Національний авіаційний університет
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ГАЛАТА ЛІЛІЯ ПАВЛІВНА

УДК 004 [.94 + .73]

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАХИСТУ КРИТИЧНИХ РЕСУРСІВ ВИРОБНИЦТВА МІНЕРАЛЬНИХ ДОБРИВ

122 – комп’ютерні науки
(технічні науки)

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Л.П. Галата

Науковий керівник – Корнієнко Богдан Ярославович, доктор технічних наук, професор

Київ – 2022

АНОТАЦІЯ

Галата Л.П. Інформаційна технологія захисту критичних ресурсів виробництва мінеральних добрив. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки. – Національний авіаційний університет Міністерства освіти і науки України, м. Київ, 2022.

Дисертаційна робота присвячена створенню теоретичних та прикладних результатів з розробки інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив з урахуванням вимог підвищення функціональної безпеки та забезпечення заданої якості готового продукту.

Пріоритетом інформаційних технологій є забезпечення доступності та цілісності керуючої та конфігураційної інформації про параметри технологічного процесу, тобто забезпечення саме функціональної безпеки. Особлива увага приділяється запобіганню несанкціонованому доступу до системи з метою збереження стабільного функціонування інформаційних технологій.

Серед найважливіших галузей, у яких інформаційні технології грають визначальну роль, особливу увагу займає управління технологічними процесами виробництва мінеральних добрив. Аналіз результатів досліджень, проведених у напрямку забезпечення інформаційної безпеки саме для таких складних неперервних виробництв та систем захисту їх критичних ресурсів, показує, що наразі питання наукового обґрунтування системи захисту інформації до кінця не вирішені. Насамперед йдеться про методи та моделі оцінки та оптимізації систем захисту інформації, які в контексті сучасних тенденцій організації виробництва відіграють вирішальну роль в успіху підприємства.

Аналіз результатів існуючих досліджень щодо стану захисту критичних ресурсів виробництва мінеральних добрив свідчить про відсутність на даний час комплексного підходу, який враховував би специфіку управління технологічними процесами виробництва мінеральних добрив та механізми формалізації та алгоритмізації процесів захисту критичних ресурсів таких виробництв.

Тому існує нагальна потреба в подальшому дослідженні методів та засобів захисту критичних ресурсів виробництва мінеральних добрив з метою їх удосконалення. А розробка моделей, методу та інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив є надзвичайно актуальною на сьогоднішній день. Таким чином, усе це і зумовило необхідність вирішення актуальної науково-технічної задачі забезпечення необхідного рівня захищеності критичних ресурсів виробництва мінеральних добрив за рахунок розроблених моделей, методу та створення і використання нової інформаційної технології.

У вступі обґрунтовано актуальність дисертаційної роботи, сформульовано мету та основні завдання дослідження, наведено відомості щодо зв'язку роботи з науковим темами. Подано анотацію отриманих в дисертації результатів, висвітлено їх наукову новизну і практичну значимість, відзначено особистий внесок здобувача у спільних публікаціях, наведено кількісні показники стосовно опублікованих наукових праць, структури та обсягу дисертації.

У *першому розділі* проведене дослідження сучасного стану розвитку інформаційних технологій захисту критичних інформаційних ресурсів, яке показало, що існуючі моделі, методи та засоби не розглядають в комплексі усі принципи забезпечення захисту критичних інформаційних ресурсів технологічних процесів.

На основі аналізу особливостей організації інформаційно-обчислювального процесу на підприємствах уточнена класифікація загроз інформаційній безпеці, а також виявлені загрози, найбільш значущі для даного типу підприємств. З метою створення математичної моделі протидії впливу внутрішніх та зовнішніх загроз при розробці методу оптимізації і інформаційної технології захисту критичних інформаційних ресурсів проведено аналіз математичних моделей захисту інформації, моделей загроз і особливостей їх реалізації.

Розглянуті основні підходи до побудови імітаційної моделі захисту критичних інформаційних ресурсів виробництва мінеральних добрив. Встановлена необхідність забезпечення функціонування інформаційної технології в умовах здійснення нових і невідомих атак.

Для підвищення стану захищеності підприємства від загроз порушення інформаційної безпеки необхідно вибрати оптимальний варіант системи захисту інформації. Забезпечення інформаційної безпеки підприємства дає перевагу по відношенню до інших підприємств в даній галузі. Необхідно вибрати найкращий варіант системи захисту інформації для підприємства, при якому рівень захищеності підприємства буде максимальним.

Проведено аналіз математичних моделей процесу виробництва мінеральних добрив у грануляторах із псевдозрідженим шаром. Визначено основні параметри, що впливають на технологічний процес виробництва мінеральних добрив та належать до критичних інформаційних ресурсів. Розглянуті математичні моделі не враховують зміну вологовмісту гранул, як одного з основних показників якості готового продукту. Разом с тим в існуючих моделях недостатньо уваги приділено урахуванню теплоти кристалізації, пароутворення і створенню математичної моделі, яка б враховувала більш повно зміну температур гранул та теплоносія.

За результатами огляду літературних джерел сформульовано напрямок досліджень з метою створення ефективної інформаційної технології захисту критичних інформаційних ресурсів виробництва мінеральних добрив і розробки для цього математичних моделей, методу оптимізації та системи захисту критичних інформаційних ресурсів.

Другий розділ присвячений створенню математичної моделі протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних інформаційних ресурсів виробництва мінеральних добрив та побудові імітаційної моделі захисту критичних інформаційних ресурсів виробництва мінеральних добрив.

Розроблено імітаційну модель захисту критичних ресурсів виробництва мінеральних добрив, на базі GNS3 та Kali Linux. Для випробування імітаційної моделі захисту критичних ресурсів виробництва мінеральних добрив розглянуто програмні засоби для проведення тестування побудованої моделі. За допомогою збудованого імітаційної моделі захисту критичних ресурсів виробництва мінеральних добрив реалізоване проєктування комп’ютерної мережі та системи захисту критичних ресурсів виробництва мінеральних добрив, здійснена перевірка системи захисту

критичних ресурсів шляхом генерації атак та їх відбиття системою захисту критичних ресурсів виробництва мінеральних добрив.

Розглянуто методи тестування та аналізу ризиків системи захисту критичних ресурсів виробництва мінеральних добрив, обрано метод для тестування системи захисту інформації на базі імітаційної моделі безпеки. Протестовано систему захисту критичних ресурсів виробництва мінеральних добрив відносно ряду вразливостей, зроблено висновки щодо стійкості побудованої мережі до конкретних загроз методом iRisk.

Запропонована математична модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних інформаційних ресурсів виробництва мінеральних добрив. Поетапно розписаний процес побудови математичної моделі протидії загрозам у системі захисту критичних інформаційних ресурсів за допомогою марківського ланцюга. Запропонована методика знаходження актуальних загроз безпеці даних при їх обробці. Наведені приклади розрахунків імовірностей знаходження математичної моделі інформаційної системи в одному з чотирьох станів (загроза не настала; загроза настала, але не була реалізована; загроза настала, була реалізована; загроза настала, але була відбита системою захисту).

У *третьому розділі* розв`язано задачу оптимізації системи захисту інформації критичних інформаційних ресурсів. Реалізовано факторно-цільовий аналіз з метою вибору критерію оптимальності. Запропоновано три критерії якості: узагальнений критерій якості, критерій якості для способу однакових інтенсивностей та критерій якості для способу пропорційності витратам. Для оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив використовуються імітаційна модель системи захисту критичних ресурсів виробництва мінеральних добрив та математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив. Розроблено метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив та методику оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив.

У *четвертому розділі* розроблена математична модель теплообміну процесу виробництва мінеральних добрив у грануляторі із псевдозрідженим шаром. На основі

проведеного аналізу гідродинаміки, тепло- і масообміну процесів зневоднення та гранулювання у псевдозрідженому шарі математична модель процесу виробництва мінеральних добрив доповнена рівнянням зміни вологовмісту гранул. На процес гранулоутворення у грануляторі великий вплив мають такі параметри як: температура гранул, температура теплоносія, яким псевдозріджується шар та вологовміст гранул. В створеній математичній моделі велика увага приділяється контролю даних параметрів, аби система керування змогла забезпечити ефективне використання ресурсів та високу якість продукції.

Розроблено оптимальну систему керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором**.**

Розроблено інформаційну технологію захисту критичних ресурсів виробництва мінеральних добрив, основними компонентами якої є наступні технічні, програмні та організаційно-методичні засоби: моделювання системи захисту критичних ресурсів виробництва мінеральних добрив, оптимізація системи захисту критичних ресурсів виробництва мінеральних добрив, система захисту критичних ресурсів виробництва мінеральних добрив, математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі та оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором. Використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив дозволило підвищити якість готового продукту на 15 %.

Розроблено методику використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив.

У висновках подані основні результати дисертаційного дослідження, що відображають методологічні основи формування інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив.

Наукова новизна отриманих результатів

На підставі теоретичних і практичних досліджень, виконаних у дисертаційній роботі:

вперше

- розроблено метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив на основі імітаційної моделі системи захисту критичних ресурсів виробництва мінеральних добрив та математичної моделі протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив, що дозволяє на основі одержаних значень інтенсивностей переходів та станів системи підвищити рівень захищеності критичних ресурсів виробництва мінеральних добрив від впливу внутрішніх та зовнішніх загроз;
- розроблено математичну модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі, яка враховує зміни основних характеристик виробництва гранул у псевдозрідженому шарі, що дозволяє забезпечити необхідну якість готового продукту;
- розроблено інформаційну технологію захисту критичних ресурсів виробництва мінеральних добрив, основними компонентами якої є наступні засоби: моделювання системи захисту критичних ресурсів виробництва мінеральних добрив, оптимізація системи захисту критичних ресурсів виробництва мінеральних добрив, система захисту критичних ресурсів виробництва мінеральних добрив, математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі та оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором. Розроблена інформаційна технологія забезпечує урахування вимог підвищення функціональної безпеки та забезпечення заданої якості готового продукту;

удосконалено

- імітаційну модель захисту критичних ресурсів виробництва мінеральних добрив, на базі GNS3 та KaliLinux, яка адаптована до структури мереж та систем захисту інформаційних ресурсів критичної інфраструктури, з метою комплексної оцінки запропонованих заходів і засобів захисту критичних інформаційних ресурсів;

отримала подальший розвиток

– математична модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних ресурсів виробництва мінеральних добрив та запропонована на основі цієї моделі методика виявлення актуальних загроз безпеки, що дозволяє розглядати поведінку системи при дії на неї кожного типу загроз окремо і визначати імовірності їх появи і відбиття ситемою захисту.

Практичне значення отриманих результатів

Розроблені в дисертаційній роботі методологічні основи інформаційного, технологічного та організаційного спрямування стали підґрунтям створення інформаційної технології, що забезпечує підвищення ефективності управління процесом виробництва мінеральних добрив за рахунок захисту критичних ресурсів.

Практично вагомими вважаються такі результати:

- методика оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив;
- оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором;
- методика використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив.

Результати дисертаційної роботи апробовано і використано у таких організаціях та установах:

- у ТОВ «НВЦ «ІНФОЗАХИСТ» при реалізації проєктів;
- у навчальному процесі Національного авіаційного університету під час викладання дисциплін «Безпека інформаційно-комунікаційних систем та мереж», «Проєктування систем безпеки ІКСМ», «Інформаційно-комунікаційні системи та мережі».

Дані про впровадження підтверджено відповідними документами.

Ключові слова: інформаційна технологія, виробництво мінеральних добрив, критичні ресурси, математична модель, імітаційна модель, методика, метод оптимізації, система захисту інформації, оптимальна система керування.

ANNOTATION

Galata L.P. Information technology of critical resources protection for mineral fertilizers production. - Qualifying scientific work on the rights of the manuscript.

The dissertation on competition of a scientific degree of the Doctor of Philosophy on a specialty 122 - Computer Science. - National Aviation University, Ministry of Education and Science of Ukraine, Kyiv, 2022.

The dissertation is devoted to creation of theoretical and applied bases for realization of information technology of critical resources protection for mineral fertilizers production, taking into account the requirements of increasing functional safety and ensuring the specified quality of the finished product.

The priority of information technologies is to ensure the availability and integrity of control and configuration information about the parameters of the technological process, that is, to ensure functional safety. Special attention is paid to preventing unauthorized access to the system in order to preserve the stable functioning of information technologies.

Among the most important industries in which information technologies play a decisive role, special attention is paid to the management of technological processes of mineral fertilizer production. Analysis of the researches results conducted in the direction of ensuring information security specifically for such complex continuous production and protection systems for their critical resources shows that currently the issues of scientific justification of the information protection system are not fully resolved. First of all, it is about the methods and models of evaluation and optimization of information protection systems, which in the context of modern trends in the production organization play a decisive role in the success of the enterprise.

The analysis of the existing research results on the state of critical resources protection for mineral fertilizers production indicates the absence of a comprehensive approach at the moment that would take into account the specifics of managing the technological processes of mineral fertilizer production and the mechanisms of formalization and algorithmization of critical resources protection processes for such productions.

Therefore, there is an urgent need for further research into methods and means of critical resources protection for mineral fertilizers production in order to improve them. And

the development of models, methods and information technology for critical resources protection of mineral fertilizers production is extremely relevant today. Thus, all this led to the need to solve the urgent scientific and technical problem of ensuring the specified level of critical resources protection for mineral fertilizers production due to the developed models, methods and creation and use of new information technology.

The introduction substantiates the relevance of the dissertation, formulates the purpose and main objectives of the study, provides information on the works' relationship with scientific programs and topics. An annotation of the results obtained in the dissertation is given, their scientific novelty and practical significance are highlighted, the applicant's personal contribution in joint publications is noted, quantitative indicators concerning the published scientific works, structure and volume of the dissertation are given.

The first section examines the current state of development of information technologies for the protection of critical information resources, which showed that existing models, methods and tools do not consider all the principles of protection of critical information resources for technological processes.

The classification of information security threats is specified, as well as the most significant threats for this type of enterprises, based on the analysis of the enterprises' information infrastructure and the principles of its functioning, the peculiarities of the organization of the information and computational process in enterprises. The analysis of mathematical models for information protection, threat models and features of their implementation has been done, in order to create a mathematical model for counteracting the impact of internal and external threats in the development of optimization methods and information technology for the protection of critical information resources.

The main approaches to building a simulation model of critical information resources protection for mineral fertilizers production are considered. The need to ensure the functioning of information technology in the context of new and unknown attacks.

To increase the enterprise security from threats of information security violations, it is necessary to choose the best option for information protection system. Ensuring information security of the enterprise gives an advantage over other enterprises in this field. It is

necessary to choose the best version of the information security system for the company, which will provide the maximum level of the enterprises' security.

The analysis of mathematical models of the process of mineral fertilizers production in granulators with a fluidized bed has been done. The main parameters that affect the technological process of mineral fertilizer production and belong to the critical information resources are identified. The considered mathematical models do not take into account the change in the moisture content of the granules, as one of the main indicators of the quality of the finished product. However, in the existing models, insufficient attention is paid to the heat of crystallization, vaporization and the creation of a mathematical model that would take into account more fully the temperature changes of the granules and the coolant.

Based on the results of the literature review, the direction of research is formulated in order to create an effective information technology for the protection of critical information resources for mineral fertilizers production and development of mathematical models, optimization methods and protection systems for critical information resources.

The second section is devoted to the creation of a mathematical model for counteracting the impact of internal and external threats on the system of protection of critical information resources for mineral fertilizers production and construction of a simulation model of protection of critical information resources for mineral fertilizers production.

A simulation model for the protection of critical resources for the production of mineral fertilizers, based on GNS3 and Kali Linux, has been developed. To test the simulation model of critical resources protection for mineral fertilizers production, software tools for testing the constructed polygon are considered. The design of computer network and system of protection of critical resources for mineral fertilizers production is realized, with the help of the built simulation model of critical resources protection for mineral fertilizers production. The protection system of critical resources was checked by generating attacks and their reflection by the protection system of critical resources of mineral fertilizers production.

Methods of testing and risk analysis of the critical resources protection system of mineral fertilizers production are considered, the method for testing the information protection system on the basis of the cybersecurity polygon is chosen. The protection system of critical resources for mineral fertilizers production was tested against a number of

vulnerabilities, conclusions were made by the iRisk method about the resilience of the constructed network to specific threats.

The mathematical model of counteraction of internal and external threats influence on critical information resources protection system of production of mineral fertilizers is offered. The process of building a mathematical model of countering threats in the protection system of critical information resources by using the Markov chain is described step by step. The methodology of finding actual threats for data security processing is offered. Examples of calculations for probabilities of finding a mathematical model of an information system in one of four states are given (threat did not come; threat came but was not realized; threat came, was realized; threat came, but was reflected by the protection system).

In the third section the problem of optimization for the information security system of critical information resources is solved. Factor-target analysis is implemented in order to select the criterion of optimality. Three quality criteria are proposed: a generalized quality criterion, a quality criterion for the method of equal intensities and a quality criterion for the method of cost proportionality. The simulation model of the protection system of critical resources for mineral fertilizers production and the mathematical model of countering threats in such system are used for optimizing the protection system of critical resources for mineral fertilizers production, The method of optimization of the protection system of critical resources for mineral fertilizers production and the optimization methodology for the protection system of critical resources of mineral fertilizers production are developed.

In the fourth section the mathematical model of heat exchange in the process of mineral fertilizers production in the granulator with a fluidized bed is developed. Based on the analysis of hydrodynamics, heat and mass transfer of dehydration and granulation processes in the fluidized bed, the mathematical model of the process of mineral fertilizers production is supplemented by the equation of moisture content of granules changing. The process of granulation in the granulator is greatly influenced by such parameters as: temperature of the granules, the temperature of the coolant, which fluidizes the layer and the moisture content of the granules. In the created mathematical model, much attention is

paid to the control of these parameters so that the control system can ensure efficient use of resources and high-quality products.

An optimal control system for the production of granular mineral fertilizers in a fluidized bed with LQR-regulator has been developed.

The information technology of critical resources protection for mineral fertilizers production is developed, the main components of which are the following technical, software and organizational-methodical means: modeling of protection system of critical resources for mineral fertilizers production, optimization of protection system of critical resources for mineral fertilizers production. protection system of critical resources for mineral fertilizers production, mathematical model of heat exchange in the process of mineral fertilizers production in the granulator with a fluidized bed and the optimal control system for the production of granular mineral fertilizers in the fluidized bed with LQR-regulator. The use of information technology to protect critical resources for the production of mineral fertilizers has improved the quality of the finished product by 15%.

The methodology of information technology creation for critical resources protection of mineral fertilizers production is developed.

The conclusions present the main results of the dissertation research, which reflect the methodological foundations of the formation of information technology for the critical resources protection of mineral fertilizers production.

Scientific novelty of the obtained results

On the basis of theoretical and practical research performed in the dissertation, the following new results were obtained:

for the first time

- the method of optimization for protection system of critical resources for production of mineral fertilizers on the basis of simulation model for the protection of critical resources for the production of mineral fertilizers and on the basis of mathematical model of counteraction to threats influence on critical information resources protection system of production of mineral fertilizers has been developed, it allows to increase the level of critical resources protection for production of mineral fertilizers from the influence of internal and external threats on the basis of the received values of transition intensities and system states;

- a mathematical model of the heat exchange of granular mineral fertilizers production in a fluidized bed has been developed, it takes into account changes in the main characteristics of the granules in a fluidized bed production, that allows to ensure the specified quality of the finished product;

- the information technology of critical resources protection for mineral fertilizers production has been developed, the main components of which are the following means: modeling of protection system of critical resources for mineral fertilizers production, optimization of protection system of critical resources for mineral fertilizers production, protection system of critical resources for mineral fertilizers production, mathematical model of heat exchange in the process of mineral fertilizers production in the granulator with a fluidized bed and the optimal control system for the production of granular mineral fertilizers in the fluidized bed with LQR-regulator. The developed information technology takes into account the requirements for increasing functional safety and ensuring the specified quality of the finished product;

improved

- simulation model of critical resources protection for mineral fertilizers production, based on GNS3 and KaliLinux, which is adapted to the structure of networks and to the information resources protection systems of critical infrastructure, with the aim of a comprehensive assessment of the proposed measures and means of critical information resources protection;

received further development

- mathematical model of counteraction of internal and external threats influence on critical resources protection system of mineral fertilizers production and the methodology of detection actual security threats is offered on the basis of this model, which allows considering the behavior of the system when each type of threat is acting on it separately and determining the probability of their appearance and reflection by the protection system.

The practical significance of the results

The methodological bases of information, technological and organizational direction developed in the dissertation work became the basis of creation of information technology,

which provides increase of efficiency of process management of mineral fertilizers production by protecting critical resources.

The following results are considered practically significant:

- the methodology of optimization for protection system of critical resources for production of mineral fertilizers has been developed;

- the optimal control system for the production of granular mineral fertilizers in a fluidized bed with LQR-regulator has been developed;

- the methodology of information technology usage for critical resources protection of mineral fertilizers production has been developed.

The results of the dissertation were tested and used in the following organizations and institutions:

• in “INFOZAHYST” R&P center” LLC by the projects implementation;

• in the educational process of the National Aviation University during the teaching of disciplines "Security of information and communication systems and networks", "Design of security systems for information and communication systems and networks", "Information and communication systems and networks".

The implementation data are confirmed by relevant documents.

Key words: information technology, mineral fertilizers production, critical resources, mathematical model, simulation model, methodology, optimization method, information protection system, optimal control system.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації у виданнях, що входять до міжнародної наукометричної бази даних (Scopus)

1. Galata L.P., Korniyenko B.Y., Yudin A.K. Research of the simulation polygon for the protection of critical information resources. *Information Technologies and Security (ITS 2017):* CEUR Workshop Proceedings, Selected Papers of the XVII International Scientific and Practical Conference*,* Kyiv. 2017. Vol. 2067. P. 23-31.

Особистий внесок автора: дослідження процесу побудови імітаційного полігону як способу вивчення поведінки системи захисту критичних інформаційних

ресурсів, розробка і реалізація топології полігону, випробування побудованого імітаційного полігону.

2. Korniyenko B., Galata L., Ladieva L. Security estimation of the simulation polygon for the protection of critical information resources. *Information Technologies and Security (ITS 2018):* CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference, Kyiv. 2018. Vol. 2318. P. 176-187.

   Особистий внесок автора: Розглянуто відомі вразливості програмно-апаратного забезпечення полігону і розраховано стійкість побудованої мережі до конкретних загроз методом iRisk.

3. Korniyenko B., Galata L. Implementation of the Information Resources Protection Based on the CentOS Operating System. *Proceedings of 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering*, Lviv. 2019. P. 1007-1011.

   Особистий внесок автора: п*обудована захищена топологія мережі на базі EVE, налаштовані програмно-апаратні засоби захисту інформації, проведені тести на проникнення з використанням Kali Linux.*

4. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. *Information Technologies and Security (ITS 2019)*: CEUR Workshop Proceedings, Selected Papers of the XIX International Scientific and Practical Conference, Kyiv. 2019. Vol. 2577. P. 281-291.

   Особистий внесок автора: запропонована математична модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних інформаційних ресурсів, розроблена та наведена на основі цієї моделі методика виявлення актуальних загроз безпеки.

5. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. *2019 IEEE Inernational Conference on Advanced Trends in Information Theory:* IEEE ATIT - Conference Proceedings, Kyiv. 2019. P. 244-248.

   Особистий внесок автора: конфігурація та налаштування компонентів мережі в GNS3, розробка програмного чотирьох-компонентного модуля захисту за

допомогою технології ASP.NET Core, проведення тестування стійкості системи до атак типу XSS та SQL Injection.

6. Galata L.P., Korniyenko B.Y. Research of the Training Ground for the Protection of Critical Information Resources by iRisk Method. *Mechanisms and Machine Science.* 2020. Vol. 70. P. 227-237.

   Особистий внесок автора: визначено оптимальну методологію iRisk для тестування системи захисту інформації на базі імітаційного полігону захисту критичних інформаційних ресурсів, протестована система захисту полігону з використанням оцінки вразливостей CVSS, проаналізовані чисельні показники значень iRisk для побудованого полігону кібербезпеки.

7. Korniyenko, B., Ladieva, L., Galata, L. Control system for the production of mineral fertilizers in a granulator with a fluidized bed. *2020 2nd IEEE International Conference on Advanced Trends in Information Theory:* ATIT 2020 – Proceedings. 2020. P. 307–310, 9349344.

   Особистий внесок автора: розробка оптимальної системи керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором.

8. Korniyenko B.Y., Ladieva L. R., Galata L.P. Mathematical Model of Heat Transfer Process of Production of Granulated Fertilizers in Fluidized Bed. *ARPN Journal of Engineering and Applied Sciences.* 2021. Volume 16, Issue 20. P. 2126-2131.

   Особистий внесок автора: розробка математичної моделі теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі з контролем вологовмісту гранул.

Публікації у наукових фахових виданнях України

9. Korniyenko B. Y., Galata L. P. Design and research of mathematical model for information security system in computer network. *Наукоємні технології.*2017.Т. 2, №34. С. 114-118.

   Особистий внесок автора: порівняльний аналіз підходів моделювання комп'ютерних мереж, дослідження функціональних можливостей пакету GNS3, вибір основних елементів і організація мережної взаємодії з урахуванням вимог з безпеки для системи захисту інформації комп'ютерної мережі.

10. Корнієнко Б.Я., Галата Л.П. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. *Наукоємні технології.*2017. Т.4,№36. С. 316-322.
Особистий внесок автора: проведено аналіз програмних засобів для проведення тестування побудованого полігону кібербезпеки, проведено сканування мережі та портів мережних пристроїв, реалізовано протидію розглянутим атакам.
11. Корнієнко Б.Я., Галата Л.П. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. *Моделювання та інформаційні технології: зб. наук. пр. Нац. акад. наук України, Ін-т пробл. моделювання в енергетиці ім. Г. Є. Пухова.* 2018. Вип. №83. С. 34-42.
Особистий внесок автора: оцінка рівня захищеності мережі методом iRisk для побудованого імітаційного полігону захисту критичних інформаційних ресурсів.
12. Korniyenko B., Galata L. Modeling of information security system in computer network. *Безпека інформаційних систем і технологій.* 2019. Т.1, №1. С. 36-41.
Особистий внесок автора: дослідження задач поведінки системи інформаційної безпеки з використанням імітаційного моделювання, моделювання системи на основі Graphical Network Simulator, тестування проникнення та аудиту безпеки на основі Kali Linux.
13. Галата Л.П., Корнієнко Б.Я., Заболотний В.В. Математична модель протидії загрозам у системі захисту критичних інформаційних ресурсів. *Наукоємні технології.* 2019. Т.3, №43. С. 300-306.
Особистий внесок автора: дослідження математичної моделі протидії загрозам у системі захисту критичних інформаційних ресурсів, одержання перехідних характеристик для станів системи.
14. Корнієнко Б.Я., Галата Л.П. Метод IRISK для оцінки рівня захищеності імітаційного полігону захисту критичних інформаційних ресурсів. *Вісник Університету «Україна».* Серія: Інформатика, обчислювальна техніка та кібернетика. 2019. Т.2, №23. С. 288-296.
Особистий внесок автора: визначено оптимальний метод тестування системи захисту інформації в контексті побудованого імітаційного полігону захисту критичних інформаційних ресурсів.

15. Галата Л.П., Корнієнко Б.Я. Дослідження системи захисту інформації корпоративної мережі на основі GNS3. *Наукоємні технології.* 2020. Т.2, №46. С. 172-179.

    Особистий внесок автора: розроблено систему, яка складається зі спільно взаємодіючих між собою мікросервісів (Gateway, Firewall, Digital Signature Verifier та Logger), для забезпечення захисту від SQL Injection та Cross-site scripting.

16. Корнієнко Б.Я., Ладієва Л.Р., Галата Л.П. Оптимальна система управління виробництвом мінеральних добрив у грануляторі із пседозрідженим шаром. *Новітні технології.* 2021. Т.2, № 12. С. 18-28.

    Особистий внесок автора: розробка оптимальної системи керування з LQR-регулятором на базі запропонованої математичної моделі теплообміну процесу виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі.

Патент на корисну модель

17. Спосіб забезпечення управління доступом у захищених багатомашинних автоматизованих системах із виявлення загроз: пат. 132248 Україна: МПК(2019.01), G06F 13/00, G06F 21/00, H04L 9/00. № u 2018 03740; заявл. 06.04.2018; опубл. 25.02.2019, Бюл. № 4, 4 с.

    Особистий внесок автора: запропоновано спосіб забезпечення управління доступом у захищених багатомашинних автоматизованих системах із виявлення загроз шляхом застосування мандатного контролю доступу Red Hat Enterprise Linux та використання загальної політики безпеки.

Публікації у збірниках матеріалів конференцій

18. Галата Л.П., М.С. Мариняк. Оцінка та менеджмент ризиків корпоративної мережі. *ПОЛІТ. Сучасні проблеми науки. Комп'ютерні технології:* тези доповідей XV міжнародної науково-практичної конференції молодих учених і студентів, Київ. 2015. С. 4.

    Особистий внесок автора: розглянуто Стандарти менеджменту інформаційної безпеки у контексті існуючих бізнес-ризиків організації.

19. Галата Л.П., Козюберда О.В. Моделювання безпеки комп'ютерної системи. *Комп'ютерні системи та мережні технології (CSNT-2015):* Збірник тез VIII Міжнародної науково-технічної конференції, Київ. 2015. С. 15-16.

Особистий внесок автора: проведено аналіз моделей безпеки комп'ютерних систем, визначені основні задачі безпеки.

20. Галата Л.П., Колесник Н.І. Дослідження моделей безпеки комп'ютерних систем. *ПОЛІТ. Сучасні проблеми науки. Комп'ютерні технології*: тези доповідей XVI міжнародної науково-практичної конференції молодих учених і студентів, Київ. 2016. С. 14.

Особистий внесок автора: запропоновано спільне використання моделей безпеки Белла-ЛаПадули і Біба.

21. Yudin O.K., Kornienko B.Y., Галата Л.П. Risk estimation of information system. *Wschodnioeuropejskie Czasopismo Naukowe.* 2016. № 5.3. P. 35 – 40.

Особистий внесок автора: проведено розрахунок ймовірності настання загроз, можливих втрат та оцінка ризиків для систем захисту інформаційних ресурсів.

22. Galata L.P., Kozuberda O.W. Modeling of security and risk assessment in information and communication system. *Sciences of Europe*. 2016. V. 2, No 2 (2). P. 61-63.

Особистий внесок автора: проаналізовано базову модель безпеки комп'ютерних систем з оцінкою інформаційних ризиків щодо класу загроз та змодельовано відповідну комп'ютерну систему.

23. Корнієнко Б.Я., Галата Л.П., Удовенко Б.В. Імітаційне моделювання системи захисту інформації комп`ютерної мережі. *Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту (ISDMCI'2016*): Збірка наукових праць міжнародної наукової конференції, Херсон. 2016. С. 77 - 79.

Особистий внесок автора: запропоновано використання прикладного програмного забезпечення GNS3 для моделювання комп'ютерної мережі.

24. Галата Л.П., Пасічник П.В. Захист інформаційно-комунікаційної мережі на основі розширеної моделі OSI. *ПОЛІТ. Сучасні проблеми науки. Комп'ютерні технології*: тези доповідей XVII міжнародної науково-практичної конференції молодих учених і студентів. Київ: НАУ. 2017. С. 6.

Особистий внесок автора: запропоновано розширити модель OSI додавши «Рівень політик» та «Рівень користувачів».

25. Galata L. Modeling of information security system in computer network. *VII Miedzynarodowa konferencja studentow oraz doktorantow "Inzynier XXI wieku",* Series: Monogrpah, Projekt interdyscyplinarny projektem XXI wieku, Bielsko-Biala. 2017. Poland: ATH. Tom 2. P. 75-82.
26. Korniyenko B., Galata L., Yudin A. Research of the simulation polygon for the protection of critical information resources. *Информационные технологии и безопасность: Материалы XVII Международной научно-практической конференции ИТБ-2017*, Київ. 2017. С. 35-51.

    Особистий внесок автора: запропоновано імітаційне моделювання для дослідження процесу побудови імітаційного полігону захисту критичних інформаційних ресурсів.
27. Korniyenko B.Y., Galata L.P.,. Borysenko O.V. Research and analysis of the information security mathematical models. *Materials of the XIV International scientific and practical Conference Cutting-edge science*, Sheffield. UK: Science and education LTD, 2018. P. 51-52.

    Особистий внесок автора: аналіз забезпечення інформаційної безпеки інформаційних технологій в контексті обгрунтування методів і моделей оцінки і оптимізації процесів виробництва мінеральних добрив.
28. Корнієнко Б.Я., Галата Л.П., Борисенко О.В. Математичне моделювання системи захисту інформаційних ресурсів. *Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту*: Матеріали міжнародної наукової конференції, Херсон. 2018. С. 69-71.

    Особистий внесок автора: запропоновано в якості елемента математичного апарату інформаційної безпеки використання загрози вразливості.
29. Корнієнко Б.Я., Галата Л.П. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів. *Прикладні системи та технології в інформаційному суспільстві*: зб. тез доповідей і наук. повідомл. учасників ІІ Міжнародної науково-практичної конференції, Київ. 2018. С. 77-80.

Особистий внесок автора: тестування імітаційного полігону захисту критичних інформаційних ресурсів програмними засобами, проведення сканування мережі і портів мережних пристроїв.

30. Корнієнко Б.Я., Галата Л.П. Визначення методу аналізу ризиків для імітаційного полігону захисту критичних інформаційних ресурсів. *Прикладні системи та технології в інформаційному суспільстві*: зб. тез доповідей і наук. повідомл. учасників II Міжнародної науково-практичної конференції, Київ. 2018. С. 80-83.
Особистий внесок автора: запропонована оптимальна методологія для тестування системи захисту інформації на базі імітаційного полігону захисту критичних інформаційних ресурсів.
31. Galata L.P., Korniyenko B.Y. Analyzing information risks of the simulation polygon for protection of the critical information resources, *The Eighth World Congress "AVIATION IN THE XXI-st CENTURY" Safety in Aviation and Space Technologies*, Київ. 2018. С. – 2.3.18-2.3.21.
Особистий внесок автора: розрахунок стійкості мережі до конкретних загроз з використанням методу iRisk.
32. Галата Л.П. Інформаційно-комунікаційні мережі на основі розширеної моделі OSI. *Інформаційні технології та взаємодії*: матеріали V міжнародної науково-практичної конференції, Київ. 2018. С. 375-376.
33. Korniyenko B.Y., Galata L.P., Ladieva L.R. Security estimation of the simulation polygon for the protection of critical information resources. *Информационные технологии и безопасность*: Материалы XVIII Международной научно-практической конференции ИТБ-2018, Київ. 2018. Вип.18. С. 183-196.
Особистий внесок автора: запропоновано використання методу iRisk для проведення розрахунку стійкості побудованої мережі до конкретних загроз, порівняння результатів.
34. Korniyenko B.Y., Zabolotnyi V.V., Galata L.P. System of protection of critical information resources of technological process. *Prospects of world science:* Materials of the XV International scientific and practical Conference, Sheffield. Science and education LTD, 2019. P. 59-60.

Особистий внесок автора: роз'яснення поняття функціональної безпеки, з точки зору цілісності і доступності критично важливих параметрів технологічного процесу.

35. Korniyenko B.Y., Galai Y.O., Galata L.P. Construction and testing of information protection system of corporate network. *Nauka: teoria i praktyka – 2019:* Materiały XV Międzynarodowej naukowi-praktycznej konferencji. Przemyśl: Nauka i studia, 2019. Volume 7. P. 53-55.

    Особистий внесок автора: розглянуто процес тестування системи захисту від веб-атак.

36. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. *Информационные технологии и безопасность*: Материалы XIX Международной научно-практической конференции ИТБ-2019, Київ. 2019. С. 86-92.

    Особистий внесок автора: запропоновано використання математичного моделювання для визначення стійкості до загроз систем захисту критичних інформаційних ресурсів.

37. Korniyenko B.Y., Ladieva L.R., Galata L.P. System of automated control of the process of production of mineral fertilizers in the fluidized bed. *Science without borders – 2020:* Materials of the XVI International scientific and practical Conference, Sheffield. Science and education LTD, 2020. P. 24-27.

    Особистий внесок автора: розроблено оптимальну систему керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором.

38. Корнієнко Б.Я., Ладієва Л.Р., Галата Л.П. Математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдорозрідженому шарі. *Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту*: матеріали міжнар. наук. конф., Херсон. 2020. С. 77-79.

    Особистий внесок автора: розроблено математичну модель, яка враховує гідродинаміку псевдозрідженого шару, а також кінетику процесів грануляції та зневоднення.

39. Korniyenko B., Ladieva L., Galata L. Mathematical model of heat transfer process of production of granulated fertilizers in fluidized bed. *Математичне та імітаційне моделювання систем. МОДС 2020:* тези доповідей П'ятнадцятої міжнародної науково-практичної конференції. Чернігів: ЧНТУ, 2020. С. 84 -87.

Особистий внесок автора: проаналізовано використання математичного моделювання в процесі виробництва мінеральних добрив.

40. Korniyenko B., Galata L., Ladieva L. Optimization of critical information resources protection system. *Інформаційні технології і безпека*: матеріали XX Міжнародної науково-практичної конференції ІТБ-2020, Київ. 2020. Випуск 20. С. 28-29.

Особистий внесок автора: запропоновано для розв`язання задачі оптимізації використання імітаційного моделювання системи захисту критичних ресурсів виробництва мінеральних добрив та математичного моделювання протидії загрозам.

41. Корнієнко Б.Я., Фесенко С.А., Галата Л.П. Оптимальна система управління виробництвом мінеральних добрив у грануляторі із пседозрідженим шаром. *Автоматика 2020*: матеріали XXVI Міжнародної конференції з автоматичного керування, Київ. 2020. С. 87-88.

Особистий внесок автора: отримання перехідного процесу для LQR-регулятора під час переведення системи до заданої температури.

42. Заболотний В.В., Корнієнко Б.Я., Галата Л.П. Оцінка ризиків в системах захисту інформації критичних ресурсів. *Science without borders*: Materials of the XVII International scientific and practical Conference, Sheffield. Science and education LTD, 2021. P 66-71.

Особистий внесок автора: обчислення значення оцінки ризиків, що використовується для оцінки ефективності системи захисту критичних ресурсів виробництва мінеральних добрив.

ЗМІСТ

ВСТУП

Актуальність теми

В даний час інформаційні технології є необхідним атрибутом підвищення ефективності функціонування підприємств, оскільки дають можливість зниження витрат на виробництво, підвищення ефективності управління, вибору правильної стратегії та тактики розвитку в умовах ринку, що швидко змінюється. Однією з найважливіших характеристик інформаційних технологій є забезпечення конфіденційності інформації при її введенні, виведенні, передачі, обробці та зберіганні, а також стійкість до її розкрадання, знищення чи спотворення. Предметом захисту є дані, що містять конфіденційну інформацію, які зберігаються, обробляються та передаються між елементами інформаційних технологій.

Також пріоритетом інформаційних технологій є забезпечення доступності та цілісності керуючої та конфігураційної інформації про параметри технологічного процесу, тобто забезпечення саме функціональної безпеки. Особлива увага приділяється запобіганню несанкціонованому доступу до системи з метою збереження стабільного функціонування інформаційних технологій. Висока вартість досліджень захищеності інформаційних технологій для управління технологічними процесами визначає необхідність побудови імітаційної моделі захисту критичних інформаційних ресурсів.

Серед найважливіших галузей, у яких інформаційні технології грають визначальну роль, особливу увагу займає управління технологічними процесами виробництва мінеральних добрив. Використання гранулятора із псевдозрідженим шаром для виробництва мінеральних добрив дозволяє поєднати декілька етапів технологічного процесу в одному пристрої: сушіння, випаровування, кристалізацію та грануляцію.

Аналіз результатів досліджень, проведених у напрямку забезпечення інформаційної безпеки саме для таких складних неперервних виробництв та систем захисту їх критичних ресурсів, показує, що наразі питання наукового обґрунтування системи захисту інформації до кінця не вирішені. Насамперед йдеться про методи та моделі оцінки та оптимізації систем захисту інформації, які в контексті сучасних

тенденцій організації виробництва відіграють вирішальну роль в успіху підприємства. Для покращення ситуації з захищеністю підприємства від загроз порушення інформаційної безпеки необхідно вибрати оптимальний варіант системи захисту інформації.

Значний внесок у розвиток теорії інформаційних технологій та розробки ефективних систем захисту критичних інформаційних ресурсів зроблено у працях вітчизняних вчених ,таких як Гнатюк С.О., Корченко О.Г., Конахович Г.Ф., Корнієнко Б.Я., Пищик Б.Н., Демидович Д.І., Астахов А.А. та інші. Так, в працях Курилова Ф.М., Росенка О.П., Шувалова І.О., Шорова А. В. отримано вагомі результати з питань математичного моделювання систем захисту інформації та побудови імітаційних моделей. Найбільш вагомих результатів у цьому напрямку досягнуто закордонними дослідниками К. Фенріхом, М. Найделом, Т. Паулі, Е. Байресем.

Разом з тим, як розглянуті роботи не вирішують завдань комплексного підходу та не враховують специфіку управління технологічними процесами виробництва мінеральних добрив і не мають механізмів формалізації та алгоритмізації процесів захисту критичних ресурсів таких виробництв.

Тому існує нагальна потреба в подальшому дослідженні методів та засобів захисту критичних ресурсів виробництва мінеральних добрив з метою їх удосконалення. А розробка моделей, методу та інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив є надзвичайно актуальною на сьогоднішній день. Таким чином, усе це і зумовило необхідність вирішення актуальної науково-технічної задачі забезпечення необхідного рівня захищеності критичних ресурсів виробництва мінеральних добрив за рахунок розроблених моделей, методу та створення і використання нової інформаційної технології.

Зв’язок роботи з науковими програмами, планами, темами

Дисертаційна робота пов’язана з планами науково-дослідної та навчальної роботи і відповідає тематичній спрямованості наукових розробок, що здійснювалися у Національному авіаційному університеті, та, зокрема кафедри комп’ютеризованих систем захисту інформації, а саме в рамках держбюджетних науково-дослідних робіт: у 2011 р. «Методологія та технології організації комплексної системи захисту

інформації вищого навчального закладу України» (шифр №0111U000172); у 2014–2015 рр. «Інформаційні технології оптимального управління процесами виробництва мінеральних добрив» (шифр №27/09.01.09); у 2019–2021 рр. «Інформаційна технологія організації імітаційного полігону захисту критичних інформаційних ресурсів» (шифр № 43/09.01.09), автор дисертації брав участь у якості відповідального виконавця.

Мета і задачі дослідження

Метою дисертаційної роботи є узагальнення, розвиток та розробка моделей, методу та інформаційної технології захисту критичних ресурсів виробництва мінеральних добрів з урахуванням вимог підвищення функціональної безпеки та забезпечення заданої якості готового продукту.

Досягнення поставленої мети передбачає розв’язання таких задач:

- провести аналіз проблемних задач в ході інформаційного захисту інформації, моделей загроз і особливостей їх реалізації, імітаційного моделювання систем захисту критичних інформаційних ресурсів та методів оптимізації систем захисту інформації;
- виявити, формалізувати та розробити математичну модель протидії загрозам у системі захисту критичних інформаційних ресурсів виробництва мінеральних добрив;
- розробити імітаційну модель захисту критичних інформаційних ресурсів виробництва мінеральних добрив;
- розробити метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив;
- розробити математичну модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі;
- створити інформаційну технологію захисту критичних ресурсів виробництва мінеральних добрив на основі розроблених моделей та методу;
- розробити оптимальну систему керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором.

Об'єкт дослідження – інформаційні процеси захисту критичних ресурсів виробництва мінеральних добрив при зневодненні та гранулюванні у псевдозрідженому шарі.

Предмет дослідження – методи та моделі захисту критичних інформаційних ресурсів, системи захисту критичних інформаційних ресурсів для інформаційно-комунікаційної системи виробництва мінеральних добрив.

Методи досліджень. Для вирішення поставлених задач у дисертаційній роботі використовувались методи математичного моделювання (при розробці математичної моделі теплообміну гранульованих мінеральних добрив у пседозрідженому шарі), числові методи розв’язання диференціальних рівнянь (у процесі розрахунку математичної моделі протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних ресурсів виробництва мінеральних добрив), методи теорії оптимального керування (при розробці методу оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив).

