

АНОТАЦІЯ

Плиська 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 зі 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 атакуювальною стороною сценаріїв для проведення атак і т. д.

Інвестиції в інноваційні проекти, 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 проектів 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 тієї 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 багатофакторної 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 алгоритму під час оптимізації пошуку стратегій відбору засобів захисту інформації 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.

ANNOTATION

Plyska L. D. Methods, models and information technologies in decisionmaking 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 %. 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.