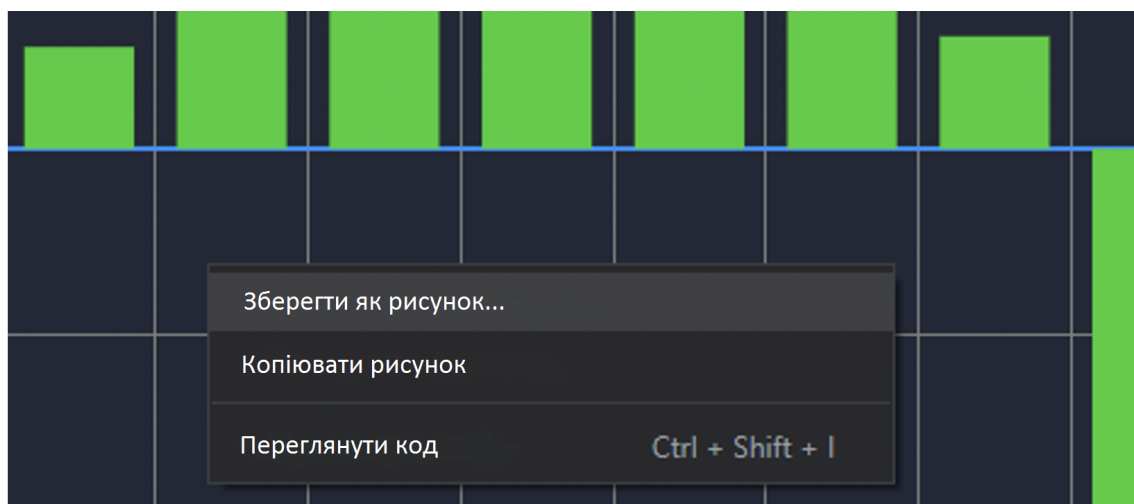


Рисунок 3.15 – Приклад збереження результатів графіка в СППР «DSS Protect&Invest» (гістограма)

Нижче показаний інтерфейс модуля СППР «DSS Protect&Invest» із 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).

НАЗВА	ВАРТІСТЬ	ПОКАЗНИК
Антивірусне ПЗ	10	12
Засіб криптографічного захисту	50	15
Засіб для резервування інформації	25	16
Фаєрвол	10	23
Система виявлення вторгнень	150	45
VPN	5	10

Максимальний інтегральний показник: 100

Додати Видалити Далі

2022 - Protect&Invest
Контакти: luba.plika@gmail.com

У процесі вирішення проблеми мультикритеріальної оптимізаційної задачі для вузлів об'єкта інформатизації (які мають аналогію з "рюкзаками") є точками розміщення ЗЗІ. Сюди входять сервери, робочі станції, комутатори, маршрутизатори тощо. У якості елементів, які знаходяться в "рюкзаках" можна зазначити антивірусне програмне забезпечення, міжмережеві екрани та інше. Тоді завдання з точки зору забезпечення КБ формулюється таким чином: необхідно розмістити якомога більше ЗЗІ у "рюкзаку". У цьому випадку необхідно: 1) забезпечити кращу ефективність елементів; 2) не перевищити задані обмеження, наприклад, щодо вартості "рюкзака".

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

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.

Protect&Invest Інструменти База результатів

НАЗВА ВАРТІСТЬ ПОКАЗНИК

НАЗВА	ВАРТІСТЬ	ПОКАЗНИК
Антивірусне ПЗ	10	5
Фаєрвол	5	5
Система виявлення вторгнень	50	15
VPN	2	1

Додати Видалити

Максимальний інтегральний показатель: 0

Далі

Формування наборів ЗЗІ та методів захисту для ОБІ

Антивірусне ПЗ	10	5
Фаєрвол	5	5
Система виявлення вторгнень	50	15

Знову Зберегти

©2022 - Protect&Invest
Контакт: luba.pliska@gmail.com

У процесі вирішення проблеми мультикритеріальної оптимізаційної задачі для вузлів об'єкта інформатизації (які мають аналогію з "рюкзаками") є точками розміщення ЗЗІ. Сюди входять сервери, робочі станції, комп'ютери, маршрутизатори тощо. У якості елементів, які знаходяться в "рюкзаках" можна зазначити антивірусне програмне забезпечення, міжмережові екрани та інше. Тоді завдання з точки зору забезпечення КБ формулюється таким чином: необхідно розмістити якомога більше ЗЗІ у "рюкзаку". У цьому випадку необхідно: 1) забезпечити кращу ефективність елементів; 2) не перевищити задані обмеження, наприклад, щодо вартості "рюкзака".

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

Із 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 «DSS Protect&Invest», крім табличного виведення результатів розрахунку, мають розвинену структуру візуалізації отриманих результатів у вигляді гістограм або графіків, що дає особі, яка приймає рішення, найбільш наочно уявити, які зміни засобів і систем захисту інформації дозволять стороні захисту побудувати ефективну багатоконтурну систему інформаційних ресурсів ОБІ.

Курс	Початкові ресурси 1-го гравця	Початкові ресурси 2-го гравця	Кінцеві ресурси 1-го гравця	Кінцеві ресурси 2-го гравця	Графік	Дата	Дія	Видалити
30	10000	40000	42515.29	-5270.6484	Есть	03/14/2022 04:53:25	Перейти	Видалити
25	25000	10000	48607.6	-833190	Есть	02/21/2022 13:04:36	Перейти	Видалити

Рисунок 3.18 – Фрагменти бази даних графіка СППР «DSS Protect&Invest»

Наприклад, на наступному рисунку, див. рис. 3.19, показано приклад візуалізації результатів роботи СППР «DSS Protect&Invest». Слід зазначити, що аналогічні засоби візуалізації результатів є і в інших модулях СППР «DSS Protect&Invest»