Наукова новизна отриманих результатів

На підставі теоретичних і практичних досліджень, виконаних у дисертаційній роботі

вперше

- розроблено метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив на основі імітаційної моделі системи захисту критичних ресурсів виробництва мінеральних добрив та математичної моделі протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив, що дозволяє на основі одержаних значень інтенсивностей переходів та станів системи підвищити рівень захищеності критичних ресурсів виробництва мінеральних добрив від впливу внутрішніх та зовнішніх загроз;
- розроблено математичну модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі, яка враховує зміни основних характеристик виробництва гранул у псевдозрідженому шарі, що дозволяє забезпечити необхідну якість готового продукту;

– розроблено інформаційну технологію захисту критичних ресурсів виробництва мінеральних добрив, основними компонентами якої є наступні засоби: моделювання системи захисту критичних ресурсів виробництва мінеральних добрив, оптимізація системи захисту критичних ресурсів виробництва мінеральних добрив, система захисту критичних ресурсів виробництва мінеральних добрив, математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі та оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором. Розроблена інформаційна технологія забезпечує урахування вимог підвищення функціональної безпеки та забезпечення заданої якості готового продукту;

удосконалено

– імітаційну модель захисту критичних ресурсів виробництва мінеральних добрив, на базі GNS3 та KaliLinux, яка адаптована до структури мереж та систем захисту інформаційних ресурсів критичної інфраструктури, з метою комплексної оцінки запропонованих заходів і засобів захисту критичних інформаційних ресурсів;

отримала подальший розвиток

– математична модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних ресурсів виробництва мінеральних добрив та запропонована на основі цієї моделі методика виявлення актуальних загроз безпеки, що дозволяє розглядати поведінку системи при дії на неї кожного типу загроз окремо і визначати імовірності їх появи і відбиття ситемою захисту.

Практичне значення отриманих результатів

Одержані в дисертаційній роботі результати стали підґрунтям створення інформаційної технології, що забезпечує підвищення ефективності управління процесом виробництва мінеральних добрив за рахунок захисту критичних ресурсів.

Практично вагомими вважаються такі результати:

- методика оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив;
- оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором;
- методика використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив.

Результати дисертаційної роботи апробовано і використано у таких організаціях та установах:

- у ТОВ «НВЦ «ІНФОЗАХИСТ» при реалізації проєктів;
- у навчальному процесі Національного авіаційного університету під час викладання дисциплін «Безпека інформаційно-комунікаційних систем та мереж», «Проєктування систем безпеки ІКСМ», «Інформаційно-комунікаційні системи та мережі».

Дані про впровадження підтверджено відповідними документами.

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи отримані автором самостійно. У працях, опублікованих у співавторстві, особистий внесок автора полягає в наступному: в [1] розроблено та реалізовано імітаційну модель захисту критичних інформаційних ресурсів на базі прикладного програмного забезпечення GNS3; в [2, 6, 11] проведено розрахунок показників захищеності моделі захисту критичних інформаційних ресурсів методом iRisk; в [3] проведено дослідження задач захисту інформаційних ресурсів на базі CentOS; в [4, 13] розробка методики знаходження актуальних загроз безпеці даних при їх обробці, проведення розрахунків імовірностей знаходження математичної моделі інформаційної системи захисту критичних інформаційних ресурсів в одному з чотирьох станів; в [5, 15] розробка програмного рішення в галузі захисту інформації корпоративних мереж з чотирьох компонентів захисту на основі патерну «мікросервісної архітектури»; в [7, 16] розробка оптимальної системи керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором; в [8] розроблено математичну модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі; в [9, 12] побудова імітаційної моделі системи захисту

інформації комп'ютерної мережі в програмному середовищі моделювання GNS3; в [10] проведено випробовування імітаційної моделі захисту критичних інформаційних ресурсів; в [14] розрахунок стійкості побудованої моделі захисту критичних інформаційних ресурсів до розглянутих загроз.

Апробація результатів дисертаційної роботи. Основні наукові положення, результати, рекомендації та висновки дисертаційної роботи доповідались та обговорювались на науково-технічних конференціях: VIII Міжнародна науково-практична конференція «Комп'ютерні системи та мережні технології» (м. Київ, квітень 2015 року); Міжнародна науково-практична конференція «Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту» (с. Залізний Порт, травень 2016, 2018, 2020 років); Miedzynarodowa konferencja studentow oraz doktorantow "Inzynier XXI wieku" (м. Бєльсько-Бяла, грудень 2017, 2018 років); Міжнародна науково-практична конференція «Информационные технологии и безопасность» (м. Київ, листопад 2017, 2018, 2019, 2020 років); XIV International scientific and practical Conference Cutting-edge science – 2018 (м. Шеффілд, травень 2018 року); II Міжнародна науково-практична конференція «Прикладні системи та технології в інформаційному суспільстві» (м. Київ, жовтень 2018 року); The Eighth World Congress "AVIATION IN THE XXI-st CENTURY" Safety in Aviation and Space Technologies (м. Київ, жовтень 2018 року); V Міжнародна науково-практична конференція «Інформаційні технології та взаємодії» (м. Київ, листопад 2018 року); IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (м. Львів, липень 2019 року); XV International scientific and practical Conference Prospects of world science – 2019 (м. Шеффілд, серпень 2019 року); XV Międzynarodowej naukowi-praktycznej konferencji «Nauka: teoria i praktyka - 2019» (м. Перемишль, серпень 2019 року); IEEE Inernational Conference on Advanced Trends in Information Theory (м.Київ, 2019, 2020 років); XVI International scientific and practical Conference Science without borders (м. Шеффілд, квітень 2020, 2021 років); П'ятнадцята міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2020» (м. Чернігів, червень 2020 року); XXVI Міжнародна конференція з автоматичного керування (м. Київ, жовтень 2020 року).

Крім того, результати дисертаційної роботи були обговорені на науково-технічних семінарах кафедри комп’ютеризованих систем захисту інформації, науково-практичних конференціях молодих учених і студентів «ПОЛІТ. Сучасні проблеми науки», які проводилися в Національному авіаційному університеті.

Публікації. Основні положення та результати дисертаційного дослідження викладено в 42 наукових публікаціях, серед них 8 публікацій у виданнях, що входять до міжнародної наукометричної бази даних (Scopus); 8 публікацій у наукових фахових виданнях України; 1 патент на корисну модель, 25 публікацій у збірниках матеріалів конференцій.

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Робота містить 197 сторінок, з них 148 – основного тексту, 53 рисунки, 5 таблиць, 2 додатки, список літературних джерел налічує 87 найменувань.

РОЗДІЛ 1. СИСТЕМНИЙ АНАЛІЗ ТА ОГЛЯД ТЕХНОЛОГІЙ, МАТЕМАТИЧНИХ МОДЕЛЕЙ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ЗАХИСТУ РЕСУРСІВ ВИРОБНИЦТВА МІНЕРАЛЬНИХ ДОБРИВ

1.1. Застосування методів моделювання систем захисту інформації

Для реалізації комплексного підходу до вирішення завдання забезпечення інформаційної безпеки необхідно використовувати такі наукові методи, як моделювання систем та процесів захисту інформації. Цілями такого моделювання є пошук оптимальних рішень щодо управління системою захисту інформації, оцінка ефективності використання різних механізмів захисту, визначення властивостей системи захисту, встановлення зв'язку між її характеристиками та показниками.

Наведемо основні види моделей, що використовуються на практиці для опису різних процесів і систем захисту інформації. Оскільки загальною ознакою будь-яких моделей є їх спроможність відображати головні для цілей дослідження признаки об'єктів, то найбільш відомими ознаками будуть: способи реалізації моделей, характер процесів і явищ, які відбуваються у системі, характер підходу до моделювання об'єкта, призначення й специфіка об'єктів дослідження, ступінь узагальнення характеристик об'єктів дослідження [1].

Відомо, що модель є логічним або математичним описом компонентів і функцій, що відображають властивості об'єкта або процесу, що моделюється, і використовується як умовний опис, призначений для спрощення їх дослідження. Для того, щоб захист інформації був максимально ефективним, використовується математичне моделювання, що дозволяє формалізувати параметри безпеки розподілених систем і вибрати найбільш оптимальний варіант, виходячи з конкретних умов роботи системи. Моделювання системи захисту інформації полягає в її формалізованому представленні в будь-якому вигляді, відповідному системі, що вивчається, і отриманні за допомогою побудованої моделі необхідних характеристик реальної системи. Таким чином, весь процес моделювання можна розділити на дві

складові: побудова моделі та реалізація моделі з метою отримання необхідних характеристик системи захисту інформації. Застосування моделей, як спрощених описів важливих компонентів системи, дає змогу спростити розв'язок завдання створення адекватної реальним загрозам системи захисту, розбити цей процес на ряд етапів, провести попереднє дослідження, зокрема із застосуванням комп'ютерної техніки, можливих варіантів побудови систем захисту, вивчити на моделі поведінки системи захисту в різних ситуаціях. Аналіз моделей захисту та перенесення їх на конкретну структуру програмних засобів, операційних систем, системи управління базами даних та на автоматизовану систему загалом здійснюють на етапі проєктування та техноробочому етапі створення систем захисту [1].

Основу моделей забезпечення безпеки інформації складають такі теорії: формально-евристичний підхід; теорія ймовірностей і випадкових процесів; еволюційне моделювання; теорія графів, автоматів та мереж Петрі; теорії ігор та конфліктів; теорія катастроф; теорія нечітких множин; ентропійний підхід. Відмінності більшості моделей полягають в тому, які параметри вони використовують в якості вхідних, а які - наводять у вигляді вихідних після проведення розрахунків. Крім того, останнім часом широкого поширення набувають методи моделювання, засновані на неформальній теорії систем: методи структурування, методи оцінювання та методи пошуку оптимальних рішень [2]. Методи структурування є розвитком формального опису, що поширюється на організаційно-технічні системи. Використання цих методів дозволяє уявити архітектуру і процеси функціонування складної системи у вигляді, що задовольняє наступним умовам: повнота відображення основних елементів і їх взаємозв'язків; простота організації елементів і їх взаємозв'язків; гнучкість - простота внесення змін до структури і т. д. Методи оцінювання дозволяють визначити значення характеристик системи, які не можуть бути виміряні або отримані з використанням аналітичних виразів, або в процесі статистичного аналізу, - ймовірності реалізації загроз, ефективність елемента системи захисту та ін. в основу таких методів належить експертне оцінювання - підхід, що полягає в залученні фахівців у відповідних галузях знань для отримання значень деяких характеристик.

Найбільш часто в публікаціях по заданій тематиці використовуються механізми нечіткої логіки. Наприклад, в роботі [3] ставиться завдання підвищення ефективності процесу управління ризиками безпеки інформаційних систем і обґрунтованості вибору захисних заходів в нечітких умовах. В роботі розроблена методика оцінки і управління ризиками безпеки в нечітких умовах, в якій запропоновано алгоритми для оцінки властивостей елементів систем, здійснено обґрунтований вибір нечітких шкал для оцінки властивостей елементів інформаційних систем, а також запропонований метод нечіткого узгодження думок експертів.

Для нечіткої оцінки властивостей об'єктів пропонується серед вимірювальних шкал ввести впорядковані множини нечітких змінних, що характеризують властивості інших об'єктів. Модель інформаційного ресурсу для задач оцінки і управління ризиками безпеки представлена у вигляді вектора нечітких базових характеристик.

Для оцінки рівня ризику інформаційній безпеці пропонується наступна теоретико-множинна модель інформаційної системи:

$$IS = \{R, \mathrm{T}, V, \mathrm{C}, Rel\},$$

де R - множина ресурсів, T - множина загроз, V – множина вразливостей, C – множина контрзаходів, Rel – множина відносин між елементами інформаційної системи.

Задача управління ризиками представлена у вигляді задачі мінімізації цільової функції $Risk(IS(E)) \rightarrow min$.

Також нечітка логіка застосовується в [4]. В даній роботі модифіковано метод нечіткого програмування та запропоновано алгоритми, що дозволяють здійснити вибір оптимальних структур багаторівневого інформаційного комплексу.

Також методи нечіткої логіки використовуються для оцінювання якості інформаційного захисту в розподілених системах. Наприклад, в [5] розроблено комплексний підхід до оцінки проєктування системи захисту інформації; прогноз її ефективності; аналіз всіх можливих слабких місць системи, можливої поведінки системи і оцінка стійкості системи.

Інший підхід оцінювання засобів захисту інформації розглянуто в [6]. У даній роботі запропонована і досліджена математична модель вибору засобів захисту персональних даних, які обробляються в інформаційних системах передачі даних, заснована на рішенні задачі багатокритеріальної оцінки альтернатив в умовах різної важливості критеріїв, що дозволяє здійснити вибір необхідних засобів захисту інформаційних систем передачі даних.

Спочатку визначається оцінка засобів захисту по різним коефіцієнтам. З урахуванням вагових коефіцієнтів будуються множини $M^{\lambda i}C_i$.

В результаті в якості оптимального рішення вибирається те, для якого функція приналежності є максимальною, тобто:

$$\mu_P(Me_j^*) = max_{i=\overline{1,n}}(\mu_P(Me_j)) .$$

Також в різних публікаціях зустрічається нейронномережний підхід до вирішення задачі оптимізації розміщення засобів захисту інформації. Найбільш яскраво він виражений в [7]. У даній роботі показано, що можливість визначення складу засобів захисту інформаційних систем і великих обсягів інформації може бути забезпечена шляхом вирішення низки завдань цілочисельної оптимізації із застосуванням обробки багатовимірних даних в нейронномережному базисі. Сукупність активних нейронів інтерпретується як план призначень засобів захисту системи.

Також подібний підхід використовується в [8]. У даній роботі запропонована комбінована модель і алгоритми захисту комп'ютерних мереж від інфраструктурних атак на основі підходу «нервова система мережі».

Таким чином, можна зробити висновок, що найбільш часто використовуваними підходами, при вирішенні задач оптимізації розміщення засобів захисту інформації, є механізми нечіткої логіки і підхід нейронних мереж. Основним недоліком систем, побудованих з використанням нечіткої логіки, є менша точність обчислень у порівнянні з імовірнісним підходом. Що стосується використання нейронномережних механізмів, то їх явним недоліком є потайний характер функціонування, так як не завжди можна точно відстежити критерії, які нейронна

мережа використовує при роботі. Цікавим видається підхід, який полягає у використанні більш суворих і формалізованих методів теорії прийняття рішень. У разі використання даного підходу може бути отримано більш точне і обгрунтованіше рішення.

Що стосується методики оцінки ефективності побудованих систем, то тут можна виділити наступні підходи:

Метод кількісної оцінки показників від несанкціонованого доступу [9]:

Розрахунок проводиться за допомогою кінцевого напівмарківського процесу, що моделює динаміку функціонування системи захисту інформації для оцінки різних показників, на підставі чого формується напівмарківська матриця:

$$H_{\text{кф}}\ (t) = \ \left\| H_{\text{кф}\,ij}\ (t) \right\|, i\ = \overline{1,n}\ , j\ = \overline{1,n}\,.$$

Довільний елемент $H_{\text{кф}\,ij}\ (t)$ в матриці є ймовірністю того, що відповідний напівмарківський процес, опинившись в стані i, перейде з нього в стан j, причому за час, менший t, і визначається за такою формулою:

$$H_{\text{кф}\,ij}\ (t) = \ P_{\text{кф}\,ij}\, G_{\text{кф}\,ij}\ (t)\ i\ = \overline{1,n}\ , j\ = \overline{1,n}\,,$$

де $P_{\text{кф}\,ij}\ (t)$- ймовірності переходу напівмарківського процесу зі стану i в стан j; $G_{\text{кф}\,ij}\ (t)$ – функції розподілу часу перебування процесу в стані i.

Недоліком даної методики є велика кількість коефіцієнтів, а також деяка невизначеність в плані прийняття рішень;

Економічний підхід [10]: при розрахунку ефективності системи особлива увага приділяється економічним аспектам, проте даний метод не дає оцінки якості інформаційного захисту безвідносно до економічних факторів;

Математична оцінка захищеності інформації, головним параметром якої є час безпечного функціонування системи [11]. Недоліком методики є відсутність розгляду роботи системи в різних умовах. Основним показником виступає ТО - середній час безпечного функціонування захищеної системи з ймовірністю виключення несанкціонованого доступу не нижче $P_{\text{нсд}}$.

Обчислення робиться за формулою:

$$\text{ТО}\ = \frac{1}{s}\ = \frac{t\ (1-\ P_{\text{нсд}})}{P_{\text{нсд}}}\,.$$

Рішення задачі оптимізаційним або комбінаторним підходом [12].

У даній роботі ставиться задача мінімізації витрат на систему захисту інформації при обмеженні на заданий рівень ефективності. При цьому алгоритм рішення доповнюється процедурою пошуку максимальних елементів в кожному стовпці матриці d(ij) та розрахунком найвищого рівня ефективності P, що дорівнює сумі знайдених максимальних елементів.

В роботі [13] розрахунок поточної ефективності інформаційної безпеки здійснюється за формулою:

$$Ke(t) = \frac{\sum_i^j \Pi ni * S'_y(t) * K'_y(t)}{\sum_i^j \Pi ni * S'_y(t)},$$

де Пni - повні потенціали окремих елементів, що обчислюються за допомогою розрахункових задач визначення співвідношень ефективність-загроза; $S'_y(t)$ – поточні ступені оснащення цих елементів механізмами захисту, що визначає їх стійкість, $K'_y(t)$ - поточні ефективності управління елементами інформаційної системи.

Таким чином, після огляду існуючих підходів та математичних моделей систем захисту інформації, та оскільки важливою якістю будь-якої інформаційної системи є її здатність протистояти різноманітним загрозам, що виникають як ззовні та і всередині системи, можна зробити висновок про необхідність розробки нових моделей впливу загроз на зазначену інформаційну систему, реалізованих на базі станів системи. Це дозволить розглянути поведінку системи при дії на неї кожного типу загроз окремо та визначати імовірності їх появи і відбиття системою захисту. Використання математичного моделювання одночасно, з використанням імітаційного моделювання дозволить виявити загрози, які є реально небезпечними для інформаційної системи. Тож однією з наших цілей є запропонувати математичну модель протидії загрозам у системі захисту інформації і на основі цієї моделі розробити методику їх виявлення.

1.2. Оцінка захищеності інформації в інформаційних системах.

Однією з першочергових задач, що передують оцінці захищеності інформації, є задача вибору системи показників, яка повинна відображати всі вимоги до захисту інформації, структуру об'єкта інформатизації (ОІ), технологію та умови обробки, зберігання та передачі інформації в ній, а також враховувати можливості зловмисника до отримання інформації.

Вибір показників оцінки захищеності інформації є складним дослідницьким завданням і в постановочному плані відноситься до області прийняття рішення. Складність вибору показників, що дозволяють дати адекватну оцінку захищеності інформації, визначається [14]:

- необхідністю контролю великої кількості коштів і елементів захисту, а також заходів, спрямованих на забезпечення безпеки конфіденційної інформації;
- випадковістю зовнішніх впливів і внутрішніх загроз в системі обробки інформації та системі її захисту;
- відсутністю показників, які враховують специфіку об'єкта інформатизації і особливості його функціонування;
- необхідністю отримання не тільки якісної, але і кількісної оцінки захищеності інформації.

Існують три методологічні підходи до вирішення задач оцінки захищеності інформації: чисто аналітичний, строго теоретичний і аналітико-емпіричний.

Аналітичний підхід полягає в тому, що на основі тривалого збору і обробки фактичних даних про реальні прояви загроз інформації і розміри заподіяного збитку, встановлюються залежності між потенційно можливим збитком і коефіцієнтами, що характеризують частоту появи відповідної загрози і величину наявного при її появі розміру збитку.

Теоретичний підхід ґрунтується на оцінці потенційно можливих проявів загроз і розмірів потенційно можливого збитку, що розглядаються як випадкові події, а тому можуть бути охарактеризовані законами розподілу і числовими характеристиками.

Аналітично-емпіричний підхід певною мірою ґрунтується на синтезі основних положень аналітичного і теоретичного підходів: на основі теоретично-ймовірнісних методів будуються моделі, необхідні для визначення і прогнозування показників захищеності. А на основі збору і обробки статистичних даних, отриманих в ході теоретичних і практичних досліджень проблем захисту інформації, формулюються вихідні дані, необхідні для побудови моделей.

Для тестування системи захисту інформації інформаційних систем (ІС) періодично проводиться аналіз інформаційних ризиків, який дозволяє виявити загрози інформаційній безпеці і в свою чергу використовувати та впроваджувати відповідні міри по їх нейтралізації. Наразі існують і використовується різні методики аналізу інформаційних ризиків, основна відмінність яких заключається в шкалах оцінювання рівня ризику: кількісних чи якісних. В кількісних методиках ризику (напр. RiskWatch, Digital Security, ISRAM, iRisk) оцінка приводиться числовими значеннями, в якості вхідних даних зазвичай використовується накопичена статистика по інцидентах. Проте відсутність достатньої кількості статистичних даних призводить до зниження адекватності результатів оцінки.

Якісні методики (напр. Facilitated Risk Analysis Process (FRAP), National Institute of Standards and Technology (NIST)) являються більш поширеними, однак в них використовуються спрощені шкали, котрі містять в собі рівні ризиків. Оцінка рівня ризику проводиться на основі експертного опитування. На сьогоднішній день існує і велика кількість методик, які використовують змішану оцінку ризиків: CRAMM, Microsoft Security Assessment Tool (MSAT), ГРИФ, метод аналізу ієрархій (AHP - Analytic hierarchy process).

Для визначення оптимального методу тестування системи захисту інформації (СЗІ) необхідно провести порівняльний аналіз методів та визначити оптимальний метод в контексті побудованої моделі СЗІ.

Метод RiskWatch є одним із найпотужніших методів кількісного аналізу системи захисту інформації. Даний метод ідеально підходить, якщо треба провести аналіз ризиків на програмно-технічному рівні захисту, без врахування організаційних і

адміністративних факторів, отримані оцінки ризиків є матиматичні очікування втрат, проте вони вичерпують розуміння ризику з системних позицій.

Метод Digital Security характеризується тим, що в його основі лежить дві основні моделі оцінки ризиків: модель інформаційних потоків, а також модель загроз та вразливостей. Метод Information security risk analysis method (ISRAM) – для оцінки факторів ризику використовує опитувальні листи і вираховує рівень ризику у вигляді добутку ймовірності реалізації загрози і їх наслідків.

Метод iRisk характеризується формально однією з найпростіших оцінок кількісних ризиків інформаційної безпеки АС. В загальному вигляді розраховується за наступною формулою:

$$iRisk = (Vulnerability * Threat) - Controls$$

де Vulnerability - оцінка вразливості, Threat – оцінка загрози, Control – оцінка мір безпеки. Дана методика використовує в собі іншу методику Common Vulnerability Scoring System v3.0 (CVSS V3) для оцінки вразливостей.

Методи якісної оцінки ризиків інформаційної системи:

Метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): ввесь процес аналізу проводиться працівниками організацій без залучення сторонніх консультантів. Під час опису профіля методика OCTAVE пропонує користуватись «деревами варіантів». При оцінці ризику дається лише оцінка очікуваного збитку без оцінки ймовірності у вигляді шкали (висока, середня, низька).

Метод National Institute of Standards and Technology (NIST) – метод передбачає попереднє оцінювання потенційного збитку і ймовірності потенційного інциденту. Даний метод є зручним та простим у використанні, постійно підтримується актуальність, міститься чітке керівництво покрокової оцінки ризику ІБ, також постійно підтримується CVSS, завдяки чому детально описуються ризики для інформаційних активів. За допомогою програмного забезпечення можливий аналіз і рекомендації щодо способів зниження ризиків [14].

Методика Facilitated Risk Analysis Process (FRAP) дозволяє знайти баланс між витратами сил та засобів захисту інформації в АС та отримуваним ефектом від цього.

Під час проведення аналізу, як правило, приймають, що в системі відсутні засоби захисту інформації, що в свою чергу дозволяє показати ефект від впровадження засобів захисту інформації. Оцінка проводиться для ймовірності виникнення загрози і збитків від неї за відповідними шкалами. Після оцінки ризику визначаються контрзаходи, які дозволяють позбутися ризику або звести його вплив до прийнятного рівня і затрати на його впровадження. Потім формується звіт на основі якого оформляються політики безпеки.

Методи, що використовують змішану оцінку аналізу ризиків:

CRAMM методика містить в собі комлексний підхід до оцінки ризиків, який використовує різні профілі, що містять в собі «бази знань» необхідні для кожного виду підприємств. Дослідження ІБ проводиться в три етапи, під час першого етапу аналізується все, що пов'язане з ідентифікацією і визначенням вартості ресурсів, відбувається збір відомостей про конфігурацію системи про те, хто відповідає за фізичні і програмні ресурси, ідентифікація користувачів і те, як вони будуть використовувати ресурси (фізичні, програмні, інформаційні). Наступним кроком будується модель інформаційної системи з позиції ІБ. Далі будується дерево зв'язків використовуваних ресурсів, в якому виділяються критичні елементи. Цінність фізичних ресурсів в системі CRAMM визначається їх вартістю відновлення у випадку виведення з ладу [15].

Для даних і програмного забезпечення обираються критерії ІС, і робиться оцінка збитків по шкалі від 1 до 10. Програмне забезпечення CRAM для кожної групи ресурсів і кожного з 36 типів загроз генерує список питань, які мають мати однозначну відповідь. На основі даної інформації розраховуються рівні ризиків в діапазоні від 1 до 7. Отримані рівні вразливостей і ризиків погоджуються з замовником. Далі будується матриця ризиків в контексті ресурсу, частоти виникнення загрози і оцінка ймовірності успішності загрози. Наступним кроком будується матриця очікуваних річних втрат. І далі формується звіт з рекомендаціями відносно контрзаходів, які треба реалізувати для адекватної протидії ризикам, щоб знизити рівень ризику до прийнятного рівня.

Метод аналізу ієрархій (AHP - Analytic hierarchy process) являється систематичною процедурою, яка дозволяє структурувати проблему в вигляді ієрархії, побудувати набір альтернатив та визначити їх характерні фактори. Задавши значимість цих факторів можна порівняти і виконати кількісну оцінку альтернативних варіантів рішення. Метод використовується для побудови шкали відношень як з дискретних так і з безперервних парних порівнянь об'єктів в багаторівневих ієрархічних структурах [16].

Для оцінки інформаційного ризику ІС будується ієрархічна модель, на нижньому рівні якої розташовуються можливі альтернативи. На проміжних рівнях ієрархії розташовуються оцінки інформаційних ризиків. Найвищий рівень – інтегральна оцінка ризиків ІС. Інтегральна шкала враховує частоту виникнення ризику, частоту реалізації ризика для даної системи і ступінь збитку. Це відбувається шляхом розрахунку вектора ризику кожного окремого елемента ієрархії. Елементи порівнюються попарно по відношенню впливу їх на загальну характеристику. І в результаті обрахунку отримується кількісне значення зменшення частоти виникнення ризику та якісне значення зменшення ступеня шкоди від реалізації ризику одного засобу захисту інформації відносно інших [16].

Таким чином, розглянувши методи тестування та аналізу ризиків автоматизованих систем, було визначено оптимальний метод для оцінювання рівня захищеності системи захисту інформації в умовах реалізації загроз, в контексті імітаційної моделі СЗІ. В першу чергу, проаналізовано існуючі методи тестування і оцінки вразливостей АС для визначення їх переваг і недоліків, що полягає у кількісно-якісному оцінюванні захисту ІС для можливості подальшого співставлення затрачених ресурсів та захищеності інформації в АС. Зроблено висновок, що проводити оцінку захищеності системи змішаними (комплексними) методиками немає доцільності, і оскільки кількісні методики при проведені аналізу ризиків на програмно-технічному рівні захисту, мають більшу ефективність, то слід обрати саме кількісну методику оцінки захищеності критичних ресурсів.

1.3. Класифікація загроз інформаційній безпеці автоматизованої системи управління технологічним процесом

Не дивлячись на велику кількість аварій з катастрофічними наслідками, проблема захисту критичних інформаційних ресурсів на промислових підприємствах хімічної та енергетичної галузей ніколи не стояла так гостро як останніми роками.

Загальний інтерес до безпеки промислових систем виник лише після інцидентів з комп'ютерними вірусами Stuxnet, Duqu, Flame, які акатували іранські атомні об'єкти, державні заклади та промислові об'єкти Індії, Китаю та інших країн. Окремо слід виділити атаки на підприємства енергетичної галузі та банківського сектору в Україні. До появи цих інцидентів вважалось, що скомпрометувати роботу системи захисту критичних інформаційних ресурсів було дуже важко. Такі уявлення будувались на наступних постулатах: програмне забезпечення кожної системи захисту критичних інформаційних ресурсів унікальне і закрите; проникнення в систему пов'язане з великими витратами інтелектуальних ресурсів, а грошова винагорода для зловмисника не очевидна; локальна мережа системи захисту критичних інформаційних ресурсів вирішує проблеми обмеження доступу. Вивчення структури та програмно-апаратних засобів, що використовуються в системах захисту критичних інформаційних ресурсів, показало, що за останній час пройшли великі зміни. Майже всюди використовується широко розповсюджене програмне забезпечення як ОС Windows, TCP/IP протоколи тощо, які разом зі своїми перевагами з стандартності, простоті та якості використання принесли також і недоліки – вразливості. У локальній мережі з'являються комп'ютери, підключені до мережі Інтернет, що також вносить велику кількість потенційних загроз до системи [17-19].

Сучасні промислові автоматизовані системи управління технологічними процесами (АСУ ТП) будуються на вже стандартизованому обладнанні (стандартні IT-платформи, SCADA-системи) і, як правило, з метою підвищення ефективності управління, підключаються до суміжних систем. Завдяки такій стандартизації, а також роблячи систему більш відкритою, підвищується вразливість АСУ до

кібератак. Таким чином повсюдне використання комп’ютерного обладнання у керуванні промисловими підприємствами створює необхідність приділення все більшої уваги до проблем інформаційної безпеки таких систем. Основні проблеми інформаційної безпеки критичних інформаційних ресурсів, які виділяють експерти, з’являються через [20]:

- слабкий захист від несанкціонованого доступу (паролі);
- незадекларованих можливостей SCADA;
- відсутность контролю керуючих впливів;
- використання бездротових комунікацій (некрипостійке шифрування
- Wi-Fi);
- відсутність чітких меж між різними сегментами мережі;
- несвоєчасне чи некоректне оновлення програмного забезпечення;
- відмову від навіть мінімальних заходів безпеки (нерідко заради зручності чи продуктивності, компанії відмовляються від встановлення не тільки, наприклад, антивірусного захисту, а навіть захисту паролем критично важливих активів);
- поширення Windows як операційної системи для робочих станцій та навіть серверів;
- розробку з розрахунком на використання у довіреному середовищі закритих індустріальних мереж;
- створення систем без врахування кращих практик розробки безпечного коду;
- людський фактор, слабку дисципліну персоналу.

Уявлення про можливі загрози (як внутрішні, так і зовнішні), а також про вразливі місця, які ці загрози зазвичай використовують, необхідне для вибору (або розробки) оптимального набору засобів забезпечення безпеки.

Загрози, як і все в інформаційній безпеці, залежать від інтересів суб'єктів інформаційних відносин, і від того, які збитки є для них неприйнятні. Під загрозою інформаційної безпеки автоматизованої системи розуміють можливі впливи на цю систему, які на пряму або побічно можуть завдати збитків.

Прийнято вважати, що ІБ інформаційної системи забезпечена в разі, якщо для будь-яких інформаційних ресурсів в системі підтримується визначений рівень конфіденційності, цілісності та доступності інформації [21]. Тому для інформаційних систем традиційно розглядають три основних види загроз безпеки:

- загроза порушення конфіденційності;
- загроза порушення цілісності;
- загроза відмови служб.

Класифікація загроз за різними критеріями [22] наведена на Рис.1.1 .

Далі для дослідження в якості основного буде розглянуто критерій по аспекту інформаційної безпеки (за потребою розглядаючи інші критерії), а саме загрози доступності, цілісності і конфіденційності даних.

Головні загрози доступності - наслідки ненавмисних помилок. Помилки в програмі або неправильно введені дані, що викликали вихід з ладу всієї системи. Зазвичай вони залишають вразливості в системі, якими може скористатися зловмисник. Решта загроз доступності АСУ класифікуємо за компонентами АСУ ТП, на які націлені загрози:

• відмова користувачів;
• відмова інформаційної системи;
• відмова підтримуючої інфраструктури.

У якості загроз відмови користувача виступає людський фактор. Це може бути відсутність відповідної підготовки у фахівця, або неможливість прийняття рішення по причині некваліфікованості фахівця.

Джерелами внутрішніх відмов системи є: відхилення від правил експлуатації; системні помилки (надмірний обсяг оброблюваної інформації); помилки адміністрування системи; відмова програмного забезпечення; відмова апаратного забезпечення; втрата даних і пошкодження апаратури (розкрадання носіїв інформації, підключення до лінії зв'язку);

По відношенню до підтримуючої інфраструктури це може бути частковий або повний вихід з ладу підсистем (порушення роботи мереж зв'язку, електропостачання, системи охоронно-пожежної безпеки).

Рис.1.1. Класифікація загроз по критеріям

Для загроз цілісності АСУ ТП потрібен безпосередній фізичний доступ до системи. Потенційно вразливими є як дані, так і програми. Дані може підмінити зловмисник, маючи безпосередній фізичний доступ до системи. Шкідливе програмне забезпечення (ПЗ), в свою чергу, є загрозою пам'яті програм.

Також до загроз цілісності можна віднести втрату інформації при передачі по каналах зв'язку [22]. Часткова втрата пакетів в мережах телекомунікації АСУ ТП може призвести до отримання невірних результатів і виконання невірних дій керування.

Конфіденційну інформацію в АСУ ТП можна розділити на службову і предметну. Службова інформація (паролі, коди доступу і т.п.) в АСУ має технічну роль, але порушення її конфіденційності може призвести до несанкціонованого доступу до всієї інформації, в тому числі і предметної.

Перехоплення даних - дуже серйозна загроза. І якщо конфіденційність даних в системі є найважливішим завданням, а дані передаються по багатьох каналах зв'язку, їх захист може виявитися досить складним і дорогоцінним. Існують спеціальні технічні засоби перехоплення, за допомогою яких зловмисник може перехоплювати

конфіденційні дані. Далі розглянемо таблицю 1.1, де наведені основні загрози інформаційній безпеці АСУ ТП, які завдають найбільшу шкоду системі.

Таблиця 1.1

Основні загрози

Способи завдання збитків	**Об’єкти впливу**
Розкриття інформації	**Устаткування**
	Розкрадання носіїв інформації, підключення до мереж ліній зв'язку, несанкціоноване використання ресурсів
	Програми
	Несанкціоноване копіювання даних, перехоплення
	Дані
	Розкрадання, копіювання, перехоплення
	Персонал
	Розголошення відомостей про захист АСУ, недбалість співробітника
Втрата цілісності інформації	**Устаткування**
	Підключення, модифікація, зміна режимів роботи, несанкціоноване використання ресурсів
	Програми
	Впровадження апаратних закладок, вірусів і троянів
	Дані
	Спотворення, модифікація
	Персонал
	Людський фактор (вербування, особиста вигода і.т.д.)
Порушення роботоздат-ності АСУ	**Устаткування**
	Зміна режимів функціонування, вихід з ладу, розкрадання, руйнування
	Програми
	Спотворення, підміна, видалення
	Дані
	Спотворення, видалення, помилкові дані
	Персонал
	Відсутність працівника

Надійність захисту інформації в АСУ може бути ефективною лише в тому випадку, якщо вона є надійною на всіх об'єктах і у всіх компонентах системи, які можуть зазнати загроз з боку дестабілізуючих факторів [23].

Наведемо приклад основних загроз для систем захисту критичних інформаційних ресурсів, знайдених після аналізу справжніх інцидентів [20]:

- атаки на SCADA;
- атаки на PLC, вразливості PLC (стандартний пароль, неавторизований доступ до оригінального програмного забезпечення);
- атаки на інфраструктуру та оперативну систему (віруси, троянські програми, черв'яки, DoS- і DDoS-атаки, ARP-спуфінг – перехват трафіку пілся оголошення себе маршрутизатором);
- атаки на протоколи, вразливість протоколів (несанкціонований доступ, SQL-ін'єкції);
- пактичні атаки (переповнення буферу – Buffer Overflow, розкриття інформації – Information Disclose, відмова в доступі – Denial of Access, підміна представлення – Manipulation of View).

Серед усіх типів вразливих компонентів систем захисту критичних інформаційних ресурсів переважають SCADA – 87%, системи, які забезпечують інтерфейси людина-машина – 49%, програмовані контролери – 20%, протоколи – 1%. Доля вразливостей по типах розділилась наступним чином: переповнення буферу – 36%, аутентифікація/управління ключами – 22.86%, вразливості Web-програм – сервер – 10.86%, клієнт – 9.14%, віддалене виконання коду – 13.14% [24-26].

Унаслідок експлуатації систем захисту критичних інформаційних ресурсів і суттєвої зміни складу і якості сучасних загроз, необхідно проєктувати і реалізовувати інформаційну безпеку систем з врахуванням тенденцій розвитку кіберзагроз. З іншого боку необхідно проводити регулярну роботу з нейтралізації виникаючих чи потенційних загроз на працюючих системах. На цьому рівні реалізуються наступні сервіси інформаційної безпеки: управління доступом, забезпечення цілісності, забезпечення безпечної міжмережевої взаємодії, антивірусний захист, аналіз

захищеності, виявлення вторгнень, управління системою інформаційної безпеки (неперервний моніторинг станів, виявлення інцидентів, реагування) [20].

Таким чином, проведена класифікація та визначення основних загроз, з точки зору обєктів впливу та способів завдання збитків, по аспекту інформаційної безпеки, дозволяє сформувати повний перелік тих об'єктів і елементів, які, з одного боку, можуть піддаватися загрозам з метою порушення захищеності інформації критичних ресурсів, а з іншого - можуть бути досить чітко визначені з метою організації захисту інформації критичних ресурсів. З урахуванням визначеного списку загроз може бути отримана найточніша оцінка ймовірності загроз і ймовірності відбиття загроз системою захисту інформації, в контексті математичної та імітаційної моделі СЗІ. Аналіз інформаційної інфраструктури підприємства і принципів її функціонування, особливостей організації інформаційно-обчислювального процесу на підприємствах дозволяє уточнити класифікацію загроз інформаційній безпеці, а також виділити загрози, найбільш значущі для даного типу підприємств. Для покращення ситуації з захищеністю підприємства від загроз порушення інформаційної безпеки необхідно вибрати оптимальний варіант системи захисту інформації.

1.4. Імітаційне моделювання систем захисту інформації підприємства

Для комплексної оцінки пропонованих заходів і засобів захисту інформації бізнес-процесів на попередньому етапі проєктування СЗІ підприємства використовуються імітаційне моделювання. Крім цього імітаційна модель дозволяє наочно в динаміці надати кінцевий або проміжний результат, що є важливим аспектом для успішного розуміння отриманих результатів особами, які не брали участі в її розробці.

Характерна особливість таких моделей полягає також у тому, що послідовність кроків їх розрахунку на комп'ютері відповідає поведінці системи, яка моделюється, тобто імітує її. Тому в літературі набув поширення термін "Імітаційна модель" [1], [27]. Узагальнюючи наявні визначення із [27], [28], [29], можна сказати, що імітаційне

моделювання служить для вивчення поведінки системи за допомогою математичного апарату, використовуючи засоби обчислювальної техніки.

Застосування засобів обчислювальної техніки дозволяє автоматизувати розрахунок необхідних результатів, маючи лише початкові дані, отримані, наприклад, статистично. Це особливо актуально, коли розглядається складна система, що складається з безлічі вузлів, тому що, як правило, для розрахунків необхідних результатів потрібно застосовувати громіздкі формули.

Імітаційне моделювання застосовується для вивчення поведінки різноманітних систем, в тому числі і інформаційних. В основному при моделювання інформаційних систем ставиться мета отримати відомості про час обробки заявки, рівня навантаження будь-якого ресурсу і т.п. Однак застосування імітаційного моделювання для вивчення поведінки інформаційної системи захисту критичних інформаційних ресурсів до теперішнього часу широко не розглядалося.

Існують спеціальні мови імітаційного моделювання, які полегшують процес створення програмної моделі в порівнянні з використанням універсальних мов програмування. Прикладами мов імітаційного моделювання можуть служити такі мови, як SIMULA, GPSS, SIMDIS.

Існують також системи імітаційного моделювання, які орієнтуються на вузький клас досліджуваних систем і дозволяють будувати моделі без програмування.

Аналізатори протоколів незамінні для дослідження реальних мереж, але вони не дозволяють отримувати кількісні оцінки характеристик для ще не існуючих мереж, що знаходяться в стадії проєктування. У таких випадках можна використовувати засоби моделювання, за допомогою яких розробляються моделі, що відтворюють інформаційні процеси, що протікають в мережі

Програмні емулятори мережного обладнання - це програмні продукти, що дозволяють з'єднати в собі функції і параметри реальної обчислювальної мережі. Вони були розроблені для проєктування, моделювання і тестування роботи мережі. Більшість емуляторів досить зручні у використанні, так як надають графічний інтерфейс для управління мережною інфраструктурою, що набагато зручніше ніж управління підключеннями реальних пристроїв.

На сьогоднішній день існує безліч компаній, які виробляють мережне обладнання, і компанія Cisco Systems вважається безумовним фаворитом на цьому ринку і пропонує пристрої для створення обчислювальних мереж від невеликого офісу до великих підприємств. З огляду на широке поширення мережного обладнання під управлінням Cisco IOS (Internetwork Operating System - міжмережна операційна система), а також високу вартість даного обладнання, ще більш зрозумілим стає необхідність в застосуванні програмних емуляторів мережного обладнання для створення моделей обчислювальних мереж.

Найпопулярнішим емулятором мережевого обладнання є Cisco Packet Tracer, це емулятор, розроблений самою компанією Cisco Systems для навчання в рамках програм Cisco Network Academy. Створення мережної інфраструктури і наступна модифікація відбуваються через графічний інтерфейс, який є інтуїтивно зрозумілим і найбільш зручним з графічних інтерфейсів управління, що надаються розглянутими програмними засобами емуляції мережного обладнання. Симулятор Cisco Packet Tracer доступний як під Windows, так і для Linux. Крім стандартних маршрутизаторів і комутаторів Packet Tracer підтримує емуляцію IP-телефонів, бездротових точок доступу і серверів з набором стандартних служб. У Packet Tracer вбудовано безліч додаткових засобів, що спрощують вивчення роботи мережевої інфраструктури. У ньому зручно перевіряти роботу сервісів DHCP / DNS / HTTP / SMTP / POP3 / NTP. Зручно в режимі simulation побачити переміщення пакетів з уповільненням часу. Cisco Packet Tracer емулює як апаратну, так і програмну частини мережного обладнання. Таким чином, Packet Tracer дозволяє створювати копії великих мережних інфраструктур, ось тільки емульовані пристрої не підтримують велику кількість технологій, що використовуються в реальних великих мережах, багато функцій, які доступні в реальних пристроях тут відсутні [30]. Головна перевага Cisco Packet Tracer - безкоштовність даного продукту.

Cisco (VIRL) - це програмний інструмент, розроблений Cisco для створення і запуску моделювання мережі без необхідності у фізичному обладнанні. VIRL представляє собою платформу на базі OpenStack, яка запускає образи програмного забезпечення IOSv, IOSvL2, IOS XRv, NX-OSv, CSR1000v і ASAv на вбудованому

гіпервізорі. VIRL забезпечує масштабоване, розширюване мережне середовище проєктування і моделювання, використовуючи інтерфейс VM Maestro. Останнім часом спостерігається велика розробка та удосконалення операцій на основі браузера з використанням HTML5. VIRL також має широкі можливості для інтеграції зі сторонніми віртуальними машинами, такими як Juniper, Palo Alto Networks, Fortinet, F5 BigIP, Extreme Networks, Arista, Alcatel, Citrix і інші. VIRL поставляється з повним набором юридичних і ліцензованих образів Cisco IOS, які є такими ж, як і на фізичних маршрутизаторах. Нові випуски Cisco IOS надаються на регулярній основі.