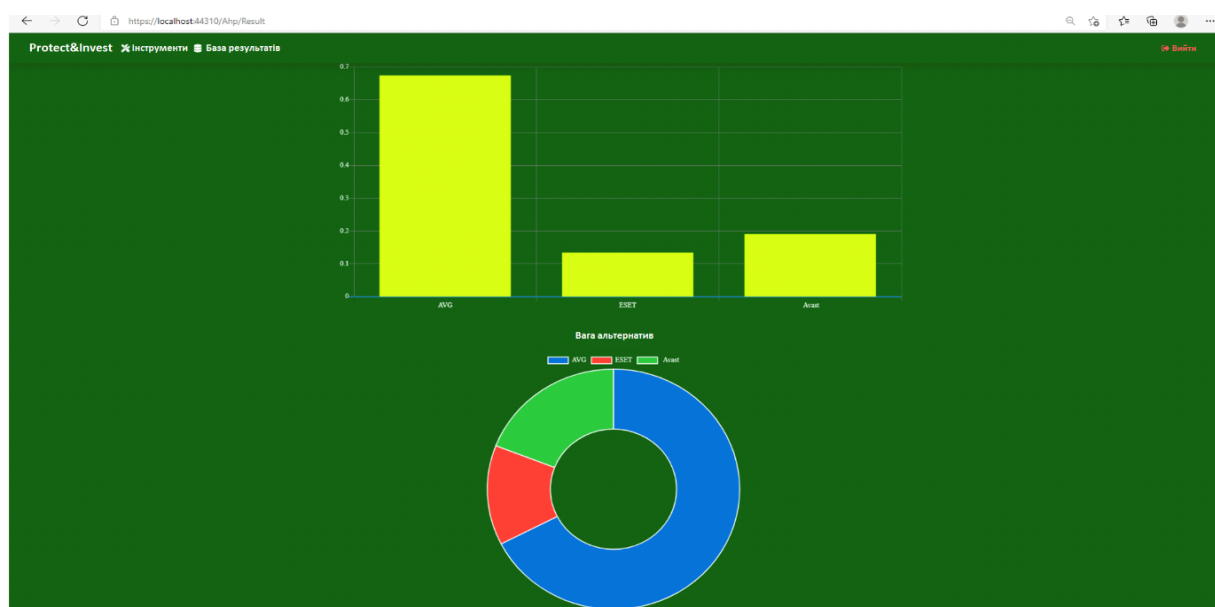


Рисунок 3.19 – Приклад візуалізації результатів вибору ЗЗІ для першого модуля СППР «DSS Protect&Invest»

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

У процесі перевірки СППР «DSS Protect&Invest» брали участь 7 експертів.

Вважається, що обсяг досвіду кожного експерта та розмір групи експертів впливають на те, наскільки надійними є їхні висновки.

Традиційно використовують декілька підходів до вибору експертів у галузі інформаційної безпеки: апріорні, апостеріорні та методи тестування.

До апріорних підходів відносять підходи оцінювання професійних навичок запрошеного фахівця не беручи до уваги результати його участі в попередніх експертизах. В першу чергу сюди можна віднести найпопулярніші техніки самооцінювання експертом своїх власних здібностей.

Апостеріорними методами називають процедури оцінювання характеристик експерта на основі знання результатів його участі в попередніх дослідженнях. Цей підхід передбачає оцінювання кваліфікації експерта за результатами його участі в попередніх опитуваннях.

Методики тестування передбачають проведення унікального тесту для оцінки кваліфікації експерта. Зазначені методи необхідні для виконання експертом заздалегідь підготовленої перевірки компетентності у заданій області. Проведення відповідних тестових процедур зумовлене насамперед необхідністю оцінки підготовленості експерта до участі в роботі експертної комісії. Вони також допомагають експертам зрозуміти зміст експертних процедур, у яких вони братимуть активну участь.

Було визначено критерії відбору експертів:

- ступінь об'єктивності та неупередженості експерта при аналізі та оцінці об'єктів у даній предметній галузі (незацікавленість експерта у прийнятті певного рішення (оцінки));
- рівень компетентності експерта у певній предметній галузі, показниками якого в сукупності є: рівень та профіль освіти; профіль роботи

(зв'язок із цією проблемною областю); досвід роботи з профілю (загальний стаж роботи з профілю та стаж роботи безпосередньо в даній предметній галузі);

- експерти не мають бути незнайомі один із одним, задля підвищення об'єктивності оцінювання запропонованого дослідження.

Для оцінки актуальності загроз витоку інформації було запрошено експертів із досвідом роботи в галузі захисту інформації та кібербезпеки не менше 5 років, які не мали зацікавленості у прийнятті певного рішення щодо розробленої системи.

У таблиці 3.1 наведено отримані дані під час проведення експерименту роботи експертів без розробленої СППР «DSS Protect&Invest» та з нею.

Таблиця 3.1

Результати проведення експерименту роботи експертів самостійно та за допомогою інтерфейсу СППР «DSS Protect&Invest»

СППР «DSS Protect&Invest»	Експерти
0,8	0,58
0,78	0,59
0,78	0,57
0,79	0,67
0,73	0,68
0,76	0,68
0,77	0,69

На рис. 3.20 та 3.21 показані порівняльні результати, отримані в ході опитування експертів та опрацювання, зроблених ними самостійно, та за допомогою, запропонованої СППР «DSS Protect&Invest».

Отже, на рис. 3.20 показані результати оцінювання експертами самостійно та за допомогою СППР «DSS Protect&Invest» 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 експертів самостійно (червоні стовпці) та за допомогою інтерфейсу СППР «DSS Protect&Invest» (сині стовпці). Еталонне значення параметрів (p), що

оцінюються, прийнято рівним 1. Якщо оцінка параметра дорівнює 0 – захист відсутній.

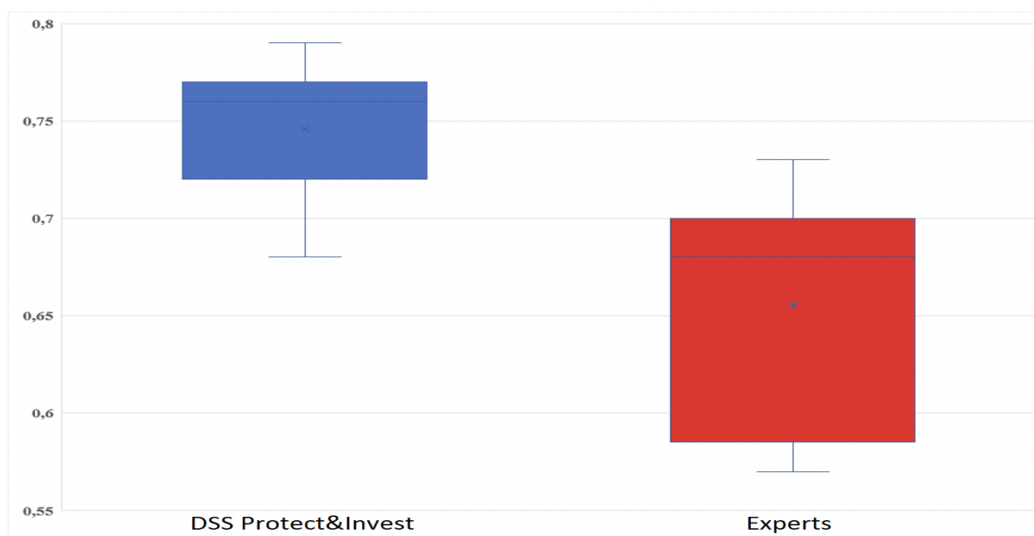


Рисунок 3.20 – Результати оцінювання експертами самотійно та за допомогою СППР «DSS Protect&Invest» ступеня захищеності ОБІ

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

Таблиця 3.2

Результати проведення експерименту порівняння часу (у хвилинах), що витрачається експертами самотійно та за допомогою інтерфейсу СППР «DSS Protect&Invest»

СППР «DSS Protect&Invest»	Експерти
9	25
12	39
16	38
16	36
10	32
11	34
12	34

На рис. 3.21. показана гістограма порівняння часу (у хвилинах), що витрачається експертами самотійно (червоні стовпці) та за допомогою

інтерфейсу СППР «DSS Protect&Invest» (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 хвиликах), за який вони впоралися з роботою самостійно та за допомогою запропонованої СППР «DSS Protect&Invest».