Відомі й інші програми. Для моделювання мережних топологій широко використовується контейнер віртуальних машин GNS3. Він являє собою графічний інтерфейс для емулятора Qemu и Dynamips. Емулятор Dynamips працює зі справжніми прошивками IOS. До GNS3 можна підключати віртуальні машини VirtualBox або VMware Workstation і створювати досить складні схеми, при бажанні можна піти далі і випустити його в реальну мережу. Платформа GNS3 (www.gns3.com) широко використовується як в ході навчання, так і для проєктування і супроводу реальних мереж. Вона забезпечує серйозне вивчення предмета і орієнтована на повністю вільні рішення [31, 32]. Для роботи емулятор GNS3 вимагає значних витрат ресурсів комп'ютера і також має певні обмеження по функціям.

Unified Networking Lab (UNetLab, UNL) - мережний емулятор, який являє собою розраховану на багато користувачів платформу для моделювання і створення віртуальних мереж, різних лабораторій, що підтримує значний список телекомунікаційного обладнання. Концептуальної новизною продукту UNetLab є можливість запуску і використання програми між різними платформами і різними виробниками пристроїв.

В даний час емулятор UNetLab є не тільки платформою для моделювання віртуальних мереж, але і інструментом для підготовки до різних сертифікаціям Cisco Крім того, UNL використовується для системного підходу у виявленні та усуненні причин неполадки мереж (troubleshooting). UNL відходить від концепції використання автономних віртуальних машин для емуляції відповідних мережних пристроїв, і створює цифрові мережні лабораторії на основі 20 програмних

емуляторів IOU / IOL, Dynamips і вузлів QEMU, об'єднуючи всі необхідні програмні модулі і сценарії у вигляді одного файлу в рамках однієї платформи. UNetLab є повністю безкоштовним, і тому може використовуватися не тільки для комерційних цілей, а й для навчання звичайними користувачами. З переваг так само слід зазначити можливість запуску необмеженої кількості примірників обладнання (роутерів, комутаторів, пристроїв безпеки і т.д.), кількість обмежена тільки апаратними можливостями робочого місця.

Ще один симулятор Boson NetSim працює тільки під Windows і виконує лабораторні роботи Cisco. Є ще такі програми як Cisco CSR (вартість ліцензії на 1 рік близько 1000 $), Cisco IOU (офіційно не поширюється). eNSP - симулятор обладнання Huawei подібний Cisco Packet Tracer.

Виходячи із загального порівняльного аналізу програмних платформ емулятора мережевого обладнання, можна виділити GNS3, який має ряд технічних переваг, за допомогою яких досягається підвищення функціоналу і, як результат, розширення спектру надання послуг в області проєктування мережі. Тому найкраще рішення використовувати моделі мереж з комбінацією віртуальних і реальних компонентів. Такий підхід дозволяє проводити експерименти на реальних працюючих мережах з використанням їхніх ресурсів, підключаючи до них віртуальні мережі. Також дозволяє одночасно працювати декільком користувачам. Кожен робить свою віртуальну мережу і включає її в реальну. Так можна збирати дуже великі складні мережі. Реальна і віртуальні мережі працюють як одне ціле і дозволяють проводити експерименти в кожній віртуальній підмережі.

Отже, в якості середовища моделювання можна використати найбільш актуальний програмний емулятор для визначеної інформаційної системи. Ця імітаційна модель буде містити безліч вузлів і відгалужень, в зв'язку з чим необхідно детально розглядати кожен її сегмент та описати загальну схему функціонування такої імітаційної моделі.

Таким чином, застосування імітаційного моделювання дозволяє наочно в динаміці вивичити поведінку інформаційної системи захисту, а не лише формалізувати параметри безпеки. Виходячи із загального порівняльного аналізу

програмних платформ емулятора мережевого обладнання, можна виділити GNS3, який має ряд технічних переваг, за допомогою яких досягається підвищення функціоналу і, як результат, розширення спектру надання послуг в області проєктування мережі. Тому найкраще рішення використовувати моделі мереж з комбінацією віртуальних і реальних компонентів. Докладне вивчення середовища моделювання показало можливість його використання і ефективність застосування для моделювання систем захисту інформації підприємств. Побудова імітаційної моделі функціонування інформаційної системи підприємства також може бути використана для виявлення актуальних загроз безпеки інформаційної системи.

1.5. Оптимізація проєктування систем захисту інформації в інформаційних системах підприємств

Методи пошуку оптимальних рішень є узагальненням великої кількості самостійних, в більшості своїй математичних теорій з метою вирішення завдань оптимізації. У загальному випадку до цієї групи можна також віднести методи неформального відомості складного завдання до формального опису з подальшим застосуванням формальних підходів. Комбінування різних методів дозволяє розширити можливості застосування формальних теорій для проведення повноцінного моделювання систем захисту [20].

Проблема побудови оптимальної системи захисту інформації в даний час є найбільш актуальною і затребуваною для більшості промислових підприємств. Мета будь-якої системи захисту визначається можливістю сталого функціонування системи в цілому, визначення та нейтралізації загроз безпеки, запобігання витоку інформації по різних каналах. Одним з головних завдань стає оптимізація проєктування системи захисту.

Моделі, методи та засоби захисту інформації (ЗІ), які використовуються на підприємствах різні, і , як правило, вибираються в результаті рішення однієї із задач виду $\langle S \to min, R \geq R_{\text{доп}} \rangle$ моделі мінімізації витрат на побудову інфраструктури ЗІ або $\langle R \to max, S \leq S_{\text{доп}} \rangle$ моделі максимізації рівня захищеності інформаційних

активів підприємства , де S - затрати на розробку, впровадження та супровід системи ЗІ на підприємстві; R - рівень захисту, який забезпечується обраним варіантом системи ЗІ; $S_{доп}$ - допустима вартість системи ЗІ на підприємстві; $R_{доп}$ - допустимий рівень якості системи ЗІ в цілому. Обидва завдання математично еквівалентні і можуть бути вирішені методами багатокритеріальної оптимізації. Традиційно в задачах багатокритеріальної оптимізації використовується підхід [33] на основі формування множини Парето-оптимальних проєктних рішень з побудови системи ЗІ, який, має обмежене практичне застосування, обумовлене значною розмірністю одержуваної множини недомінуючих рішень і невирішеністю компромісу при допустимих значеннях параметрів {S, R}. Для вирішення завдання проєктування інфраструктури системи ЗІ пропонується використовувати метод послідовних поступок [34], в якому виділяється ряд приватних показників якості ЗІ, що мають перева гу над іншими показниками.

Як випливає з вихідної задачі оптимізації, основою для висновку про абсолютну перевагу одних показників над іншими служить ступінь розбіжності окремих показників за важливістю, при якій порівняння оцінок варіантів побудови системи ЗІ здійснюється тільки по найважливішому показнику без урахування інших, потім тільки по другому показнику і т.д. У загальному вигляді задача оптимізації еквівалентна задачі знаходження умовного екстремума основного критерію.

Інформація про абсолютну перевагу певних показників дозволяє проранжувати можливі варіанти з використанням процедури лексикографічної оцінки. Реалізація цієї процедури передбачає декомпозицію вихідної багатовимірної задачі оцінки методом послідовних поступок в певну послідовність завдань (стратегію) оцінки по ієрархічно впорядкованим скалярним показниками $\{\xi_1, \xi_2, \dots, \xi_\zeta\}$.

Таким чином, передбачається, що перший показник ξ_1 важливіше другого ξ_2, другий ξ_2 третього ξ_3, і т.д. до ξ_ζ, так що $G_F \supseteq F_1 \supseteq F_2 \supseteq \dots \supseteq F_\zeta$, за умови $F_\zeta \neq \emptyset$, тобто кожний наступний приватний показник звужує безліч G_F проєктних рішень, одержаних за допомогою всіх попередніх показників. Це означає, що якщо у вихідній задачі оптимізації з одним скалярним показником є кілька рішень і для подальшого вибору послідовно застосовуються додаткові показники, то одержувані в результаті

стратегії рішення будуть оптимальними для відповідної лексикографічної задачі з векторним показником, що складається з усіх цих почергово розглянутих показників.

Очевидно, для прийнятої моделі мінімізації витрат вирішальне правило по вибору конкретного варіанту структури системи ЗІ має вигляд

$$\hat{\imath} = \underset{i}{arg\,min}\{S_i | R_i \geq R_{\text{доп}}\}.$$

Аналогічно в моделі максимізації рівня захищеності вирішальне правило по вибору конкретного варіанту структури системи ЗІ має вигляд

$$\hat{\imath} = \underset{i}{arg\,max}\{R_i | S_i \leq S_{\text{доп}}\}.$$

Оцінка значення величини $S_{\text{доп}}$ не викликає ускладнень і визначається фінансовою спроможністю підприємства і ризиками (збитком) від реалізації атак на інфраструктуру ЗІ. Табульована шкала переваг за рівнем показника захищеності підприємства дозволяє оцінювати прийнятну для конкретного підприємства якість захисту $R_{\text{доп}}$.

Розглянуті математичні моделі розрахунку показників якості роботи системи захисту інформації на підприємстві дозволяють для довільно обраного числа компонентів і складності структури системи захисту інформації здійснювати оцінку ефективності її використання для відбиття інформаційних загроз. Такі моделі враховують імовірнісний характер загроз та систему бінарних правил спеціалізації кожного засобу захисту для відповідного типу загроз. Вони призначені для забезпечення оптимального проектування системи захисту інформації. Причому під оптимальністю системи розуміється забезпечення максимального рівня захищеності інформаційних ресурсів підприємства при заданому рівні витрат, або забезпечення заданого рівня безпеки при мінімальному рівні витрат на побудову інфраструктури системи захисту інформації.

1.6. Проблемні питання процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі

Тверді продукти у вигляді порошків, виготовлених з рідкої сировини, мають ряд переваг: їх часто легше транспортувати, переробляти та зберігати, ніж у рідкому вигляді. Одним із прикладів може бути молоко: у рідкому вигляді йому потрібне зберігання у прохолоді, щоб воно не зіпсувалося. Однак, якщо його висушити розбризкуванням, тобто видалити всю вологу з емульсії сушкою, то отримана консистенція може зберігатися при кімнатній температурі протягом тривалого часу. При цьому, рідкий стан можна легко відновити в будь-який час, розчинивши порошок у певній кількості води. Властивості продукту часто можна охарактеризувати властивостями частинок. Найважливішими властивостями частинок є форма частинок і розмір, поруватість, температура та вміст вологи. Температура та вміст вологи впливають на складність транспортування та зберігання продукту.

Основні переваги гранулятора (рис 1.2) із псевдозрідженим шаром: поверхня фазового контакту є достатньо розвинутою, висока інтенсивність процесів теплообміну, питома продуктивність на високому рівні, мінімальні витрати на розробку та виготовлення апарату, гранульований продукт однорідний та має високу якість, наявність можливості повної автоматизації і механізації безперервного ведення процесу, процеси висушування та гранулювання є суміщеними, що спрощує схему виробництва.

Оскільки процеси теплообміну проходять водночас з процесами масообміну, але закони переходу теплоти та маси залишаються незмінними, то їх вивчення об’єднали у тепломасообмін. Тепломасообмін – це наука про процеси поширення теплоти в змінному полі температур та процеси поширення маси в змінному полі концентрацій [35]. У рухомих середовищах вище вказані процеси залежать від швидкості руху середовища в якому вони протікають. Відповідно до другого закону термодинаміки мимовільних процесів про поширення теплоти, її поширення напрямлене в сторону зменшення температури. Так само і потік маси у змінному полі концентрацій напрямлений у сторону даного компонента суміші.

Методи термодинамічного аналізу відрізняються від методів тепломасообміну тим, що тут розглядається розвиток процесів перенесення у просторі та часі. Після розв'язання задачі тепломасообміну на виході отримують розподіл температур, потоків теплоти і маси з функціями координат та часу, і концентрацію компонентів суміші [35]. Характер тепломасообміну в псевдозрідженому шарі визначає характер формування гранул та швидкість їхнього утворення, за умовами взаємодії між частинками та краплями дисперсного розчину. Висушування та кристалізація речовини яка гранулюється проходить в умовах зіткнення крапель з теплоносієм або окремими гранулами. Характер грануляції та її перебіг залежить також від змоги гранул акумулювати тепло, тобто теплозбереження.

Рис. 1.2. Гранулятор із псевдозрідженим шаром

Грануляція розпиленням в псевдозрідженому шарі дозволяє отримувати сипучі грануляти із заданими властивостями безпосередньо з рідин. Рідини з вмістом твердої фази, наприклад розчини, суспензії або розплави, розпорошуються в установці псевдозрідженого шару. Внаслідок активного теплообміну вода і органічні розчинники миттєво випаровуються, а що утворилися при цьому тверді частинки стають центрами гранулоутворення. Вони змочуються новими порціями рідини, яка також випаровується, та утворює нові шари оболонки навколо вихідного центру.

Під час цього безперервного процесу в псевдозрідженому шарі гранули ростуть пошарово, утворюючи структуру, яка подібна цибулині. Альтернативно, в гранулятор можна подати необхідну кількість частинок, які будуть виконувати роль зародків для

гранул [36]. При цьому рідина служить лише засобом транспортування речовини для зростання гранул (рис. 1.3 та рис. 1.4).

Рис. 1.3. Початкові центри грануляції (d_e = 1.85 мм)

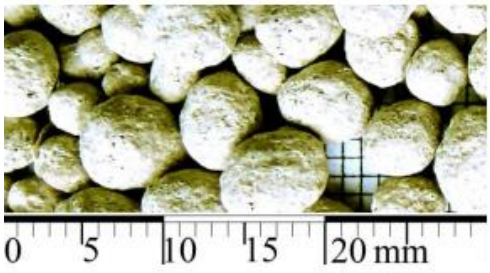

Рис. 1.4. Загальний вигляд гранульованого продукту (d_e = 3,58 мм)

Найбільш часто реалізуються агломераційний та пошаровий механізми грануляції (рис. 1.5).

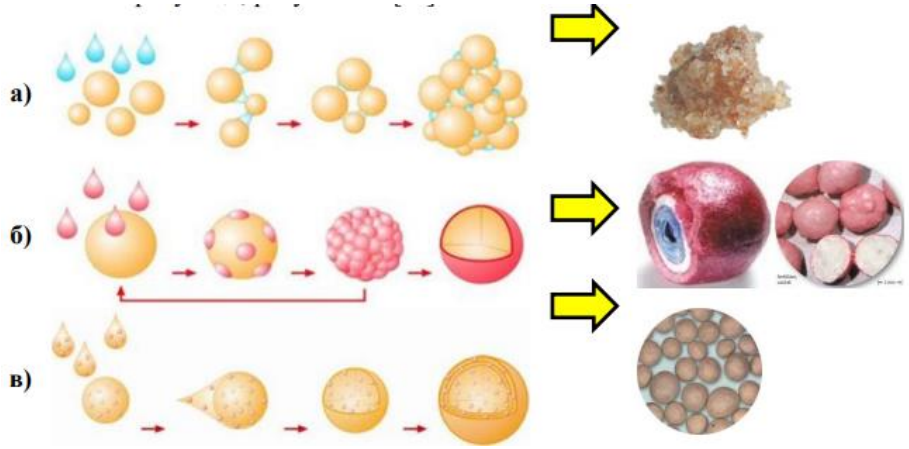

Рис. 1.5 – Найбільш поширені механізми грануляції: а) агломерація; б) капсулювання; в) нашарування гомогенних та гетерогенних систем.

Окрім розшарування частинок, відбувається перенесення тепла та маси через фазові межі. Для спрощення подальшого моделювання рідина розглядається не як самостійно окрема фаза, а як складова або твердої фази (у вигляді рідини), або газової фази (у вигляді пари). В основному частинки в неоднакові; вони можуть відрізнятися за своїми властивостями, наприклад розмір, вологість, ентальпія, поруватість або форма тощо. Моделювання зміни такого розподілу властивостей, а отже, і моделювання процесу, можна здійснити при використанні моделі балансу популяції.

Зазвичай гранулятор (рис. 1.6) з псевдозрідженим шаром розглядається як апарат, що складається з технологічної камери з розподільною пластиною на дні, яка пропускає потік рідини або газу.

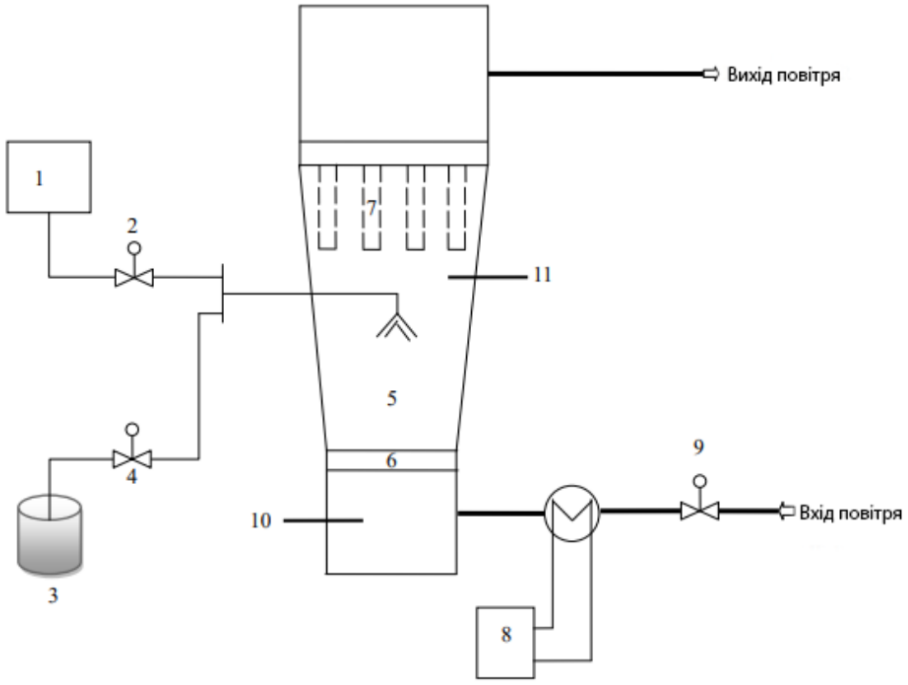

Рис. 1.6. Функціональна схема гранулятора: 1- компресор, 2- регулятор тиску, 3 - контейнер з розчином, 4- регулятор швидкості потоку розчину, 5 - контейнер для продукту, 6 – розподільник повітря, 7 - фільтр вихідного повітря, 8 - контролер нагрівача, 9- регулятор швидкості вхідного повітря, 10 - вимірювання температури вхідного повітря, 11 - вимірювання температури повітря на виході.

Відносна вологість повітря на вході впливає на швидкість зростання частинок кінцевого продукту, і була розглянута рядом дослідників. Було виявлено, що більш

великі гранули утворюються при збільшенні відносної вологості повітря на вході. Оскільки здатність води випаровуватися зменшується, а утворення рідких і твердих мостів збільшується. Швидкість повітря на вході в псевдозріджений шар є важливим робочим параметром, що впливає як на гідродинаміку псевдозрідження, так і на зростання гранул, і він грає ключову роль в забезпеченні однорідності змішування порошку. Температура повітря на вході є ключовим параметром, що впливає на температуру киплячого шару і випаровування вологи. Більш висока температура повітря на вході може швидко висушити вологі гранули і скоротити час грануляції[35].

Існує кілька фізико-хімічних властивостей, які впливають на процес гранулювання. Найбільш досліджувані включають розмір частинок первинного порошку, кількість рідини на твердій речовині, розчинність та властивості зв'язувальної речовини: концентрація зв'язувальної речовини, в'язкість.

Грануляція розпиленням в псевдозрідженому шарі дозволяє отримувати сипучі грануляти із заданими властивостями безпосередньо з рідин. Шарувата структура гранул надає їм високу щільність і стійкість до стирання. Змінюючи такі параметри, як розмір гранул, залишкову вологість і вміст твердої фази, можна отримувати продукти з різними властивостями[36].

Відносна вологість повітря на вході впливає на швидкість зростання частинок кінцевого продукту, швидкість повітря на вході в псевдозріджений шар є важливим робочим параметром, так як і властивості вихідного матеріалу. Більш висока температура повітря на вході може швидко висушити вологі гранули і скоротити час грануляції.

Окрім розшарування частинок, відбувається перенесення тепла та маси через фазові межі. Для спрощення подальшого моделювання рідина розглядається не як окрема фаза, а як частина або твердої фази (у вигляді рідини), або газової фази (у вигляді пари).

Протягом останніх десятиліть розроблена велика кількість математичних моделей процесів переносу у дисперсних системах із різним рівнем деталізації.

Застосування моделі двофазного потоку має переваги перед іншими моделями, тому що вона не вимагає вхідних емпіричних параметрів, таких як середній розмір частинки або час знаходження пакета. Гідродинаміка шару розвивається вільно з розв’язку рівнянь збереження маси і моменту по двофазному підходу. Однак ця модель включає два емпіричні вирази відповідно для коефіцієнту міжфазової передачі моменту і коефіцієнту міжфазової теплопередачі. Для побудови моделі необхідно створити механістичні моделі, які описують передачу моменту і теплопередачу.

Двофазний підхід було застосовано для моделі теплопередачі [37], яка описує модель збереження маси, рівняння моментів і теплової енергії у векторній формі. Дана модель не враховує компонентів турбулентності.

Для газо-твердих псевдозріджених шарів двофазні моделі базуються на підході, що називається підходом Лагранжа чи Ейлера. В підході Лагранжа динаміка фаз описується набором дискретних частинок, які підпорядковані закону Ньютона. У підході Ейлера прийнято поняття контінуума описання фази, яка описується рівняннями Нав'є-Стокса. На основі цих двох варіантів для кожної фази запропонована класифікація різних моделей для газу і твердих частинок [38].

На основі проведеного аналізу технологічного процесу виробництва мінеральних добрив у грануляторах із псевдозрідженим шаром, можна визначити основні параметри, що впливають на технологічний процес та належать до критичних інформаційних ресурсів, а саме: температура гранул, температура теплоносія та вологовміст гранул. Відомі математичні моделі не враховують зміну вологовмісту гранул, як одного з основних показників якості готового продукту, що спонукає до розробки математичної моделі процесу зневоднення та гранулювання мінеральних добрив у псевдозрідженому шарі, яку можна було б використовувати для задач оптимального керування технологічним процесом.

1.7. Обгрунтування та постановка задач дослідження

На сучасному етапі стану суспільства інформаційні технології активно впроваджуються в усі сфери національної економіки. Сьогодні керівництво будь-якого промислового підприємства, по суті, має справу з корпоративною інформацією, на основі якої приймаються відповідальні рішення. Інформаційні технології в даний час є необхідним атрибутом підвищення ефективності бізнес-процесів, дозволяють господарюючим суб'єктам знизити витрати виробництва, підвищити достовірність економічного аналізу, правильно вибирати стратегію і тактику проведення заходів в умовах настання форс-мажорних обставин. Однією з найбільш серйозних проблем, що ускладнюють застосування сучасних інформаційних технологій, є забезпечення їх інформаційної безпеки.

Актуальність і важливість проблеми забезпечення безпеки інформаційних технологій обумовлені наступними причинами:

- різке збільшення обчислювальної потужності сучасних комп'ютерів при одночасному спрощенні їх експлуатації;

- високі темпи зростання парку персональних комп'ютерів, що знаходяться в експлуатації в різних сферах людської діяльності;

- різке збільшення обсягів інформації, що накопичується, зберігається на електронних носіях (у вигляді електронних документів) і оброблюваної за допомогою засобів обчислювальної техніки;

- концентрація інформації і зосередження в єдиних базах даних інформації різного призначення і різної приналежності;

- динамічний розвиток програмних засобів, які не задовольняють вимоги безпеки;

- різке розширення кола користувачів, що мають безпосередній доступ до обчислювальних ресурсів і масивів даних;

- демократизація доступу до інформації, обумовлена розвитком як локальних, так і глобальних комп'ютерних мереж;

- розвиток електронної пошти і зростання електронного документообігу в комп'ютерних мережах на підприємствах;

- впровадження електронних технологій в різні види професійної діяльності на фінансових і товарних ринках (електронна комерція, мережеві банківські та фінансові послуги);

- розвиток глобальної мережі Інтернет, практично не перешкоджає порушень безпеки систем обробки інформації в усьому світі.

В результаті виникло гостре протиріччя між можливостями методів і засобів інформаційних технологій та можливостями методів і засобів захисту інформаційних ресурсів.

Сучасні інформаційні технології в багатьох випадках управляють складними та небезпечними технологічними процесами, збій у яких потенційно може призвести до аварій на виробництві або, у гіршому випадку, до техногенних катастроф. Це значно збільшує вартість ризику через порушення інформаційної безпеки, оскільки реалізація загроз може призвести до шкоди людям, навколишньому середовищу, а також, звичайно, до фінансових та репутаційних втрат.

Ускладнення засобів, методів, форм автоматизації процесів обробки інформації підвищує залежність промислових підприємств від ступеня безпеки використовуваних ними інформаційних технологій, при цьому якість інформаційної підтримки управління безпосередньо залежить від організації системи захисту інформації. При проектуванні та експлуатації інформаційних технологій необхідно постійно аналізувати систему на зручність використання, надійність та стійкість до загроз. Висока вартість досліджень захищеності інформаційних технологій для управління технологічними процесами визначає необхідність побудови імітаційної моделі захисту критичних інформаційних ресурсів. Проблема побудови оптимальної системи захисту інформації також в даний час є найбільш актуальною для більшості промислових підприємств. Мета будь-якої системи захисту визначається можливістю сталого функціонування системи в цілому, визначення та нейтралізації загроз безпеки, запобігання витоку інформації по різних каналах. Одною з головних задач стає оптимізація проєктування системи захисту.

Таким чином, сучасний стан розвитку інформаційних технологій захисту критичних інформаційних ресурсів показує, що існуючі моделі, методи та засоби не розглядають в комплексі усі принципи забезпечення захисту критичних інформаційних ресурсів технологічних процесів. Аналіз результатів існуючих досліджень і теперішнього стану захисту критичних ресурсів виробництва мінеральних добрив свідчить про відсутність на даний час узагальнюючої оцінки рівня захищеності критичних інформаційних ресурсів.

Функціональна безпека визначає властивість системи (компонента) хімічного виробництва, що полягає у здатності виконувати всі потрібні функції, важливі для безпеки, зберігати потрібні властивості та відповідати заданим характеристикам в усіх передбачених проектом режимах й умовах експлуатації. Закон України від 16.11.2021 «Про критичну інфраструктуру» регламентує питання захисту критичних інформаційних ресурсів та критичної інфраструктури, до якої належить виробництво мінеральних добрив.

Впровадження нових інформаційних технологій дозволяє значно підвищити ефективність технологічних процесів виробництва мінеральних добрив. Але разом з тим розширюється коло вразливостей та загроз для критичних ресурсів виробництва мінеральних добрив. Складність технологічних процесів гранулювання у псевдозрідженому шарі при виробництва мінеральних добрив зумовлює необхідність створення математичної моделі, яка б описувала процеси на мікрорівні, на макрорівні, для задач оптимального керування. Оптимальне керування процесом виробництва мінеральних добрив враховує різноманітні задачі складного виробництва: покращення умов гідродинаміки шару, підвищення ефективності процесу, зменшення вартості процесу переробки.

Завдання дисертаційної роботи

Таким чином, забезпечення функціональної безпеки технологічного процесу виробництва мінеральних добрив, одержання готового продукту заданої якості, вирішення питання оптимального керування процесом отримання гранульованих мінеральних добрив для забезпечення заданого рівня захищеності основних параметрів технологічного процесу передбачає розв’язання таких задач:

- виявити, формалізувати та розробити математичну модель протидії загрозам у системі захисту критичних інформаційних ресурсів виробництва мінеральних добрив;
- розробити імітаційну модель захисту критичних інформаційних ресурсів виробництва мінеральних добрив;
- розробити метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив;
- розробити математичну модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі;
- створити інформаційну технологію захисту критичних ресурсів виробництва мінеральних добрив на основі розроблених моделей та методу;
- розробити оптимальну систему керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором.

Висновки до розділу 1

1. Проведений аналіз сучасного стану розвитку інформаційних технологій захисту критичних інформаційних ресурсів, яке показало, що існуючі моделі, методи та засоби не розглядають в комплексі усі принципи забезпечення захисту критичних інформаційних ресурсів технологічних процесів.

2. На основі аналізу особливостей організації інформаційно-обчислювального процесу на підприємствах уточнена класифікація загроз інформаційній безпеці, а також виявлені загрози, найбільш значущі для даного типу підприємств. З метою створення математичної моделі протидії впливу внутрішніх та зовнішніх загроз при розробці методу оптимізації і інформаційної технології захисту критичних інформаційних ресурсів проведено аналіз математичних моделей захисту інформації, моделей загроз і особливостей їх реалізації.

3. Розглянуті основні підходи до побудови імітаційної моделі захисту критичних інформаційних ресурсів виробництва мінеральних добрив. Встановлена

необхідність забезпечення функціонування інформаційної технології в умовах здійснення нових і невідомих атак.

4. Для підвищення стану захищеності підприємства від загроз порушення інформаційної безпеки необхідно вибрати оптимальний варіант системи захисту інформації. Проаналізовано методи та принципи оптимізації системи захисту інформації критичних ресурсів.

5. Проведено аналіз технологічного процесу виробництва мінеральних добрив у грануляторах із псевдозрідженим шаром. Визначено основні параметри, що впливають на технологічний процес виробництва мінеральних добрив та належать до критичних інформаційних ресурсів. Відомі математичні моделі не враховують зміну вологовмісту гранул, як одного з основних показників якості готового продукту. Разом с тим в існуючих моделях недостатньо уваги приділено урахуванню взаємозв’язку параметрів теплоти кристалізації та пароутворення, що може бути основою для створенню математичної моделі, яка б враховувала більш повно зміну температур гранул та теплоносія.

РОЗДІЛ 2. МОДЕЛЮВАННЯ СИСТЕМИ ЗАХИСТУ КРИТИЧНИХ РЕСУРСІВ ВИРОБНИЦТВА МІНЕРАЛЬНИХ ДОБРИВ

Моделювання системи захисту інформації полягає в її формалізованому представленні в будь-якому вигляді, адекватному системі, що вивчається, і отриманні за допомогою побудованої моделі необхідних характеристик реальної системи. Таким чином, весь процес моделювання можна розділити на дві складові: побудова моделі та реалізація моделі з метою отримання необхідних характеристик системи захисту інформації.

Усі моделі, що використовуються в процесі вивчення та розробки систем захисту інформації, можна поділити на відповідні класи:

До першого класу належать моделі аналізу, які використовуються для визначення поточних чи прогнозованих майбутніх значень характеристик системи. Моделі аналізу призначені для поділу об'єкта на елементи та подальшого їхнього наукового дослідження шляхом вивчення окремих сторін, властивостей, складових, визначення поточних та прогнозування майбутніх значень показників інформаційної безпеки.

Другий клас - моделі синтезу, які використовуються з метою побудови систем і схем їх функціонування, оптимальних за заданим критерієм чи їх сукупності. Моделі синтезу - це процес поєднання різних елементів об'єкту захисту в єдине ціле (систему), дослідження компонентів системи. Вони призначені для забезпечення оптимальної побудови систем захисту інформації. Причому під оптимальністю цих систем розуміється як забезпечення максимального рівня захищеності при заданому рівні витрат, або як забезпечення заданого рівня безпеки при мінімальному рівні витрат.

Третій клас - моделі управління, які використовуються з метою пошуку оптимальних керуючих впливів в процесі функціонування систем захисту інформації. Функціональне призначення моделей цього класу полягає в методичному і

інструментальному забезпеченні прийняття оптимальних рішень в процесі створення і організації функціонування систем захисту інформації.

2.1. Імітаційна модель системи захисту критичних ресурсів виробництва мінеральних добрив

Для комплексної оцінки пропонованих заходів і засобів захисту критичних ресурсів виробництва мінеральних добрив на попередньому етапі проєктування системи захисту інформації підприємства використовується імітаційна модель. При побудові імітаційної моделі захисту критичних інформаційних ресурсів, який буде складатися з реального обладнання, виникає основна проблема, яку необхідно вирішити. Це висока вартість компонентів для побудови захищеної мережі. Тому пропонується побудувати захищену комп'ютерну мережу на базі спеціальної платформи-емулятора, яка дозволяє віртуалізувати різне мережеве обладнання, створити на їх базі повноцінну віртуальну мережу і провести необхідне тестування.

Для побудуви захищеної віртуальної мережі скористались платформою GNS3(Graphical Network Simulator-3). GNS3 -це графічний емулятор мережі, який дозволяє моделювати віртуальну мережу з мережевого обладнання більше ніж 20 різних виробників на локальному комп'ютері, приєднувати віртуальну мережу до реальної [39], додавати в мережу повноцінний комп'ютер, підтримується сторонні програми для аналізу мережевих пакетів, зокрема Wireshark. Також наявна підтримка утиліти SolarWinds Response Time Viewer, яка приймає на вхід збережені дампи трафіка і аналізує час відклику мережі і об'єми переданих даних, а також представляє які додатки і ресурси були виявлені в дампі, що піддавався аналізу. Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проєктів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також серверів під управлінням мережевих операційних систем. Для зручності тестування відразу після встановлення реалізована підтримка програм для віртуалізації, що дозволяє додати в мережу віртуальну машину і проводити відповідні тести мережі, зокрема VMware та VirtualBox.

Для побудови імітаційної моделі захисту критичних інформаційних ресурсів на базі прикладного програмного забезпечення GNS3 обрано комп'ютерну мережу підприємства виробництва мінеральних добрив, з використанням одного брандмауера Cisco ASA 5520, який поділяє мережу компанії на демілітаризовану зону, внутрішню та зовнішню мережу [24-26, 40]. Зональна модель є доволі гнучкою, інтерфейси присвоюються зонам, а політика перевірки – трафіку, що передається між зонами (рис. 2.1).

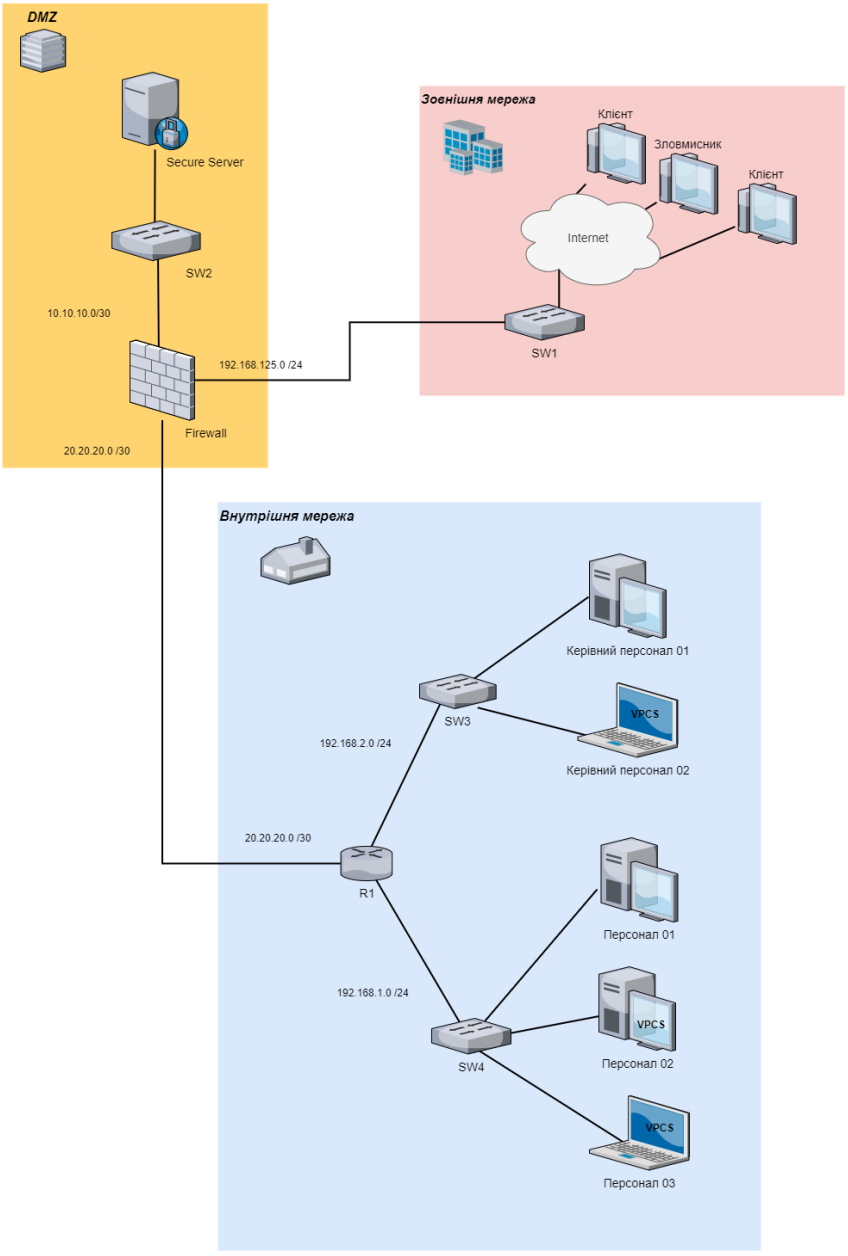

Рис. 2.1. Топологія мережі в GNS3

Наведена таблиця маршрутизації віртуальної мережі, всі мережеві пристрої інтерфейси їх підключення з IP-адресою кожного, маска підмережі та шлюз за замовчуванням (табл. 2.1).

Таблиця 2.1

Таблиця маршрутизації віртуальної мережі

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
Firewall	Gig0	192.168.125.130	255.255.255.0/24	192.168.125.1
	Gig1	20.20.20.1	255.255.255.252/30	-
	Gig2	10.10.10.1	255.255.255.252/30	10.10.10.2
R1	Fa0/0	20.20.20.2	255.255.255.252/30	20.20.20.1
	Fa1/0	192.168.2.1	255.255.255.0/24	-
	Fa2/0	192.168.1.1	255.255.255.0/24	-
Internet		192.168.158.1	255.255.255.0/24	-
Керівний персонал 01- ПК	Мер. адапт	192.168.2.10	255.255.255.0/24	192.168.2.1
Керівний персонал 02- ПК	Мер. адапт	192.168.2.11	255.255.255.0/24	192.168.2.1
Персонал 01-ПК	Мер. адапт	192.168.1.10	255.255.255.0/24	192.168.1.1
Персонал 02-ПК	Мер. адапт	192.168.1.11	255.255.255.0/24	192.168.1.1
Персонал 03-ПК	Мер. адапт	192.168.1.12	255.255.255.0/24	192.168.1.1
Secure Server	Мер. адапт	10.10.10.2	255.255.255.252/30	10.10.10.1

В даній топології для побудови імітаційної моделі захисту критичних інформаційних ресурсів використовуються наступні мережеві пристрої: міжмережевий екран Cisco ASA 5520 (ім’я хоста Firewall), маршрутизатор Cisco 3745 (ім’я хоста R1), мережеві комутатори (SW1, SW2, SW3, SW4) [17, 41]. Для надання доступу віртуальній мережі до інтернету використовується loopback інтерфейс (Internet). Також в мережу додані дві віртуальні машини на операційній системі Windows 8.1 (Керівний персонал 01- ПК, Персонал 01-ПК) аби імітувати реальні комп’ютери в мережі. Робочі станції інших працівників та заступника керівника емулюються якраз за допомогою VPCS (virtual PC simulator). Virtual PC Simulator (VPCS) - це простий спосіб емуляції ПК. VPCS використовує малу кількість пам'яті,

дозволяє емулювати ПК без графічного інтерфейсу, виконувати прості команди, такі як ping, для перевірки підключення до вашої мережі GNS3.

Мережа керівництва та мережа працівників знаходиться за інтерфейсом Gig1 міжмережевого екрану Firewall, за маршрутизацію трафіку між ними відповідає маршрутизатор R1 [42-43]. На брандмауері Cisco ASA налаштовується NAT, для запобігання та обмеження запитів ззовні. Для більш зручних функцій управління і моніторингу налаштовується можливість підключення по протоколу HTTPS до ASDM. Доступ до Cisco ASDM здійснюється безпосередньо за допомогою Web-браузера з будь-якого комп'ютера мережі, що підтримує Java, таким чином, адміністраторам системи безпеки надається можливість швидкого і надійного доступу до пристроїв захисту Cisco ASA і має функціонал аналогічний консольному підключенню. Для безпечного віддаленого підключення до маршрутизатора R1 на ньому налаштовується SSH версії 2, а також заборонено всі інші з’єднання не по протоколу SSH. В демілітаризованій зоні знаходиться SecureServer, який виконує функції Веб-сервера та FTP сервера. Веб-сервер доступний для керівництва та працівників, а також з мережі інтернет. Користувачі маються доступ в інтернет лише по 80-му порту та по ftp. Інші порти закриті. З мережі інтернет доступ відкритий тільки на Веб-сайт і лише по 80-му порту [44-48].

Програмні засоби для тестування.

Hping3 це безкоштовний генератор пакетів і аналізатор для TCP/IP протоколу. Hping, де факто, один з обов'язкових інструментів для аудиту безпеки і тестування міжмережевих екранів і мереж, він використовувався для виконання експлойта техніки сканування Idle Scan, яка зараз реалізована в сканері портів Nmap. Як і більшість інструментів, що використовуються в комп'ютерній безпеці, hping3 корисний для експертів з безпеки, та використовується для [49]:

- traceroute / ping / probe (трасування / пінг / зондування) хостів;
- тестування правил брандмауера;
- тестування IDS (систем виявлення вторгнення);
- мережевих досліджень;
- стрес-тестувань мережі;

- вивчення TCP / IP (hping була використана в мережевих курсах AFAIK);
- написання реальних програм, пов'язаних з TCP / IP тестуванням і безпекою;
- автоматизації тестів по фільтрації трафіку;
- створення робочої моделі експлойтів;
- досліджень в звіряння мереж і безпеки, коли потрібно емулювати комплексне TCP / IP поведінку.

Zenmap - офіційний GUI для програми Nmap Security Scanner. Zenmap - це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Вона розроблена для швидкого сканування великих мереж, хоча прекрасно справляється і з одиничними цілями. Zenmap використовує сирі IP пакети оригінальними способами, щоб визначити які хости доступні в мережі, які служби (назва програми і версію) вони пропонують, які операційні системи (і версії ОС) вони використовують, які типи пакетних фільтрів/брандмауерів використовуються і ще дюжини інших характеристик. У той час як Zenmap зазвичай використовується для перевірки безпеки, багато мережеві і системні адміністратори знаходять її корисною для звичайних завдань, таких як контролювання структури мережі, управління розкладами запуску служб і облік часу роботи хоста або служби [50].

Вихідні дані Nmap це список просканованих цілей з додатковою інформацією щодо кожної залежно від заданих опцій. Ключовий інформацією є "таблиця важливих портів". Ця таблиця містить номер порту, протокол, ім'я служби і стан. Стан може мати значення open (відкритий), filtered (фільтрується), closed (закритий) або unfiltered (не фільтрують). Відкрито означає, що додаток на цільовій машині готове для встановлення з'єднання / прийняття пакетів на цей порт. Фільтрується означає, що брандмауер, мережевий фільтр або якась інша перешкода в мережі блокує порт, і Nmap не може встановити відкритий цей порт або закритий. Закриті порти не пов'язані ні з яким додатоком, так що вони можуть бути відкриті в будь-який момент.

Wireshark - це аналізатор мережевого трафіку. Його завдання полягає в тому , щоб перехоплювати мережевий трафік і відображати його в детальному вигляді. Wireshark може перехоплювати трафік різних мережевих пристроїв, відображаю- чи

його ім'я (включаючи бездротові пристрої). Підтримування того або іншого пристрою залежить від багатьох факторів, наприклад від операційної системи та має безліч протокольних декодувальників (TELNET , FTP , POP , RLOGIN , ICQ , SMB , MySQL , HTTP , NNTP , X11 , NAPSTER , IRC , RIP , BGP , SOCKS 5 , IMAP 4 , VNC , LDAP , NFS , SNMP , MSN , YMSG і інші). Wireshark дозволяє зберігати і відкривати раніше збережений мережевий трафік. Системні адміністратори використовують його для вирішення проблем в мережі, розробники використовують його для налагодження мережевих додатків, звичайні користувачі використовують його для вивчення внутрішнього устрою мережевих протоколів [51].

Сканування мережі.

Для сканування мережі обрано програму Zenmap, утиліта для дослідження мережі та сканер портів. Для сканування обираються діапазони адрес для сканування задля економії часу. Проведено збір інформації про мережу глобальної мережі, як наслідок налаштування NAT відображається лише налаштований інтерфейс Cisco ASA (рис. 2.2).