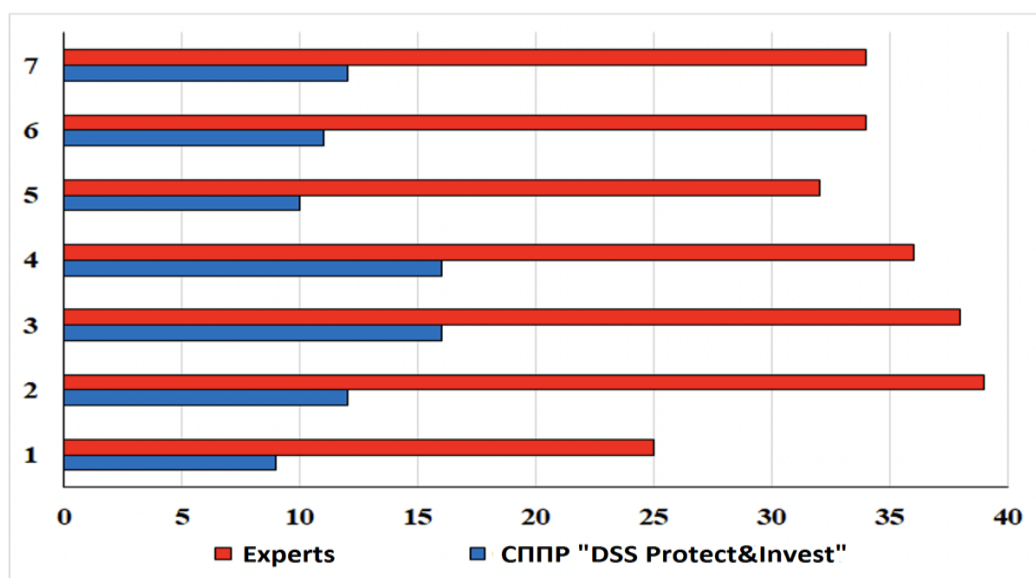


Рисунок 3.21 – Час, що витрачається експертами самостійно та за допомогою інтерфейсу СППР «DSS Protect&Invest» для вибору стратегії інвестування в КБ захисного вузла ОБІ

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

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

Отже, проаналізувавши вже існуючі математичні моделі стратегій інвестування для систем кібербезпеки та порівнявши їх із запропонованим

методом, у даній роботі можна зробити висновок, що заявлений метод переважає інші моделі по зазначених у таблиці 3.3 критеріях порівняння.

Таблиця 3.3

Порівняльна характеристика моделей стратегій інвестування в засоби захисту та загальну ІБ ОБІ, що розглядалися в роботі, та розробленого методу

	Математичні моделі стратегій інвестування для інформаційної безпеки						
Критерії порівняння	Модел ль Gordon -Loeb	Модел ь Woohy un Shim	Моде ль Архіп о- ва	Модел ь Левчен -ко- Прус	Модел ь Задира ки	Модель Малюко ва - Ахмето- ва- Лахно	Новий метод, запропо нований в роботі
Розрахунок оптимального рішення в динамічному режимі	-	-	+	+	-	+	+
Врахування вразливості об'єктів	-	-	+	+	-	-	+
Оптимізація розподілу ресурсів	+	+	-	+	-	+	+
Облік засобів захисту	+	+	+	+	+	-	+
Облік засобів нападу	-	-	+	+	-	-	+/-
Відмінність позитивних та негативних ефектів	-	+	-	-	-	-	+
Облік вартості кожного засобу захисту	-	-	+	-	-	-	+

Таким чином, порівняно з аналогічними рішеннями, розглянутими у [45, 13], ПЗ СППР «DSS Protect&Invest» має такі переваги:

- можлива інтеграція розробленого ПЗ в існуючі системи захисту інформації;
- покращується оперативність прийняття рішень у системах управління ІБ;
- можливе гнучке налаштування СППР «DSS Protect&Invest» під профілі КБ конкретного ОБІ (таблиця 3.4).

Таблиця 3.4

Опис переваг розробленого методу за запропонованими критеріями порівняння

Критерії порівняння	Новий метод, запропонований у роботі
Розрахунок оптимального рішення в динамічному режимі	Зокрема за допомогою СППР «DSS Protect& Invest»
Врахування вразливості об'єктів	Використовуючи метод аналізу ієрархій, який реалізовано у СППР
Оптимізація розподілу ресурсів	За допомогою ігрової моделі
Облік засобів захисту	За допомогою генетичного алгоритму
Облік засобів нападу	Можна враховувати витрати зловмисників на проведення атаки
Відмінність позитивних та негативних ефектів	З точки зору витрат на побудову ефективної системи захисту та мінімізації зайвих витрат та розв'язання завдання динамічного перерозподілу ресурсів сторони захисту
Облік вартості кожного засобу захисту	Ігрова модель + генетичний алгоритм

Фрагменти вихідного коду СППР «DSS Protect&Invest» наведено у додатку А.

ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ

У процесі роботи, під час написання третього розділу дисертації було зроблено такі висновки та отримано наступні результати.

Розроблено СППР «DSS Protect&Invest» у процесі аналізу та вибору раціонального (оптимального) варіанта стратегії інвестування в системи КБ. Розглянуто та досліджено ключові функціональні модулі подібної СППР, які сприяють забезпеченню безперервного та ефективного функціонування системи захисту інформаційних ресурсів ОБІ будь-якого масштабу.

Показано, що ця СППР дозволяє експертам у режимі онлайн оцінювати стратегії інвестування в різні об'єкти інформатизації, зокрема, критично важливі комп'ютерні системи (КВКС). СППР «DSS Protect&Invest» дозволяє реалізовувати оцінку привабливості інвестиційних проєктів у сфері захисту інформації та кібербезпеки підприємств. Обчислювальне ядро СППР «DSS Protect&Invest» базується на методах теорії ігор, а також на вперше отриманому математичному рішенні, яке засноване на інструментарії багатограних ігор якості з кількома термінальними поверхнями, причому, що дуже важливо, пошук траєкторії на безлічі точок, які формують термінальну поверхню інвестора вперше реалізований на основі ГА. СППР «DSS Protect&Invest» дозволяє автоматизувати в режимі онлайн отримання прогнозованих оцінок для різних варіантів розподілу фінансових ресурсів інвестора (інвесторів), що витрачаються на фінансування різних об'єктів контурів захисту інформації КВКС, адже розрахунок оптимального рішення відбувається в динамічному режимі. Розроблена СППР «DSS Protect&Invest» враховує вразливості об'єктів, відмінність позитивних та негативних ефектів, оптимізацію розподілу ресурсів, облік засобів захисту та нападу, а також їх вартість.

Слід зазначити, що реалізація СППР «DSS Protect&Invest» виконана за модульним принципом. А саме це дає можливість доповнювати СППР іншими модулями. Отже, запропонована СППР «DSS Protect&Invest» є досить універсальною і може бути розширена за рахунок функціоналу інших підзадач.

Все вищесказане підтверджує думку дослідників про те, що СППР «DSS Protect& Invest» 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 «DSS Protect&Invest», на 13–16 % менша, ніж для варіанта оцінювання без використання даного ПЗ. У ході тестування на СППР «DSS Protect&Invest» на 45–55 % скоротилися витрати часу на оцінювання стратегій інвестування в КБ ОБІ. Окрім того, можлива оптимізація стратегій вкладення коштів в ОБІ різними сторонами інвестиційного процесу.