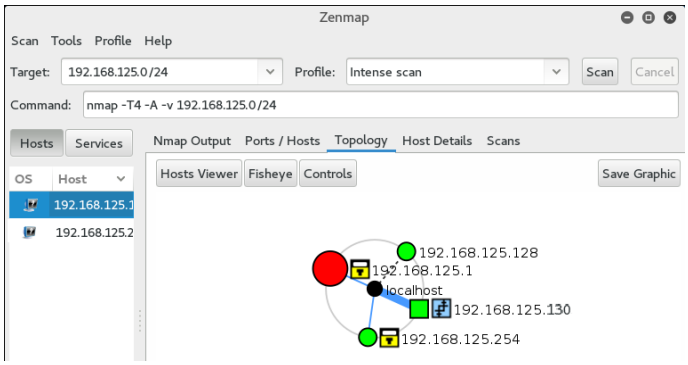

Рис. 2.2. Сканування локальної мережі з зовнішньої мережі

Якщо зловмисник має доступ до мережі зсередини, то йому вдасться просканувати топологію мережі і знайти можливі вразливості. Утиліта дозволяє визначити, які хости доступні в мережі (рис. 2.3), версію операційної системи, які служби на них запущені, назви запущених додатків і номера і стани портів. Якщо не заборонити стандартне підключення до маршрутизатора по мережевому протоколу telnet, то Zenmap це виявить (рис. 2.4).

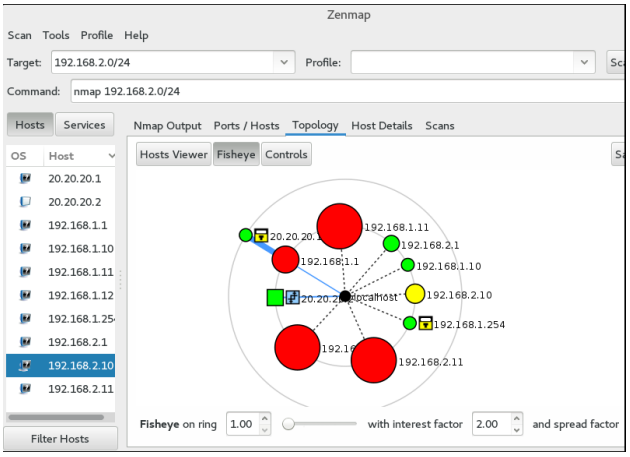

Рис. 2.3. Сканування локальної мережі зсередини

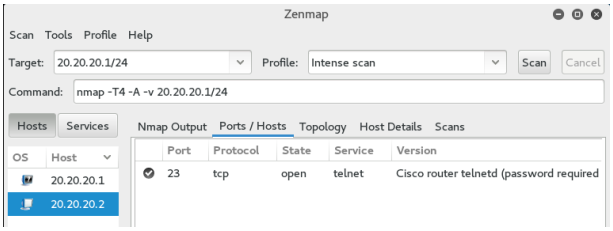

Рис. 2.4. Сканування маршрутизатора Cisco 3745 з ввімкненим Telnet

В загальному вигляді після детального сканування мережевого пристрою матимемо результат утиліта Cisco 3745 з ввімкненим Telnet, утилітой Zenmap зроблено припущення щодо операційної системи, знайдено відкритий порт, визначена мережева адреса, як показано на рис. 2.5.

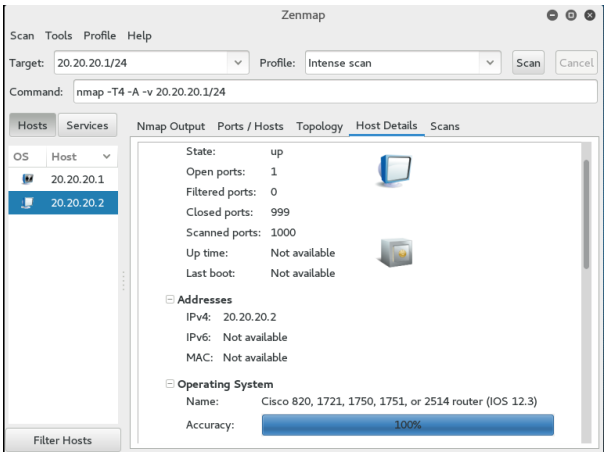

Рис. 2.5 Детальна інформація про відсканований Zenmap хост

На Cisco ASA присутній функціонал захисту від сканування, зокрема якщо в повідомленнях вказано одна і та ж адреса джерела, це повідомлення може говорити

про збір базових відомостей або спробі сканування портів та IP-пакет відхиляється ACL (рис. 2.6).

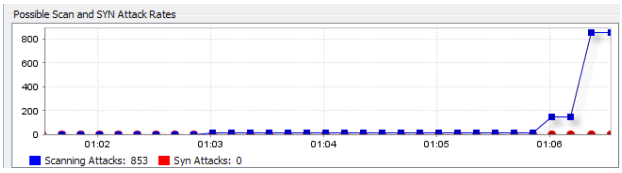

Рис. 2.6. Статистика відхилених пакетів Cisco ASA під час сканування мережі

Стрес-тест мережі.

Атака на відмову в обслуговуванні (DoS) або атака розподілена відмова вобслуговуванні (DDoS) - це спроба зробити ресурси машини едоступними для користувачів. Хоча кошти, мотиви і цілі DoS розрізняються, головна її суть залишається незмінною - на час або на невизначений термін перервати або призупинити послуги хоста, з'єднаного з Інтернетом. Один із загальних методів атаки - це насичення цільової машини зовнішніми запитами з'єднання, в зв'язку з чим вона не може відповісти на легітимний трафік або відповідає так повільно, що є по суті недоступною [18, 43].

Syn-Flood Attack - це атака при якій ініціатор в пакеті SYN ставить підроблений Source IP-address або ігнорує відповіді від сервера Syn + Ack. При відкритті тисяч таких половинчастих сесій витрачаються ресурси сервера, який змушений запам'ятовувати параметри кожної і в підсумку може відмовити.

Для проведення DoS використаємо влаштовану в збірку Kali Linux утиліту hping3 використовуючи випадкові IP-адреси джерела DoS. Дана програма без графічного інтерфейсу, для здійснення Syn-Flood Attack атаки обрані наступні команди, як показано на рис. 2.7:

hping3 - ім'я додатка.

-c 10000 - Кількість пакетів для відправки.

-d 120 - Розмір кожного пакету, який буде відправлений на цільову машину.

-S - Відправка тільки пакети SYN.

-w 64 - Розмір вікна TCP.

-p 80 - Порт призначення, ви можете використовувати будь-який порт.

-flood - Відправлення пакетів так швидко, як можливо, не піклуючись про відображення вхідних пакетів (Syn-Flood Attack).

-rand-source - Використання випадкових IP адрес джерела. Також можна використовувати -a або -spoof щоб заховати ім'я хоста

192.168.125.130 - Цільовий IP адреса або IP адреса цільової машини. Також можна використовувати адресу сайту.

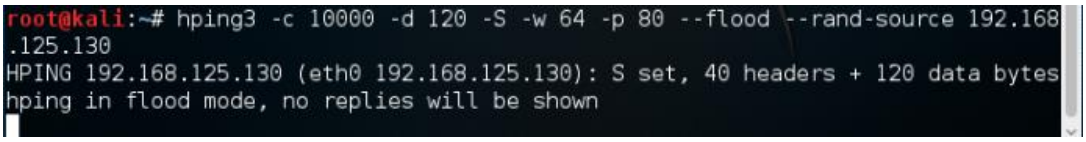

Рис.2. 7. DoS-атака в hping3

Cisco ASA автоматично транслює пакети які надходять до неї по 80 порту на сервер, а при атаці на відмову ресурсів це спричиняє додаткове навантаження на сервер, що спричиняє відмову у доступі звичайним користувачам.

Пропінгуємо мережу без навантаження (результат показано на рис. 2.8) та мережу під навантаженням (рис. 2.9). А також скористаємось програмою Wireshark, за допомогою якої можна проаналізувати проведену DoS атаку. Відфільтрувавши прослуханий за допомогою Wireshark трафік між зловмисником та Cisco ASA за критерієм ICMP можна побачити, що в зв’язку з DoS атакою створюється навантаження на Cisco ASA, в зв'язку з яким створюються черги на оброблення запитів і відповіді приходять з певною затримкою або відповідь відсутня взагалі, як показано на рис. 2.10.

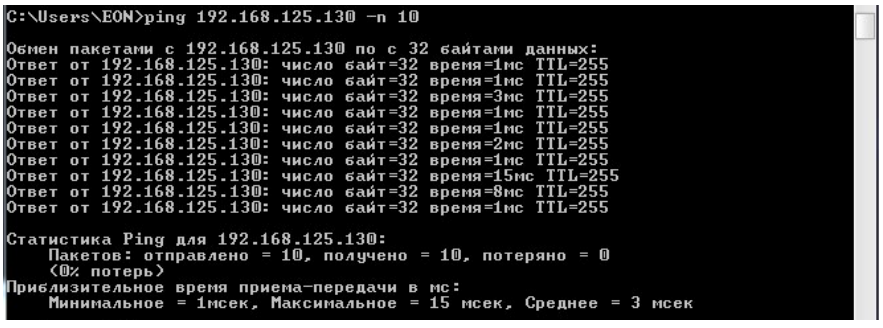

Рис. 2.8. Пінг мережі без навантаження

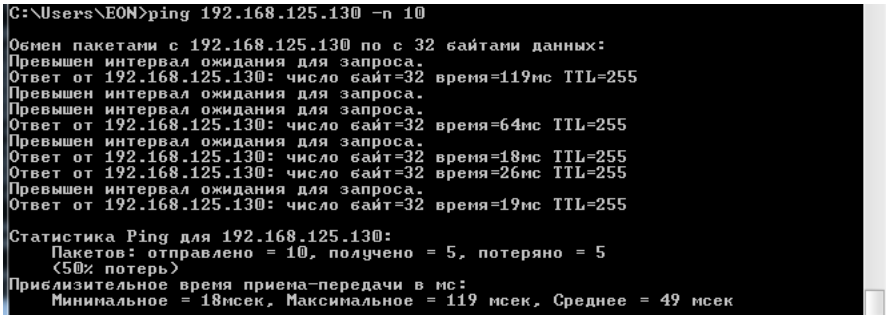

Рис. 2.9. Пінг мережі під навантаженням 10000 пакетів/секунду

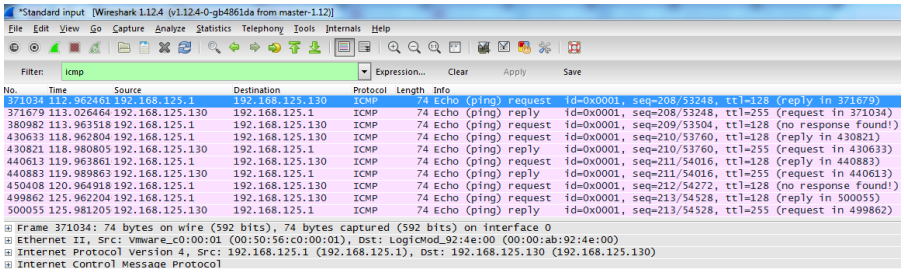

Рис. 2.10. Відфільтрований ICMP трафік під час DoS-атаки

Для вирішення даної проблеми ASA використовує TCP SYN Cookies: ASA захищає сервер і не транслює на нього всі з'єднання. Замість того щоб запам'ятовувати всі ці половинчасті сесії, ASA відповідає на кожну з них, але фактичне з'єднання з сервером здійснює тільки при отриманні 3-го відповіді Ack. Embryonic-conn-max 5 означає, що максимум буде дозвіл до 5 половинчастих з'єднань. Необхідно задати наступні налаштування:

access-list outside_mpc line 1 extended permit tcp any object dmz-server real

class-map no-syn-flood-class

match access-list outside_mpc

policy-map NO-SYN-FLOOD

class no-syn-flood-class

set connection conn-max 0 embryonic-conn-max 5 per-client-max 0 per-client-embryonic-conn-max 0 random-sequence-number enable

service-policy NO-SYN-FLOOD interface outside

Без додаткових налаштувань при Syn-Flood атаці в нас відбувається 1625 активних підключень до сервера, що й спричиняє відмову в обслуговуванні, як показано на рис. 2.11.

Якщо застосувати дані налаштування ASA буде створювати окрему чергу з половинчастих сесій, які не зможуть кардинально вплинути на робот сервера, як наслідок отримаємо лишень 5 половинчастих з'єднань, що і продемонстровано на рис. 2.12 та свідчить про ефективність захисту відданого типу атак при правильному налаштування міжмережевого екрану.

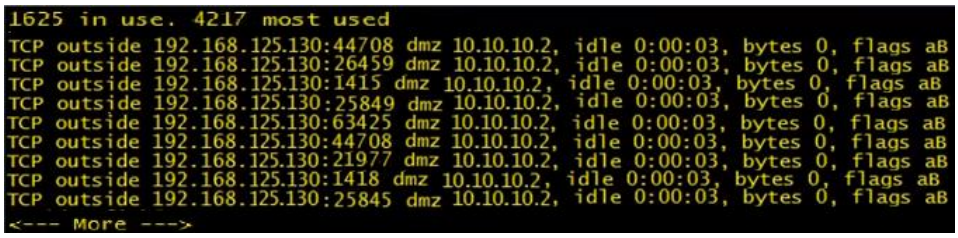

Рис. 2.11. Активні сесії при SYN-flood атаці без налаштувань захисту від неї

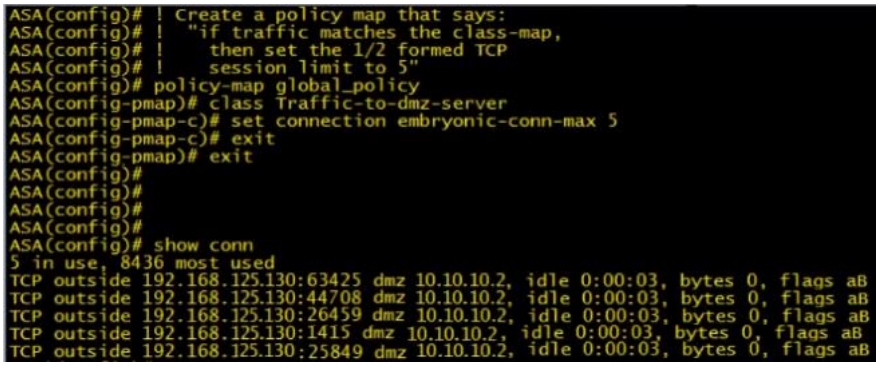

Рис. 2.12. Активні сесії при SYN-flood атаці з налаштуваннями захисту від неї

Таким чином, для тестування побудованої імітаційної моделі системи захисту критичних ресурсів проведено сканування мережі та портів мережних пристроїв за допомогою утиліти Zenmap ззовні та налаштувань ASA та NAT, сканування не дало нічого окрім знайденої IP-адреси зовнішнього інтерфейсу ASA, та сканування зсередини, в результаті якого була зібрана інформація про внутрішню мережу включаючи внутрішній інтерфейс Cisco ASA. За допомогою утиліти hping3 було реалізовано стрес-тест мережі - Syn-Flood атака на відмову сервера. Реалізовано протидію даній атаці щляхом використанням TCP SYN Cookies.

2.2. Метод тестування системи захисту критичних ресурсів виробництва мінеральних добрив на імітаційній моделі

Для тестування системи захисту критичних ресурсів періодично проводиться аналіз інформаційних ризиків, який дозволяє виявити загрози інформаційній безпеці і в свою чергу використовувати та впроваждувати відповідні заходи їх нейтралізації. В кількісних методиках ризику оцінка приводиться числовим значення, в якості вхідних даних зазвичай використвується накопичена статистика по інцидентах. Проте відсутність достатньої кількості статистичних даних призводить до зниження адекватності результатів оцінки.

Метод iRisk характеризується формально однією з найпростіших оцінкою кількісних ризиків інформаційної безпеки системи захисту критичних ресурсів. В загальному вигляді розраховується за наступною формулою:

$$iRisk = (Vulnerability * Threat) - Controls \qquad (2.1)$$

де Vulnerability - оцінка вразливості, Threat – оцінка загрози, Control – оцінка мір безпеки.

Дана методика використовує в собі іншу методику CommonVulnerability Scoring System v3.0 (CVSS V3) для оцінки вразливостей. При оцінці загрози виконується оцінка ймовірності реалізації загрози і міри її впливу. Міра впливу загрози оцінюється через показники збитків. Для оцінки ймовірності реалізації конкретної загрози використовують оцінки двох показників: ARO–очікувана кількість реалізацій загроз протягом року, а також рівень знань і необхідний рівень доступу порушника в АС.

Формально розрахунок відбувається за не складною формулою, проте через те, що методика в собі містить загальну систему оцінки вразливостей CVSS, який на практиці підтримується лідерами ринку в сфері захисту інформації, що дає змогу користуватись постійно актуальними коефіцієнтами для розрахунку вразливостей, а також мати перелік всіх основних вразливостей, які пов'язані з всіма сучасними

програмними продуктами, що можуть використовуватись в системах захисту критичних ресурсів.

Виходячи з ріняння *iRisk = (Vulnerability x Threat) – Controls* узагальнена оцінка ризику iRisk розраховується з урахуванням наступних параметрів: Vulnerability - оцінка вразливості, Threat – оцінка загрози, Control – оцінка мір безпеки [52].

Спершу розрахуємо Vulnerability (вразливість), для чого використаємо стандарт CVSS v3 [53]. Розрахунок відбувається за схемою яка наведена на рис. 2.13. Під час обрахунку використовується велика кількість коефіцієнтів, тому для зручності скористаємось програмним забезпеченням Національного інституту стандартів і технологій і просто задавши правильно параметри отримаємо результат обчислень у вигляді шкали від 1 до 10, де 1 відповідатиме найнижчий рівень, тобто відсутність вразливості, а значенню 10 відповідатиме критична вразливість, яку необхідно негайно усунути.

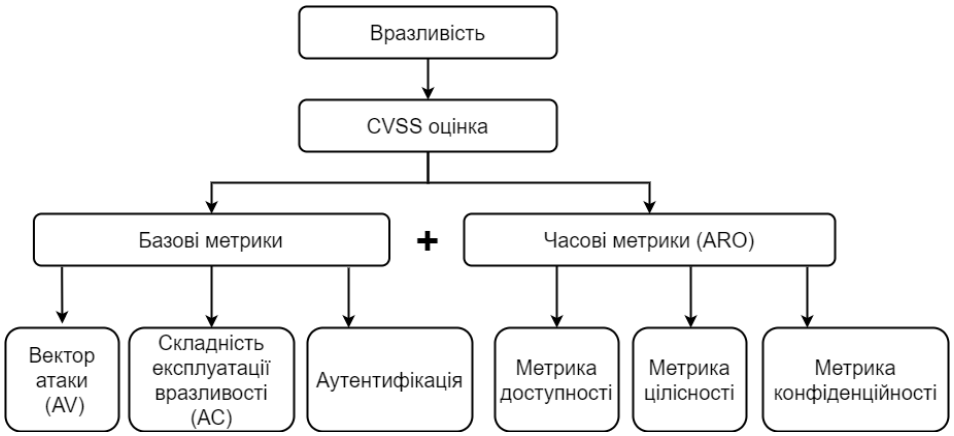

Рис. 2.13. Загальна схема розрахунку вразливості CVSS v3

В стандарт входить три групи метрик, необхідних для розрахунку, базова, часова та контекстна.

Базові метрики описують характеристики вразливості, котрі не змінюються з часом і не залежать від середовища виконання. Цими метриками описується складність експлуатації вразливостей і потенційний збиток конфіденційності, цілосності і доступності.

Часові метрики вносять в загальну оцінку поправку на повноту інформації про вразливість.

Контексні метрики експерти з безпеки можуть внести в результуючу оцінку поправки з урахуванням інформаційного середовища.

Значення метрики прийнято публікувати у вигляді пари з вектора (конкретні значення окремих показників) і числового значення, розрахованого на основі всіх показників і за допомогою формули, визначеної в стандарті. На рис. 2.14 зображено всі необхідні параметри для прозрахунку контекстної метрики.

Вектор атаки – ступінь віддаленості потенційного атакуючого від об'єкта атаки. В випадку імітаційної моделі кібербезпеки розглядаємо випадок, коли атака проводиться з мережі. Local в тому випадку коли атакуючому необхідна локальна сесія, або він авторизований користувач, а Physical, у випадку коли необхідний фізичний доступ до підсистеми.

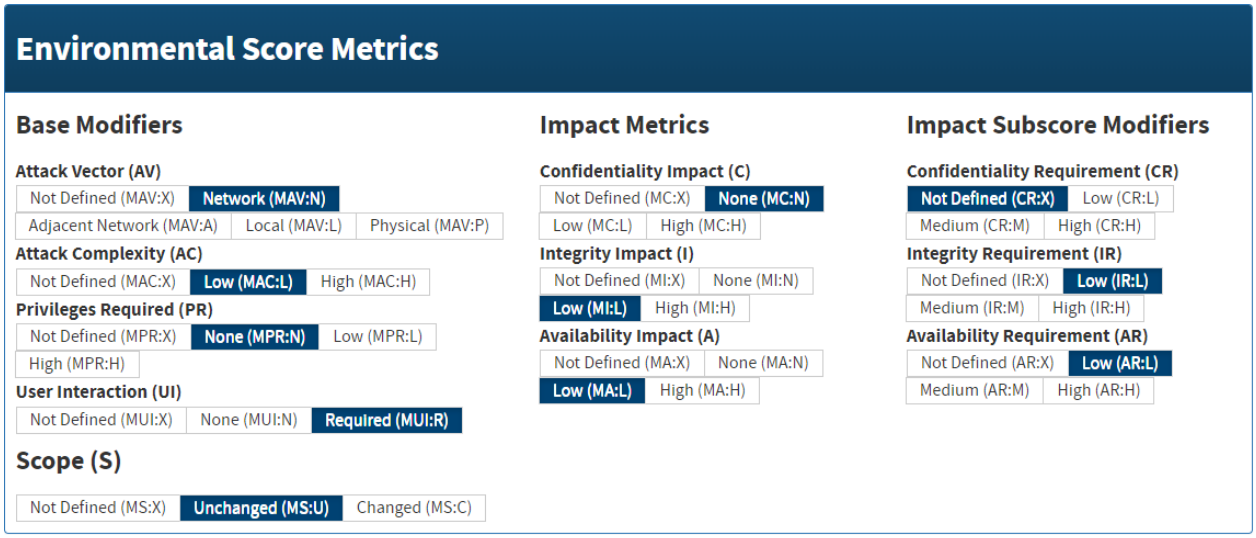

Рис. 2.14. Контекстна метрика імітаційної моделі

Access Complexity – це якісна оцінка складності проведення атаки. Вона трактується з суб'єктивної точки зору експерта. Для прикладу реалізація підробки SSL сертифіката шляхом проведення атаки на сертифікат додатку Microsoft Outlook оцінюється в рівень High, а на web додаток Amazon medium.

Аутентифікація, мається на увазі чи потрібна вона взагалі і засновується на тому яку кількість незалежних процесів аутентифікації необхідно пройти зловмиснику аби скористатись вразливістю.

User Interaction (UI) мається на увазі чи треба для успішності атаки зробити якісь дії користувачу.

Границі експлуатації (Scope) чи дозволяє есплуатація вразливості порушити конфіденційність, цілісність чи доступність іншого компонента системи.

Метрики взаємодії Confidentiality Impact (C), Integrity Impact (I), Availability Impact (A) оцінюють ступінь впливу на конфіденційність, цілісність і доступність компонента, котрий піддається атаці.

Часові метрики мають на увазі, чи описана вразливість і засоби як нею можна скористатися публічно чи навпаки існує лише теоретична можливість есплуатації.

Контексні метрики дозволяють Confidentiality Requirement (CR), Integrity Requirement (IR), Availability Requirement (AR) задекларувати яка характеристика даних об’єкта, на який проволиться атака найбільше впливає на функціональність системи.

Оцінка загрози (Threat)

Згідно з даним стандартом загроза пояснюється як негативна подія, котра може виникнути в результаті того, що буде використано переваги вразливості. Для того аби зробити рівняння максимально простим і зрозумілим, методика iRisk концентрується на двох основних компонентах: вплив і вірогідність. На рис. 2.15 представлена схема оцінки загроз в методі iRisk.

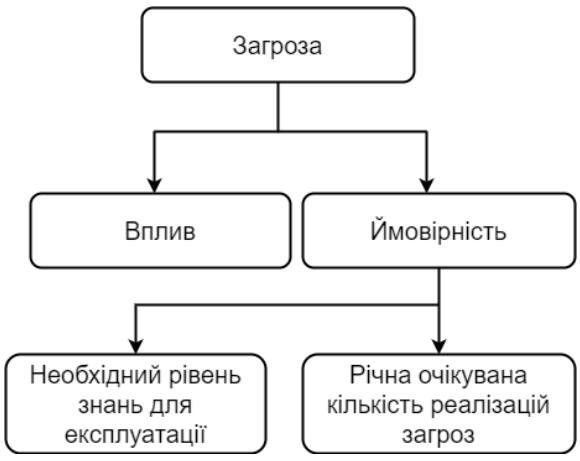

Рис. 2.15. Схема оцінки загроз в методі iRisk

Вплив (Impact) - це сума шкоди, яку ця інцидент принесе організації. В рамках рівняння iRisk SecureState в даний час використовуються наступні критерії для

визначення впливу. За замовчуванням втановлено наступні значення, проте їх можна змінити відповідно до потреб оцінюваного об’єкту.

Фінансовий(25) – чи можуть загрози зруйнувати фінансові потоки організації.

Стратегічний(15) – чи можуть загрози призвести до довгострокових стратегіних втрат .

Операціний(25) – чи матимуть загрози на безперебійність роботи.

Відповідність законодавству (25) – чи зможуть загрози вплинути на здатність дотримуватися стандартів.

Репутація (10) чи може вплинути на відпосини з клієнтами.

Іншим основним компонентом є загрози є ймовірність. Для оцінювання ймовірності в iRisk береться до уваги два чинника, річна очікувана кількість реалізацій загроз та рівень знань, та доступу необхідний зловмиснику.

Загроза розраховується за формулою 2.2, де Likelihood (ймовірність) – це кореляція з таблиці 2.2. Якщо загроза знаходиться в шкалі від 100 до 50 – рівень ризику високий, від 50 до 10 – середній від 1 до 10 – низький.

$$Threat = \text{Impact} * \text{Likelihood} \quad (2.2)$$

Таблиця 2.2

Таблиця кореляції між рівень знань/доступу та річною кількістю реалізації загроз (ARO)

	Річна очікувана кількість реалізацій загроз			
Рівень знань/доступу	Дуже часто (1.0 - 0.81)	Часто (0.8 - 0.51)	Нечасто (0.5 - 0.21)	Рідко (0.0 - 0.2)
Ззовні, немає технічних навичок (1.0)	1.0 - 0.81	0.8 - 0.51	0.5 - 0.21	0.0 - 0.2
Ззовні, деякі технічні навички (0.9)	0.9 - 0.729	0.72 - 0.459	0.45 - 0.189	0.0 - 0.18
Інсайдер, звичайний користувач (0.8)	0.9 - 0.729	0.72 - 0.459	0.45 - 0.189	0.0 - 0.18
Ззовні, продвинуті технічних навичок(1.0)	0.8 - 0.648	0.64 -0.408	0.4 - 0.168	0.0 - 0.16
Ззовні, есперт (0.7)	0.7 - 0.567	0.56 -0.357	0.35 - 0.147	0.0 - 0.14
Ззовні, есперт зі злому (0.6)	0.6 - 0.486	0.48 -0.306	0.3 - 0.126	0.0 - 0.12
Спонсорований державою (0.5)	0.5 - 0.405	0.4 - 0.255	0.25 - 0.105	0.0 - 0.1
Інсайдер, привілейований доступ (0,5)	0.5 - 0.405	0.4 - 0.255	0.25 - 0.105	0.0 - 0.1
Інсайдер, адміністратор (0.2)	0.2 - 0.162	0.16 -0.102	0.1 - 0.042	0.0 - .04
Інсайдер експерт зі злому (0.1)	0.1 - 0.081	0.08 -0.051	0.05 - 0.021	0.0 - 0.02

Структура параметра Control (оцінка мір безпеки) представлена на рис. 2.16. На підставі визначення організаціх ISACA iRisk для забезпечення безпеки можуть застосовуватись профілактичні, засоби направлені на виявлення, виправлення чи стримування.

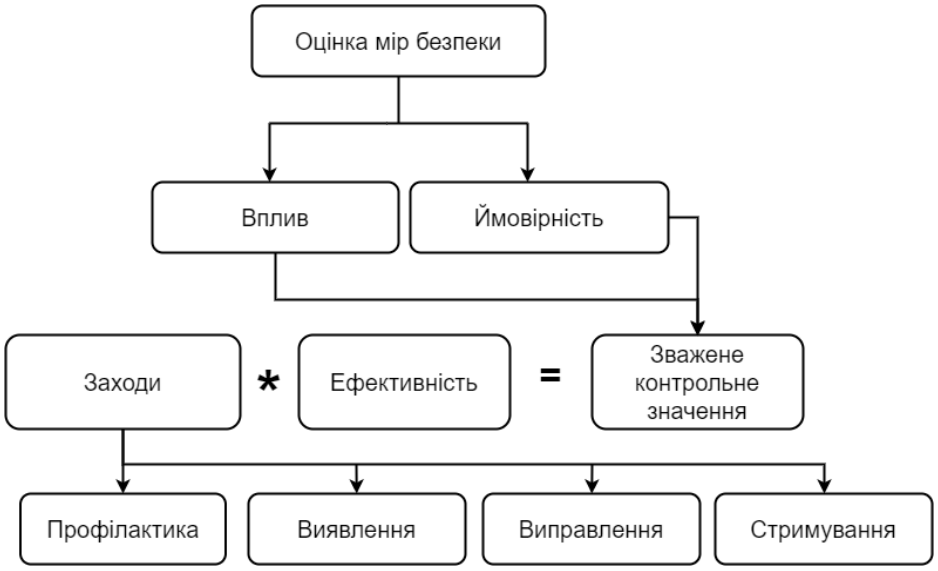

Рис. 2.16. Структура параметра Control метода iRisk

Відповідно до стандарту заходи мають наступні рейтинги профілактичний – 5, виявлення – 4, виправлення – 3, стримування –3.

Наступним кроком є визначення Controls (ефективності), вона згідно стандарту має п’ятибальну шкалу, оцінка 5 ставиться у тому випадку, якщо засоби захисту інформаціїї в мережі значно перевищують мету, 4 – перевищує мету, 3 – реалізація відповідає меті, 2 – реалізація не повністю задовольняє свою мету, 1 – трохи відповідає своїй меті.

Склавши показники за CMMI отримуємо наступні значення:

- Optimized (801 – 1000) – засіб не може бути розроблений або реалізований краще
- Managed (601 – 800) – продовжує вдосконалюватись
- Defined (401 – 600) – засоби захисту чвтко визначені та зменшують ризик до помірного
- Initial/Ad-Hoc (1 – 200) – забезпечує лише деяку цінність захисту

Три основні компоненти, які фігурують в методі iRisk збалансовують один одного. Найвищий можливий бал для загрози становть 100, який помножений на максимальну вразливість (10). Тобто потенційно 1000 балів, яка компенсується потенційно ідеально реалізованим захистом, в кінці лишатиме нульовий ризик. На практиці, це маже не досяжно і в будь-якому випадку лишається якась частина залишкового ризику. Тобто ризик варіюється в значеннях від 0 до 1000, в даному випадку чим менше значення отримуємо, тим захищенішою є АС.

Побудована імітаційна модель захисту критичних ресурсів виробництва мінеральних добрив має не так багато вразливостей, через якісне обладнання, розмежування доступу, яке поділяє мережу на демілітаризовану зону, внутрішню та зовнішню мережу, а також налаштувань мережі, через які, обмежена можливість доступу до мережі ззовні, обмежена кількість половинчастих з'єднань, що призводить до зменшення ефективності DdoS атак, можливості сканування мережі та ін. Та все ж, залишаються вразливості на програмно-апаратному рівні. Далі ми розглянемо деякі з них, розрахунок захищеності імітаційна модель захисту критичних ресурсів виробництва мінеральних добрив буде проведено методом iRisk.

2.2.1 Вразливість Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384)

Вразливість мережевого обладнання Cisco, якою може скористатись зловмисник зсередини мережі, якщо він авторизований як користувач. Вразливість виникає через помилку у реалізації авторизації HTTP/ HTTPS AAA авторизації (user profile) AAA, що дозволяє автентифікованому користувачеві виконувати будь-які довільні команди програмного забезпечення Cisco IOS, налаштовані для рівня привілеїв користувача [54].

Так як *iRisk = (Vulnerability x Threat) – Controls*, то для розрахунку Vulnerability обрахуємо базову метрику, для більшої коректності робимо поправку на захищеність імітаційної моделі і розраховуємо метрику середовища і часову, як і було описано вище.

Base Score Metrics{ Attack Complexity = Low; Privileges Required = Low; User Interaction = None; Scope= Unchanged; Confidentiality Impact = High; Integrity Impact = High; Availability Impact = High}

Temporal Score Metrics Score Metrics { Exploitability = Functional exploit exist; }

Environmental Score Metrics{ Base Modifiers{ Attack Vector = Local; Attack Complexity = Low; Privileges Required = Low; User Interaction = None;} { Scope = Unchanged;} { Impact Metrics{ Confidentiality Impact = Low; Integrity Impact = Low; Availability Impact = High;}}{ Impact Subscore Modifiers{ Confidentiality Requirement = Low; Integrity Requirement = Low; Availability Requirement = Low}}}}

Результуючим обчисленням базового рівня є оцінка разливості в 7.8/10, що і наведено на рис. 2.17.

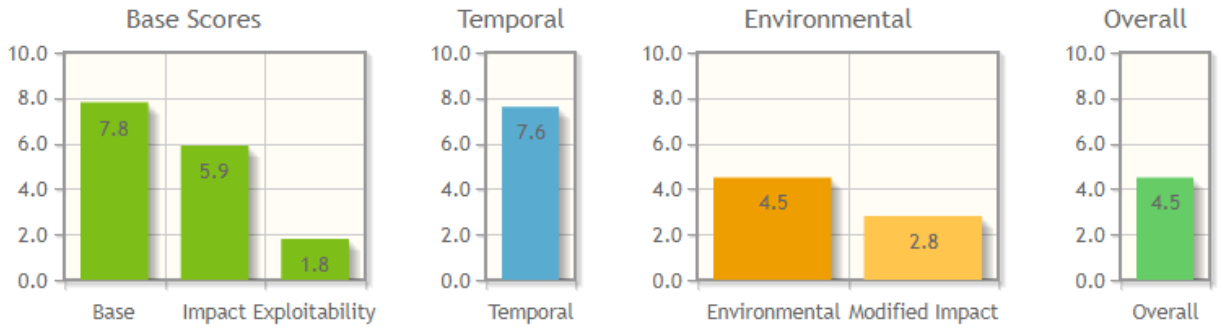

Рис. 2.17. Результуюча вразливість CVE-2012-0384 для імітаційної моделі

*Threat = Impact*Likelihood*, враховуючи те, що загроза повинна реалізовуватись з середини і перш за все орієнтована на те, що нею скористається звичайний користувач без адміністраторських прав, і очікувану кількість загроз оцінити як високу, то з таблиці 2.2 оберемо кореляційне значення *Impact = 0.9*. Звісди, *Threat = 0.9 * 100 = 90.*

Судячи з наведеного вище, значення Controls оцінюємо в 650, що означатиме продовжує розвиватись.

Тобто значення для вразивості Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384) *iRisk = (7.8 * 90) – 650 =50*.

2.2.2. Вразливість Cisco Access Control Bypass Vulnerability (CVE-2012-1342)

Вразливість маршрутизаторів Cisco, яка дозволяє віддаленим атакам обходити Access Control List (ACL), тобто список контролю доступу, який визначає хто або що

може отримувати права доступу до об'єкта. Вразливість дозволяє неаутентифікованому віддаленому зловмиснику обходити список контролю доступу та відправляти мережевий трафік, який повинен бути відхилений. Реалізація вразливості призводить до порушення цілісності АС [55].

За аналогічною схемою як і для вразливості CVE-2012-0384 розрахуємо значення iRisk.

Base Score Metrics{ Attack Vector = Network; Attack Complexity = Low; Privileges Required = None; User Interaction = None; Scope= Changed; Confidentiality Impact = None; Integrity Impact = Low; Availability Impact = Impact None}

Що при розрахунку в CVSS v3.0 калькуляторі дає значення *Vulnerability = 5.8.*

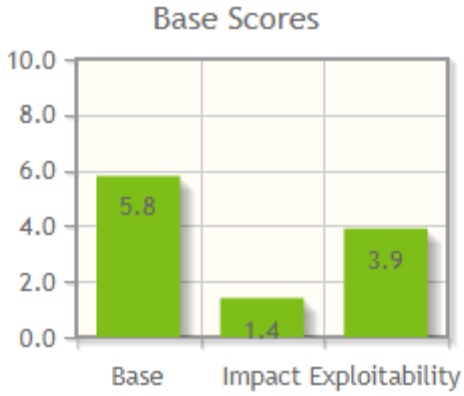

Рис. 2.18. Базова метрика вразливості Cisco Access Control Bypass Vulnerability

Розрахунок значення *Threat* (загрози) = *1.4 *0.72*100 = 108,* звідси значення iRisk= (5.8 * 108) – 610 =16.4, що означатиме, що вразливість буде приблизно рівна нулю, тобто можна зробити висновок, що даною вразливістю зловмисник може скористатись з малою ймовірнюстю.

2.2.3. Вразливість EternalBlue (CVE-2017-0144)

Дана вразливість використовує вразливість в реалізації протоколу Server Message Block v1 (SMB). Зловмисник, сформувавши і передавши на віддалений вузол особливим чином підготовлений пакет, здатний отримати віддалений доступ до системи і запустити на ній довільний код.

На основі данної вразливості був побудований вірус шифрувальник Wana Decryptor. Від вірусу постраждали близько 450 тисяч ЕОМ по всьому світу. Більше

всього уражених ЕОМ виявлено в Україні та Індії. Після запуску шкідлива програма діє як класична програма-вимагач: вона генерує унікальну для кожного інфікованого комп'ютера пару ключів асиметричного алгоритму RSA-2048. Потім WannaCry починає сканувати систему в пошуках призначених для користувача файлів певних типів, залишаючи критичні для подальшого її функціонування нетронутими. Кожен відібраний файл шифрується за алгоритмом AES-128-CBC унікальним (випадковим) для кожного ключем, який в свою чергу шифрується відкритим RSA-ключем інфікованої системи і зберігається в заголовку зашифрованого файлу. При цьому до кожного зашифрованого файлу додається розширення .wncry. Пара RSA-ключів інфікованої системи шифрується відкритим ключем зловмисників і відправляється до них на сервери управління, розташовані в мережі Tor, після чого всі ключі з пам'яті інфікованої машини видаляються. Завершивши процес шифрування, програма виводить на екран вікно з вимогою перевести певну суму в біткоіни (еквівалентну 300 доларам США) на вказаний гаманець протягом трьох днів. Якщо викуп не надійде вчасно, то його сума буде автоматично подвоєна. На сьомий день, якщо WannaCry не буде видалений з інфікованої системи, зашифровані файли знищуються [56].

Згідно з дослідженням компанії Symantec, алгоритм відстеження зловмисниками індивідуальних виплат кожної жертви і відправки їй ключа для розшифровки реалізовано з помилкою. Це робить виплати викупу безглуздою, оскільки індивідуальні ключі в будь-якому разі не будуть надіслані, а файли так і залишаться зашифрованими.

Якщо в класичній схемі програма-вимагач потрапляла на комп'ютер завдяки діям самого користувача через електронну пошту або веб-посилання, то в разі WannaCry участь користувача повністю виключено. Мінімальна тривалість часу між виявленням уразливої ЕОМ і повним її зараженням становить близько 3 хвилин.

Проведемо розрахунок значення iRisk для вразливості CVE-2017-0144 EternalBlue.

Базова метрика для вразливості EternalBlue буде мати наступні параметри. Резулятат відображено на рис. 2.19.

Base Score Metrics{ Attack Vector = Network; Attack Complexity = High; Privileges Required = None; User Interaction = None; Scope= Unhanged; Confidentiality Impact = High; Integrity Impact = High; Availability Impact = High}

Так як атаку проводиться ззовні і ймовірність її є дуже великою, зловмисник повинен бути експертом в зі злому, згідно методології iRisk в данному випадку значення загрози *Threat = Impact*Likelihood*, в даному випадку значення *Impact= 100,* а кореляцыйне значення *Likelihood = 0.7.*

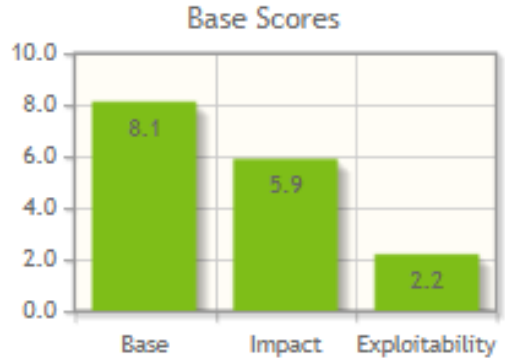

Рис. 2.19. Базова метрика вразливості CVE-2017-0144 EternalBlue

Звідси можна розрахувати значення iRisk для CVE-2017-0144, без патча безпеки від 14 березня 2017. *iRisk = (8.1*70) – 0 = 567*

2.2.4 Вразливість Meltdown (CVE-2017-5754)

Вразливість експлуатує побічний ефект out-of-order execution виконання поза чергою в сучасних процесорах. Для того аби прочитати дані з ядра, в тому числі особисту інформацію і паролі. Виконання поза чергою сильно впливає на продуктивність і включено в більшість сучасних процесорів. Атака не залежить від операційної системи і не експлуатує программні вразливості. Meltdown по суті ламає всю систему безпеки засновану на ізоляції адресного простору в тому числі віртуального Meltdown дозволяє читати частину пам’яті інших процесів і віртуальних машин.

Процесор замість того аби чекати дані з зовнішніх шин з великою затримкою і простоювати починає виконання інструкцій і заповнює частини ядра, які простоюють. Данні дії значно пришвидшують час виконання інструкцій, проте

дозволяють непривілейованому процесу виконувати код поза чергою і завантажувати данні з пам’яті ядра в тимчасовий регістр. Навіть більше – процемор виконує обчислення на основі значення цього регістра, наприклад завантажує данні з масива даних в залежності від значення регістра. Процесор гарантує коректне виконання коду однак побічний ефект — заповнення кешу в залежності від виконуваного коду поза чергою. Таким чином зловмисник може прочитати всі дані використовуючи особливість мікроархітектури. Патч KAISER виключає дану вразливість, проте зменшує швидкодію процесора [57].

Розрахуємо значення iRisk для імітаційної моделі, рахуючи, що не встановлений патч KAISER.

Розрахуємо базову метрику для вразливості Meltdown (CVE-2017-5754), результат якої відображено на рис. 2.20.

Base Score Metrics{ Attack Vector = Local; Attack Complexity = High; Privileges Required = Low; User Interaction = None; Scope= Changed; Confidentiality Impact = High; Integrity Impact = None; Availability Impact = Impact None}

Враховуючи, що зловмисник може діяти як зовні так і з середини і атака може проводитись часто, а зловмисник може мати просто продвинутий рівень навичок, і код атаки викладено в великих кількостях статей, то це дасть кореляційне значення *Impact = 0.9*, а значення *Threat* (загрози) буде рівним *100*0.9 = 90*

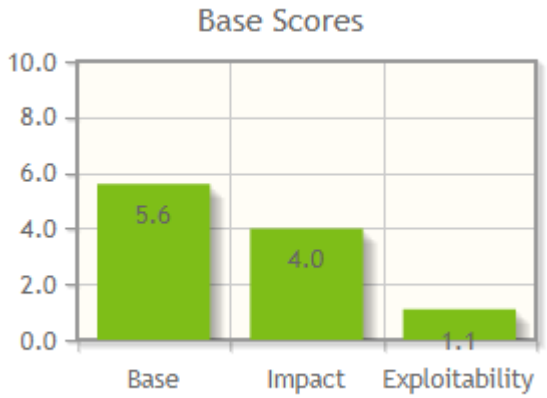

Рис. 2.20. Базова метрика вразливості Meltdown (CVE-2017-5754)

Результуюче значення iRisk для Meltdown (CVE-2017-5754) буде рівним *iRisk=5.6*90*-0 = 504, так як без патча KAISER данна вразивість ніяк не виявлялась і була закладена в архітектуру більшості сучасних процесорів.

2.2.5. Вразливість SPECTRE (CVE-2017-5753, CVE-2017-5715)

Вразливість SPECTRE, даній вразливості присвоєно одразу два ідентифікатори CVE-2017-5753, CVE-2017-5715 і по своїй суті дії вона схожа на Meltdown, проте з деякими відмінностями, зокрема тим, що в ході спекулятивного виконання коду процесор може виконати інструкції, які він не став би виконувати за умови строго послідовного (неспекулятивного) обчислення, і, хоча в подальшому результат їх виконання відкидається, його відбиток залишається в процесорному кеші і може бути використаний.

Блок передбачення працює статистично, тобто накопичує дані про виконані на даний момент схожих розгалуження, і на їх основі прогнозує результат кожного наступного розгалуження.

Тобто, наприклад, якщо код *if (a < b)*, для розрахунку якого треба довго і сумно завантажувати a і b, тисячу разів поспіль видав true, то на тисяча перший раз можна з великою впевненість вирішити, що і зараз буде true, ще до того, як з пам'яті завантажилися a і b і власне сталася перевірка. Між тим процесори не роблять різниці між тим, в яких процесах обчислюється ця умова.

Вразливість Spectre не має прямого доступу до чужої пам'яті, ні в якому вигляді, навіть при спекулятивному виконанні. Замість цього Spectre робить так, щоб атакуючий процес (це може бути як ядро системи, так і інша призначена для користувача програма) сам видав відомості про зміст власної пам'яті.

Програмп, яка експлуатує уразливість, створює максимально схожу конструкцію, і виконуємо її багато разів, причому кожного разу чесно обчислене умова видає true, індекси масиву абсолютно валідні. Блок передбачення розгалужень таким чином набирає статистику, яка говорить, що ця конструкція завжди обчислюється в true, тому, зустрівши її, можна не чекати закінчення обчислення умови, а відразу переходити до вмісту.

Тоді в атакуючу програму передаються такі дані, що *x* раптом вискакує кудись далеко за межі масиву *array1*. Якби спекулятивного виконання не було б, процесор порахував би умову *x <array1_size*, знайшов його невалідним і перейшов би далі. Але блок передбачення видає йому, що *x <array1_size* майже напевно буде виконано, тому, поки звідкись із пам'яті повільно і сумно підсмоктується значення *array1_size*, щоб дійсно порівняти інший результат, процесор починає виконувати тіло цього шматка коду [58].

Вразливість Specter не є простою в реалізації - проте, за умови атаки на конкретне ПЗ, відоме атакуючому і по можливості доступне в відкритому коді в тій же версії і на тій же системі, на якій передбачається атака, вона може бути реалізована.

Інший варіант реалізації Specter полягає в «перебаченні розгалужень» - в процесорі є аналогічний блок передбачення переходів, суть роботи якого полягає в передбаченні адреси за якою буде здійснений перехід чергової інструкції непрямого переходу (Meltdown, але тут вони грають іншу роль).

Для спрощення роботи цей блок не виконує трансляцію між віртуальними і реальними адресами, а значить, може бути натренований в адресному просторі атакуючого на певні дії.

Тобто, якщо ми знаємо, що потрібна нам інструкція в програмі, яка атакується лежить за адресою 123456, а також у цій програмі регулярно виконується непрямий перехід. В атакуючій програмі створюється конструкція, максимально схожа на перехід в програмі що атакується, але при цьому завжди виконує перехід за адресою 123456. У нашому адресному просторі, звичайно, абсолютно валідний і легальний перехід. Що саме у нас лежить за адресою 123456, ніякого значення не має.

Через деякий час блок передбачення переходів абсолютно впевнений, що всі переходи такого виду ведуть на адресу 123456, тому, коли атакуюча програма доходить під час виконання до аналогічного переходу, процесор радісно починає спекулятивне виконання інструкцій з адреси 123456. Вже в адресному просторі атакованої програми [58].

Через деякий час справжню адресу переходу буде вирахувано, процесор визначає помилку і відкидає результати спекулятивного виконання, проте, як і у всіх інших випадках застосування Meltdown і Spectre, більшість результатів виконання залишається в кеші.

Розрахуємо значення iRisk для вразливості Spectre. Базова метрика в обох варіацях реалізації вразливостей однакова, результати розрахунку представлені на рис 2.21.

Base Score Metrics{ Attack Vector = Local; Attack Complexity = High; Privileges Required = Low; User Interaction = None; Scope= Changed; Confidentiality Impact = High; Integrity Impact = None; Availability Impact = Impact None}

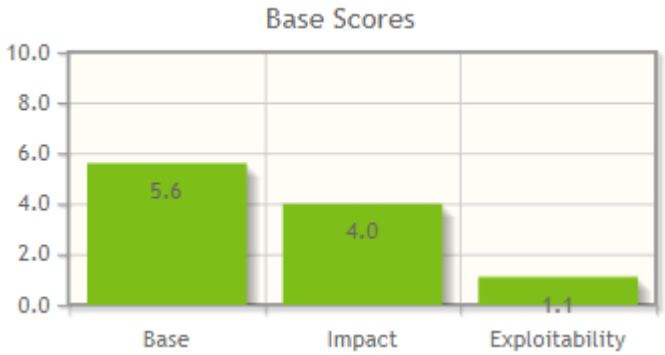

Рис. 2.21. Базова метрика вразливості Spectre CVE-2017-5753 і CVE-2017-5715

В обох випадках з Spectre ми маємо справу з тим, що процесор вчиться швидше виконати один процес на прикладі виконання іншого процесу, тим самим фактично дозволяючи другому процесу контролювати хід виконання першого. Універсальних патчів для виправлення Specter пока немає, і захистом від CVE-2017-5715 пропонується постійно очищувати кеш і прибирати коду ядра.

Розрахуємо значення iRisk для CVE-2017-5715, враховуючи складність точної реалізації і вплив лише на конфіденційність інформації, тому значення *Impact = 50,* (включаючи фінансовий, репутаційний та стратегічний вплив), враховуючи те, що вразливістю будуть намагатися скористуватись в основному зовні і зловмисник повинен мати продивнуті технічні навички, то кореляційне значення *Likelihood = 0.*64. Дані параметри характерні як для CVE-2017-5753 так і CVE-2017-5715.

Проте параметри *Controls* в данному випадку треба оцінювати по різному, зокрема враховуючи що для вразливості CVE-2017-5715 випущені патчі які частково вирішують дану проблему лише в деяких випадках, то значення *Controls* можна вважати *Initial/Ad-Hoc=100* забезпечує лише деяку цінність захисту, що стосується CVE-2017-5753, то *Controls* можна вважати ріним 0, так як наразі дана проблема не вирішена.

Звідси для CVE-2017-5715 *iRisk* = (5.6*50*0.64) – 100 = 79.2.

Для CVE-2017-5753 *iRisk* = (5.6*50*0.64) – 0 = 179.2

Розглянуто методи тестування та аналізу ризиків АС, визначено метод для тестування імітаційної моделі системи захисту критичних ресурсів виробництва мінеральних добрив. Насамперед проаналізовано існуючі методи тестування і оцінки вразливостей АС для визначення їх переваг і недоліків, що полягає у кількісно-якісному оцінюванні захисту ІС для можливості подальшого співставлення затрачених ресурсів та захищенності ІС. Зроблено висновок, що проводити оцінку захищеності мережі змішаними(комплексними) методиками немає доцільності.

Для тестування було обрано методологію iRisk, перш за все тому, що дана методика є безкоштовною, достатньо інформативною, включає в собі іншу методику CVSS v3 для оцінки вразливостей, яка активно підтримується Національним інститут стандартів і технологій. Розрахунок проводиться за формулою *iRisk = (Vulnerability x Threat) – Controls*.

Протестовано АС відносно наступних вразливостей: Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384), Cisco Access Control Bypass Vulnerability (CVE-2012-1342), EternalBlue (CVE-2017-0144), Meltdown (CVE-2017-5754), Spectre (CVE-2017-5753) (CVE-2017-5715), зроблено висновки щодо стійкості побудованої мережі до конкретних загроз методом iRisk, де значення ранжуються від 0 до 1000, а нулю відповідає АС, в якій можна знехтувати даною вразливістю, тоді як при максимально великому значенні, якщо воно перевищує 100 необхідно вирішувати данну вразливість. Чим вище значення iRisk тим критичнішою є

вразливість і має більший пріоритет для захисту АС. Результати розрахунків наведено в (табл. 2.3).

Таблиця 2.3

Таблиця значень iRisk для побудованої імітаційної моделі

Вразливість	*Значення iRisk*
Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384)	50
Cisco Access Control Bypass Vulnerability (CVE-2012-1342)	16.4
EternalBlue (CVE-2017-0144)	567
Meltdown (CVE-2017-5754)	504
Spectre (CVE-2017-5715)	79.2
Spectre (CVE-2017-5753)	179.2

2.3. Математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив

Проведена розробка та дослідження математичної моделі протидії загрозам у системі захисту критичних інформаційних ресурсів, одержання перехідних характеристик для станів системи.

Запропонована математична модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних ресурсів виробництва мінеральних добрив. Поетапно розписаний процес побудови математичної моделі протидії загрозам у системі захисту критичних інформаційних ресурсів за допомогою марковського ланцюга [59]. Запропонована методика знаходження актуальних загроз безпеці даних при їх обробці. Наведені приклади розрахунків імовірностей знаходження математичної моделі інформаційної системи в одному з чотирьох станів (загроза не настала; загроза настала, але не була реалізована; загроза настала, була реалізована; загроза настала, але була відбита системою захисту).

Систему можна інтерпретувати як систему масового обслуговування, в яку надходять загрози. Для початку розглянемо ситуацію, коли на вхід до системи надходять загрози одного типу, припускаючи, що загроза не може бути реалізована

та надходити кілька разів в один і той же період часу. Якщо ці умови виконуються, то система може знаходитись у одному з чотирьох станів (рис. 2.22):

- Загроза не надходила і, відповідно, не була реалізована;
- Загроза надійшла, але не була реалізована;
- Загроза надійшла та була реалізована;
- Загроза надійшла, але була відбита системою захисту.

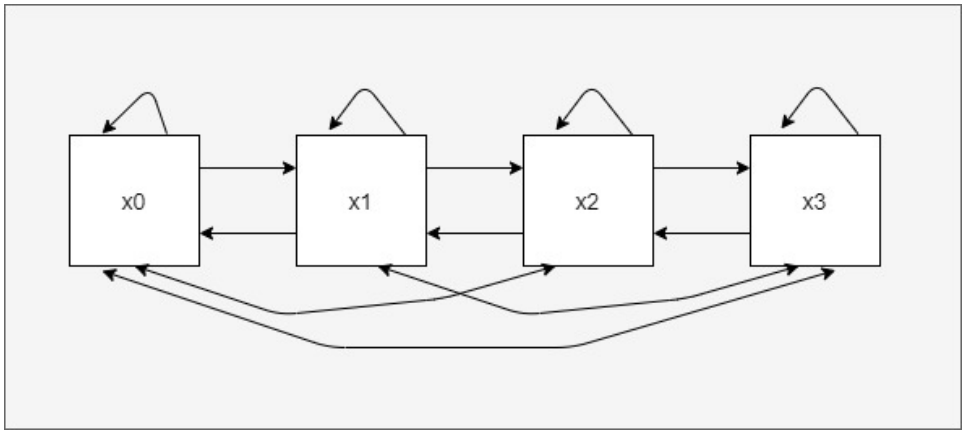

Рис. 2.22. Граф станів системи

Система, яка розглядається є системою з відновленням, тобто система може переходити з будь-якого стану у початковий. Будемо розглядати систему з неперервним часом. Перехід зі стану у стан відбувається згідно орієнтованого графу (рис. 2.22). Для опису процесу переходу зі стану у стан, побудуємо матрицю інтенсивностей переходу:

$$\lambda_{ij} = \begin{vmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} & \lambda_{14} \\ \lambda_{21} & \lambda_{22} & \lambda_{23} & \lambda_{24} \\ \lambda_{31} & \lambda_{32} & \lambda_{33} & \lambda_{34} \\ \lambda_{41} & \lambda_{42} & \lambda_{43} & \lambda_{44} \end{vmatrix}. \tag{2.3}$$

З попередніх погоджень випливає, що елементи цієї матриці мають такі властивості:

$$\sum_{j=1}^{n} \lambda_{ij} = 0, \quad (i = 1, n) \tag{2.4}$$

Для визначення імовірностей перебування системи у станах x_0, x_1, x_2, x_3, побудуємо систему диференційних рівнянь:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = p_0(t)\cdot\lambda_{11} + p_1(t)\cdot\lambda_{21} + p_2(t)\cdot\lambda_{31} + p_3(t)\cdot\lambda_{41} \\ \dfrac{dp_1(t)}{dt} = p_0(t)\cdot\lambda_{12} + p_1(t)\cdot\lambda_{22} + p_2(t)\cdot\lambda_{32} + p_3(t)\cdot\lambda_{42} \\ \dfrac{dp_2(t)}{dt} = p_0(t)\cdot\lambda_{13} + p_1(t)\cdot\lambda_{23} + p_2(t)\cdot\lambda_{33} + p_3(t)\cdot\lambda_{43} \\ \dfrac{dp_3(t)}{dt} = p_0(t)\cdot\lambda_{14} + p_1(t)\cdot\lambda_{24} + p_2(t)\cdot\lambda_{34} + p_3(t)\cdot\lambda_{44} \end{cases} \tag{2.5}$$

з початковими умовами

$$p_0(0) = 1, \quad p_1(0) = 0, \quad p_2(0) = 0, \quad p_3(0) = 0.$$

Оскільки вектор $p(0) = (1,0,0,0)$ заданий, то вектор абсолютних ймовірностей $p(n) = (p_0(n), p_1(n), p_2(n), p_3(n))$ визначається співвідношенням:

$$p(n) = p(0)\left\| p_{ij}(n) \right\|. \tag{2.6}$$

Після проведення дослідження на імітаційній моделі було визначено два результати знаходження коефіцієнтів λ_{ij}, які будуть наведені нижче [41, 60-65].

Варіант 1. Нехай матриця інтенсивностей переходів λ_{ij} має вигляд:

$$\begin{vmatrix} -0,040 & 0,015 & 0,010 & 0,015 \\ 0,225 & -0,250 & -0,025 & 0,050 \\ 0,625 & -0,160 & -0,855 & 0,390 \\ 0,000 & 0,075 & 0,200 & -0,275 \end{vmatrix} \tag{2.7}$$

Отримаємо розв’язок системи рівнянь методом Рунге-Кутти четвертого порядку для моменту часу $t = 50$ с. Для реалізації розв’язку розроблено програмний модуль на мові програмування Python. У результаті проведених обчислень були знайдені значення імовірності знаходження системи у кожному зі станів (рис.2.23).

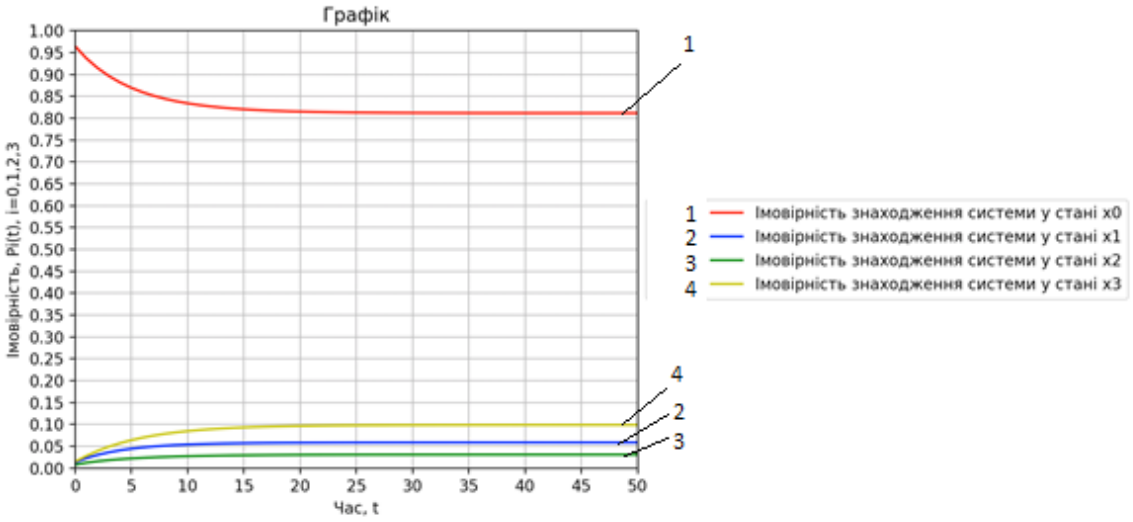

Рис. 2.23. Імовірність знаходження системи у кожному зі станів

Варіант 2. Нехай матриця інтенсивностей переходів λ_{ij} має значення:

$$\begin{vmatrix} -0,040 & 0,015 & 0,010 & 0,015 \\ 0,225 & -0,250 & -0,025 & 0,050 \\ 0,575 & -0,200 & -0,875 & 0,500 \\ -0,125 & 0,145 & 0,180 & -0,200 \end{vmatrix} \qquad (2.8)$$

У результаті отримаємо такий графік (рис.2.24):

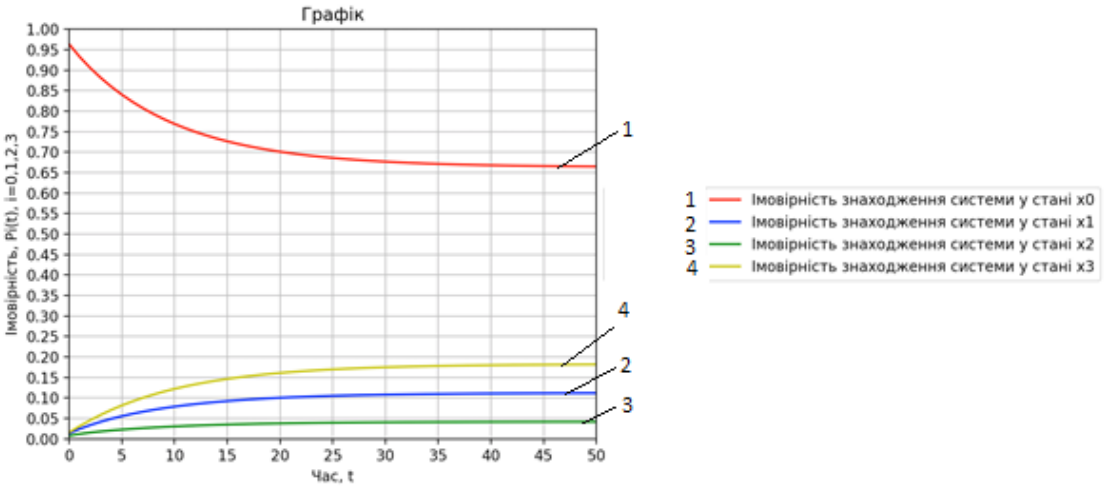

Рис. 2.24. Імовірність знаходження системи к кожному з станів

На основі отриманих результатів можна сказати, що у варіанті 2 більша імовірність знаходження системи у стані, який викликаний отриманням загрози, хоча також велика вірогідність успішного відбиття загрози системою захисту.

Запропонована математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив. Також розроблена та наведена на основі цієї моделі методика виявлення актуальних загроз безпеки.

Приклади аналізу числових результатів за допомогою запропонованої методики наочно показують, що їх використання допомагає з визначенням загроз, які є актуальними для досліджуваної системи та можуть використовуватись на практиці. Недоліком запропонованої методики є необхідність розгляду поведінки системи при дії на неї кожного типу загроз окремо і неможливість визначення поведінки про одночасній дії кількох загроз. Але з іншого боку вивчення впливу кожної загрози окремо дозволяє більш детально вивчити кожен її тип та визначити ті, вірогідність появи яких є найбільшою.

Висновки до розділу 2

1. Розроблено імітаційну модель захисту критичних ресурсів виробництва мінеральних добрив, на базі GNS3 та KaliLinux. Для випробування імітаційної моделі захисту критичних ресурсів виробництва мінеральних добрив розглянуто програмні засоби для проведення тестування побудованої імітаційної моделі. За допомогою збудованого імітаційної моделі захисту критичних ресурсів виробництва мінеральних добрив реалізоване проєктування компютерної мережі та системи захисту критичних ресурсів виробництва мінеральних добрив, здійснена перевірка системи захисту критичних ресурсів шляхом генерації атак та їх відбиття системою захисту критичних ресурсів виробництва мінеральних добрив.

2. Розглянуто методи тестування та аналізу ризиків системи захисту критичних ресурсів виробництва мінеральних добрив, обрано метод для тестування системи захисту інформації на базі імітаційної моделі. Протестовано систему захисту критичних ресурсів виробництва мінеральних добрив відносно наступних

вразливостей: Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384), Cisco Access Control Bypass Vulnerability (CVE-2012-1342), EternalBlue (CVE-2017-0144), Meltdown (CVE-2017-5754), Spectre (CVE-2017-5753) (CVE-2017-5715), зроблено висновки щодо стійкості побудованої мережі до конкретних загроз методом iRisk.

3. Розроблено математичну модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних ресурсів виробництва мінеральних добрив. Запропонована на основі цієї моделі методика виявлення актуальних загроз безпеки. Математичну модель протидії впливу внутрішніх та зовнішніх загроз може використовуватись для оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив.

РОЗДІЛ 3. ОПТИМІЗАЦІЯ СИСТЕМИ ЗАХИСТУ КРИТИЧНИХ РЕСУРСІВ ВИРОБНИЦТВА МІНЕРАЛЬНИХ ДОБРИВ

Інформатизація є характерною рисою життя сучасного суспільства. Нові інформаційні технології активно впроваджуються у виробництво мінеральних добрив. У міру розвитку і ускладнення засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суспільства від ступеня безпеки інформаційних технологій, що використовуються. Інформаційні технології в даний час є необхідним атрибутом підвищення ефективності функціонування підприємств, зокрема, дозволяють знизити витрати виробництва, підвищити якість готової продукції. Однією з найбільш серйозних проблем, що ускладнюють застосування сучасних інформаційних технологій, є забезпечення їх інформаційної безпеки.

Розглядаються основні підходи до розробки методики оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив. Запропоновано перехід від багатокритеріальної задачі оптимізації, до однокритеріальної. При сформульованому понятті захищеності системи оптимізаційна задача полягає в забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи.

3.1. Факторно-цільовий аналіз з метою вибору критерію опимальності

Проблема побудови оптимальної системи захисту інформації в даний час є найбільш актуальною для більшості промислових підприємств. Мета будь-якої системи захисту визначається можливістю сталого функціонування системи в цілому, визначення та нейтралізації загроз безпеки, запобігання витоку інформації по різних каналах. Одною з головних задач стає оптимізація проєктування системи захисту. Сьогодні для промислових підприємств інформація являє собою основний комерційний товар. З розвитком інформаційних технологій і доступу до ринків є потреба в її захисті для забезпечення конфіденційності, цілісності і доступності. Для

багатьох промислових підприємств впровадження систем захисту є необхідним етапом на шляху до успішного розвитку, кожне з них має свою критичну інформацію, втрата якої може звести до мінімуму конкурентоспроможність і шанси на успішний розвиток на ринку. Поширення такої інформації може призвести до втрати репутації і завдати матеріальної шкоди. Слід зазначити, що активне запровадження автоматизованих інформаційних систем обумовлює виникнення проблем, пов'язаних з інформаційною безпекою. Рішення даних проблем може бути реалізовано з застосуванням спеціальних автоматизованих програмно-технічних засобів [66-69].

Запропонована методика оптимізації системи захисту критичних інформаційних ресурсів.

У будь-якій галузі діяльності для вибору ефективної системи, ця система повинні характеризуватися деякими параметрами, на підставі яких і робиться вибір. В якості таких параметрів для системи захисту інформації можна виділити наступні: продуктивність, вартість, керованість, сумісність, захищеність тощо. Як вже було зазначено вище, вибір оптимальної системи по такій множині її характеристик є класичною задачею оптимізації і не завжди може мати ефективне рішення. Тим більше що багато параметрів є суперечливими: зі зростанням рівня захищеності, наприклад, зростає вартість, складність настройки, в той же час падає продуктивність.

Методи багатокритеріальної оптимізації більш повно відображають завдання, що ставляться перед реальними системами захисту інформації. Перед особою, яка приймає рішення, з'являється проблема вибору найбільш підходящого методу багатокритеріальної оптимізації, і, як наслідок, прийняття припущень, умовностей, меж теоретичних аналогів реальних об'єктів. Ставиться завдання вибору оптимального варіанту системи захисту критичних інформаційних ресурсів, який спроєктований для конкретного підприємства. Оптимізація проводиться за кількома критеріями: рівнозначним, незалежним, що найбільш повно відображає об'єкти вибору.

Розглянемо різні способи вибору оптимизаційного варіанту. На основі проведеного аналізу виберемо метод, який відповідає поставленому завданню і має мінімальні недоліки.

При багатокритеріальної оцінюванні об'єктів застосовується метод рейтингування [70]. Якщо в задачі йде пошук мінімальних значень, зменшення значень характеристик відповідає збільшенню ступеня привабливості системи. Необхідно зважування окремих показників в світі значущості їх рейтингової оцінки [71]. Нормовані зважені показники складаються, і на підставі отриманої суми відбувається ранжування об'єктів.

У методі поступок [72] критерії оцінюються за значимістю і використовуються в порядку зростання. Вибирається перший критерій і вирішується однокритеріальних завдання. Потім знаходять величину можливого відхилення. Не виходячи за розміри фіксованих відхилень, ітераційно знаходяться наступні екстремальні завдання. В кінці використовують останній критерій, і вирішується завдання, аналогічна задачі з головним критерієм. При досягненні граничних умов рішення може бути слабо ефективним.

Метод згортки застосовують при агрегування всіх критеріїв в скалярную величину, і на підставі цієї величини відбувається оцінювання об'єкта [73]. Згортка має адитивний або мультиплікативний вигляд. Мультиплікативна запис залежить від зменшення значень окремих критеріїв і може прагнути до нуля. При адитивній згортці зменшення значень деяких критеріїв компенсується збільшенням інших, що мають велику «вагомість».

Важливим етапом методу згортки є завдання вибору вагових коефіцієнтів, яке допускає різні рішення. Метод логічного аналізу заснований на прямому експертному присвоєння конкретних значень критеріям. Експерти присвоюють значення критеріям в діапазоні натурального ряду від одиниці до величини кількості критеріїв [74]. У разі різної компетентності експертів, їм присвоюються коефіцієнти значущості експертів, які включаються в формули. У цьому методі важливі не тільки коефіцієнти значущості експертів, а й достатня кількість експертів.

Метод аналізу ієрархій [74] заснований на побудові матриць парних порівнянь різних критеріїв. Матриця повинна бути квадратна, назад-симетрична і узгоджена. Оцінюється критерій натуральними числами від 1 до 9. Діагональні елементи після

нормалізації і утворюють вагові коефіцієнти. При побудові початкової матриці, якщо критерій менш важливий його значення оцінюється оберненим числом.

При побудові траєкторії вибору найкращого варіанту можна скоротити кількість варіантів, наприклад, до множини Парето, прибравши свідомо гірші. Згідно з принципом Еджворта-Парето [75], при багатокритеріального виборі один варіант кращий за інший, якщо по одному окремому критерію він кращий за інший, а по решті не гірший. Сформована множина Парето не більше початкової кількості варіантів, і завдання знаходження найкращого варіанту, спрощується.

Ще один шлях спрощення завдання - скорочення кількості критеріїв. Метод головного критерію зменшує множину критеріїв до одного [72]. Один критерій оголошується головним, за ним шукається екстремум, а інші критерії формують обмеження.

Можна записати критерій якості за вартістю інформації, що захищається, за ймовірністю злому, за вартістю системи захисту інформації, за продуктивністю системи, за захищеністю. З урахуванням сказаного може бути зроблений висновок про багатокритеріальний характер завдання проектування системи захисту інформації. При цьому, крім забезпечуваного рівня захищеності, повинен враховуватися ще ряд найважливіших характеристик системи. Наприклад, обов'язково повинен враховуватися вплив системи захисту на завантаження обчислювального ресурсу, що захищається [42, 61, 62].

Кінцевою метою вирішення загальної задачі прийняття рішень є вибір з допустимої множини рішень X єдиного найкращого, тобто екстремального за обраними окремими критеріями рішень

$$x^{opt} = \arg \underset{x \in X}{extr} \left\{ k_i \left(x \right) \right\}, i = 1, n \qquad (3.1)$$

Задача багатокритеріальної оптимізації (формула 3.1) є некоректною, оскільки в загальному випадку не забезпечує визначення єдиного оптимального рішення з допустимої множини X. Ця некоректність може бути усунена шляхом регуляризації задачі, тобто введенням деякої додаткової інформації. математичних співвідношень або правил, що дозволяють забезпечити вибір єдиного рішення [60].

Один шляхів розв'язку багатокритеріальної задачі оптимізації полягає в формуванні зведеного критерію оптимальності, коли використовується згортка частинних критеріїв, чи використання нормативних показників, чи справедливий компроміс, чи оптимальність за Парето.

Інший підхід базується на виділенні головного критерію та перетворення всіх інших критеріїв в обмеження. Для цього проводиться аналіз конкретних особливостей багатокритеріальної задачі, з множини окремих критеріїв вибирається один - найважливіший, і він приймається в якості єдиного критерію оптимізації. Для кожного з інших окремих критеріїв призначається граничне значення, нижче якого він не може опускатися.

Тому в нашому методі буде проводитися оцінка ефективності системи за параметром захищеності, як основним показником, що характеризує рівень забезпечення захисту системи захисту інформації, а на інші характеристики вводяться обмеження. Будемо оцінювати захищеність системи (Z) кількісно залежно від вартості інформації, що захищається, ймовірності злому, вартості самої системи захисту, продуктивності системи:

$$Z = f\left(C\ , p\ , B\ , G\right),$$

де C - вартість інформації, що захищається; p - ймовірність злому; B - вартість системи захисту інформації; G - продуктивність системи.

З урахуванням введеного поняття захищеності системи оптимізаційна задача полягає в забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи:

$$Z^{opt} = \max Z\left(C\ , p, B, G\right).$$

Таким чином, всі окремі критерії, крім одного перетворюються на обмеження, додатково звужують область допустимих рішень X. Тоді вихідна багатокритеріальна задача (3.1) перетворюється в однокритеріальну виду

$$\begin{aligned} x^{opt} &= \arg \underset{x \in X}{extr}\, k^{*}\left(x\right), \\ k_i\left(x\right) &\geq \left(\leq\right) k_i^{B}\left(x\right), i = 1, n-1, \end{aligned} \tag{3.2}$$

де $k^*(x)$ - оптимізаційний скалярний критерій; $k_i^B(x)$ - найгірші допустимі значення окремих критеріїв-обмежень; знак ">" використовується для критеріїв, які необхідно максимізувати, а знак "<" - мінімізувати.

Виведення головного (оптимізаційного) критерію і рівнів обмежень для $k_i^B(x)$ всіх інших критеріїв є суб'єктивною операцією, здійснюваною експертами. Слід зазначити, що можна розглянути декілька різних варіантів і порівняти результати.

Розглянемо захищеність системи з точки зору ризику. Зауважимо, що використання теорії ризиків для оцінки рівня захищеності на сьогоднішній день є підходом, який найбільш часто використовується на практиці. Ризик (R) - це потенційні втрати від загроз захищеності:

$$R\ (p) = C \cdot p$$

По суті, параметр ризику тут вводиться як мультиплікативна згортка двох основних параметрів захищеності.

З іншого боку, можна розглядати ризик як втрати в одиницю часу:

$$R(\lambda)=C \cdot \lambda\ ,$$

де λ - інтенсивність потоку зломів (під зломом будемо розуміти вдалу спробу реалізації загрози інформації).

Ці дві формули пов'язані наступним співвідношенням:

$$p = \frac{\lambda}{\Lambda},$$

де Λ - загальна інтенсивність потоку несанкціонованих спроб порушення основних властивостей інформації зловмисниками.

В якості основного критерію захищеності будемо використовувати коефіцієнт захищеності *(D)*, що показує відносне зменшення ризику в захищеній системі в порівнянні з незахищеною системою:

$$D = \left(1 - \frac{R_s}{R}\right) \cdot 100\%, \qquad (3.3)$$

де R_s - ризик в захищеній системі; R - ризик в незахищеною системі.

Для вирішення цієї задачі зведемо її до однокритеріальної за допомогою введення обмежень. В результаті отримаємо:

$$\begin{cases} D(C, p\ ) \to \max; \\ \quad B \le B_t; \\ \quad G \ge G_t. \end{cases}$$

де B_t і G_t - задані обмеження на вартість системи захисту і продуктивність системи.

Цільова функція обрана виходячи з того, що саме вона відображає основне функціональне призначення системи захисту - забезпечення безпеки інформації [18].

Тепер виразимо коефіцієнт захищеності через параметри загроз. У загальному випадку в системі присутня безліч видів загроз. У цих умовах задамо такі величини: W - кількість видів загроз, що впливають на систему; $C_i(i=1,w)$ - вартість втрати від злому і-того виду; $\lambda_i(i=1,w)$ - інтенсивність потоку зломів і-того виду, відповідно; $Q_i(i=1,w)$ - ймовірність появи загроз і-того виду в загальному потоці спроб реалізації загроз, причому $Q_i = \dfrac{\lambda_i}{\Lambda}$; $p_i(i=1,w)$ - ймовірність відбиття загроз і-того виду системою захисту. Відповідно, для коефіцієнта втрат від зломів системи захисту маємо:

$$R(p) = \sum R_i\left(p\right) = \sum C_i \cdot p_i;$$

де $R_i(p)$ - коефіцієнт втрат від злому і-того типу; показує, які в середньому втрати припадають на один злом і-того типу. Для незахищеною системи $P_i = Q_i$, для захищеної системи

$$P_i = Q_i \cdot (1 - p_i).$$

Відповідно, для коефіцієнта втрат від зломів системи захисту в одиницю часу маємо:

$$R(\lambda) = \sum_1^w R_i(\lambda) = \sum_1^w C_i \cdot \lambda_i,$$

де $R_i(\lambda)$- коефіцієнт втрат від зломів і-того типу в одиницю часу.

Для незахищеною системи $\lambda_{u\_i} = \lambda_i$, для захищеної системи $\lambda_{s\_i} = \lambda_i \cdot \left(1 - p_i\right)$. Відповідно, з (3.3) маємо:

$$D = 1 - \frac{\sum_{1}^{w} C_i \cdot Q_i \cdot (1 - p_i)}{\sum_{1}^{w} C_i \cdot Q_i} = 1 - \frac{\sum_{1}^{w} C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_{1}^{w} C_i \cdot \lambda_i}. \quad (3.4)$$

Основним способом завдання інтенсивностей потоків загроз λ_i (ймовірностей загроз Q_i) і ймовірностей зломів p_i є отримання цих значень на основі наявної статистики загроз безпеки інформаційних систем, в яких реалізується система захисту. Якщо існує статистика для аналогічної інформаційної системи, то задавати вихідні параметри для оцінки захищеності можна на її основі. При цьому бажано, щоб подібні інформаційні системи експлуатувалася на підприємствах з подібною специфікою діяльності.

Однак при практичній реалізації такого підходу виникають наступні складності. По-перше повинен бути зібраний досить великий матеріал про події в даній області. По-друге даний підхід виправданий далеко не завжди. Якщо інформаційна система досить велика (містить багато елементів, розташована на великій території), має давню історію, то подібний підхід, швидше за все, можна застосувати. Якщо ж система порівняно невелика і експлуатує нові елементи технології (для яких поки немає достовірної статистики), оцінки загроз можуть виявитися недостовірними.

Статистика загроз періодично публікується авторитетними виданнями, тобто завжди існують вихідні дані для використання даного підходу для більшості засобів захисту інформації. Якщо ж необхідна статистика по загрозам безпеки відсутня, то можна скористатися одним з інших підходів, описаних далі.

Перший спосіб - це спосіб однакових інтенсивностей $\forall\lambda_i = \alpha$, $\alpha = const$. У підсумку захищеність в даному випадку буде залежати тільки від втрат:

$$D = 1 - \frac{\sum_{i=1}^{w} C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_{i=1}^{w} C_i \cdot \lambda_i} = 1 - \frac{\sum_{i=1}^{w} C_i \cdot \alpha \cdot (1 - p_i)}{\sum_{i=1}^{w} C_i \cdot \alpha} = 1 - \frac{\alpha \sum_{i=1}^{w} C_i \cdot (1 - p_i)}{\alpha \sum_{i=1}^{w} C_i} =$$
$$= 1 - \frac{\sum_{i=1}^{w} C_i \cdot (1 - p_i)}{\sum_{i=1}^{w} C_i} \quad (3.5)$$

Другий спосіб - це спосіб пропорційності втратам $\lambda_i = \alpha \cdot C_i,\ \alpha = \text{const}$.

При цьому способі передбачається, що чим більше втрати від злому, тим частіше здійснюються спроби несанкціонованого доступу до цієї інформації. Тобто інтенсивності потоків загроз прямо пропорційні втратам. В цьому випадку захищеність буде залежати від квадрата втрат:

$$D = 1 - \frac{\sum_{i=1}^{w} C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_{i=1}^{w} C_i \cdot \lambda_i} = 1 - \frac{\sum_{i=1}^{w} C_i \cdot \alpha \cdot C_i (1 - p_i)}{\sum_{i=1}^{w} C_i \cdot \alpha \cdot C_i} = 1 - \frac{\alpha \sum_{i=1}^{w} C_i^2 \cdot (1 - p_i)}{\alpha \sum_{i=1}^{w} C_i^2} = \quad (3.6)$$

$$= 1 - \frac{\sum_{i=1}^{w} C_i^2 \cdot (1 - p_i)}{\sum_{i=1}^{w} C_i^2}$$

Для розв`язання задачі оптимізації використовуємо імітаційну модель системи захисту критичних ресурсів виробництва мінеральних добрив та математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив. Значення λ_i одержимо з імітаційної моделі системи захисту критичних ресурсів виробництва мінеральних добрив. Значення p_i одержимо з математичної моделі протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив. Для оптимізації використовуються кінцеві усталені значення p_i.

3.2. Метод послідовно квадратичного програмування

Як правило, загальний підхід до розв`язання задач оптимізації при наявності обмежень полягає у заміні вихідної задачі з обмеженнями на іншу більш просту задачу, яка надалі використовується як основа для деяких ітераційних методів. Основною особливістю таких методів є те, що вихідна задача з обмеженнями заміняється на задачу без обмежень, але із застосуванням методу штрафних функцій поблизу значень, що накладають, для обмежень. При такому підході задача

оптимізації при наявності обмежень вирішувалася через введення деякої послідовності параметричних задач оптимізації без накладання обмежень, які в межі (обраної послідовності) збігалися до шуканої задачі з обмеженнями. У наш час такий підхід вважається відносно малоефективним і , відповідно, був замінений на методи розв`язку, засновані на формулюванні і наступному розв`язку так званих рівнянь Куна-Таккера. У рівняннях Куна-Таккера вводяться додаткові припущення про характер обмежень і поняття оптимальності для задачі оптимізації при наявності обмежень. Якщо поставлена задача є так званою задачею опуклого програмування, то рівняння Куна-Таккера є необхідними й достатніми умовами для загальної постановки задачі.

$$\begin{aligned} &\nabla f(X^*) + \sum_{i=1}^{m} \mu_i^* \nabla G_i(X^*) = 0; \\ &\mu_i^* G_i(X^*) = 0 \qquad i = 1,...,m; \\ &\mu_i^* \geq 0. \end{aligned} \tag{3.7}$$

Перші рівняння являють собою опис процесу зникнення градієнта між цільовою функцією й активними обмеженнями в точці розв`язку. Оскільки градієнти підлягають виходу на нульові значення, то множники Лагранжа $(\mu_i, i = 1,...,m)$ будуть необхідні для того, щоб зрівноважити відхилення по величині даної цільової функції й градієнтів обмежень. Оскільки тільки активні обмеження залучені в дану процедуру обнулення, а неактивні обмеження не повинні піддаватися даній процедурі, й тому відповідні множники Лагранжа будуть дорівнювати нулю. Ця обставина неявно виражена у двох останніх рівняннях (3.7).

Подібне розв`язання рівнянь Куна-Таккера є основою для більшості алгоритмів нелінійного програмування. У цих алгоритмах часто використовується пряме обчислення множників Лагранжа. Квазіньютонівські методи забезпечують лінійну збіжність шляхом нагромадження інформації другого порядку щодо рівнянь Куна-Таккера, що використовують процедуру квазіньютонівського коригування. У загальному випадку ці методи можна віднести до задач послідовного квадратичного програмування, оскільки проблема квадратичного програмування розв`язується на кожній головній ітерації (іноді їх ще називають методами ітераційного квадратичного

програмування, рекурсивного квадратичного програмування або змінної метрики при наявності обмежень).

Метод послідовного квадратичного програмування є одним з найсучасніших методів в області нелінійного програмування. Заснований на роботах [76-79] даний метод дозволяє досить точно імітувати метод Ньютона для оптимізації при наявності обмежень, як це зроблено для оптимізації при відсутності обмежень. На кожній основній ітерації здійснюється апроксимація Гессіана для функції Лагранжа за допомогою квазіньютонівського модифікованого методу. Такий підхід далі буде потрібний для постановки у квадратичному програмуванні, розв`язання якої далі вже використовується для формування напрямку пошуку в процедурі лінійного пошуку. Відповідно до опису основної задачі основна ідея постановки підзадачі квадратичного програмування полягає у квадратичній апроксимації функції Лагранжа.

$$L(X,\mu) = f(X) + \sum_{i=1}^{m} \mu_i g_i(X). \tag{3.8}$$

При припущенні, що зв`язані обмеження можуть бути представлені через обмеження у вигляді нерівностей. За допомогою лінеаризації нелінійних обмежень можна одержати підзадачу квадратичного програмування.

$$\begin{aligned} &\min_{D\in R^n} \frac{1}{2} D^T H_k D + \nabla f(X_k)^T D; \\ &\nabla g_i(X_k)^T D + g_i(X_k) = 0 \qquad i = 1,...,m_e; \\ &\nabla g_i(X_k)^T D + g_i(X_k) \le 0 \qquad i = m_e + 1,...,m. \end{aligned} \tag{3.9}$$

Дана підзадача може бути вирішена за допомогою алгоритму квадратичного програмування. Таке рішення основане на формуванні нової ітерації наступного вигляду

$$X_{k+1} = X_k + \alpha_k D_k. \tag{3.10}$$

Параметр при довжині кроку α_k визначається з відповідної процедури лінійного пошуку, що забезпечує прийнятне зменшення одержуваної цільової функції. Матриця H_k є додатно визначеною апроксимацією матриці Гессе для функції Лагранжа

(рівняння (3.9)), H_k може коригуватися за допомогою кожного із квазіньютонівських методів, але метод Бройдена-Флетчера-Голдфарба-Шанно є найбільш ефективним.

На відміну від розв`язання методом послідовно квадратичного програмування для задач без обмежень, нелінійні задачі при наявності обмежень вирішуються за певне число ітерацій. Однією з причин такого факту є те, що внаслідок наявності меж на доступні для огляду області оптимізації можуть прийматися усвідомлені рішення щодо напрямків пошуку та розміру кроку.

Реалізація методу послідовно квадратичного програмування складається з трьох основних стадій:

- Коригування матриці Гессе для функції Лагранжа.
- Розв`язання задачі квадратичного програмування.
- Обчислення лінійного пошуку та критерію якості.