ВИСНОВКИ

У ході написання дисертаційної роботи було детально вивчено теоретичну базу досліджуваної проблеми, виконано комплекс важливих досліджень та випробувань, у результаті яких науково обґрунтовано створення системи підтримки прийняття рішень DSS Protect&Invest. Основні наукові і практичні результати дисертаційної роботи полягають у наступному:

1. Показано, що в умовах нестійкої ринкової економіки процес інвестування в 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. Доведено, 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 проєктів у сфері захисту інформації та КБ.

2. Вперше запропоновано метод вибору раціональної стратегії інвестування в проєкти із забезпечення кібербезпеки (КБ) об'єкта інформатизації (ОБІ) на основі комбінації теорії ігор та генетичного алгоритму, як методу багатофакторної оптимізації. Показано, що використання на першому етапі даного методу тільки апарату білінійних динамічних ігор якості, дає результат, при якому кожна точка, що відповідає стратегії інвестора, буде набором певних компонентів інвестування. Ці компоненти відповідають ФР. Набори точок, що розташовуватимуться на термінальній поверхні кожного з інвесторів, характеризують конкретні інвестиційні програми. Самі собі рішення на основі застосування системи диференціальних рівнянь для білінійної динамічної гри якості з кількома термінальними поверхнями дають досить великий розкид варіантів точок на термінальних поверхнях інвесторів. Як наслідок, це диктує необхідність витрат додаткового часу для аналізу зазначених точок та пошуку області переваги інвестора. Показано, що застосування ГА на другому етапі

запропонованого методу вибору раціональної стратегії інвестування у проєкти із забезпечення КБ ОБІ усуває зазначений вище недолік.

3. Отримав подальший розвиток метод розв'язання багатокритеріальних задач по вибору методів та засобів забезпечення кібербезпеки на базі використання модифікованого генетичного алгоритму та відповідна інформаційна технологія опрацювання даних для розв'язання завдання, пов'язаного з отриманням прогностної оцінки віддачі від різних напрямків інвестування у проєкти КБ для ОБІ. Це дозволяє потенційним інвесторам на стадії оцінки привабливості окремих проєктів, пов'язаних із розвитком КБ ОБІ, отримувати прогностні оцінки перспективності обраних стратегій інвестування шляхом визначення значущих факторів зростання віддачі від інвестування в КБ ОБІ, а також відстеження точок зростання та структурних змін. Крім того, запропонований метод може бути застосований для скорочення часу в ході вирішення задачі пошуку раціональних (оптимальних) стратегій інвесторів на основі ігрових моделей у поєднанні з ГА, зокрема в умовах динамічного протистояння зі стороною, що атакує, коли оцінка раціональної стратегії інвестування виключно важлива для сторони захисту. Комбінований підхід показує коротший час для пошуку рішень, приблизно на 15-17%.

4. Отримала подальший розвиток методика проектування СППР, для розв'язання завдань оцінки стратегій інвестування у кібербезпеку об'єктів інформатизації. Розроблена СППР, на відміну від вже існуючих рішень, дозволяє експертам у режимі онлайн оцінювати стратегії інвестування в різні об'єкти інформатизації, у тому числі у критично важливі комп'ютерні системи (КВКС). Запропонована СППР дозволяє реалізовувати оцінку привабливості інвестиційних проєктів у сфері захисту інформації та кібербезпеки підприємств.

5. Було розроблена СППР «DSS Protect& Invest», обчислювальне ядро якої базується на комбінації методів теорії ігор, зокрема на інструментарії багатогранних ігор якості з кількома термінальними поверхнями та ГА. Зокрема, СППР «DSS Protect&Invest» дозволяє автоматизувати в режимі онлайн отримання прогностних оцінок для різних варіантів розподілу фінансових

ресурсів інвестора (інвесторів), що витрачаються на фінансування систем КБ ОБІ. Показано, що СППР «DSS Protect& Invest» 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 «DSS Protect&Invest», на 13–16 % менша, ніж для варіанта оцінювання без використання даного ПЗ. У ході тестування на СППР «DSS Protect&Invest» 45–55 % скоротилися витрати часу на оцінювання стратегій інвестування в КБ ОБІ. Окрім всього зазначеного вище також можлива оптимізація стратегій вкладення коштів в ОБІ різними сторонами інвестиційного процесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 15 найбільших венчурних угод на ринку кібербезпеки 2021 року [Електронний ресурс] // AIN.UA. – Режим доступу: <https://ain.ua/ru/2021/09/15/15-najbilshih-venchurnih-ugod-na-rinku-kiberbezpeki-2021-roku/>
2. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій: Науковий вісник НЛТУ України. – 2008, вип. 18.9. С. 270.
3. Архипов О. Є. Застосування онтологічних ієрархій у задачах визначення цінності інформації [Електронний ресурс] / О. Є. Архипов, М. А. Петренко // Ukrainian Information Security Research Journal. – 2012. – Т. 14, № 1 (54). – Режим доступу: <https://doi.org/10.18372/2410-7840.14.2061>
4. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ : НІСД, 2012. 96 с.
5. Браїловський М.М. Технології захисту інформації / М.М. Браїловський, С.В. Зибін, І.В. Піскун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.
6. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К.: ТОВ «СІК ГРУП Україна», 2015. – 449 с.
7. 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.
8. Герасименко О.В. Інформаційна безпека підприємства: поняття та методи її забезпечення / 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/>

9. Григоревська О. О. Захист облікової інформації в умовах забезпечення кібербезпеки підприємства [Електронний ресурс] : thesis / Григоревська Олена Олександрівна. – [Б. м.], 2020. – Режим доступу: <https://er.knutd.edu.ua/handle/123456789/17377>

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

11. 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.

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

13. Гульков М., Толкачов В. Технічний захист інформації, як складова інформаційної безпеки, у контексті євроатлантичної інтеграції України //Сучасні інформаційні технології у сфері безпеки та оборони. – 2019. – Т. 36. – №. 3. – С. 59-64.

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

15. 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.

16. 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.

17. Джеймс Л. Фішинг. Техніка комп'ютерних злочинів. М. : НТ Пресс, 2008. 320 с.

18. Довбиш А.С. Основи проектування інтелектуальних систем : Навч. посіб. / А.С. Довбиш. – Суми : СумДУ, 2009. – 170 с.
19. Досенко С. Д. Технічний захист інформації. Основні проблеми та способи їх вирішення. 2021. – № 27. – С. 27–32.
20. Журиленко, Б. - 2012. - Математична модель вірогідної надійності комплексу технічного захисту інформації. Безпека інформації, (2), 61-65.
21. Журиленко, Б., Ніколаєва, Н., & Пелих, Н. - 2011. - Оптимальні фінансові витрати і основні критерії побудови або модернізації комплексу технічного захисту інформації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 33-43.
22. Зибін, С. В. - 2017. - Підсистеми і модулі системи підтримки прийняття рішень. Алгоритми функціонування. Телекомунікаційні та інформаційні технології, (4), 58-70.
23. Карпинский Н.П., Корченко А.А., Ахметова С. Т. Метод формування базових детекційних правил для систем виявлення вторгнень // Захист інформації. 2015. Том 17, № 4. С. 312–324.
24. Катрич Д. В. Захист інформації в ERP-системі підприємства [Електронний ресурс] / Дмитро Вікторович Катрич, Володимир Михайлович Бурлаков // Адаптивні системи автоматичного управління. – 2017. – Т. 2, № 31. – С. 17–25. – Режим доступу: <https://doi.org/10.20535/1560-8956.31.2017.128054>
25. 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.
26. 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.
27. 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.