Коригування матриці Гессе для функції Лагранжа

На кожній головній ітерації додатно визначена квазіньютонівська апроксимація *H* для функції Лагранжа, розраховується за допомогою методу Бройдена-Флетчера-Голдфарба-Шанно, де $\lambda_i, i = 1,...,m$ являють собою оцінку множників Лагранжа.

$$H_{k+1} = H_k + \frac{Q_k Q_k^T}{Q_k^T S_k} - \frac{H_k^T H_k}{S_k^T H_k S_k}, \tag{3.11}$$

де

$$S_k = X_{k+1} - X_k;$$

$$Q_k = \nabla f\left(X_{k+1}\right) + \sum_{i=1}^{n} \lambda_i \nabla g_i\left(X_{k+1}\right) - \left(\nabla f\left(X_k\right) + \sum_{i=1}^{n} \lambda_i \nabla g_i\left(X_k\right) \right).$$

У роботах [80] рекомендовано підтримувати значення матриці Гессе додатно визначеною, навіть незважаючи на те, що ці розв`язки можуть і не мати додатного. Додатнє значення матриці Гессе підтримується в тому випадку, якщо величина $Q_k^T S_k$ буде більше нуля для кожного коригування *H*. Коли величина $Q_k^T S_k$ не є додатною, то параметр Q_k модифікується поелементно, крок за кроком, так щоб виконувалась

умова $Q_k^T S_k > 0$. Узагальнена мета такої модифікації полягає в тім, щоб трохи змінити елементи Q_k, які становлять основний внесок у додатне визначення коригування. Таким чином, на початковій стадії прийнятої модифікації, найбільший від`ємний елемент з набору $Q_k^T S_k$ послідовно зменшується на половину. Така процедура триває доти, поки $Q_k^T S_k$ більше або дорівнює $10^{-5}$. Якщо після такої процедури $Q_k^T S_k$ однаково залишається від`ємним, то створюється модифікація Q_k шляхом додавання якогось вектора ν, помноженого на якусь скалярну постійну ω, а саме,

$$Q_{k+1} = Q_k + \omega\nu, \tag{3.12}$$

де

$$\nu_i = \begin{cases} \nabla g_i(X_{k+1}) g_i(X_{k+1}) - \nabla g_i(X_k) g_i(X_k), \textit{якщо } (q_k)_i \omega < 0 \wedge (q_k)_i (s_k)_i < 0, i = 1, \ldots, m \\ 0, \textit{інакше} \end{cases}$$

або ж у протилежному випадку методично збільшують ω доти, поки член $Q_k^T S_k$ стане додатнім.

У пакеті Matlab програми *fmincom, fminmax, fgoalattain* та *fseminf* реалізовані на основі методу послідовно квадратичного програмування. При виконанні функцій виводиться різна інформація, включаючи значення функції та максимальне порушення поставлених обмежень. Також відображається модифікований Гессіан, у випадку, якщо він зазнає певної корекції на початковій стадії процедури, що виконується з метою підтримки його доданого значення. Якщо Гессіан піддається повторному коригуванню на другій стадії наведеного вище підходу, то відображається його вторинне значення. Якщо підзадача квадратичного програмування не є здійсненною, то цей факт так само відображається. Така відображувана інформація, як правило, не є особливо цікавою, але вказує на те, що дана задача є істотно нелінійною, а збіжність може бути більш тривалою, ніж зазвичай. Іноді відображуване повідомлення про те, що величина $Q_k^T S_k$ не змінюється, вказує на те, що вона буде рівна нулю. Це може вказувати, що постановка задачі є неправильною або проводиться оптимізація розривної функції.

Розв`язання задачі квадратичного програмування

На кожній основній ітерації методу послідовно квадратичного програмування вирішується задача квадратичного програмування у наступній формі, де A_i ставиться до *i*-го рядку матриці *A* розмірністю $m \times n$:

$$\begin{aligned} &\min_{D \in R^n} q(D) = \frac{1}{2} D^T H D + C^T D; \\ &A_i D = b_i \qquad i = 1,...,m_e; \\ &A_i D \le b_i \quad i = m_e + 1,...,m \ . \end{aligned} \tag{3.13}$$

Оптимізаційний метод заснований на стратегії активних наборів (більше відомий як метод проекцій) і аналогічний методу, описаному в роботах [81]. Цей метод був модифікований стосовно для задач лінійного програмування і квадратичного програмування.

Процедура розв`язання містить у собі дві фази. Перша фаза являє собою розрахунок найбільш імовірної точки. Друга фаза містить у собі генерацію якоїсь ітеративної послідовності найбільш імовірних точок, що вже збігається до необхідного розв`язку. У такому методі стверджується, що активний набір $\overline{A}_k$, є певною оцінкою активних обмежень (тобто те, що являє собою обмежувальні межі) у даній точці розв`язку. Фактично всі алгоритми квадратичного програмування є методами активних наборів. Це варто особливо підкреслити, оскільки існує багато різних методів, які надзвичайно схожі по своїй суті, але представлені у вигляді різних способів свого подання.

$\overline{A}_k$ коригується на кожній ітерації та *k* будови основи для напрямку пошуку $\hat{D}_k$. Обмеження у вигляді рівностей завжди залишаються в даному активному наборі $\overline{A}_k$. Позначення для змінної у вигляді $\hat{D}_k$ в цьому випадку використовується для того, щоб розрізнити ці змінні від D_k, що використовуються на головних ітераціях методу послідовно квадратичного програмування. Напрямок пошуку $\hat{D}_k$ розраховується та далі використовується для мінімізації цільової функції, незважаючи на те, що залишаються в силі всі можливі межі активних обмежень. Весь можливий простір для

змінних $\hat{D}_k$ утвориться з базису Z_k, стовпчики якого є ортогональними щодо отриманих результатів розрахунку активного набору $\overline{A}_k$ (тобто, $\overline{A}_k Z_k = 0$). Таким чином, напрямок пошуку, що формується шляхом підсумовування всіх можливих сполучень колонок Z_k забезпечує збереження межі активних обмежень.

Прийнята матриця Z_k формується з останніх *m-l* стовпчиків квадратичного програмування – розкладання матриці $\overline{A}_k^T$, де *l* є число активних обмежень, а так само справедливо *m<l*. Z_k визначається наступним чином

$$Z_k = Q\left[l+1:m\right], \tag{3.14}$$

де

$$Q^T \overline{A}_k^T = \begin{bmatrix} R \\ 0 \end{bmatrix}.$$

Як тільки Z_k буде знайдено, то далі шукатимемо новий напрямок пошуку $\hat{D}_k$, що ц свою чергу приводить до мінімуму *q(D)*, де $\hat{D}_k$ є нульовий простір активних обмежень. $\hat{D}_k$ є лінійна комбінація стовпців $Z_k : \hat{D}_k = Z_k P$ для деякого вектора *P*. На наступному етапі, якщо за допомогою відповідної постановки для $\hat{D}_k$ ввести квадратичне рівняння як деяку функцію від *P*, одержимо:

$$q\left(P\right) = \frac{1}{2} P^T Z_k^T H Z_k P + C^T Z_k P. \tag{3.15}$$

Після диференціювання по *P* одержимо

$$\nabla q(P) = Z_k^T H Z_k P + Z_k^T C\,. \tag{3.16}$$

Член $\nabla q\left(P\right)$ має відношення до проекції градієнта квадратичної функції, оскільки він є проекцією градієнта в підпросторі функцій Z_k. Член $Z_k^T H Z_k$ є так звана проекція Гессіана. Вважаючи, що матриця Гессе *H* є додатно визначена (що справедливо стосовно до реалізації методу послідовно квадратичного програмування), то мінімум функції *q(P)* у підпросторі функцій Z_k буде визначатися

умовою $\nabla q(P) = 0$, отже для пошуку мінімуму функції необхідне розв`язання системи лінійних рівнянь

$$Z_k^T H Z_k P = -Z_k^T C. \tag{3.17}$$

А крок у напрямку мінімуму буде в наступному вигляді

$$X_{k+1} = X_k + \alpha \hat{D}_k, \text{ де } D_k = Z_k^T P. \tag{3.18}$$

Внаслідок квадратичної природи цільової функції на кожній ітерації потрібне тільки одне можливе значення розміру кроку α. Одиничний крок у напрямку $\hat{D}_k$ саме і є крок у напрямку мінімуму функції, обмеженої межами нульового простору $\overline{A}_k$. Якщо буде можливо прийняти такий крок, без порушення прийнятих обмежень, то це саме й буде розв`язок квадратичного програмування. У протилежному випадку, крок уздовж напрямку $\hat{D}_k$ у бік найближчого обмеження буде менше одинці та в активний набір на наступній ітерації будуть включені нові обмеження. Відстань до границь обмежень у будь-якому напрямку $\hat{D}_k$ можна представити як

$$\alpha = \min \left\{ \frac{-\left(A_i X_k - B_i\right)}{A_i \hat{D}_k} \right\}, \quad i = 1,...,m, \tag{3.19}$$

яке визначено для обмежень не з активного набору, де напрямок $\hat{D}_k$ показує напрямок до границь обмежень, тобто $A_i \hat{D}_k > 0, \quad i = 1,...,m.$

У випадку включення *n* незалежних обмежень в активний набір, без локалізації мінімуму, то для відповідності невиродженої системі лінійних рівнянь

$$\overline{A}_k \mu_k = C. \tag{3.20}$$

варто розраховувати множники Лагранжа.

Якщо всі елементи μ_k більше нуля, то X_k є розв`язком для точки оптимуму задачі. Однак, якщо який-небудь із елементів μ_k буде менше нуля, то ці компоненти не будуть відповідати обмеженням у вигляді рівностей, а отже, відповідний елемент необхідно визначати з активного набору, так само потрібний обіг до нової ітерації.

В даному алгоритмі для успішного початку роботи потрібна якась припустима початкова точка. Якщо поточна точка з методу послідовно квадратичного

програмування не є припустимою, то тоді якусь точку можна знайти з розв`язку задачі лінійного програмування

$$\begin{aligned} &\min_{\gamma\in R, X\in R^n} \gamma; \\ &A_i X = b_i, \quad i = 1,...,m_e \\ &A_i X - \gamma \le 0, \quad i = m_e + 1,...,m\ . \end{aligned} \tag{3.21}$$

Позначення A_i вказує на i-у точку матриці. Припустиму точку для рівнянь (3.21) можна визначити з розв`язку недо- або перевизначеної системи лінійних рівнянь, отриманої з системи обмежень типу рівностей. Якщо розв`язок такої задачі існує, то фіктивна змінна γ встановлюється в цьому випадку як якась максимальна розбіжність.

Алгоритм квадратичного програмування можна модифікувати до задач лінійного програмування шляхом установки на кожній ітерації напрямку пошуку в напрямок найшвидшого спуску, де g_k є градієнтом узятої цільової функції (рівність коефіцієнтів лінійної цільової функції).

$$\hat{d}_k = -Z_k Z_k^T g_k. \tag{3.22}$$

Якщо після використання методу лінійного програмування знайдена якась припустима точка, то далі запускається основна фаза методу квадратичного програмування. Напрямок пошуку $\hat{D}_k$ ініціалізується разом напрямком пошуку $\hat{d}_1$, отриманим з розв`язку системи лінійних рівнянь

$$H\hat{d}_1 = -g_k, \tag{3.23}$$

де g_k є градієнт цільової функції для поточної ітерації X_k

(тобто $HX_k + C$).

Якщо для задачі квадратичного програмування неможливо визначити припустиму точку, то напрямок пошуку для основної підпрограми послідовно квадратичного програмування $\hat{D}_k$ приймається з умови мінімізації величини γ.

Лінійний пошук та критерій якості.

Розв`язання підзадачі квадратичного програмування приводить до формування вектора D_k, що у свою чергу, використовується при формуванні нової ітерації типу

$$X_{k+1} = X_k + \alpha D_k. \tag{3.24}$$

Для того, щоб одержати додатнє зменшення критерію якості оцінюється параметр довжини кроку α_k. Реалізований в даному алгоритмі критерій якості був використаний [77], [80] і має такий вигляд

$$\Psi(X) = f(X) + \sum_{i=1}^{m_e} r_i g_i(X) + \sum_{i=m_e+1}^{m} r_i \max\{0, g_i(X)\}. \tag{3.25}$$

Вводиться наступний штрафний параметр:

$$r_i = (r_{k+1})_i = \max_i \left\{ \mu_i, \frac{1}{2}\left((r_k)_i + \mu_i\right) \right\}, \quad i = 1,...,m. \tag{3.26}$$

Даний підхід дає позитивний внесок для прийнятих обмежень, але які є неактивними для розв`язання задачі квадратичного програмування, хоча раніше це були активні значення. У прийнятому методі реалізації параметр штрафу як вихідний параметр має вигляд:

$$r_i = \frac{\|\nabla f(X)\|}{\|\nabla g_i(X)\|}, \tag{3.27}$$

де $\|.\|$ являє собою евклідову норму.

Такий підхід забезпечує істотний внесок від обмеження з невеликими параметрами в значення штрафних параметрів, що особливо актуально для активних обмежень поблизу точки розв`язку.

3.3. Практична реалізація методу оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив

Для розв`язання задачі оптимізації використовуємо математичну модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних

добрив. Значення матриця інтенсивностей переходів λ_{ij} одержимо з імітаційної моделі системи захисту критичних ресурсів виробництва мінеральних добрив:

$$\begin{vmatrix} -0,040 & 0,015 & 0,010 & 0,015 \\ 0,225 & -0,250 & -0,025 & 0,050 \\ 0,625 & -0,160 & -0,855 & 0,390 \\ 0,000 & 0,075 & 0,200 & -0,275 \end{vmatrix}$$

Результати p_i одержимо з математичної моделі протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив (рис.3.1). Для реалізації розв'язку розроблено програмний модуль у Matlab (Додаток А). Для оптимізації використовуються кінцеві усталені значення p_i - імовірність знаходження системи у кожному зі станів.

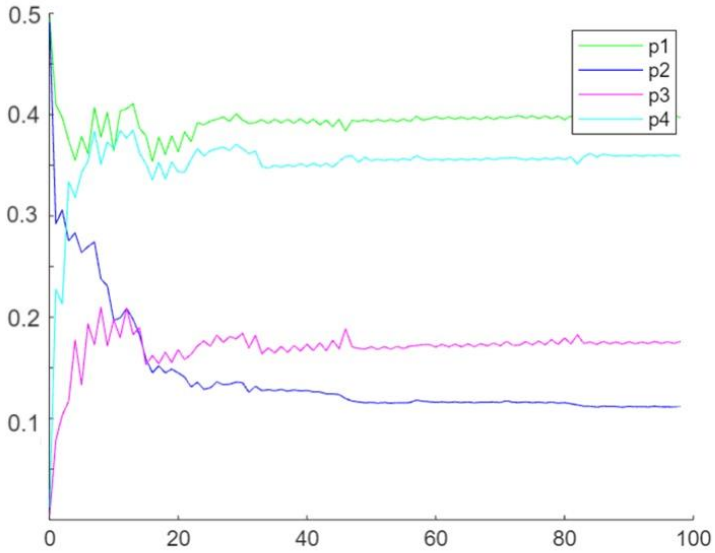

Рис. 3.1. Імовірність знаходження системи у кожному зі станів

Обчислено значення критеріїв оптимальності: узагальненого критерію якості (рис. 3.2), критерію якості для способу однакових інтенсивностей (рис. 3.3) та критерію якості для способу пропорційності витратам (рис. 3.4). Оскільки метод послідовно квадратичного програмування реалізує пошук мінімуму, а критерії (3.4)-

(3.6) спрямовані на пошук максимуму знак у критеріях при обчисленні змінено на протилежний.

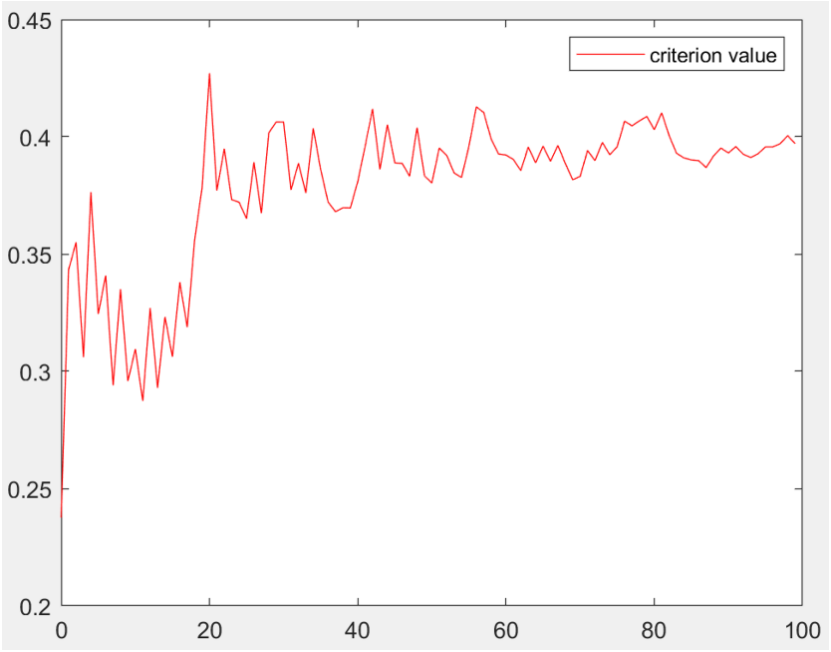

Рис. 3.2. Зміна узагальненого критерію якості протягом оптимізації

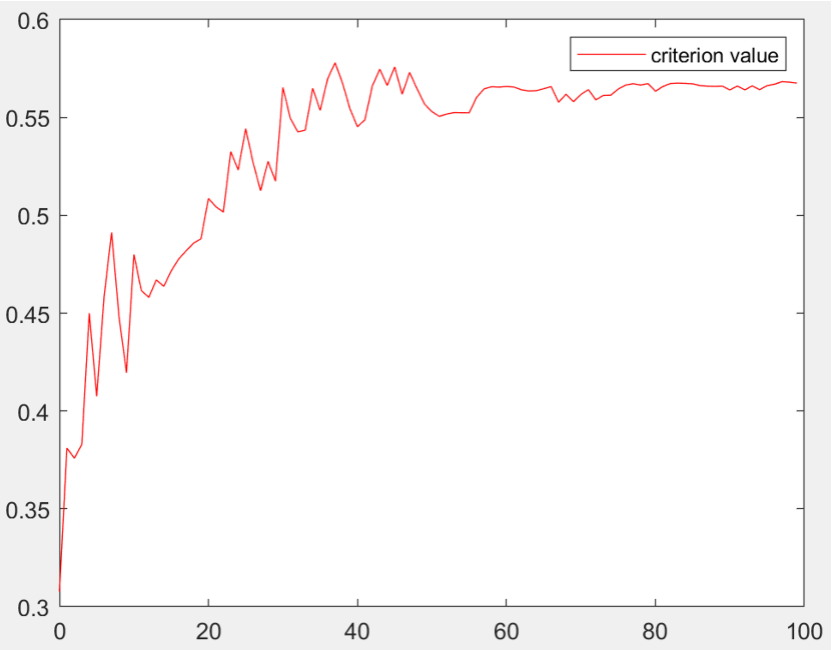

Рис. 3.3. Зміна критерію якості для способу однакових інтенсивностей протягом оптимізації

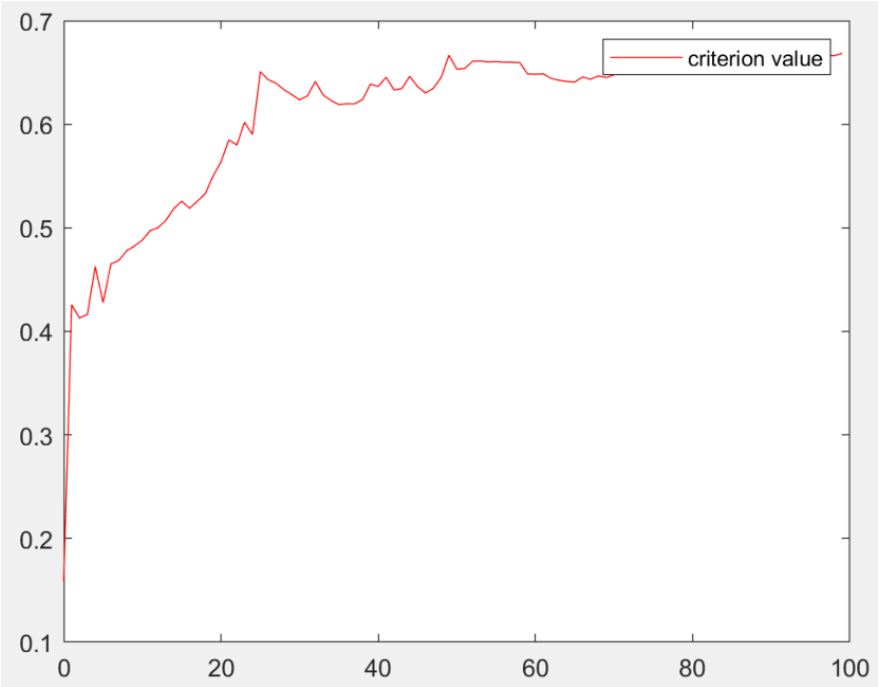

Рис. 3.4. Зміна критерію якості для способу пропорційності витратам протягом оптимізації

Методика оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив.

В результаті проведених досліджень сформульована методика оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив:

- Здійснити факторно-цільовий аналіз з метою вибору критерію опимальності.
- Обрати математичну модель. Використовуються імітаційна модель системи захисту критичних ресурсів виробництва мінеральних добрив та математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив.
- Обрати метод оптимізації. Використовується метод послідовно квадратичного програмування.

Висновки до розділу 3

1. Здійснено системний аналіз підходів до оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив. Запропоновано перехід від

багатокритеріальної задачі оптимізації, до однокритеріальної. При сформульованому понятті захищеності системи оптимізаційна задача полягає в забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи.

2. Реалізовано факторно-цільовий аналіз з метою вибору критерію оптимальності. Запропоновано три критерії якості: узагальнений критерій якості, критерій якості для способу однакових інтенсивностей та критерій якості для способу пропорційності витратам.

3. Для оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив використовуються імітаційна модель системи захисту критичних ресурсів виробництва мінеральних добрив та математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив. За допомогою імітаційної моделі системи захисту критичних ресурсів виробництва мінеральних добрив одержимо матрицю інтенсивностей переходів. За допомогою математичної моделі протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив одержимо значення імовірностей перебування системи у чотирьох станах.

4. Реалізовано оптимізацію системи захисту критичних ресурсів виробництва мінеральних добрив за допомогою методу послідовно квадратичного програмування. Для даного методу використовуються запропоновані критерії оптимальності та рівняння математичної моделі протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив у якості обмежень.

5. Розроблено методику оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив.

РОЗДІЛ 4. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАХИСТУ КРИТИЧНИХ РЕСУРСІВ ВИРОБНИЦТВА МІНЕРАЛЬНИХ ДОБРИВ

Для підвищення якості готового продукту необхідно розробити інформаційну технологію захисту критичних ресурсів виробництва мінеральних добрив. Створення ІТ ЗКР виробництва мінеральних добрив дозволяє поєднати наступні технічні, програмні та організаційно-методичні засоби: моделювання системи захисту критичних ресурсів виробництва мінеральних добрив, оптимізація системи захисту критичних ресурсів виробництва мінеральних добрив, система захисту критичних ресурсів виробництва мінеральних добрив, математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі та оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі.

Застосування ІТ ЗКР виробництва мінеральних добрив дозволяє у повній мірі здійснювати вимірювання основних параметрів технологічного процесу, оперативно керувати процесом, забезпечуючи одержання готового продукту заданої якості та забезпечувати функціональну безпеку технологічного процесу виробництва мінеральних добрив.

4.1. Математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі

Одним із найпоширеніших методів виготовлення мінеральних добрив є грануляція. Добрива у вигляді гранул мають ряд переваг перед звичайними добрива у вигляді порошку чи рідини, а саме, легкість у транспортуванні, добре засвоюються та менше піддаються вивітрюванню із ґрунту, зручні у застосування.

Щоб отримати тверді частинки з рідкого вихідного матеріалу такого як: розчини, емульсії чи суспензії, застосовують такі процеси як: кристалізація, грануляція, сушка розпиленням. Кристалізація і грануляції є складними динамічними процесами, що

включають кілька фаз (рідина і тверда речовина), тепло – і масообмін між цими фазами, а також процеси формування частинок.

Один із процесів, який часто використовується у фармацевтичній галузі, галузі виробництва продуктів харчування та добрив – це грануляція у псевдозрідженому шарі. Конструкція апаратів для процесу грануляції проста і завдяки високим показникам теплоперенесення та масоперенесення можна спроєктувати компактні установки для грануляції в порівнянні з іншими технологіями. У промислових масштабах, для процесу грануляції необхідна велика кількість енергоресурсів, а саме природнього газу, який використовується для нагрівання повітря у технологічній камері. Зменшення використовуваного газу для процесу грануляції хоча б на 10 – 15% при сталих показниках якості продукту дозволило б значно підвищити ефективність процесу грануляції та значно зменшити витрати на виробництво. Одним із важливих етапів вирішення проблеми – створення математичної моделі процесу, яка повинна адекватно описувати всі етапи процесу грануляції. Тому завдання розробки математичної моделі, що дасть можливість створити енергоефективну систему управління процесом грануляції, яка буде підтримувати вологовміст гранул на заданому рівні, є актуальною задачею.

Основна перевага грануляторів із псевдозрідженим шаром полягає в тому, що декілька етапів технологічного процесу можна поєднати в одному пристрої, включаючи попереднє змішування твердого порошку, грануляцію з відповідним рідким розчином з подальшим сушінням гранул до заздалегідь встановленого рівню вологості. Крім того, ця методика має ряд переваг в порівнянні з іншими методами, наприклад, висока швидкість теплопередачі та масопередачі, одержання частинок заданого розміру. Зважаючи на вищезгадані переваги, процес грануляції у грануляторі із псевдозрідженим шаром широко застосовується у фармацевтичній, харчовій та хімічній промисловості і має довгу історію понад 40 років. У наступні десятиліття процес грануляції псевдозрідженим шаром досліджували ширше, що призвело до появи різних математичних моделей [82-83].

Реалізовані системи керування в основному концентруються на регулюванні процесу тепло- та масоперенесення (наприклад, вологості і температури продукту) та

інтегральних значеннях(наприклад, загальної маси продукту) або середніх значеннях (наприклад, середнього розміру частинок) частинок. Хоча системи керування здебільшого задовольняють вимогам, які перед ними поставленні, вони не можуть гарантувати, що розподіл властивостей в цілому відповідає специфікаціям. Це означає, що системи керування виробництвом повинні бути покращені.

Основою для проєктування контролера є динамічна модель процесу. В принципі, чим точніше опис процесу, тим більше можна сказати про результат процесу. Але надмірна кількість деталей може також різко ускладнити процес проєктування контролера, тому в певний момент робляться припущення, які згодом спростять конструкцію контролера.

На процес гранулоутворення у грануляторі великий вплив мають такі параметри як: температура гранул, температура теплоносія та вологовміст гранул. В створеній математичній моделі велика увага приділяється контролю даних параметрів, аби система керування змогла забезпечити ефективне використання ресурсів та високу якість продукції.

Математична модель повинна відповідати наступним вимогам:

- температурний діапазон в якому працює гранулятор повинен бути в межах від 360 К до 480 К;
- початкові умови для параметрів вологовмісту гранул, температури гранул, та температури теплоносія при яких починає працювати гранулятор повинні бути в межах 90 – 92 %, 358 – 360 К та 470 – 475 К відповідно;
- граничні умови для параметрів вологовмісту – вологовміст гранул на виході повинен лежати в межах від 15 % до 25 %, температури гранул – температура гранул не повинна перевищувати 360 К – 380 К, температура теплоносія – не повинна виходити за рамки температурного діапазону.

Вологовміст гранул, температура теплоносія та температура гранул тісно пов’язані між собою, тому що якщо температура теплоносія буде перевищувати температурний діапазон, відбудеться надлишкове нагрівання гранул та критичне зниження вологовмісту в гранулі. В результаті чого буде використовуватися надлишкова кількість енергії на нагрівання повітря, що є не ефективним з точки зору

енергоефективності, а зменшення кількості вологи у гранулах може призвести до їх хрупкості, що негативно впливає на процес транспортування та використання мінеральних добрив, тому важливо, що розроблена математична модель відповідала встановленим до неї вимогам.

При створенні математичної моделі були висунуті наступні припущення:

– зміна параметрів псевдозрідженого шару відбувається в часі, без урахування радіальної складової та зміни по висоті;
– теплообмін між повітрям, частинками та краплями є конвективним;
– зміна температури та вологовмісту по ширині шару не суттєво впливає на процес утворення гранул, тому нею ми можемо знехтувати;
– псевдозріджений шар добре перемішаний, відсутній застійні зони.

Процеси зневоднення та грануляції описує розроблена математична модель у вигляді системи з трьох диференціальних рівнянь. Формула (4.1) описує зміну температури повітря, яке використовується для нагрівання шару та гранулоутворення:

$$\rho \cdot C \cdot \frac{\partial T_r}{\partial t} + V_r \cdot \varepsilon \cdot \rho \cdot \frac{\partial T_r}{\partial x} = \varepsilon \cdot a \cdot \frac{\partial^2 T_r}{\partial y^2} - \alpha \cdot F \cdot \left(T_r - T_{gr}\right) + G_p \cdot \left(1 - x_p\right) \cdot \left(r + C_n \cdot T_{gr}\right); \quad (4.1)$$

де ρ – густина гранул, кг/м^3, C – теплоємність гранул Дж/(кг · К), T_r – температура теплоносія, К, V_r – швидкості теплоносія, м/с, ε – поруватість потоку гранул, %, α – коефіцієнт тепловіддачі, 1/с, a – коефіцієнт горизонтальної температуропровідності, м^2/с; F – площа газорозподільної решітки, м^2, T_{gr} – температура гранул, К, G_p – витрати вихідного розчину, м^3/с, x_p – концентрація вихідного розчину, r – теплота пароутворення, Дж/кг, C_n – питома теплоємність повітря, Дж/(кг · К), x – висота апарату, м, y – ширина апарату, м.

Формула (4.2) описує зміну температури гранул:

$$\begin{aligned}&(1-\varepsilon)\cdot\rho\cdot C\cdot\frac{\partial T_{gr}}{\partial t}-V_{gr}\cdot(1-\varepsilon)\cdot\rho\cdot\frac{\partial T_{gr}}{\partial x}=\alpha\cdot F\cdot\left(T_r-T_{gr}\right)-\\&-G_p\cdot\left(1-x_p\right)\cdot\left(r+C_n\cdot T_{gr}\right)+G_p\cdot x_p\cdot q;\end{aligned}\tag{4.2}$$

де V_{gr} – швидкість розбризкування розчину, м/с, q – теплота, що виділяється під час кристалізації розчину, Дж/кг.

Рівняння (4.3) описує зміну вологовмісту гранул:

$$\varepsilon\cdot\rho\cdot\frac{\partial W_g}{\partial t}+V_r\cdot\varepsilon\cdot\rho\cdot\frac{\partial W_g}{\partial x}=D\cdot\varepsilon\cdot\frac{\partial^2 W_g}{\partial y^2}+\beta\cdot F\cdot(\varsigma_1\cdot T_a-\varsigma_2\cdot T_g);\tag{4.3}$$

де W_g – вологовміст гранул, %, D – коефіцієнт дифузії, м^2/с, β – коефіцієнт масовіддачі кг/м^{2}с, ς_1, ς_2 – вагові коефіцієнти.

Розроблена математична модель у вигляді формул (4.1) – (4.3) враховує гідродинаміку псевдозрідженого шару, а також кінетику процесів грануляції та зневоднення.

Розв’язок системи диференціальних рівнянь математичної моделі здійснювався за допомогою методу Рунге-Кутти четвертого порядку.

Для отримання результатів роботи розробленої математичної моделі системи реалізовано програму, яка обраховує та виводить графіки температури повітря, температури гранул та вологовмісту на мову програмування Python в середовищі PyCharm. Для додавання результатів в таблицю та побудову графіків використовувалася бібліотека xlsxwriter. Після виконання програми, дана бібліотека формує файл з результатами та графіками формату .xslx, який можна відкрити за допомогою Microsoft Exel.

Моделювання процес грануляції та зневоднення відбувалося на основі даних наведених в таблиці 4.1.

Таблиця 4.1

Основні параметри процесу грануляції у псевдозрідженому шарі

Назва параметра	**Умовні позначення**	**Значення**	**Розмірність**
Коефіцієнт тепловіддачі	a	5,56	Вт/м^{2}К
Витрати розчину	Gp	0,0068	кг/с
Теплоємність повітря	Cp	1970	Дж/кг·К
Концентрація розчину	Xp	0,4	%
Питома теплота пароутворення	r	129000	Дж/кг
Витрати повітря	G2	0,0031	м^3/с
Теплота, що виділяється під час кристалізації розчину	q	82300	Дж/кг
Коефіцієнт теплоємності розчину	C	3897	Дж/кг·К
Молекулярна маса сульфата амонія	MH	18000	кг/моль
Поверхня масообміну	Fm	10	м^2
Універсальна газова стала	Rg	281	Дж
Поруватість потоку гранул	e	0,4	%
Густина гранул	ro	1450	кг/м^3
Швидкість розчину	V2	$2{,}3\cdot10^{-4}$	м/с
Швидкість повітря	V1	$2{,}4\cdot10^{-5}$	м/с
Коефіцієнт тепловіддачі	aL	800	Вт/м^{2}К
Площа газорозподільної решітки	F	16	м^2
Коефіцієнт масообміну	b	0,054	кг/м^{2}с
Коефіцієнт дифузії	D	0,000245	м^2/с
Початкова температура теплоносія	T1	473	К
Початкова температура гранул	T2	360	К
Початковий вологовміст гранул	W1	90	%

Дослідження адекватності розробленої математичної моделі проведено з кроком інтегрування 0,01 та з кількістю ітерації 60 000. На графіках наведено значення температури повітря, температури гранул та вологовмісту гранул на висоті x=0,5 м у грануляторі із псевдозрідженим шаром. Графік зміни температури повітря в грануляторі наведено на рисунку 4.1. Температура теплоносія у грануляторі із початкового значення 473 К спадає до значення 415 К – 410 К. Оскільки для процесу утворення гранул та їх подальшого висушування потрібна велика кількість тепла, ми спостерігаємо спад температури теплоносія.

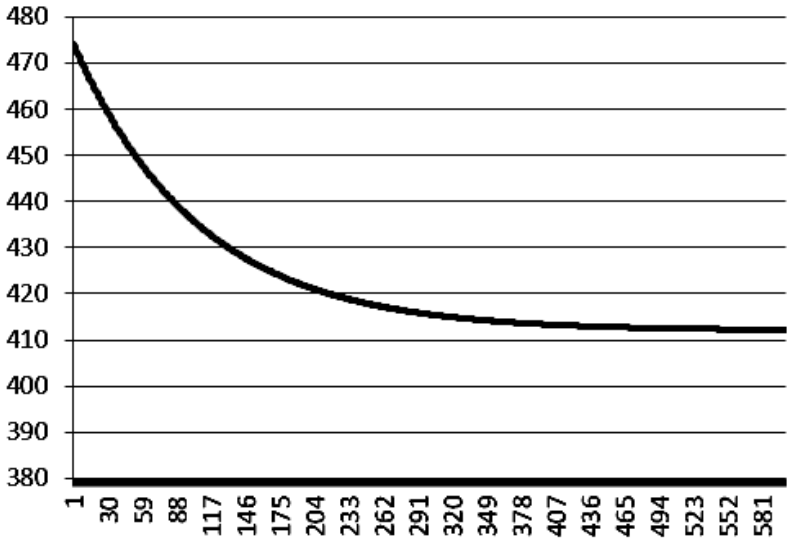

Рис. 4.1. Графік зміни температури теплоносія в грануляторі із псевдозрідженим шаром.

Перехідна характеристика температури гранул наведено на рисунку 4.2. Перехідна характеристика вологовмісту гранул наведено на рисунку 4.3.

В процесі сушки температура гранул повинна зростати, а кількість вологи повинна зменшуватись, що ми можемо спостерігати із перехідних характеристик.

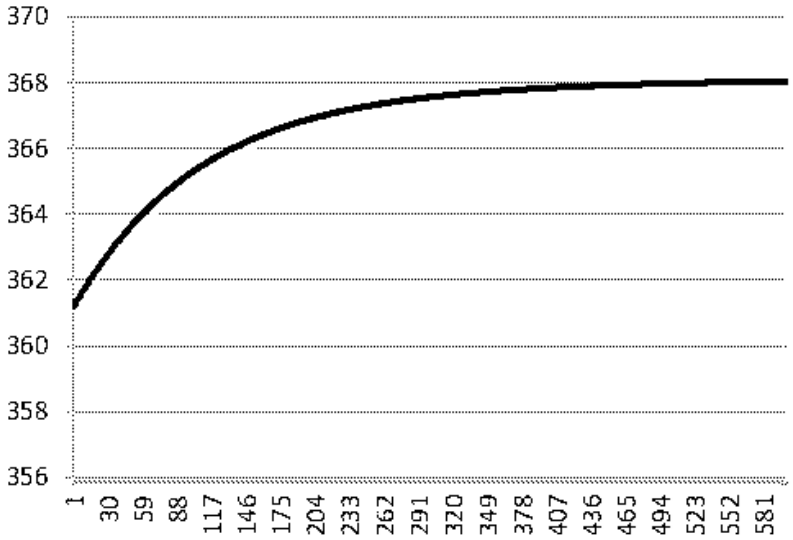

Рис. 4.2. Перехідна характеристика температури гранул в грануляторі із псевдозрідженим шаром.

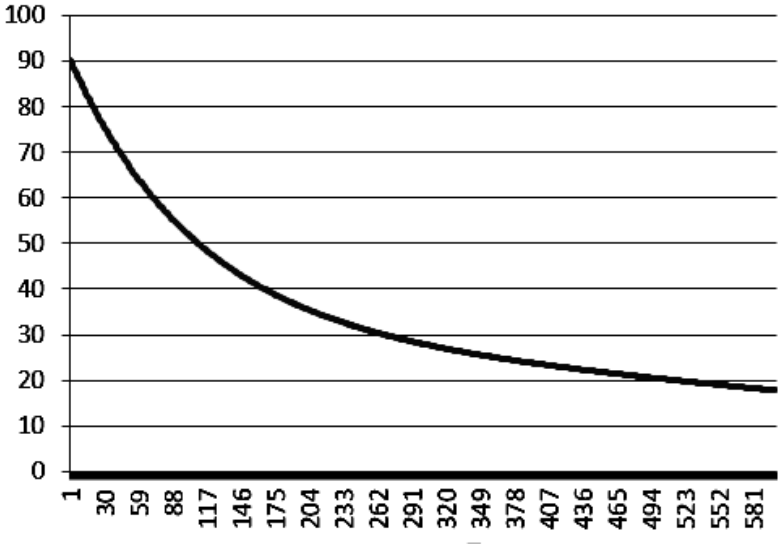

Рис. 4.3. Перехідна характеристика вологовмісту гранул в грануляторі із псевдозрідженим шаром.

Як можемо побачити з отриманих графіків, характер поведінки температури теплоносія у грануляторі залишається незмінним, тобто він залишається в діапазоні 410 К – 415 К, але чим довше триває процес, тим більше будуть нагріватись гранули, тим більше буде випаровуватись з них вологи відповідно і витрати енергії для виконання даного процесу будуть більші. Заданий вологовміст гранул повинен бути в межах від 15% до 25 %. Продовження сушіння може призвести до втрати якісних характеристик гранул та збільшення їх крихкості.

Розроблено математичну модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі. Проведено аналіз математичних моделей процесу зневоднення та гранулювання у псевдозрідженому шарі. Визначено основні процеси, що впливають на виробництво гранульованих мінеральних добрив – теплообмін, масообмін, пароутворення, кристалізація. Одержано перехідні характеристики температури повітря, температури гранул та вологовмісту гранул. Комп`ютерний експеримент підтвердив адекватність запропонованої математичної моделі процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі. Основними характеристиками, що впливають на виробництва гранул у псевдозрідженому шарі є температура теплоносія та температура гранул. Для одержання мінеральних добрив заданої якості необхідно

контролювати вологовміст гранул. Запропонована математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі разом з регулятором може використовуватись для побудови системи керування процесом.

4.2. Оптимальна система керування виробництвом гранульованих мінеральних добрив у пседозрідженому шарі з LQR-регулятором

У грануляторі відбувається процес утворення гранул при висушуванні шарів та наростанню нових шарів, при цьому відбувається випаровування і передача тепла частинкам.

Так як основним каналом керування є T1 → T2, то далі розглянемо перехідну характеристику залежності температури теплоносія та температури гранул (рис 4.4).

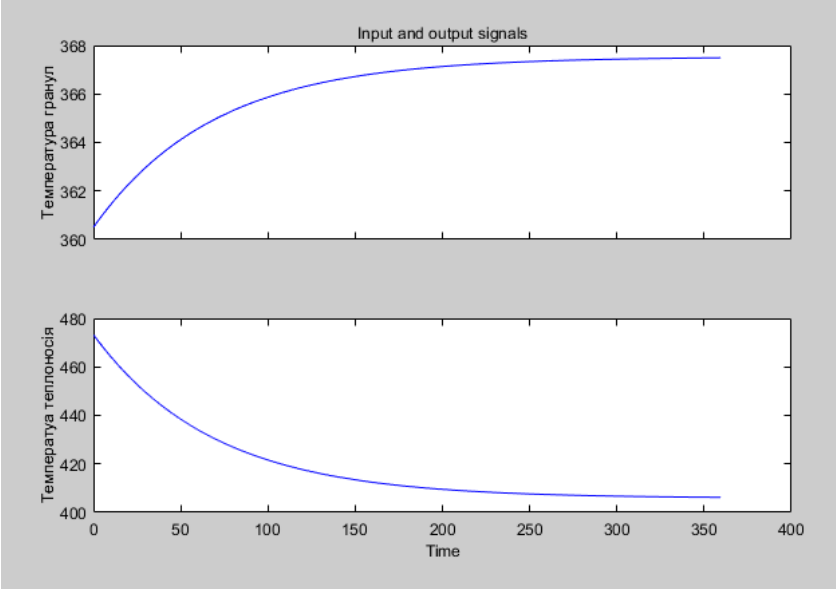

Рис. 4.4. Перехідна характеристика температури теплоносія та гранул

З використанням модулю MATLAB System Identification (рис. 4.5) отримано передавальну функцію виду:

$$W(p) = \frac{4481s+66.4}{s\text{^}2+5916s+73.32} \qquad (4.4)$$

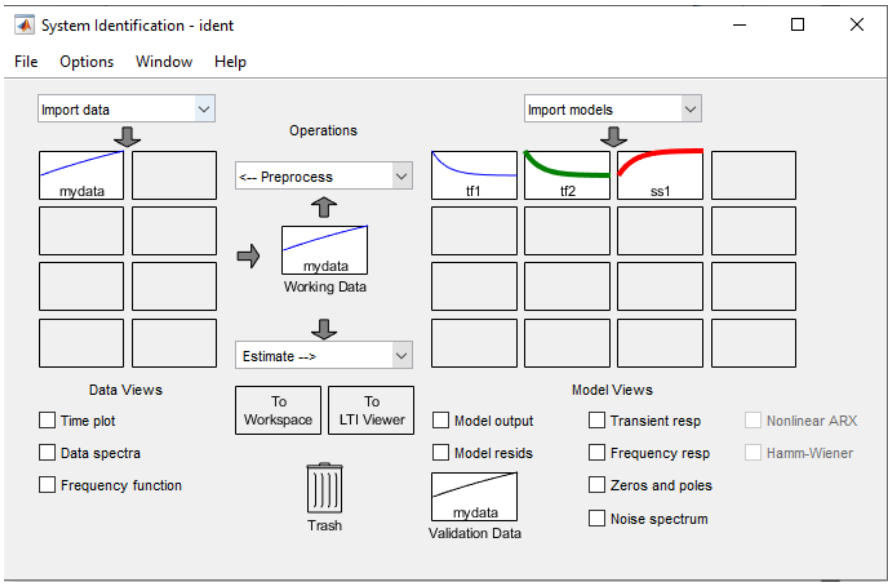

Рис. 4.5. Синтез передавальної функції у модулі System Identification

Графік передавальної функції, який показує реакцію системи на одиничний крок наведений на рис. 4.6.