28. 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.

29. Л.Д. Плиска, В.А. Лахно. Методи, моделі та інформаційні технології в СППР 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. Мехед Д. Б. Захист інформації на підприємстві / Д. Б. Мехед // Вісник Чернігівського державного технологічного університету. Серія "Технічні науки". – 2014. – № 2 (73). – С. 143–148.

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

37. Норткат С. Аналіз типових порушень безпеки в мережах. М. : «Вільямс», 2006. 424 с.

38. Рогов П. Д., Малахов М. А., Бухало Л. В. Методика визначення рівнів загроз інформаційній безпеці держави у війсьній сфері // Збірник наукових праць Військового інституту КНУ імені Тараса Шевченка. 2013. № 39. С.143–147.

39. 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

40. Сотниченко В. М. Інформаційна безпека як базова складова економічної безпеки телекомунікаційного підприємства / В. М. Сотниченко // Економіка. Менеджмент. Бізнес. – 2017. – № 1 (19). – С. 58–66.

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. [та ін.] Віддалені атаки в розподілених комп'ютерних мережах та internet [Електронний ресурс] // Ukrainian Information Security Research Journal. – 2023. – Т. 24, № 3. – С. 136–143. – Режим доступу: <https://doi.org/10.18372/2410-7840.24.17265>

44. Хорошко В.А. [та ін.]. Методи та засоби захисту інформації. Київ : Юніор, 2003. 504 с.

45. Чубаєвський В. [та ін.]. Застосування СППР у завданнях організаційно-економічного забезпечення захисту інформації // *Information technology and society*. – 2022. – № 2 (4). – С. 107–116. – Режим доступу: <https://doi.org/10.32689/maup.it.2022.2.14>

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

47. 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.

48. 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>

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

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

51. 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.

52. A. Fielder, E. Panaousis, P. Malacaria et al. Game theory meets information security management, in *Proceedings of the IFIP International Information Security Conference, Marrakech, Morocco, 2–4 June 2014*, Berlin, Springer, pp. 15–29.

53. 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. – T. 78. – C. 436-444. (2016) DOI <https://doi.org/10.1016/j.ijepes.2015.11.041>

54. 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.

55. 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. – C. 162-171. (2018) DOI https://doi.org/10.1007/978-3-030-00184-1_15

56. 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. – C. 162-171. (2018) DOI: 10.1007 / 978-3-030-00184-1_15

57. 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.

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

59. Arhypov O.Y. Informacijni ryzyky: metody ta sposoby doslidzhennja, modeli ryzykiv I metody ih identyfikacii / A.Y. Arhypov, A.V. Skyba // Zahyst informacii. – 2013. – №4. – pp.366-375.

60. Arkhypov O. Y. Methods and Approaches to Investigating Information Risks by Means of Economic Cost Models/O. Arkhypov, A. Skyba// The Advanced Science Journal. – 2014. – №2(12). – pp.75-82.

61. B. B. Akhmetov, V. A. Lakhno, A. B. Adranova, L. M. Kydyralina, L. D. Pliska. Analysis of mathematical models of investment strategies in the university on cyber security systems / *Bulletin of national academy of sciences of the republic of Kazakhstan*, 2020. Volume 1, Number 383 (2020), 128 – 139.

62. Bergström E., Lundgren M., Ericson Å. M. Revisiting information security

risk management challenges: a practice perspective //Information and Computer Security. – 2019. – T. 27. – №. 3. – C. 358-372. (2019) DOI <https://doi.org/10.1108/ICS-09-2018-0106>

63. Berruga L. Council Post: Investing In Cybersecurity Amid Rising Digital Threats [Electronic resource] / Luis Berruga // Forbes. – Mode of access: <https://www.forbes.com/sites/forbesfinancecouncil/2022/05/31/investing-in-cybersecurity-amid-rising-digital-threats/?sh=6e3fc30185b9>.

64. Chapaliuk B. Review of SemiSupervised Learning Methods for Medical Computer-Aided Diagnosis Systems. // B. Chapaliuk, Y. Zaychenko// In 2020 IEEE 2nd International Conference on System Analysis & Intelligent Computing (SAIC), pages 1–4. IEEE, 2020. [Chen et al., 2020] Alvin I Chen, Max

65. Chhetri S. R. et al. Security trends and advances in manufacturing systems in the era of industry 4.0 // 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). – IEEE, 2017. – C. 1039-1046. (2017) DOI: 10.1109 / ICCAD.2017.8203896

66. Chinh H. N., Hanh T., Dinh N. T. Fast detection of DDOS attacks using non-adaptive group testing // International Journal of Network Security & Its Applications (IJNSA). 2013. Vol.5, № 5. P. 63–71.

67. Choo, K. K. R., Gai, K., Chiaraviglio, L., & Yang, Q. (2021). A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. Computers & Security, 102, 102136.

68. Chronopoulos, M., Panaousis, E., & Grossklags, J. - 2017. - An options approach to cybersecurity investment. IEEE Access, 6, 12175-12186.

69. Cui M., Wang J., Yue M. Machine learning-based anomaly detection for load forecasting under cyberattacks //IEEE Transactions on Smart Grid. – 2019. – T. 10. – №. 5. – C. 5724-5734. (2019) DOI: 10.1109/tsg.2018.2890809

70. Dhunny, A. Z., Timmons, D. S., Allam, Z., Lollchund, M. R., & Cunden, T. S. M. (2020). An economic assessment of near-shore wind farm development using a weather research forecast-based genetic algorithm model. Energy, 201, 117541.

71. Diesch R., Pfaff M., Krcmar H. A comprehensive model of information security factors for decision-makers //Computers & Security. – 2020. – T. 92. – C. 101747. (2020) DOI <https://doi.org/10.1016/j.cose.2020.101747>

72. Dor D., Elovici Y. A model of the information security investment decision-making process //Computers & security. – 2016. – T. 63. – C. 1-13. (2016) DOI: 10.1016 / j.cos.2016.09.006

73. Fazlida M. R., Said J. Information security: Risk, governance and implementation setback //Procedia Economics and Finance. – 2015. – T. 28. – C. 243-248. (2015) DOI [https://doi.org/10.1016/S2212-5671\(15\)01106-5](https://doi.org/10.1016/S2212-5671(15)01106-5)

74. Filimonova L. A., Skvortsova N. K. On issue of algorithm forming for assessing investment attractiveness of region through its technospheric security //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2017. – T. 262. – №. 1. – C. 012196. (2017) DOI:10.1088/1757-899X/262/1/012196

75. Fu Y., Zhu J., Gao S. CPS information security risk evaluation system based on Petri net // 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC). – IEEE, 2017. – C. 541-548. – 2017. - DOI: 10.1109 / DSC.2017.65

76. Gordon L. A. et al. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities //Journal of Accounting and Public Policy. – 2006. – T. 25. – №. 5. – C. 503-530. (2006) DOI <https://doi.org/10.1016/j.jaccpubpol.2006.07.005>

77. Gordon L. A., Loeb M. P., Lucyshyn W. Sharing information on computer systems security: An economic analysis //Journal of Accounting and Public Policy. – 2003. – T. 22. – №. 6. – C. 461-485. – 2003. - DOI <https://doi.org/10.1016/j.jaccpubpol.2003.09.001>

78. Gordon L. The Economics of Information Security Investment / L. Gordon, M. Loeb // ACM Transactions on Information and System Security. – Nov. 2002. – Vol. 5. – №4. – pp.438-457.