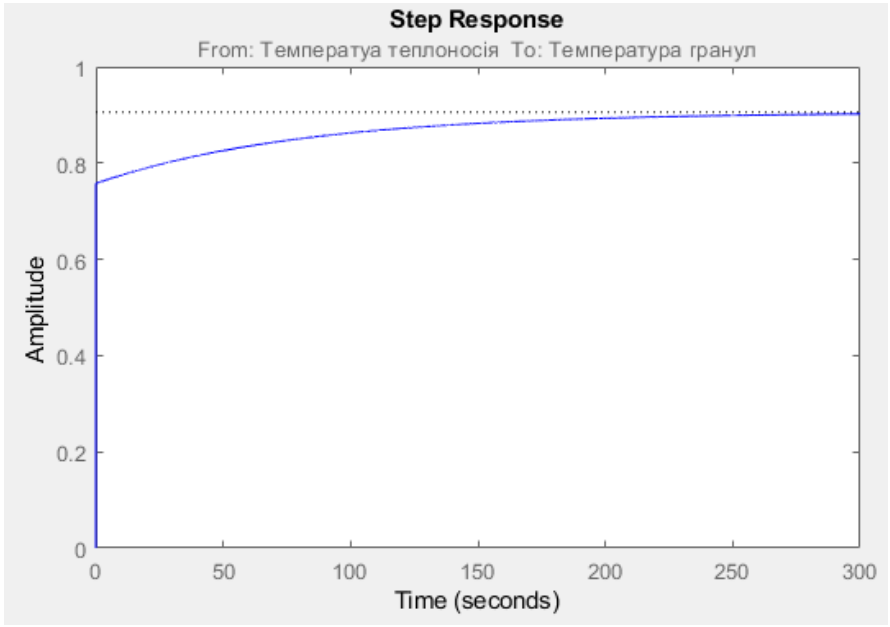

Рис. 4.6. Графік передавальної функції

4.2.1. Дослідження системи на керованість та спостережуваність

Керованість – це здатність системи при керуючому впливі переводитися з початкового стану (x_0) в кінцевий стан($x_к$), за скінченний проміжок часу. Якщо

система виконує ці умови повністю, то система називається повністю керованою. Якщо спостерігається відповідність тільки деяким станам, то система називається частково керованою, а якщо система не відповідає жодній з умов її називають повністю некерованою[82]. Для аналізу системи на керованість за допомогою пакету MATLAB треба проаналізувати матрицю:

$$P = [B\ AB\ A^2B\ A^{n-1}B] \tag{4.5}$$

У випадку якщо порядок системи рівний рагу матриці то, система вважається повністю керованою. Якщо ранг матриці менший за порядок системи, але більший за нуль, то система рахується частково керованою, а коли ранг матриці дорівнює нулю, то система повністю некерована.

Спостережуваність – властивість системи за вихідними величинами x(t), при вказаних вхідних керуваннях, знайти координати станів системи за скінченний проміжок часу. Для визначення спостережуваності системи, треба знайти приведену нижче матрицю:

$$H = [C^T\ A^TC^T\ (A^T)^2C^T \dots\ (A^T)^{n-1}C^T] \tag{4.6}$$

Для знаходження рангу системи береться найбільший порядок ненульового мінора в матриці. У випадку якщо порядок системи рівний рагу матриці то, система вважається повністю спостережувана. Якщо ранг матриці менший за порядок системи, але більший за нуль, то система рахується частково спостережуваною, а коли ранг матриці дорівнює нулю, то система повністю не спостережувана[82].

За допомогою функцій в MATLAB перевіримо чи є система спостережуваною та керованою:

H = obsv(A,C) – Знаходимо матрицю спостережуваності системи;

rank(H) – Знаходимо ранг для матриці спостережуваності;

P = ctrb(A,B)– Знаходимо матрицю керованості системи;

rank(P) – Знаходимо ранг для матриці керованості.

Результати перевірки показали ранги матриць рівні 2, це означає що дана система є спостережуваною та керованою водночас.

4.2.2. Синтез оптимальної системи керування з LQR-регулятором

Сучасні потужні комп'ютери та програмні модулі, які підтримуються на цих комп'ютерах дозволяють інженеру моделювати системи керування та досліджувати їх. В такий спосіб можна оцінити систему, якість її керування та відразу бачити недоліки та доречність зроблених рішень. Для досягнення цієї мети були винайдені програмні пакети візуального моделювання.

MATLAB є одним з найкращих програмних продуктів у цій ніші. Він має потужні функціональні можливості та перевірений часом. Користувач може використовувати його при вирішенні задач у різних областях людської діяльності.

Лінійно-квадратичний регулятор (англ. Linear quadratic regulator, LQR) – один із типів регуляторів в теорії управління, який використовує квадратичний функціонал якості [84]. Динамічна система, яка описується лінійними диференціальними рівняннями, а показником якості є квадратичний функціонал є завданням лінійно-квадратичного управління.

Переваги лінійно квадратичного регулятора:

– Безінерційність;
– Недоліки лінійно квадратичного регулятора:
– Велика кількість ітерацій;
– Необхідність зв'язку по всьому вектору стану;
– Потрібна точна модель об'єкта.

Для безперервних систем описуваних в просторі станів маємо:

$$x' = \mathrm{Ax} + \mathrm{Bu}, \tag{4.7}$$

де A та B матриці моделі.

Критерій оптимальності:

$$J = \int_0^\infty (\mathrm{x}^T \mathrm{Qx} + \mathrm{U}^T \mathrm{Ru}\ )dt, \tag{4.8}$$

де для синтезу LQR регулятору потрібні матриці моделі A, B та матриці при критерію якості Q, R. Де Q та R – це позитивно визначені матриці. $\mathrm{x}^T\mathrm{Qx}$ – інтегральна квадратична похибка, яка відповідає за якість регулювання системи на інтервалі від нуля до нескінченності. Якість може задаватися відповідною матрицею Q. $\mathrm{U}^T\mathrm{Ru}$ –

характеризує енергію яка буде затрачена для регуляції. Цей параметр задається одиничною матрицею R.

Знаходимо матриці A та B з отриманою передавальної функції і при використанні команди: sys = ss(Wp); пакета Control System Toolbox. Де – sys - це модель, Wp – це передавальна функція об'єкту управління.

В результаті отримуємо такі матриці:

$$\mathrm{A} = \begin{bmatrix} -5916 & -9.165 \\ 8 & 0 \end{bmatrix}, \tag{4.9}$$

$$\mathrm{B} = \begin{bmatrix} 64 \\ 0 \end{bmatrix}, \tag{4.10}$$

$$\mathrm{C} = [70.02 \quad 0.1297], \tag{4.11}$$

$$\mathrm{D} = [0]. \tag{4.12}$$

Маємо рівняння:

$$x' = \begin{bmatrix} -5916 & -9.165 \\ 8 & 0 \end{bmatrix} \mathrm{x} + \begin{bmatrix} 64 \\ 0 \end{bmatrix} \mathrm{u} \tag{4.13}$$

Керування, знайдене по LQR - алгоритму повинно задовольняти критерій:

$$u = -\mathrm{R}^{-1}\mathrm{B}^{T}\mathrm{P}\mathrm{x} \tag{4.14}$$

Матриця P знаходиться з рівняння Ріккаті:

$$\mathrm{AP} + \mathrm{A}^{\mathrm{T}}\mathrm{P} + \mathrm{PBR}^{-1}\mathrm{B}^{\mathrm{T}}\mathrm{P} + \mathrm{Q} = 0 \tag{4.15}$$

Структурна схема замкнутої системи у якій використовується лінійно-квадратичний регулятор в колі зі зворотнім зв'язком зображена на рис. 4.7.

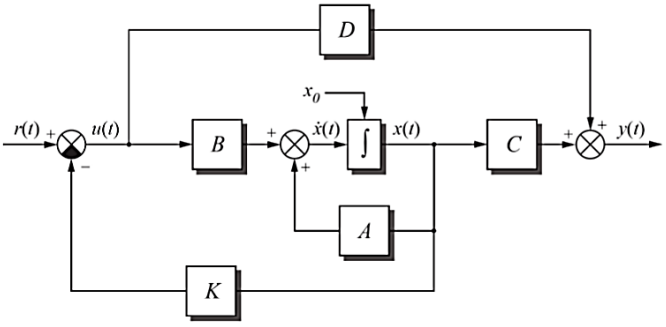

Рис. 4.7. Структурна схема замкнутої системи з лінійно-квадратичним регулятором, де r(t) - вхід системи; x(t) – змінна стану системи; y(t) – вихід системи; u(t) – закон керування; A,B,C,D - матриці простору – станів системи; K – матриця зворотного зв'язку.

Для отримання рішення була використана функція з пакету Control System Toolbox MATLAB – lqr(A,B,Q,R) та отримані коефіцієнти K зворотної матриці зв’язку.

$$K = lqr(A, B, Q, R); \quad (4.16)$$

$$K = [\,0.0066 \quad 0.8670]; \quad (4.17)$$

Для отримання графіку регулятора структурна схема побудована в MATLAB Simulink (рис 4.8).

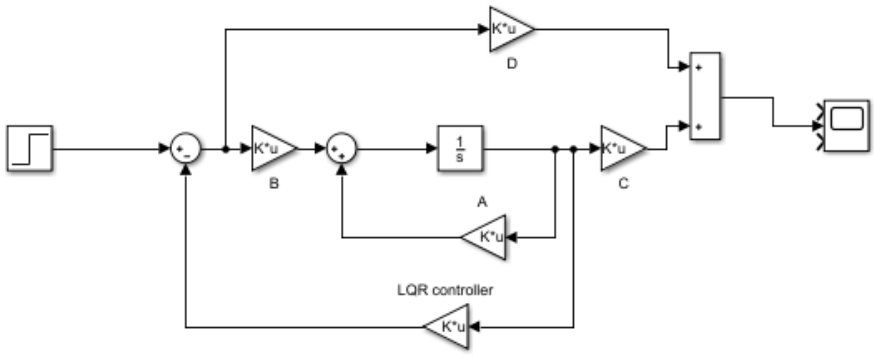

Рис. 4.8. Структурна схема замкнутої системи з лінійно-квадратичним регулятором

Графік перехідної характеристики оптимальної системи керування з LQR-регулятором: (рис 4.9)

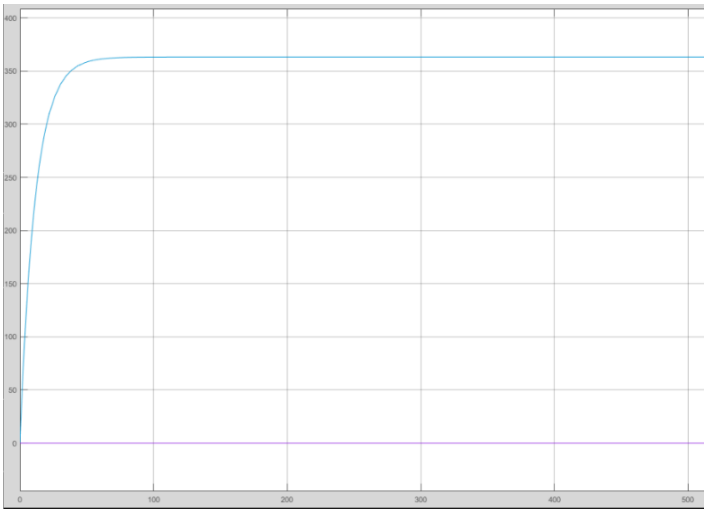

Рис. 4.9. Перехідна характеристики оптимальної системи керування з LQR-регулятором

Як видно з графіку система стабільна, керована, виходить на задану температуру T2 = 364K та має час перехідного процесу t_p = 18.7 секунди, що прийнятно для регулятора такого типу. Перерегулювання відсутнє.

Для того щоб впевнитися, що розрахований регулятор побудовано правильно, та він надає швидке регулювання системи створимо реакцію системи на вихід температури 364K без регулятора, підібравши step належним чином

Створимо схему для перевірки ефективності регулятору в порівняні з графіком передавальної функції (рис 4.10).

Як можна побачити з графіку регулятора температура починається з 0 К. Щоб змоделювати систему, яка найбільш наближена до реальних умов виберемо стартування з температури 300K що приблизно дорівнює кімнатній температурі. Для цього змінимо параметр інтегратора «Початкові умови».

Грануляторі часто забиваються при процесі грануляції тому середній час роботи не дуже великий. Час моделювання був вибраний 600 секунд, відповідно до режиму роботи грануляторів такого типу.

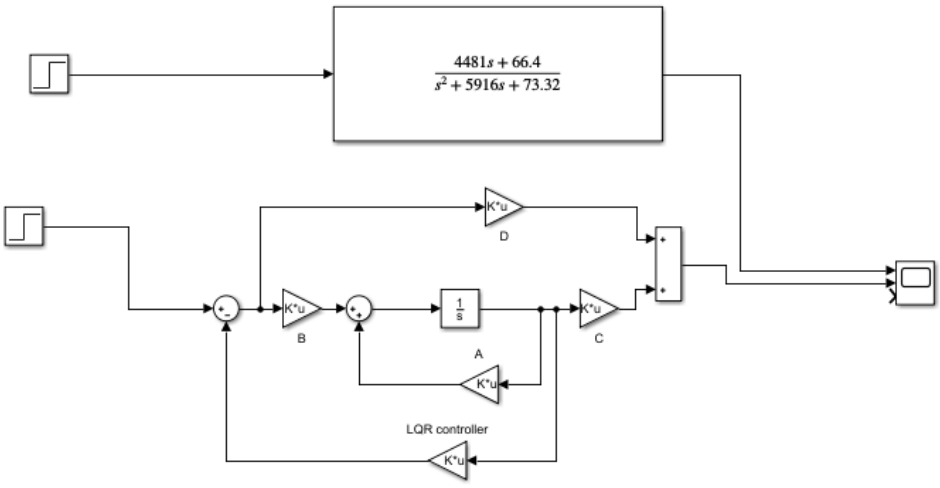

Рис. 4.10. Схема регулятору та передавальної функції

Накладемо отриманий графік з графіком передавальної функції (рис 4.11).

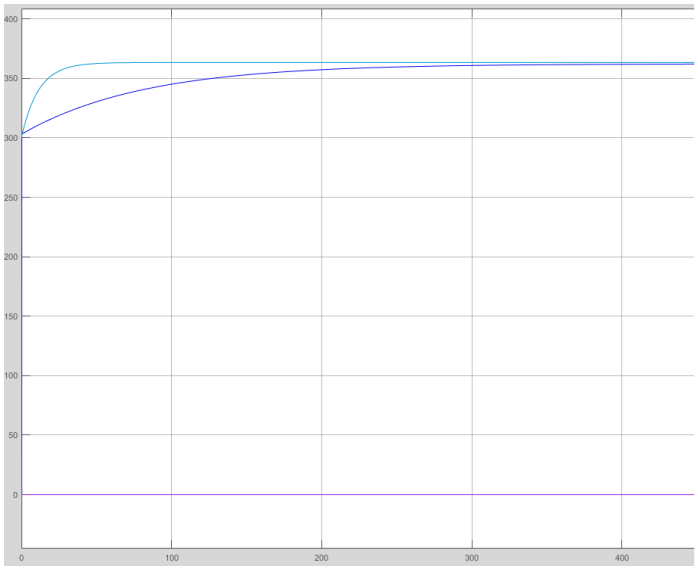

Рис. 4.11. Графіки передавальної функції та перехідної характеристики з LQR-регулятором

Як видно з графіків, керована система виходить швидше на задану температуру при тому що час перехідного процесу системи t_p = 143.564 секунди в порівнянні з перехідною характеристикою з LQR регулятором t_p = 18.7 секунд та з нульовим перерегулюванням. Такий час перехідного процесу означає, що створений LQR-регулятор заощаджує час на переведення системи до заданої температури, тобто заощаджує витрати на нагрівання гранул.

4.2.3. Порівняння систем керування з LQR- регулятором та з PID-регулятором

Створимо модель з PID- регулятором в Simulink (рис 4.12).

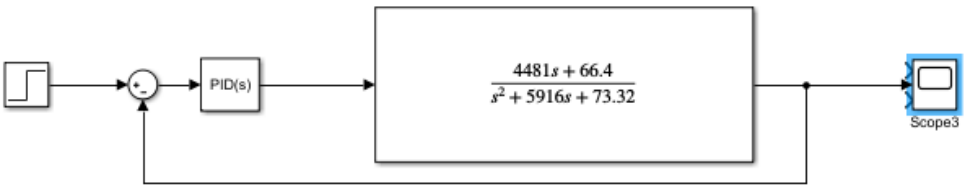

Рис. 4.12. Схема з PID-регулятором у Simulink

Після налагодження параметрів у блоці Control System Design MATLAB (рис. 4.13) отримуємо перехідний процес, який виводить температуру гранул на заданий рівень в 364К. Отримаємо перехідну характеристику системи керування з PID-регулятором на рис 4.14.

Схема системи керування з PID-регулятором та LQR-регулятором в Simulink наведена на рис. 4.15.

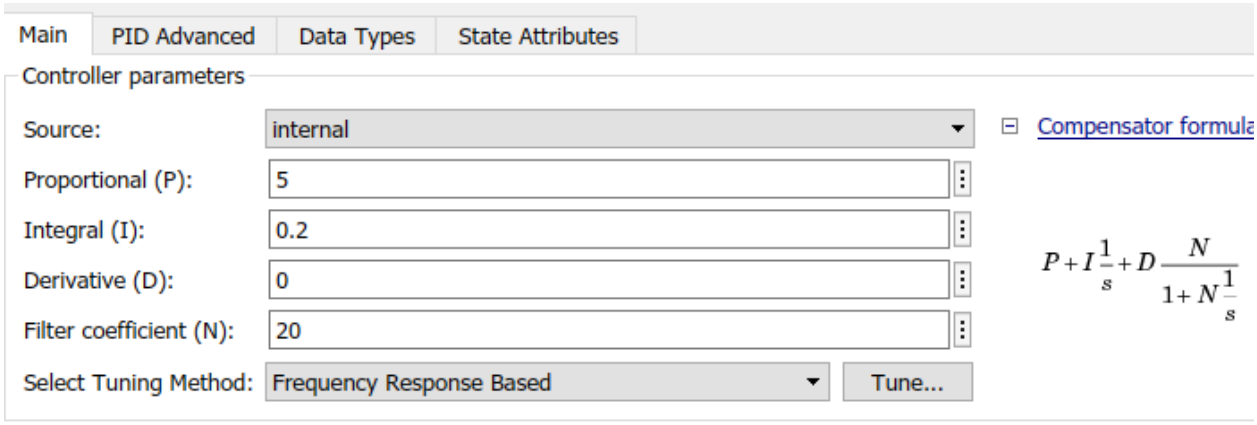

Рис. 4.13. Налаштування параметрів PID-регулятора

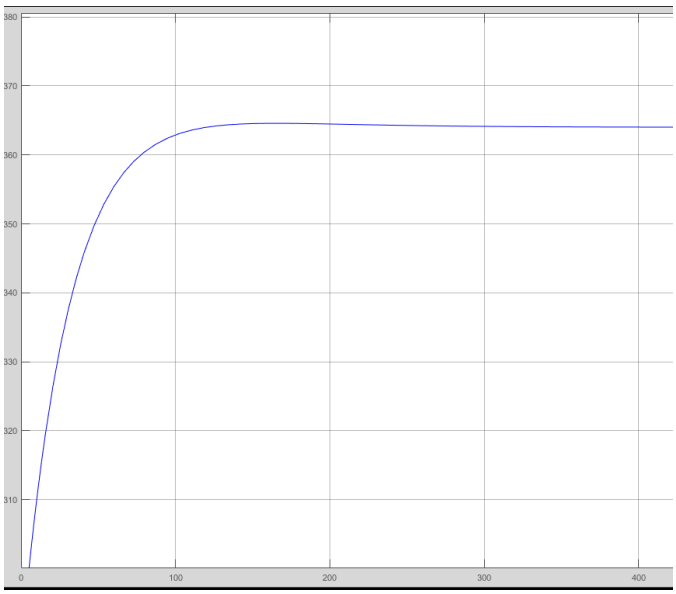

Рис. 4.14. Перехідна характеристику системи керування з PID регулятором

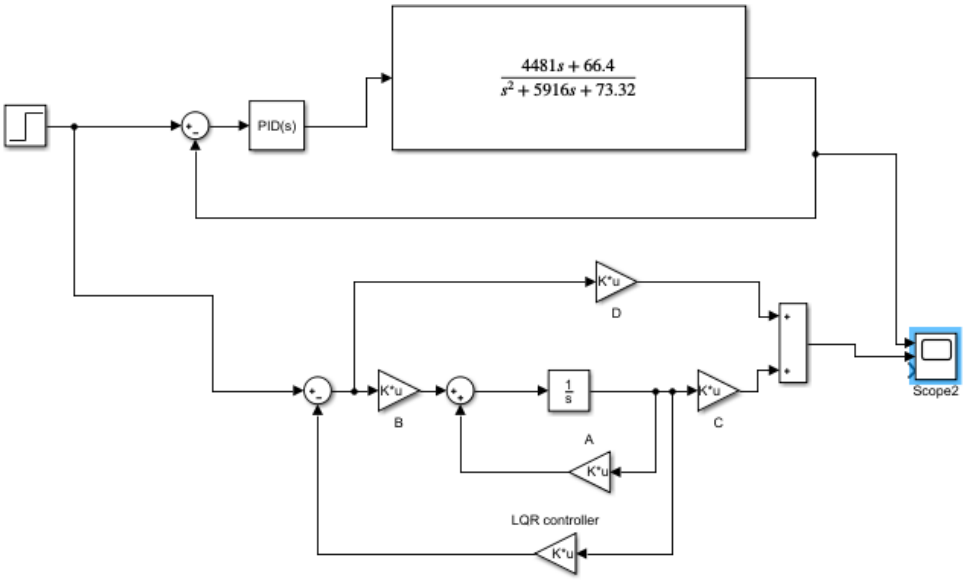

Рис. 4.15. Схема системи керування з PID-регулятором та LQR-регулятором

Накладемо графіки регулювання системи керування з PID-регулятором та LQR-регулятором (рис 4.16).

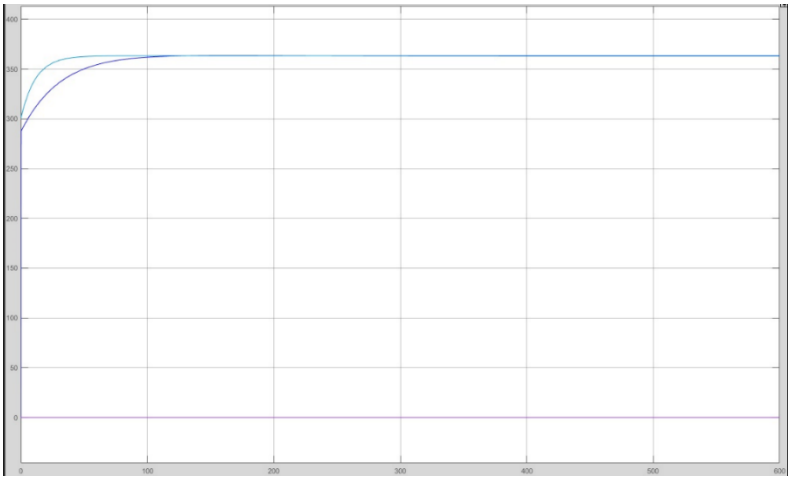

Рис. 4.16. Графіки регулювання системи керування з PID-регулятором та LQR-регулятором

Як видно з графіків, керована система з LQR-регулятором виходить швидше на задану температуру при тому що час перехідного процесу системи $t_p = 18.7$ секунди в порівнянні з керуванням з PID-регулятором $t_p = 57.5$ секунд та з нульовим перерегулюванням. Такий час перехідного процесу означає, що створений LQR-

регулятор заощаджує час на переведення системи до заданої температури, тобто заощаджує витрати на нагрівання гранул.

Грануляція з псевдозрідженим шаром - це складний процес взаємодії, на який впливає велика кількість факторів. Так як основним каналом керування є T1 → T2, то було розглянуто перехідну характеристику залежності температури теплоносія та температури гранул.

З використанням пакету MATLAB System Identification отримано передавальну функцію, а з неї здійснено перехід до векторно-матричної моделі. Результати перевірки в MATLAB показали ранги матриць рівні 2, це означає що дана система є спостережуваною та керованою водночас.

Виділені основні фактори, які впливають на процес та створено LQR- регулятор системи, який відповідає вимогам стабільності, динаміки та надійності. Отримано перехідний процес, який виводить температуру гранул на заданий рівень в 364К. Перехідний процес з LQR-регулятором триває t_p = 18.7 секунд, що є реальним значенням для регуляторів такого типу.

В порівнянні з PID регулятором t_p = 57.5 секунд, система управління з LQR-регулятором так само не має перерегулювання, але швидше виходить на задане значення

4.3. Інформаційна технологія захисту критичних ресурсів виробництва мінеральних добрив

Проблема алгоритмізації управління виробничими процесами, підкріплена потужним розвитком засобів обчислювальної техніки, обумовила велику кількість досліджень і плідних розробок в області теорії управління в цілому і оптимізації управління виробничими процесами, зокрема. До теперішнього часу розроблено значну кількість методів і алгоритмів управління складними технологічними об'єктами та установками. Здебільшого вони забезпечують прийнятні результати і дозволяють синтезувати ефективні системи управління. Однак у багатьох випадках, пов'язаних з автоматизацією складних технологічних процесів і виробництв, що

функціонують в умовах інтенсивних збурювань, неточності і невизначеності апріорної інформації, непередбачуваних змін характеристик сировини, нестаціонарності об'єктів управління, ці методи недостатньо ефективні. У зв'язку з цим виникає нагальна необхідність розробки нових конструктивних підходів і методів, які дозволяли б враховувати специфіку завдань управління складними технологічними об'єктами та комплексами і більш повно реалізовувати потенціал системи управління.

Аналіз з критичних позицій сучасного стану проблеми розробки інформаційно-керуючих систем для промислових підприємств з безперервним технологією і тенденцій їх подальшого вдосконалення і модернізації свідчить, що загальносвітові процеси глобалізації систем (в тому числі і технічних) і підвищення їх відкритості актуалізували в останні роки створення інтегрованих інтелектуальних інформаційно-керуючих систем на промислових підприємствах з безперервним характером виробництва, з'явилися локальні і корпоративні обчислювальні мережі і де проводиться модернізація технологічних і економічних систем. Ці процеси ініціювали запит на комплексну інформацію про різні аспекти виробничо-технологічної діяльності промислових підприємств - те інформацію, яка необхідна для обґрунтованого прийняття управлінських рішень. Еволюція систем індустріальної автоматизації показує, що розвиток відбувався від найбільш простих приладових систем до локальних систем автоматизації обмеженою пов'язаності, а потім - до великих інформаційних систем. Нарешті, спостерігається в даний час глобальна інтеграція АСУ. Аналіз еволюції систем автоматизації в промисловості дозволяє виділити наступні проблеми інформаційно-керуючих систем (ІКС): нестійкість ІКС вимагає підвищених витрат інженерної праці; наявність в системі так званої «брудної інформації» (чим більше прагнення до жорсткої впорядкованості в інформаційній системі, тим більше в ній ентропії «брудних даних» і більше структурна нестійкість системи); необхідність врахування всього спектру соціально-технологічних факторів. Аналіз основних напрямків інтеграції автоматизованих систем управління, які забезпечують доступність всієї інформації, необхідної для прийняття управлінських рішень та управління на всіх рівнях, координується з

позицій досягнення загальних цілей, що свідчить про основне завдання інтегрованих АСУ- узгодження рішень, прийнятих на різних рівнях управління і які оцінюються за кількома критеріями. Деякі з них несумісні та призводять до задачі упорядкування критеріїв шляхом їх ранжування, задання пріоритетів або вагових коефіцієнтів. При розробці планів і графіків в цілому розклад доцільно складати на більш тривалий час, ніж потрібно, але після закінчення певного інтервалу графік переглядається, що забезпечить стійкість виробничих графіків в умовах невизначеного майбутнього ходу процесу. Принцип багаторазової адаптації в інтегрованих АСУ передбачає неухильне поліпшення раніше прийнятих рішень за рахунок пристосування вихідної моделі до умов функціонування: накопичення інформації про поточний стан об’єкту для оцінки неузгодженості: підготовки рекомендацій про місце, час і форми керування, його можливі наслідки. Цьому принципу в повній мірі відповідає багаторівнева концепція адаптації управління виробництвом. Декомпозиція загальної задачі управління, передбачає послідовну деталізацію розв'язуваної задачі і координацію локальних задач, які, в свою чергу, можуть підлягати подальшій декомпозиції, яка завершується, коли кожна з локальних задач прийняття рішень може бути досягнута з застосуванням наявних засобів за прийнятний час. Декомпозиція та узгодження рішень в ІКС вимагає взаємозв'язку локальних рішень, їх подання з урахуванням цілей інтеграції. Саме синергізм (тобто спільна дія всіх умов), множинне узгоджене кооперативне управління промисловим виробництвом як єдиною системою дозволяє найбільш повно реалізувати можливості виробничого підприємства. Узгоджене множинне корпоративне ієрархічне управління забезпечує це при еквівалентних витратах у вигляді підвищення якості вихідного продукту, зменшення шкідливих відходів, можливості використання більш простих елементів, підвищення надійності всієї системи і, нарешті, підвищення гнучкості і пластичності системи, що робить доступним швидка зміни режимів виробництва, включення нових технологічних процесів, підключення нових споживачів без зупинки основного виробництва. Система автоматизації повинна послідовно в часі підвищувати свій клас (для кожного класу характерний свій рівень взаємодії з навколишнім середовищем, власний рівень складності і насиченості інтелектуальними ресурсами). Цьому рівню взаємодії

відповідають характеристики всіх частин системи (технічного та математичного забезпечення, програмно-технічних комплексів тощо) [17].

Найбільш раціональною автоматизованою системою управління представляється нелінійна система, адекватна організаційній та інтелектуальній структурі виробництва і відноситься до класу відкритих систем, здатних до нелінійної еволюції). Нелінійна система також має загальну інформаційну шину, структуровану за організаційною ознакою. Звісно ж, що введення гнучкої структури зміни оперативно відстежує зовнішні структурні зміни, знижує вимоги до впорядкованості даних, що створює об'єктивні передумови до підвищення чистоти бази даних і стійкості синтезованих автоматизованих систем управління. Сучасний підхід до оптимізації управління технологічними процесами і виробництвами передбачає створення алгоритмічного забезпечення у взаємозв'язку з питаннями розвитку інформаційних технологій, що означає перехід до якісно нового об'єднання різнорідних технологій, що дозволяє здійснювати розробку алгоритмів з урахуванням можливості модифікації і розвитку систем зберігання і переробки інформації. Аналіз публікацій свідчить про перспективність підходу - інформаційних технологій до побудови високоефективних інтелектуальних інформаційно-керуючих систем для промислових підприємств з безперервною технологією. Виділимо два аспекти розгляду архітектури інформаційно-керуючих систем. Перший розглядає ІКС як систему взаємодії щодо рівноцінних модулів, які використовуються для автоматизації окремих функцій (управління фінансами, управління матеріалами, збутом тощо) або елементи структури підприємства (центр, філії). Другий –передбачає погляд на ІКС як на систему у вигляді набору рівнів управління (як правило, трьох-чотирьох). Відповідно до методології управління проєктами програма вдосконалення виробничої діяльності промислового підприємства може бути визначена як мега-проєкт, тобто сукупність проєктів, що відрізняються особливою складністю створюваної продукції і методів управління. При цьому основними способами, що використовуються при розробці програми вдосконалення, є метод техніко-економічного проєктування і нормативно-балансовий метод. Такий підхід перетворює мистецтво проєктування і управління виробництвом в строгу інженерну

дисципліну, оскільки являє собою сукупність методів і засобів, орієнтованих на поліпшення основних показників діяльності об'єкта шляхом моделювання, аналізу і перепроєктування існуючих бізнес-процесів. Фази створення і функціонування системи управління проєктом (СУП) ІКС також розглядаються як своєрідний проєкт, для якого застосовні методи управління проєктами. Результатом побудови системи управління проєктом є концепція розвитку, створення і функціонування системи управління промисловими виробництвами. Модель управління проєктом ІКС є стандартний набір компонентів і функцій стосовно аналізованої предметної галузі. Відповідно до моделей СУП ІКС та управління проєктами для вироблення управлінських рішень і визначення складу робіт по реалізації бізнес-процесів управління проєктом ІКС прийнята багаторівнева система класифікації бізнес-процесів, що реалізуються в рамках виробничої діяльності підприємства. Схема класифікації є згорнуте дерево множини бізнес-процесів, які теоретично мають місце в предметній галузі. Кожен бізнес-процес визначається компонентами векторів за логікою проходження рівнів класифікації «знизу-вгору». Модель формування бізнес-процесів розробляється на підставі аналізу функціональної діяльності об'єкта і є методологічним інструментарієм для генерації і проєктування цілісної інтегрованої системи управління. Такий підхід дозволяє здійснювати перевірку на повноту і достатність множини бізнес-процесів в системі і встановити логіку і взаємозв'язки між ними. Потім виділяються рівні завдань управління і описуються бізнес-процеси на всіх щаблях ієрархії, визначаються типи зв'язків між комплексами бізнес-процесів на рівнях промислового підприємства. При цьому технологічний тип зв'язків відображає основний технологічний процес виробництва; управлінський же тип зв'язків здійснює регулюючий вплив на об'єкт; нарешті, допоміжні зв'язки призначені для підтримки основного виробничого процесу. Виділені зв'язку класифікуються за типом процесу управління. На рівні технологічного комплексу або установки виділяються два типи зв'язків - між комплексами (установками) і елементами комплексу. Принципи, на яких повинні будуватися сучасні ІКС, полягають у: комп'ютерно-орієнтованій автоматизації всіх етапів життєвого циклу системи; інтеграції всіх систем автоматизації виробничої діяльності всередині одного

підприємства; інтелектуалізації; спеціалізації інтегрованої системи автоматизації кожного підприємства; базування на досягненнях сучасних інформаційних технологій інжинірингу. ІКС є системою, що безперервно розвивається. Однак вести пошук найкращих напрямків розвитку на діючому підприємстві не є можливим. Тому одночасно з розробкою ІКС створюється імітаційна модель функціонування підприємства спільно з інтегрованою системою управління. Вона служить інструментальним засобом для отримання кращих рішень при створенні і експлуатації ІКС та здійснює пошук її найвигіднішого розвитку [17].

Пропонована технологія автоматизації передбачає уніфікацію уявлення, обміну і структурування даних і знань про об'єкти і процеси. Важливим завданням є розробка нормативної, методичної бази уніфікації даних і знань та засобів їх програмної підтримки, наприклад, на основі - інформаційних технологій для підтримки життєвого циклу продуктів і виробів. Підрозділи виробничих підприємств з безперервною технологією зобов'язані кооперуватися і ефективно координувати свою виробничо-технологічну діяльність. Для цього доцільно глобально пов'язувати стан кожної установки зі станом будь-якої іншої, особливо з огляду на вимоги реального часу, що властиві діяльності безперервних виробництв.

Пропонуються комплексні рішення в області засобів автоматизованого управління технологічними процесами, але незалежно від розробника, всі сучасні АСУ ТП будуються на єдиних загальноприйнятих принципах.

В АСУ ТП можна виділити три рівні. Нижній рівень – це рівень апаратних давачів – давачі, пристрої вимірювання технологічних параметрів, приводи та виконавчі пристрої, встановлені на технологічному обладнанні і призначені для збору первинної інформації і реалізації виконавчих впливів. Якщо деякі або всі пристрої нижнього рівня є інтелектуальними, обмін інформації між ними може здійснюватися безпосередньо за допомогою мережі передачі даних [85].

Середній рівень – це рівень програмованих логічних контролерів (ПЛК) і пристроїв з’єднання об’єктів. Їх головною функцією є безпосереднє автоматизоване управління технологічними процесами. Управління виконавчими механізмами

здійснюється за допомогою спеціальних алгоритмів шляхом обробки даних про стан технологічних параметрів, отриманих від вимірювальних пристроїв.

Верхній рівень реалізується за допомогою персональних комп'ютерів (ПК), які виконують роль автоматизованих робочих місць (АРМ), де з допомогою спеціальних програмних пакетів (SCADA систем) реалізується інтерфейс з оператором-технологом, які виконує моніторинг і безпесереднє керування технологічним процесом.

На рис. 4. 17. наведена типова структурна схема трьохрівневої АУС ТП.

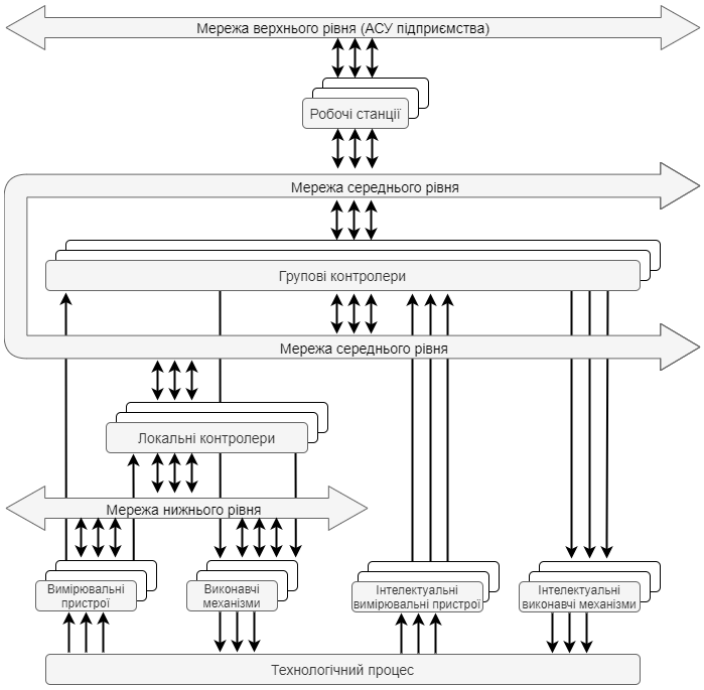

Рис. 4.17. Типова структурна схема трьохрівневої АСУ ТП

Для функціонування АСУ ТП потрібна взаємодія наступних компонентів [85]:

- технічне забезпечення;
- програмне забезпечення;
- інформаційне забезпечення;
- організаційне забезпечення;
- операційний персонал.

Технічним забезпеченням АСУ ТП називають повну сукупність технічних засобів, достатніх для функціонування АСУ ТП і реалізації системою всіх її функцій.

Програмне забезпечення АСУ ТП – це сукупність програм, які необхідні для реалізації функцій АСУ ТП, заданого функціонування комплексу технічних засобів АСУ ТП та прогнозованого розвитку системи.

Інформаційне забезпечення АСУ ТП складається з:

- інформації про стан технологічного процесу;
- системи класифікації і кодування технологічної і техніко-економічної інформації;
- масивів даних і документів.

Організаційне забезпечення АСУ ТП – це сукупність описів функціональної, технічної і організаційної структур та інструкцій для операційного персоналу АСУ ТП, яка забезпечує задане функціонування операційного персоналу.

До операційного персоналу відносяться технологи-оператори і експлуатаційний персонал, які забезпечують правильне функціонування комплексу технічних засобів.

Одним з головних технічних компонентів АСУ ТП є SCADA-система і програмовані логічні контролери.

Мережі передачі даних, які входять у склад АСУ ТП, можна умовно розділити на два класи: мережі нижнього рівня (польові шини) та мережі верхнього рівня (Рис. 4.17).

Промислові мережі передачі даних – базовий елемент для побудови АСУ ТП. Саме поява промислових комунікаційних протоколів стало одним з чинників початку використання територіально розподілених систем управління, які здатні охопити безліч технологічних установок і процесів.

Головною функцією польової шини є забезпечення мережевої взаємодії між контролерами і віддаленої периферією. Також до польової шини можуть підключатись інтелектуальні пристрої, якщо вони підтримують високорівневі протоколи мережевого обміну.

Найчастіше використовують такі протоколи мереж зв’язку для нижнього рівня:

- Modbus RTU;

– Modbus ASCII;
– Profibus DP;
– Profibus PA.

Незважаючи на наявність особливостей кожного з стандартів (швидкість передачі, формат кадру, фізичне середовище), у всіх них є спільна особливість – алгоритм мережевого обміну даними, заснований на класичному принципі Master-Slave (головний-підпорядкований) (Profibus PA – один підпорядкований). Як лінія зв'язку використовується екранована вита пара, довжина кадру – 246 байт, а максимальна кількість контрольованих вузлів не перебільшує 127 (Profibus PA - 32). Практично всі існуючі протоколи мають апаратну реалізацію перших двох рівнів моделі OSI (фізичний і канальний рівні). У мережах ІКС ТП нижнього рівня у всіх стандартах зв'язку реалізований захист даних CRC-кодом.

Мережі верхнього рівня використовуються для передачі даних між контролерами, серверами та робочими станціями. Основний стандарт мереж верхнього рівня – Ethernet (IEEE 802.3). Причина широкого використання цього стандарту зрозуміла: за допомогою Ethernet легко об'єднують обладнання верхнього рівня АРМ і сервери, які у більшості випадків є персональними комп'ютерами.

4.3.1. Система захисту критичних ресурсів виробництва мінеральних добрив

Проблеми захисту інформації в системах управління реального часу, в тому числі АСУ ТП, довгий час перебували поза зоною уваги фахівців з інформаційної безпеки. Певним поштовхом, послужили широко обговорювані в пресі вірусні атака Stucksnet. По суті, було поставлено масштабний натурний експеримент, який показав, до яких катастрофічних наслідків може призвести відступ від правил експлуатації захищеної автоматизованої системи, а також невисока ефективність поширених систем захисту, побудованих на ідеології захисту периметра.

Проведені за результатами цього і інших менш значущих подій дослідження [86] показали вкрай низький рівень інформаційної безпеки АСУ ТП. Так, з 2015 року в 20 разів зросла кількість виявлених вразливостей програмного забезпечення, що використовується зловмисниками. При цьому половина вразливостей дає можливість

зловмиснику запускати довільний виконуваний код (для 35% вразливостей є експлойти, що дозволяє зламати захист навіть малокваліфікованому порушнику). Більш ніж 90% вразливостей мають середній або високий рівень небезпеки, а в 9% випадків їх використання не викликає труднощів. У третини перевірених систем недоліки в системі безпеки пов'язані з помилками конфігурації, використанням стандартних технологічних паролів тощо.

Стурбованість експертного співтовариства викликає активне впровадження інформаційних технологій для управління технологічними та іншими процесами реального часу, в тому числі на критично важливих об'єктах інформаційної інфраструктури, що не підкріплюється адекватними заходами захисту. При цьому для інформаційно-аналітичних систем, що обробляють інформацію обмеженого доступу, питання захисту в достатній мірі опрацьовані, а реалізація встановлених вимог залежить в більшій мірі від правової культури і фінансового стану власника системи.

Необхідно забезпечити безпеку АСУ критично важливих об'єктів, її основні принципи та напрямки, а також основні механізми і етапи її реалізації. Разом з тим розробка засобів і систем захисту інформації в АСУ ТП потребують підготовки цілогоряду нормативних і методичних документів. Однією з першочергових завдань у цьому напрямку є встановлення відповідності між категоріями критично важливих об'єктів і існуючими класами систем захисту інформації або введення нової класифікації систем захисту для таких об'єктів. Другий підхід є кращим, оскільки існуюча класифікація систем захисту прив'язана до ступеня конфіденційності інформації, але в АСУ ТП критично важливих об'єктів навіть високої категорії небезпеки необов'язково містить інформацію обмеженого доступу. Рівень захисту такого об'єкта, очевидно, повинен бути досить високим. Система захисту інформації АСУ ТП та інших систем реального часу має специфічні особливості, головна з яких полягає в тому, що на перший план виходить забезпечення функціональної безпеки і таких традиційних характеристик безпеки, як цілісність і доступність ресурсів системи. Під функціональною безпекою тут мається на увазі стан АСУ ТП, при якому ризик настання небажаних (потенційно небезпечних) подій в системі знижений до прийнятного рівня. Чинні нормативні та методичні документи щодо захисту

інформації орієнтовані в основному на забезпечення конфіденційності інформації, а такі характеристики безпеки, як цілісність і доступність, відіграють допоміжну роль. Однак в АСУ ТП порушення доступності окремих ресурсів або цілісності критично важливих параметрів технологічного процесу часто може призвести до катастрофічних наслідків. Функціональна безпека в літературі нерідко ототожнюється з надійністю функціонування системи в умовах як випадкових збоїв і несправностей, так і навмисних дій потенційного порушника. Але в разі помилок реалізації алгоритму технологічних процесів або в його описі навіть надійна робота програмно-технічних засобів системи не рятує від негативних наслідків. Таким чином, важливими елементами в забезпеченні інформаційної безпеки АСУ ТП є аналіз алгоритму функціонування АСУ і верифікація його програмного забезпечення. Рішення першого із зазначених завдань неможливе без активної участі профільних міністерств і відомств, а також власника критично важливого об'єкта. З метою здешевлення і прискорення проведення відповідних робіт з безпеки інформації необхідна розробка галузевих стандартів і типових рішень АСУ ТП. Проблема верифікації сучасного програмного забезпечення з урахуванням високої трудомісткості цієї роботи вимагає наукового підходу і розробки відповідних методичних рекомендацій.