79. Gordon, L.A., and Loeb, M.P. and Lucyshyn, W. And Zhou, L. Externalities and the Magnitude of Cyber Security Under investment by Private Sector Firms: A

Modification of the Gordon-Loeb Model // Journal of Information Security, 2015, vol. 6, pp.24-30.

80. Govindarajan M., Chandrasekaran R. M. Intrusion Detection Using an Ensemble of Classification Methods // World Congress on Engineering and Computer Science. 2012. Vol. 1. P. 459–464.

81. Granneman, J. – 2018. - The business guide to improving information security. The Journal of Equipment Lease Financing (Online), 36(3), 1-9.

82. Gryshuk R.V. Hierarchical differential-gaming model for evaluation efficiency of information systems protection/ R.V. Gryshuk// Informatics & Mathematical Methods in Simulation. - 2011. - №2.

83. Gyanchandani M., Rana J.L., Yadav R.N. Taxonomy of anomaly based intrusion detection system: a review // International Journal of Scientific and Research Publications. 2012. Vol. 2, Iss. 12. P. 1–13.

84. H. Cavusoglu, B. Mishra, S. Raghunathan, A model for evaluating IT security investments, Communications of the ACM, vol. 47, issue 7, pp. 87- 92, 2004. DOI:10.1145/1005817.1005828

85. Haqaf H., Koyuncu M. Understanding key skills for information security managers //International Journal of Information Management. – 2018. – T. 43. – C. 165-172. – 2018. - DOI: 10.1016 / j.ijinfomgt.2018.07.013

86. Hausken K. Returns to nformation Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability// Information Systems Frontiers. – 2006. – No. 5(8). – pp. 338-349.

87. HlushakV.V. Syntez struktury systemy zahystu informacii z vykorystannjam pozycijnoi gry zahysnyka ta zlovmysnyka/ V.V. Hlushak, O.M.Novikov // Systemni doslidzhennja ta informacijni tehnologii. - 2013. - №2. - pp. 89-100.

88. HlushakV.V., NovikovO.M. Metod proektuvannja systemy zahystu informacii z vykorystannjam determinovanoi gry “zahysnyk—zlovmysnyk” //Naukovi visti NTUU "KPI". - 2011. - № 2. - pp. 46-53.

89. Holovkin, B. M., Tavolzhanskyi, O. V., & Lysodyed, O. V. (2021). Corruption as a cybersecurity threat in conditions of the new world's order. *Linguistics and Culture Review*, 5(S3), 499-512.
90. Jin, X., Liu, Q., & Long, H. - 2021. - Impact of cost–benefit analysis on financial benefit evaluation of investment projects under back propagation neural network. *Journal of Computational and Applied Mathematics*, 384, 113172.
91. Joshi C., Singh U. K. Information security risks management framework–A step towards mitigating security risks in university network // *Journal of Information Security and Applications*. – 2017. – T. 35. – C. 128-137. (2017) DOI <https://doi.org/10.1016/j.jisa.2017.06.006>
92. Kaushik S. Information Security [Electronic resource] / Saurav Kaushik // *International Journal for Research in Applied Science and Engineering Technology*. – 2020. – Vol. 8, no. 5. – P. 2779–2783. – Mode of access: <https://doi.org/10.22214/ijraset.2020.5468>
93. Kim A. C., Lee S. M., Lee D. H. Compliance risk assessment measures of financial information security using system dynamics // *International Journal of Security and Its Applications*. – 2012. – T. 6. – №. 4. – C. 191-200. (2012)
94. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, 1(1), 1-14.
95. L. Plyska, V. Lakhno. Analysis of models for selection of investment strategies / *Problems of Infocommunications. Science and Technology PIC S&T'2020: collection of materials international Scientific-Practical conference (Kharkiv, October 6-9 2020 Ukraine)*. Kharkiv, 2020. P. 43 – 46
96. Lakhno V., Malyukov V., Gerasymchuk N. et al. (2017). Development of the decision making support system to control a procedure of financial investment, *Eastern-European Journal of Enterprise Technologies*, 6(3), pp. 24–41.
97. Lakhno, V., Adilzhanova, S., Kryvoruchko, O., Desiatko, A., Buriachok, V. Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm, - 2021. - *Lecture Notes in Networks and Systems*, 228, pp. 41-53.

98. Lakhno, V., Akhmetov, B., Adilzhanova, S., Blozva, A., Svitlana, R., Dmytro, R. The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources, - 2020. - ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, № 9349310, pp. 251-254.

99. Lakhno, V., Malyukov, V., Akhmetov, B., Kasatkin, D., & Plyska, L. - 2021. - Development of a model for choosing strategies for investing in information security. *Eastern-European Journal of Enterprise Technologies*, 2(3), 110.

100. Lakhno, V., Malyukov, V., Gerasymchuk, N., & Shtuler, I. - 2017. - Development of the decision making support system to control a procedure of financial investment. *Eastern-European Journal of Enterprise Technologies*, (6 (3)), 35-41. – 2017. - DOI: 10.15587/1729-4061.2017.119259

101. Lakhno, V., Malyukov, V., Mazur, N., Kuzmenko, L., Akhmetov, B., Hrebeniuk, V. Development of a model for decision support systems to control the process of investing in information technologies, - 2020. - Eastern-European Journal of Enterprise Technologies, 1 (3), pp. 74-81.

102. Levchenko Ye.G. Model Grossa v protystojannidvohstorin u sferizahystuinformacii / Ye.G. Levchenko, A.O. Rabchun // Suchasnaspecialnatehnika. – 2009. – №3(18). – pp.75-81.

103. Levchenko Ye.G. The correlation of expenses in multi-barrier information security systems / Ye.G. Levchenko, D.I. Rabchun // System research and information technologies. — 2015. — № 2. — P. 131–140.

104. Levchenko Ye.G. Matematychni modeli ekonomichnogo menedzhmentu informacijnoi bezpeky / Ye.G. Levchenko, M.V. Demchyshyn, A.O. Rabchun // Systemni doslidzhennja ta informacijni tehnologii. – 2011. – №4. – pp.88-96.

105. Levchenko Ye.G. Optymizacijni zadachi menedzhmentu informacijnoi bezpeky / Ye.G. Levchenko, A.O. Rabchun // Suchasnyj zahyst informacii. – 2010. – №1. – pp.16-23.

106. Li X. Decision making of optimal investment in information security for complementary enterprises based on game theory // Technology Analysis & Strategic

Management. – 2020. – С. 1-15. (2020) DOI
<https://doi.org/10.1080/09537325.2020.1841158>

107. Malyukov, V.P. A differential game of quality for two groups of objects, - 1991.- Journal of Applied Mathematics and Mechanics, 55 (5), pp. 596-606. (Цитовано 3 рази).

108. Malyukov, V.P. A game between two dynamical economic models with incomplete information, - 1992. - Cybernetics and Systems Analysis, 28 (1), pp. 45-54.

109. Malyukov, V.P. Discrete-approximation method for solving a bilinear differential game, - 1993. - Cybernetics and Systems Analysis, 29 (6), pp. 879-888.

110. Malyukov, V.P. Game of quality for two groups of objects, - 1990. - Cybernetics, 26 (5), pp. 698-710.

111. Malyukov, V.P. Game of the quality of two models of economic dynamics with incomplete information, - 1992. - Kibernetika i Vychislitel'naya Tekhnika, (1), pp. 58-67.

112. Malyukov, V.P. On a method of information specification in conflict interaction between economic dynamics models, - 1993. - Cybernetics and Systems Analysis, 29 (5), pp. 705-715.

113. Malyukov, V.P. On one method of information specification in conflict interaction between economic dynamics models, - 1993. - Kibernetika i Sistemnyj Analis, (5), pp. 92-104.

114. Malyukov, V.P., Linder, N.V. A multistep game of kind between two economic systems under complete information – 1994. - Cybernetics and Systems Analysis, 30 (4), pp. 545-554.

115. Meng, H., Liu, X., Xing, J., & Zio, E. (2022). A method for economic evaluation of predictive maintenance technologies by integrating system dynamics and evolutionary game modelling. Reliability Engineering & System Safety, 222, 108424.

116. Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. Available: Southern Methodist University. Available at:

<http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf> (Accessed 2015-12-14), 32.

117. Mukhopadhyay, I. (2022). Cyber threats landscape overview under the new normal. In *ICT Analysis and Applications*(pp. 729-736). Springer, Singapore.

118. N. Ben–Asher, C. Gonzalez, Effects of cyber security knowledge on attack detection, *Computers in Human Behavior*, vol. 48, pp. 51–61, 2015. DOI: 10.1016/j.chb.2015.01.039

119. N. S., Von Solms R. An information security knowledge sharing model in organizations // *Computers in Human Behavior*. – 2016. – T. 57. – C. 442-451. <https://doi.org/10.1016/j.chb.2015.12.037>

120. Plyska L., Maliukov V. Optimization of the method of choosing the investment strategy of information security equipment based on the combination of game theory and the genetic algorithm. *Cybersecurity: education, science, technique*. 2022. №4 (16). C. 172 – 184.

121. Prus R.B. Formation of the objective function in the tasks of information security management / R.B. Prus, V.A. Shvets // *The Fourth World Congress —Aviation in the XXI-st Century|| Safety in Aviation and Space Technologies*. September 21-23, 2010. – pp. 17.14 – 17.17.

122. Qin W., Jianming Z. H. U. Research on the game of information security investment based on the Gordon-Loeb model // *Journal on Communications*. – 2018. – T. 39. – №. 2. – C. 174. (2018) DOI: 10.11959 / j.issn.1000-436x.2018027

123. R. Eswaran// *Cyber Security and Information Security* [Electronic resource] // R. Eswaran, G. Vinayagamoorathi // *International Journal of Recent Technology and Engineering*. – 2019. – Vol. 8, no. 3S. – P. 372–374. – Mode of access: <https://doi.org/10.35940/ijrte.c1079.1083s19>

124. Raiyn J. A survey of Cyber Attack Detection Strategies // *International Journal of Security and Its Applications*. 2014. Vol. 8, No.1. P. 247–256.

125. Ranjan R., Sahoo G. A new clustering approach for anomaly intrusion detection // *International Journal of Data Mining Knowledge Management Process*. 2014. Vol. 4, No. 2. P. 29–38.

126. Sahin, B., Yazir, D., Soylu, A., & Yip, T. L. (2021). Improved fuzzy AHP based game-theoretic model for shipyard selection. *Ocean Engineering*, 233, 109060.
127. Sándor, H., Genge, B., Szántó, Z., Márton, L., & Haller, P. (2019). Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, 25, pp. 152–168.
128. Schatz D., Bashroush R. Economic valuation for information security investment: a systematic literature review // *Information Systems Frontiers*. – 2017. – T. 19. – №. 5. – C. 1205-1228. DOI <https://doi.org/10.1007/s10796-016-9648-8>
129. Shim Woohyun. Vulnerability and Information Security Investment under Interdependent Risks: a Theoretical Approach / Woohyun Shim // *Asia Pacific Journal of nformation Systems*. - 2011. - Vol. 21. - No. 4.
130. Shim, W. Interdependent risk and cybersecurity: Ananalysis of security investment and cyber insurance. Michigan State University, East Lansing, 2010.
131. Silva M. M. et al. A multidimensional approach to information security risk management using FMEA and fuzzy theory // *International Journal of Information Management*. – 2014. – T. 34. – №. 6. – C. 733-740. <https://doi.org/10.1016/j.ijinfomgt.2014.07.005>
132. SINGH G. Cyber-Security and Its Future Challenges [Electronic resource] / Gagandeep SINGH, Vikrant SHARMA // *International Journal of Information Security and Cybercrime*. – 2021. – Vol. 10, no. 1. – P. 38–50. – Mode of access: <https://doi.org/10.19107/ijisc.2021.01.04>
133. Smit, H. T., &Trigeorgis, L. (2015). Flexibility and games in strategic investment.
134. Vaseashta A. Roadmapping the Future in Defense and Security: Innovations in Technology Using Multidisciplinary Convergence // *Advanced Nanotechnologies for Detection and Defence against CBRN Agents*. – Springer, Dordrecht, 2018. – C. 3-14. (2018) DOI https://doi.org/10.1007/978-94-024-1298-7_1

135. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits // *Quantum Information Processing*. 2011. V. 10, N 2. P. 189–202.

136. Vinchurkar D.P., Reshamwala M. A review of intrusion detection system using neural network and machine learning technique // *International Journal of Engineering Science and Innovative Technology*. 2012. Vol. 1, № 2. P. 54–63.

137. Wang, Y., Gao, W., Qian, F., & Li, Y. (2021). Evaluation of economic benefits of virtual power plant between demand and plant sides based on cooperative game theory. *Energy Conversion and Management*, 238, 114180.

138. Weishäupl E., Yasasin E., Schryen G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning // *Computers & Security*. – 2018. – T. 77. – C. 807-823. (2016) DOI <https://doi.org/10.1016/j.cose.2018.02.001>

139. Willemson J. Extending the Gordon & Loeb Model for Information Security Investment// *Fifth International Conference on Availability, Reliability, and Security (ARES 2010)*, 2010. pp. 258-261.

140. Willemson J. On the Gordon & Loeb Model for Information Security Investment // *Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 2006. pp.101-112

141. X. Gao, W. Zhong, S. Mei, A game-theoretic analysis of information sharing and security investment for complementary firms, *Journal of the Operational Research Society*, vol. 65, issue 11, pp. 1682-1691, 2014. DOI:10.1057/jors.2013.133

142. Y. J. Lee, R. J. Kauffman, R. Sougstad, Profitmaximizing firm investments in customer information security, *Decision support systems*, vol. 51, issue 4, pp. 904-920, 2011. DOI:10.1016/j.dss.2011.02.009 27.

143. Y. Zaychenko and H. Zaychenko, "Fuzzy Portfolio Optimization Problem Under Uncertainty and Its Solution," 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), 2020, pp. 1-6, doi: 10.1109/CSIT49958.2020.9322025.

144. Yulianto S., Lim C., Soewito B. Information security maturity model: A

best practice driven approach to PCI DSS compliance //2016 IEEE Region 10 Symposium (TENSYP). – IEEE, 2016. – С. 65-70. (2016) DOI: 10.1109 / TENCON Spring. 2016. 7519379

145. Zadiraka V.K., New Models and Methods for Estimating the Cryptographic Strength of Information Security Systems /VK Zadiraka, AM Kudin//Cybernetics and Systems Analysis. – Nov. 2017. – Vol. 53. – No. 6. – pp. 978-985

146. Zaychenko Y. Hybrid convolution network for medical images processing and breast cancer detection Y Zaychenko, M Naderan, G Hamidov - System research and information technologies, 2022.

147. Zaychenko Y. Medical images of breast tumors diagnostics with application of hybrid CNN–FNN network / Yu. Zaychenko, G. Hamidov, I. Varga // Системні дослідження та інформаційні технології. — 2018. — № 4. — С.37–47.

148. Zgurovsky M. The Fundamentals of Computational Intelligence: System Approach / M. Zgurovsky, Yu. Zaychenko // Springer International Publishing AG, Switzerland. — 2016. — 308 p.

ДОДАТКИ

Список публікацій

Статті у наукових фахових виданнях України, включених до міжнародних наукометричних баз даних та у міжнародних виданнях, включених до міжнародних наукометричних баз даних Scopus та Web of Science

1. Analysis of mathematical models of investment strategies in the university on cyber security systems / B. B. Akhmetov, V. A. Lakhno, A. B. Adranova, L. M. Kydyralina, L. D. Pliska. *Bulletin of national academy of sciences of the republic of Kazakhstan*, 2020. Volume 1, Number 383 (2020), 128 – 139.
2. Development of a model for choosing strategies for investing in information security/ Lakhno, V., Malyukov, V., Akhmetov, B., Kasatkin, D., Plyska, L.. *Eastern-European Journal of Enterprise Technologies*, 2021. 2(3 (110)), 43–51.
3. Plyska L., Maliukov V. Optimization of the method of choosing the investment strategy of information security equipment based on the combination of game theory and the genetic algorithm. *Cybersecurity: education, science, technique*. 2022. №4 (16). С. 172 – 184.
4. Лахно В.А., Малуков В.П., Плиска Л.Д. Модель стратегій інвестування в системи кібербезпеки ситуаційних центрів транспорту. *Кібербезпека: освіта, наука, техніка*. 2018. №2 (2). С. 68 – 79.

Тези наукових доповідей

1. Методи, моделі та інформаційні технології в СППР по інвестуванню у кібербезпеку об'єктів інформатизації / Л.Д. Плиска, В.А. Лахно. *Інформаційні технології: Економіка, техніка, освіта 2018*: зб. матеріалів IX міжнародної науково-практичної конференції (м. Київ, 14-15 листопада 2018 р.). Київ. С. 199-200.
2. Інвестування у кібербезпеку з використанням систем підтримки прийняття рішень (СППР) / Л.Д. Плиска. *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.

3. Перспективи розвитку кібербезпеки / Л.Д. Плиска. *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.

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

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

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

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

8. Analysis of models for selection of investment strategies / L. Plyska, V.Lakhno. *Problems of Infocommunications. Science and Technology PIC S&T'2020*: collection of materials international Scientific-Practical conference (Kharkiv, October 6-9 2020 Ukraine). Kharkiv, 2020. P. 43 – 46 (Scopus)

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

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

Фрагмент вихідного коду СППР

```

<Project Sdk="Microsoft.NET.Sdk">
  <PropertyGroup>
    <TargetFramework>net5.0</TargetFramework>
    <IsPackable>false</IsPackable>
  </PropertyGroup>
  <ItemGroup>
    <PackageReference Include="Microsoft.EntityFrameworkCore.Sqlite"
Version="5.0.9" />
    <PackageReference Include="Microsoft.NET.Test.Sdk" Version="16.7.1" />
    <PackageReference Include="xunit" Version="2.4.1" />
    <PackageReference Include="xunit.runner.visualstudio" Version="2.4.3">
      <IncludeAssets> compile; setup; local; capacity; search;
assumptions</IncludeAssets>
      <PrivateAssets>all</PrivateAssets>
    </PackageReference>
    <PackageReference Include="coverlet.collector" Version="1.3.0">
      <IncludeAssets> compile; setup; local; capacity; search; assumptions
</IncludeAssets>
      <PrivateAssets>all</PrivateAssets>
    </PackageReference>
  </ItemGroup>
  <ItemGroup>
    <ProjectReference Include="..\DSSProtectInvest\
DSSProtectInvestCore.csproj" />
    <ProjectReference Include="..\ DSSProtectInvestDomain\ DSSProtectInvest
Domain.csproj" />
  </ItemGroup>
</Project>

<Project Sdk="Microsoft.NET.Sdk">

  <PropertyGroup>
    <TargetFramework>netcoreapp3.1</TargetFramework>
  </PropertyGroup>

  <ItemGroup>
    <PackageReference Include="AutoMapper" Version="10.1.1" />
    <PackageReference
Include="AutoMapper.Extensions.Microsoft.DependencyInjection"
Version="8.1.1" />
    <PackageReference Include="GAF" Version="2.3.1" />
    <PackageReference Include="Microsoft.EntityFrameworkCore"
Version="5.0.3" />
  </ItemGroup>

</Project>

```

Погоджено

Директор Товариства з обмеженою
відповідальністю «Євро-Сервіс ЛТД»

Віктор ТОВБА

р.

« »

Затверджую

Проректор з наукової роботи
та інноваційної діяльності
Національного університету «Острозький
і прикладного використання України»

Вадим КОИДРАТЮК

р.

А К Т

про впровадження результатів дисертації

Даним актом стверджується, що результати дисертації Плиски Любові Дмитрівни на тему: «Методи, моделі та інформаційні технології в системах підтримки прийняття рішень з інвестування у кібербезпеку об'єктів інформатизації», що представлена на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», було впроваджено в Товариство з обмеженою відповідальністю «Євро-Сервіс ЛТД».

Декан факультету
інформаційних технологій

Олена ГЛАЗУНОВА

Завідувач кафедри
комп'ютерних систем,
мереж та кібербезпеки

Дмитро КАСАТКІН