Проблема забезпечення безпеки інформації в АСУ ТП носить міжвідомчий, комплексний характер, вимагає розробки цілого ряду документів правового, нормативного та методичного характеру, а також типових програмно-технічних рішень.

Розробка інформаційної технології пов'язана з широким використанням телекомунікацій в автоматизованих системах управління технологічними процесами (АСУ ТП) і високим рівнем небезпеки спотворення або втрати інформації.

Готовність організацій і підприємств, що розробляють і експлуатують АСУ ТП, виконувати аналіз їх надійності та безпеки є обов'язковою умовою державної та міжнародної сертифікації. Однак більшість систем управління технологічними процесами малої і середньої складності найчастіше проєктуються малими організаціями в умовах жорстких фінансових і кадрових обмежень. І в силу цього

питаннями інформаційної безпеки (ІБ) не займаються взагалі. Якщо в атомній промисловості і енергетики наслідки порушення безпеки, в тому числі інформаційної, можуть бути масштабними і катастрофічними, то масштаб збитку в АСУ ТП хімічної промисловості далеко не завжди так очевидний і великий. Розмір збитку і його характер визначається, перш за все, самим технологічним процесом. При системному підході необхідно розглядати систему управління у взаємозв'язку і взаємовпливом не тільки з об'єктом управління (в даному випадку - технологічним процесом), але і з джерелами енергії, і з навколишнім середовищем. У хімічній промисловості вплив на навколишнє середовище необхідно завжди піддавати ретельному аналізу не тільки в аварійному, а й в нормальному режимі роботи АСУ ТП. Порушення екології може бути викликано не тільки витоками і технологічними викидами шкідливих речовин, але і, наприклад, зміною температури води у водоймі при скиданні в нього технологічної води, забраної з артезіанської свердловини для охолодження процесу.

Забезпечити ІБ АСУ ТП на досить високому рівні, при постійно зростаючому рівні інформатизації та постійному збільшенні кількості загроз, вже неможливо тільки комплексом зовнішніх заходів захисту. Пропонується такий підхід до забезпечення ІБ АСУ ТП, коли зовнішню захисну оболонку створюватиме комплексна система ІБ, а внутрішні бар'єри утворюють вбудовані механізми захисту програмних і технічних компонентів АСУ ТП. Такий підхід можна назвати системним. Обійти зовнішній захист можна, внутрішній - набагато складніше. Тому звертаємо особливу увагу на переваги розробки і застосування програмних і апаратурних засобів АСУ ТП, що мають вбудовані механізми захисту, якими користувач може управляти для створення необхідної пропорції механізмів захисту в системі захисту інформації (СЗІ).

Засоби телекомунікацій в АСУ ТП - це різноманіття апаратури і програмного забезпечення, які повинні мати внутрішні механізми власної безпеки. Тому від виробників технічних засобів і програмного забезпечення АСУ ТП потрібна розробка інструментів забезпечення безпеки своїх продуктів.

Розглянуто особливості захисту інформації в АСУ ТП в хімічній промисловості, визначені вимоги до пристроїв і телекомунікацій на всіх рівнях ієрархічної структури

АСУ ТП. АСУ ТП відрізняється від інших систем управління перш за все тим, що здійснює вплив на об'єкт в тому ж темпі, що і протікають в ньому технологічні процеси, а технічні засоби АСУ ТП беруть участь у виробленні рішень з управління. Перша особливість вимагає застосування в АСУ ТП телекомунікацій з гарантованим часом доставки, друга - інтелектуалізації всіх компонентів. В ієрархічній багаторівневій архітектурі сучасної АСУ ТП нижній рівень характеризується великою кількістю (сотні) і різноманітністю технічних засобів, які розрізняються також інформаційним, математичним і програмним забезпеченням.

Підприємства хімічної галузі різномасштабні (малі, середні та великі) і мають, крім загальної специфіки, вибухонебезпечність, пожежонебезпечність, агресивністю робочого середовища, вплив на екологію і життєдіяльність суспільства навіть в штатному режимі роботи. Рекомендовано, поряд з комплексом зовнішніх заходів захисту, застосовувати в АСУ ТП апаратурні компоненти і програмні продукти, що мають вбудовані механізми захисту інформації. Особливу увагу вирішено приділити ефективної, з точки зору швидкості виявлення вторгнення, і надійної діагностики програмно-апаратурних засобів і телекомунікацій.

Внаслідок тривалості експлуатації АСУ ТП (розробка та експлуатація можуть становити більше десяти років) і істотної зміни складу і якості сучасних загроз необхідно проєктувати і реалізовувати інформаційну безпеку систем з урахуванням тенденцій розвитку кіберзагроз. З іншого боку, необхідно проводити регулярну роботу по нейтралізації потенційних загроз на працюючих системах.

Сукупність заходів безпеки можна розділити на дві групи: адміністративно-організаційні та програмно-технічні.

Перша група заходів пов'язана з формуванням програми робіт щодо забезпечення ІБ АСУ ТП і розробкою набору документів, які регламентують високорівневий підхід щодо забезпечення ІБ, а також описують політику розвитку системи ІБ АСУ ТП. Крім того, формується пакет організаційної документації, спрямованої на створення та підтримання режиму ІБ АСУ ТП.

Програмно-технічні заходи утворюють основний набір засобів забезпечення ІБ АСУ ТП. На цьому рівні реалізуються наступні сервіси ІБ: управління доступом,

забезпечення цілісності, забезпечення безпечної міжмережевої взаємодії, антивірусний захист, аналіз захищеності, виявлення вторгнень, управління системою ІБ (безперервний моніторинг стану, виявлення інцидентів, реагування). Конкретні вимоги до перерахованих сервісів пред'являються на підставі аналізу оброблюваної інформації і оцінки загроз безпеки АСУ ТП.

Кожна група заходів в залежності від необхідності і можливостей підприємства може здійснюватися на одному з трьох рівнів. Базовий рівень включає механізми, традиційні для більшості інформаційних систем. Середній рівень передбачає виконання початкових тактичних заходів, що забезпечують реалізацію керованих захисних функцій по забезпеченню ІБ. На розширеному (високому) рівні реалізуються заходи, що підтримують і розширюють базовий і середній рівень, але для їх реалізації може знадобитися додаткова експертиза.

Так, для першої групи заходів на базовому рівні передбачається розробка документів, що описують політику кібербезпеки, впровадження політик і процедур з державних стандартів з безпеки критично важливих об'єктів. На середньому рівні ведуться роботи по впровадженню кращих індустріальних практик, здійснюється контроль виконання політик і процедур. На розширеному рівні впроваджується процес безперервного поліпшення політик і процедур ІБ, періодично проводиться навчання і аудит. Для ілюстрації різних рівнів другої групи заходів розглянемо сервіс забезпечення безпечної міжмережевої взаємодії.

На базовому рівні потрібно впровадження електронного периметра і відключення всіх необов'язкових для основного процесу з'єднань. Складається і підтримується в актуальному стані список критичних об'єктів. На середньому рівні електронний периметр розділяється на зони: локальна мережа АСУ ТП, демілітаризована зона і зона корпоративної мережі. Аналізується і мінімізується кількість ресурсів, доступних одночасно з мережі АСУ ТП і мережі корпоративної ЛВС. Постачальники обладнання та інтегратори періодично проводять навчання співробітників. Так, схема зонування в архітектурі Cisco SAFE for PCN (Process Control Network) розділена на 6 рівнів [87].

Зона локальної мережі АСУ ТП (рівень 0 - рівень 3) відокремлює критичні системи АСУ ТП і складається з декількох функціональних мінізон. Нульовий рівень - давачі збору даних і виконавчі механізми. Перший рівень - вузли комутації, що забезпечують підключення давачів до ПК. Другий-третій рівень - ПК, робочі місця операторів, сервери зберігання даних. Можуть використовуватися міжмережні екрани і IDS.

Демілітаризована зона забезпечує зв'язність корпоративної мережі і локальної мережі АСУ ТП. Вона містить тільки некритичні системи, яким необхідний доступ до корпоративної мережі і локальної мережі АСУ ТП, складається з декількох функціональних мінізон і відділена міжмережними екранами і IPS. Зона корпоративної мережі містить типові бізнес-додатки: пошта, АСУП (четвертий рівень), Інтернет (п'ятий рівень).

На розширеному рівні здійснюється впровадження VLAN, PVLAN, NIPS / HIPS, засобів виявлення аномалій і вторгнень, інтелектуальних комутаторів тощо.

В області захисту систем управління (ControlSystems, SCADA) в даний момент існує цілий ряд стандартів і рекомендацій [86]. Їх можна класифікувати наступним чином:

1) галузеві рішення:

- стандарти NERC для систем управління електричними мережами,

- стандарти ChemITC для хімічної індустрії,

- Cisco SAFE for PCN .

2) рекомендації загального рівня (стандарти NIST, ISA і ін.):

- ISA S99 - Комітет суспільства приладобудування, системотехніки і автоматизації (ISA),

- NIST PCSRF Security Capabilities Profile for Industrial Control Systems,

- IEC 61784-4.

При цьому будь-яких обов'язкових вимог до відповідності певним критеріям безпеки для комерційних компаній не пред'являється.

Відповідно до запропонованих підходів реалізована система захисту критичних ресурсів виробництва мінеральних добрив (рис. 4.18).

Для побудови системи захисту критичних ресурсів виробництва мінеральних добрив обрано модель зонування, яка забезпечує розбиття системи на кластери, в залежності від вимог до забезпечення безпеки і функціонального призначення компонентів системи.

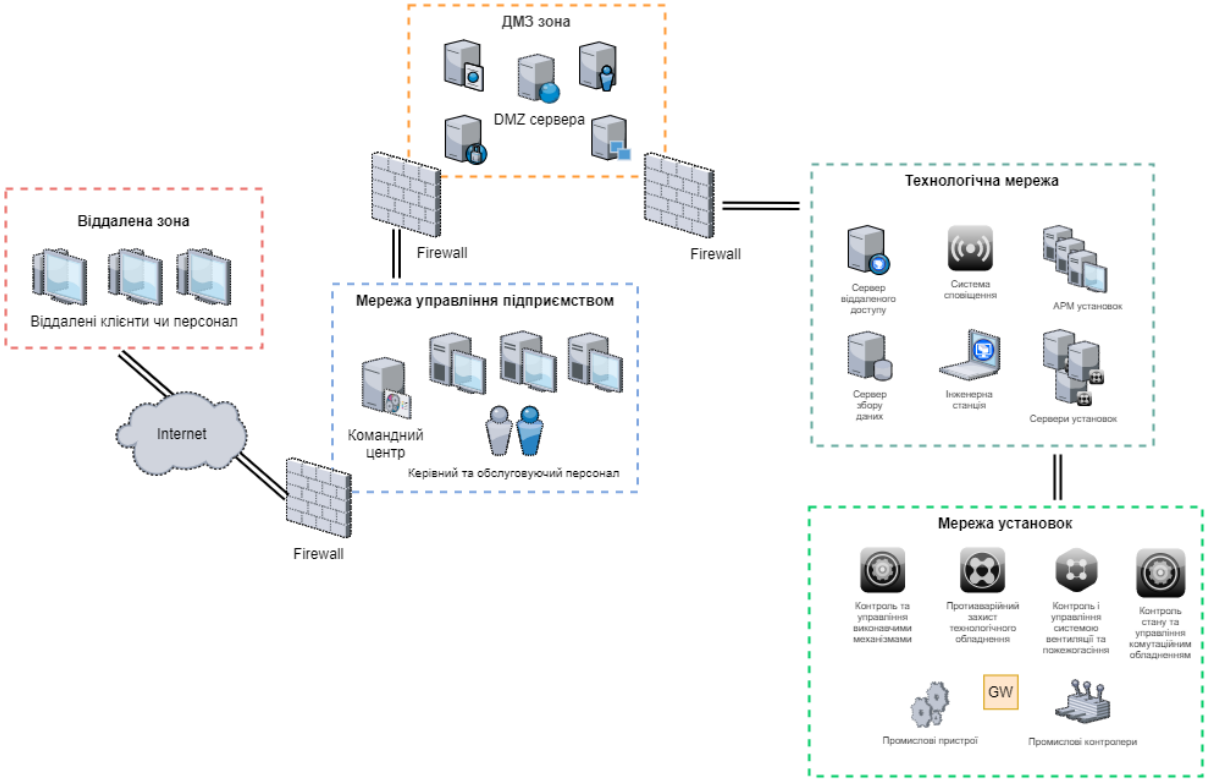

Рис. 4.18. Система захисту критичних ресурсів виробництва мінеральних добрив

Ця модель включає в себе наступні зони: зону виконання операцій, зону контролю та керування технологічним процесом, зону управління підприємством, демілітаризовану та віддалену зони.

Зона виконання операцій - являє собою мережу установок, яка об’єднує промислові пристрої та локальні контролери і відповідає за безпосередній зв'язок з технологічним обладнанням та забезпечує технології екплуатації промислового процесу. Для трансляції протоколів між різними технологіями промислових мереж та для забезпечення необхідної продуктивності кожного окремого набору пристроїв та контролерів доцільно використати додаткові шлюзи зв’язку (GW).

Для сприймання фізичних процесів та маніпулювання ними використовуються ряд пристроїв, таких як, давачі технологічних процесів, аналізатори, виконавчі механізми та відповідні прилади. Інтелектуальні польові пристрої можуть зберігати інформацію, яка має значення і для процесу, і для самого пристрою і надсилати повідомлення до блоків управління вищого рівня. Потужні пристрої можуть додатково виконувати діагностичні процедури, завдяки чому оператори установки можуть створювати чіткі повідомлення про технічне обслуговування.

Такі пристрої дозволяють зчитати необхідні данні наприклад, для подальшого контролю та управління виконавчими механізмами, для протиаварійнийного захисту технологічного обладнення, для контролю і управління системою вентиляції та пожежогасіння, для контролю за станом комутаційного обладнання, тощо.

Зона контролю та керування технологічним процесом – являє собою технологічну мережу, яка відповідає за контроль систем з польового рівня і безпосереднє управління технологічним процесом. Зона охоплює системи управління та забезпечує наглядовий контроль та моніторинг за усіма контролерами. Система контролю включає програмне забезпечення для нагляду та збору даних (SCADA), пристрої інтерфейсу людина-машина (HMI), робочі станції диспетчерської на базі автоматизованих робочих місць (АРМ), системи сигналізації/оповіщення та сервери установок, які можуть безпосередньо взаємодіяти із системами з мережі установок.

Система управління технологічним процесом включає пристрої, які управляють роботою контрольної станції та включають додатки, послуги та системи, такі як забезпечення надійності, планування та звітність виробництва, інженерні робочі станції, служби віддаленого доступу та сервери збору даних.

Система управління технологічним процесом взаємодіє із системами з зони управління підприємством через "демілітаризовану зону", підмережу, розміщену між промисловою мережею та мережею підприємства, щоб додати додатковий рівень безпеки довіреній мережі.

Зона управління підприємством – являє собою мережу на рівні підприємства, яка відповідає за роботу командного центру керівного та обслуговуючого персоналу (керівники змін, технологи, метрологи, керівники цехів). Ця зона охоплює усі бізнес-

процеси та логістичні системи, і це частина інформаційних технологій (IT), що складається із загального планування ресурсів підприємства. Вона включає звітність, планування, управління запасами, планування потужності, управління експлуатацією та технічним обслуговуванням, електронну пошту та телефонні послуги.

Демілітаризована зона – сегмент мережі, який обмежує пряму взаємодію між корпоративною мережею підприємства та технологічною мережею. По суті, ДМЗ - це Інтранет, захований від мережі підприємства за допомогою міжмережного екрану, що обмежує доступ до активів мережі підприємства та послуг з Інтернету. Міжмережний екран має бути налагоджений так, щоб будь-який доступ до технологічної мережі проходив через ДМЗ. В якості додаткових заходів безпеки, ДМЗ повинна використовувати адреси підмережі, незалежні від адрес мережі підприємства, та технологічної мережі. Весь мережний трафік з будь-якого боку демілітаризованої зони в ній і закінчується. Немає ніякого перетину трафіку ДМЗ безпосередньо. Сервери цієї ДМЗ забезпечують клієнтські пристрої мережі підприємства даними і подіями з технологічної мережі, які вони отримують шляхом незалежних і ізольованих комунікацій з останньою. Також необхідно реалізувати проксі-сервери для сервісів технологічної мережі, взаємодіючих з ресурсами корпоративної мережі.

В ДМЗ доцільно винести сервер антивірусного захисту і сервер оновлень із забороною підключення до них з корпоративного сегмента. Захищений файловий сервер забезпечує роботу служб безпечної передачі файлів для оновлення безпеки або файлів інсталяції програмного забезпечення для встановлення на об’єкти в промисловій зоні. Також в ДМЗ встановлені сервери, додатки або служби для безпечної реплікації або дзеркального відображення даних з промислової мережі до зони підприємства.

Крім того, в ДМЗ може бути додатково встановлена IDS система виявлення вторгнень, яка забезпечує додатковий рівень безпеки, щоб зупинити загрози або напади, які можуть виходити від віддалених систем. Розгортання Remote desktop gateway в ДМЗ забезпечить роботу служби віддаленого доступу до авторизованих ресурсів у промисловій зоні.

Віддалена зона – представляє собою сегмент віддалених зон промислової автоматизації. Для побудови захищеного підключення використовуються корпоративні рішення віддаленого доступу до мережі підприємства у вигляді технології VPN шифрування IPSec для підключення прикордонної зони та забезпечення конфіденційності в Інтернеті. Створення VPN вимагає аутентифікації RADIUS для віддаленого користувача і зазвичай реалізується і управляється IT-організацією провайдера. Обмежується доступ віддалених партнерів, що приєднуються через IPSec до ДМЗ/міжмережних екранів, використовуючи ACL. Підключення до ДМЗ через безпечний браузер тільки за протоколом HTTPS.

Після того, як безпечне підключення браузера до ДМЗ було здійснено, міжмережний екран може дозволити користувачеві отримати доступ до сервера віддаленого доступу через термінальну сесію. Міжмережний екран пропонує користувачеві провести аутентифікацію за допомогою сервера RADIUS, перш ніж дати дозвіл на підключення до сервера віддаленого доступу. Міжмережний екран повинен постачається з Java плагіном, який підтримує технологію термінальній сесії «віддалений сеанс робочого столу» в рамках SSL VPN. Віддалений інженер або користувач, за допомогою термінальної сесії, виконує обраний набір додатків промислового управління обладнанням, що знаходяться на сервері віддаленого доступу, що дозволяє значно знизити потенціал для вірусів або атак через віддалений сеанс.

Модель розгортання системи захисту критичних ресурсів виробництва мінеральних добрив повинна встановлювати надійну взаємодію усіх її компонентів, забезпечуючи як захист на фізичному рівні, так і захист усіх логічних зон для авторизованих бізнес комунікацій, та своєчасно реагувати на зміни і події у системах промислової автоматизації.

Таким чином, узагальнена схема інформаційної технології захисту критичних ресурсів (ІТЗКР) виробництва мінеральних добрив наведена на рис. 4.19. Основними компонентами ІТЗКР виробництва мінеральних добрив є наступні технічні, програмні та організаційно-методичні засоби: моделювання системи захисту критичних ресурсів виробництва мінеральних добрив, оптимізація системи захисту

критичних ресурсів виробництва мінеральних добрив, система захисту критичних ресурсів виробництва мінеральних добрив, математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі та оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором. Застосування ІТЗКР виробництва мінеральних добрив дозволяє у повній мірі здійснювати вимірювання основних параметрів технологічного процесу, оперативно керувати процесом, забезпечуючи одержання готового продукту заданої якості та захист інформації, що передається та оброблюється в системі керування.

Так, у модулі «Введення значень вхідних параметрів» відбувається введення значень вхідних параметрів для їх подальшого використання у модулі «Математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив» та компоненті «Математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі»: для математичної моделі протидії загрозам вводяться початкові значення імовірностей $p_i(0)$ та для математичної моделі теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі вводяться початкові значення температури теплоносія, гранул та вологовмісту гранул T_r^0, T_{gr}^0, W_g^0, коефіцієнт тепловіддачі α, коефіцієнт масовіддачі β, коефіцієнт горизонтальної температуропровідності a, поруватість потоку гранул ε, витрати вихідного розчинуG_p.

У модулі «Імітаційна модель системи захисту критичних ресурсів виробництва мінеральних добрив» одержуємо значення інтенсивностей переходу λ_{ij} , які потім надходять до модулю «Математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив» та «Метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив». У модулі «Математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив» обчислюються значення імовірностей p_i , що надходять до модулів «Метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив» та «Метод тестування системи захисту критичних

ресурсів виробництва мінеральних добрив на імітаційній моделі». У модулі «Метод тестування системи захисту критичних ресурсів виробництва мінеральних добрив на імітаційній моделі» обчислюється значення оцінки ризику *iRisk*, що використовується для оцінки ефективності у компоненті «Система захисту критичних ресурсів виробництва мінеральних добрив».

У компоненті «Оптимізація системи захисту критичних ресурсів виробництва мінеральних добрив» спочатку здійснюється вибір критерію оптимальності у модулі «Факторно-цільовий аналіз з метою вибору критерію оптимальності», далі за допомогою модулю «Метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив» обчислюється коефіцієнт захищеності *D* і реалізовується модуль «Методика оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив». Інформація компоненту «Оптимізація системи захисту критичних ресурсів виробництва мінеральних добрив» надходить до компоненту «Система захисту критичних ресурсів виробництва мінеральних добрив».

У компоненті «Математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі» одержуємо значення температури теплоносія, гранул та вологовмісту гранул T_r, T_{gr}, W_g. Дані з компоненту «Математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі» надходять до компоненту «Оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором» та використовуються для оптимального керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі із обчисленням критерію якості *I*. Інформація з компоненту «Оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором» надходить до компоненту «Система захисту критичних ресурсів виробництва мінеральних добрив», з метою контролю параметрів технологічного процесу та їх перебуванню у робочому діапазоні. Використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив дозволило підвищити якість готового продукту на 15%.

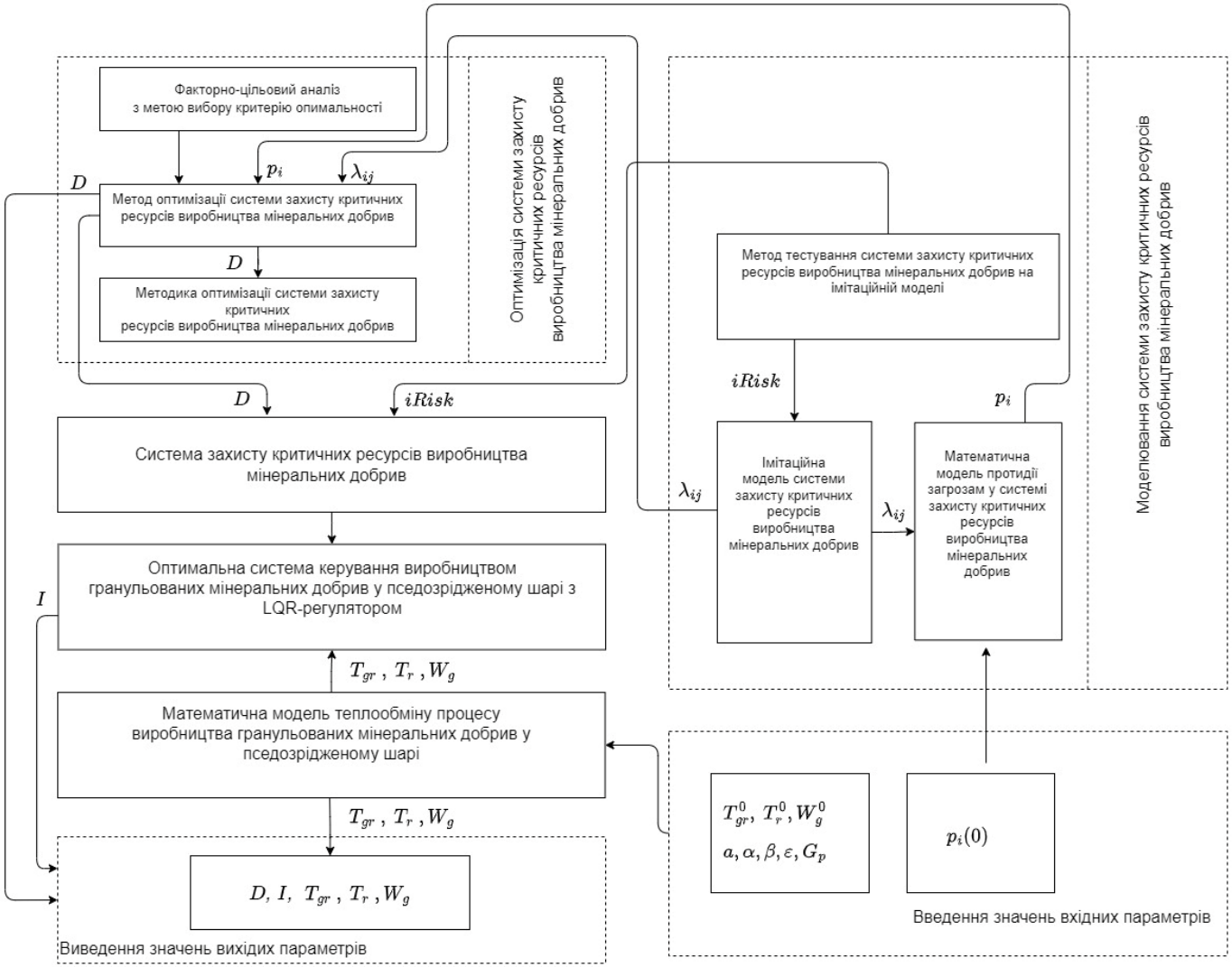

Рис. 4.19. Інформаційна технологія захисту критичних ресурсів виробництва мінеральних добрив

Розроблено методику використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив, що заснована на запропонованому поєднанні комплексу зовнішніх заходів захисту з вбудованими в апаратурні і програмні компоненти механізмами захисту інформації, що враховує особливості АСУ ТП і хімічної промисловості.

Методика передбачає таку послідовність дій:

1. Вивчення нормативно-правової та наукової бази в області захисту критичних ресурсів промислових систем підвищеної небезпеки.

2. Визначення інформації, що підлягає захисту в робочих станціях, контролерах, телекомунікаційних мережах, пристроях підключених до об'єкту.

3. Виявлення повної множини потенційно можливих загроз і каналів витоку інформації в штатному, передаварійному та аварійному режимах роботи АСУ ТП.

4. Складання реєстру вбудованих механізмів захисту апаратних і програмних засобів АСУ ТП.

5. Проведення оцінки вразливості інформації та ризиків за допомогою моделювання системи захисту критичних ресурсів виробництва мінеральних добрив та оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив.

6. Визначення вимог до система захисту критичних ресурсів виробництва мінеральних добрив з урахуванням використання вбудованих механізмів захисту.

7. Включення вбудованих і вибір зовнішніх засобів захисту інформації та їх характеристик.

8. Оформлення документації на система захисту критичних ресурсів виробництва мінеральних добрив як на підсистему АСУ ТП.

9. Впровадження і організація використання обраних заходів, способів і засобів захисту.

10. Здійснення контролю цілісності і керування система захисту критичних ресурсів виробництва мінеральних добрив протягом всього терміну експлуатації.

Зазначена послідовність дій повинна здійснюватися безперервно по замкненому циклу, з проведенням оперативного аналізу (силами розробників) стану система захисту критичних ресурсів АСУ ТП і уточненням вимог до неї після кожного кроку.

Оцінка вразливості інформації та ризиків рекомендується як до створення система захисту критичних ресурсів (крок 5), так і після її впровадження (крок 9).

Висновки до розділу 4

1. Розроблено математичну модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі. Основними характеристиками, що впливають на виробництва гранул у псевдозрідженому шарі є температура теплоносія та температура гранул. Для одержання мінеральних добрив заданої якості необхідно контролювати вологовміст гранул. Запропонована математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі разом з регулятором може використовуватись для побудови системи керування процесом.

2. Розроблено оптимальну систему керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором.

3. Розроблено інформаційної технології захисту критичних ресурсів (ІТЗКР) виробництва мінеральних добрив, основними компонентами якої є наступні технічні, програмні та організаційно-методичні засоби: моделювання системи захисту критичних ресурсів виробництва мінеральних добрив, оптимізація системи захисту критичних ресурсів виробництва мінеральних добрив, система захисту критичних ресурсів виробництва мінеральних добрив, математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі та оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором. Використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив дозволило підвищити якість готового продукту на 15 %.

4. Розроблено методику використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-прикладну задачу – забезпечення необхідного рівня захищеності критичних ресурсів виробництва мінеральних добрив за рахунок розроблених моделей, методу та створення і використання нової інформаційної технології.

У процесі дослідження отримано наступні результати:

1. Виконано аналіз основних принципів математичного моделювання систем захисту інформації, моделей загроз і особливостей їх реалізації, імітаційного моделювання систем захисту критичних інформаційних ресурсів та методів оптимізації систем захисту інформації.

Проведене дослідження показало необхідність розробки нових моделей впливу загроз на базі станів інформаційної системи. Визначено оптимальний підхід для оцінювання рівня захищеності системи захисту інформації в умовах реалізації загроз, в контексті імітаційного моделювання. Уточнена класифікація загроз інформаційній безпеці, а також виявлені загрози, найбільш значущі для даного типу підприємств. Встановлена необхідність забезпечення функціонування інформаційної технології в умовах здійснення нових і невідомих атак.

Виконано порівняльний аналіз програмних платформ емуляторів мережевого обладнання, описано переваги використання рішення для імітаційного моделювання на основі моделі мереж з комбінацією віртуальних і реальних компонентів.

Для оптимізації проєктування системи захисту інформації обґрунтовано поєднання математичного та імітаційного моделювання, що дозволить здійснювати оцінку ефективності її використання для відбиття інформаційних загроз.

Визначено основні параметри, що впливають на технологічний процес та належать до критичних інформаційних ресурсів. Проведений аналіз технологічного процесу виробництва мінеральних добрив у гранулляторах із псевдозрідженим шаром показав необхідність врахування гідродинаміки псевдозрідженого шару, а також кінетики процесів грануляції та зневоднення.

Проведене дослідження сучасного стану розвитку інформаційних технологій захисту критичних інформаційних ресурсів, показало, що існуючі моделі, методи та

засоби не розглядають в комплексі усі принципи забезпечення захисту критичних інформаційних ресурсів технологічних процесів.

Сформульвані завдання, які необхідно розв’язати для досягнення теоретичних та прикладних результатів з розробки інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив, що дозволить забезпечити одержання готового продукту заданої якості та підвищити рівень захищеності технологічного процесу виробництва мінеральних добрив.

2. Розроблено імітаційну модель захисту критичних ресурсів виробництва мінеральних добрив, з метою комплексної оцінки заропонованих заходів і засобів захисту критичних ресурсів виробництва мінеральних добрив. За допомогою збудованого імітаційної моделі захисту критичних ресурсів виробництва мінеральних добрив, на базі GNS3 та KaliLinux, реалізоване проєктування комп’ютерної мережі підприємства та системи захисту критичних ресурсів виробництва мінеральних добрив. Проведене тестування та випробування розробленої імітаційної моделі захисту критичних ресурсів виробництва мінеральних добрив за допомогою програмних засобів, здійснена перевірка системи захисту критичних ресурсів шляхом генерації атак та їх відбиття системою захисту критичних ресурсів виробництва мінеральних добрив. Проведено розрахунок захищеності імітаційної моделі захисту критичних ресурсів виробництва мінеральних добрив методом iRisk, який дозволив виявити загрози інформаційній безпеці для подальшої їх нейтралізації. Запропонований метод оцінки ризиків, може бути використаний для оцінки ефективності системи захисту критичних ресурсів виробництва мінеральних добрив.

В процесі дослідження імітаційної моделі одержано значення інтенсивностей переходів системи захисту критичних ресурсів виробництва мінеральних добрив.

3. Розроблено математичну модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних ресурсів виробництва мінеральних добрив. Запропонована на основі цієї моделі методика виявлення актуальних загроз безпеки.

Дана модель, для опису переходу системи зі стану у стан, використовує побудовану матрицю інтенсивностей переходу. Після проведення дослідження на імітаційній моделі захисту критичних ресурсів виробництва мінеральних добрив

запропоновано два результати знаходження коефіцієнтів для матриці. Запропонована математична модель протидії загрозам дозволяє обчислити значення імовірностей перебування системи у кожному з чотирьох станів і отримати перехідні характеристики для станів системи захисту. Для реалізації розв'язку розроблено програмний модуль. Приклади аналізу числових результатів за допомогою запропонованої методики наочно показують, що їх використання допомагає з визначенням загроз, які є актуальними для досліджуваної системи та можуть використовуватись на практиці.

4. Розроблено метод оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив.

На основі здійсненого аналізу підходів до оптимізації системи захисту, запропоновано перехід від багатокритеріальної задачі оптимізації, до однокритеріальної. Запропонований метод оптимізації проводить оцінку ефективності системи захисту за параметром захищеності, як основним показником, що характеризує рівень забезпечення захисту системи, а на інші характеристики вводяться обмеження. При сформульованому понятті захищеності системи оптимізаційна задача полягає в забезпеченні максимального рівня захищеності, як функції вартості інформації, що захищається і ймовірності злому, при обмеженнях вартості системи захисту і впливу на продуктивність системи. Для оцінки рівня захищеності розглянуто захищеність системи з точки зору теорії ризиків, через параметри загроз.

Реалізовано факторно-цільовий аналіз з метою вибору критерію оптимальності. Запропоновано три критерії якості: узагальнений критерій якості, критерій якості для способу однакових інтенсивностей та критерій якості для способу пропорційності витратам. Для оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив використовуються імітаційна модель системи захисту критичних ресурсів виробництва мінеральних добрив та математична модель протидії загрозам у системі захисту критичних ресурсів виробництва мінеральних добрив, що дозволяє на основі одержаних значень інтенсивностей переходів та станів системи підвищити рівень захищеності критичних ресурсів виробництва мінеральних добрив від впливу

внутрішніх та зовнішніх загроз. Для реалізації розв’язку розроблено програмний модуль.

5. Розроблено методику оптимізації системи захисту критичних ресурсів виробництва мінеральних добрив, яка визначає три основні кроки на шляху організації ефективної роботи підприємства та проєктування оптимальної системи захисту інформації.

6. Розроблено математичну модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі, з метою підвищення ефективності технологічного процесу виробництва мінеральних добрив, а саме для одержання мінеральних добрив заданої якості. Основними характеристиками, що впливають на виробництва гранул у псевдозрідженому шарі є температура теплоносія та температура гранул. Для одержання мінеральних добрив заданої якості необхідно контролювати вологовміст гранул. Розроблена математична модель враховує гідродинаміку псевдозрідженого шару, а також кінетику процесів грануляції та зневоднення. Моделювання враховує задані початкові та граничні вимоги, що відповідають технологічному процесу виробництва мінеральних добрив, тому дана математична модель, дає можливість створити енергоефективну систему управління процесом грануляції, яка буде підтримувати вологовміст гранул на заданому рівні. Одержано перехідні характеристики температури повітря, температури гранул та вологовмісту гранул, які підтверджують ефективність запропонованої математичної моделі процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі.

7. Розроблено оптимальну систему керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором**.** Запропонована математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у пседозрідженому шарі у поєднанні з регулятором може використовуватись для побудови системи керування процесом. Основним каналом керування є залежність температури теплоносія та температури гранул, тому було розглянуто перехідну характеристику залежності саме температури теплоносія та температури гранул. Отримано передавальну функцію, а з неї здійснено перехід до векторно-

матричної моделі з подальшим обчисленям критерію якості. Виділені основні фактори, які впливають на процес та створено LQR- регулятор системи, який відповідає вимогам стабільності, динаміки та надійності. Керована система з LQR-регулятором, в порівнянні з PID регулятором, заощаджує час на переведення системи до заданої температури, тобто заощаджує витрати на нагрівання гранул.

8. Розроблено інформаційну технологію захисту критичних ресурсів виробництва мінеральних добрив, основними компонентами якої є наступні засоби: моделювання системи захисту критичних ресурсів виробництва мінеральних добрив, оптимізація системи захисту критичних ресурсів виробництва мінеральних добрив, система захисту критичних ресурсів виробництва мінеральних добрив, математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдозрідженому шарі та оптимальна система керування виробництвом гранульованих мінеральних добрив у псевдозрідженому шарі з LQR-регулятором.

Застосування розробленої інформаційної технології дозволяє здійснювати вимірювання основних параметрів технологічного процесу, оперативно керувати процесом, забезпечуючи функціональну безпеку технологічного процесу виробництва мінеральних добрив та одержання готового продукту заданої якості, чим забезпечує підвищення ефективності процесів отримання гранульованих мінеральних добрив. Використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив дозволило підвищити якість готового продукту на 15 %.

9. Розроблено методику використання інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив.

Дана методика заснована на запропонованому поєднанні комплексу зовнішніх заходів захисту з вбудованими в апаратурні і програмні компоненти механізмами захисту інформації, що враховує особливості систем керування підприємством і хімічної промисловості. Зазначена послідовність дій повинна здійснюватися безперервно по замкненому циклу, з проведенням оперативного аналізу стану системи захисту критичних ресурсів і уточненням вимог до неї після кожного кроку.

Отримані результати дослідження призначені для використання, в першу чергу, в хімічній промисловості. Крім того, вони можуть знайти своє застосування в інших галузях критичної інфраструктури, де виникає потреба забезпечення захисту параметрів технологічного процесу і отримання готового продукту заданої якості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Опірський І.Р. Класифікація моделей захисту інформації в інформаційних мережах держави. *Науковий вісник НЛТУ України*. 2015. Вип. 25.10. С. 329-335.

2. Курилов Ф.М. Моделирование систем защиты информации. Приложение теории графов. *Технические науки: теория и практика*: материалы III Междунар. науч. конф. Чита: Издательство Молодой ученый, 2016. С. 6-9

3. Гильмуллин Т.М. Модели и комплекс программ процесса управления рисками информационной безопасности: автореф. дис. … канд. техн. наук: 05.13.18. Казань, 2010. 21 с.

4. Ширинкин М.С. Модели и методы синтеза оптимальной иерархической структуры многоуровневого информационного комплекса промышленного предприятия: автореф. дис. … канд. техн. наук: 05.13.01. Москва, 2011. 21 с.

5. Тихонов Д.В. Модели оценки эффективности систем информационной безопасности: автореф. дис. … канд. эк. наук: 08.00.13. Санкт-Петербург, 2009. 19 с.

6. Голембиовская О.М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищённости: автореф. дис. … канд. техн. наук: 05.13.19. Брянск, 2013. 19 с.

7. Асмолов Т.А. Защита информационных систем музейных и библиотечных фондов на основе решений задач комбинаторной оптимизации: автореф. дис. … канд. техн. наук: 05.13.19. Москва, 2012. 24 с.

8. Шоров А. В. Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода "Нервная система сети": Автореф. дис. канд. техн. наук: 05.13.19. - Санкт-Петербург, 2012. - 24 с.

9. Скрыль С.В. Метод количественной оценки показателейэффективности систем защиты информации от несанкционированного доступа. *Вестник Воронежского института МВД России*. 2013. №3. С. 78-83.

10. Охрименко С.А., Черней Г.А. Экономические аспекты эффективности систем защиты информации. *Молдавская Экономическая Академия.* 2019. URL:http://www.security.ase.md/publ/pubru59.

11. Иванов В.П. Математическая оценка защищенности информации от несанкционированного доступа. *Специальная техника.* 2004. №1. С. 35-41.

12. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем. *Искусственный интеллект.* 2008. Вип. 4. С. 253–264.

13. Чемин А. А. Разработка методов оценки эффективности систем защиты информации в распределенных информационных системах специального назначения: автореф. дис. …канд. техн. наук: 05.13.19. Москва, 2009. 22 с.

14. Бучик С.С., Шалаєв В.О. Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаціних систем. *Наукоємні технології.* 2017. Том 3, №35. С. 215 - 223.

15. Arber B., Davey J. The use of the CCTA risk analysis and management methodology CRAMM. *Proc. MEDINFO92*, North Holland, 1992. P. 1589 –1593.

16. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. *DPHU*. 2018. URL: http://www.dphu.org/uploads/attachements/books/books_91_0.pdf.

17. Корниенко Б.Я. Информационная безопасность и технологии компьютерных сетей: монография. Deutschland: LAMBERT Academic Publishing, Saarbrucken. 2016. 102 с.

18. Корниенко Б.Я. Кибернетическая безопасность - операционные системы и протоколы. Deutschland: LAMBERT Academic Publishing, Saarbrucken. 2017. 122 с.

19. Корнієнко Б.Я. Безпека інформаційно-комунікаційних систем та мереж: навчальний посібник для студентів спеціальності 125 «Кібербезпека». К.:НАУ, 2018. 226 с.

20. Корнієнко Б.Я., Галата Л.П., Заболотний В.В. Математична модель протидії загрозам у системі захисту критичних інформаційних. *Наукоємні технології*: науковий журнал. Київ. 2019. Том №3 (43). С. 300-306.

21. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003. 752 с.

22. Галкин А.П., Защита каналов связи предприятий и учреждений от несанкционированного доступа к информации: учеб. пособие. Владимир: ВлГУ, 2003. 128 с.

23. Киселев О.В., Есиков А.С. Защита информации в системах ее передачи и обработки. М.: Солид, 2000. 202 с.

24. Корнієнко Б.Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки. *Наукоємні технології*. 2012. Том 3, №15. С. 83 – 89. doi.org/10.18372/2310-5461.15.5120 (ukr).

25. Korniyenko B.Y., Yudin O., Novizkij E. Open systems interconnection model investigation from the viewpoint of information security. *The Advanced Science Journal*. 2013. Issue 8. P. 53 – 56.

26. Юдін О.К., Корнієнко Б.Я. Реалізація інформаційної безпеки у моделі взаємодії відкритих систем. *Комп'ютерні системи та мережні технології (CSNT-2013)*: збірник тез VI Міжнародної науково-технічної конференції, 11-13 червня, 2013. С.73.

27. Управління інформаційною безпекою / Л.Ф. Єжова та ін. В 2-х т. Київ: Вид-во ДУІКТ, 2011. 236 с.

28. Шеннон Р. Имитационное моделирование систем – искусство и наука. Москва: Мир, 1978. 212 с.

29. Строгалев В.П., Толкачева И.О. Имитационное моделирование: учеб. пособие. Москва: Изд–во МГТУ им. Н.Э. Баумана, 2008. 280 с.: ил.

30. Andrea Finardi. IoT Simulations with Cisco Packet Tracer. *Theseus*. 2018. URL: https://www.theseus.fi/bitstream/handle/10024/150158/Andrea%20Finardi%20%20Master%20of%20Engineering%20%20Informion%20technology.pdf?sequence =1&isAllowed=y.

31. GNS3 and Cisco Packet Tracer Student applications. *UPWEEK*. 2018. URL: https://upweek.ru/prilozheniya-gns3-i-cisco- packet-tracer-student-chto-nam-stoit-set-postroit-narisuem-budem-zhit.

32. Olkov E. Fundamentals of gns3. Connect gns3 to the real network. *Netskills*. 2018. URL: http://blog.netskills.ru/2015/12/12-gns3-connect-realnetwork.html.

33. Ногин В.Д. Проблема сужения множества Парето: подходы к решению. *Искусственный интеллект и принятие решений*. 2008. № 1. С. 98-112.

34. Трояников И.Б. Методы оценки информационной безопасности предприятия на основе процессного подхода: дисс. … канд. техн. наук: 05.13.19. СПб: СПбГУ ИТМО, 2010. 134 с.

35. Horio, M., Wen, C.Y.An Assessment of Fluidized-Bed Modeling. *AIChE Symp*. Ser. 1977. Vol. 73, No. 161. P. 9-21.

36. Grace, J.R. Fluidized beds as chemical reactors, in gas fluidization technology. 1986. John Wiley & Sons, Chichester, New York, Brisbane, Toronto, Singapore.428 p.

37. Kuipers, J. A. M., K. J. van Duin, F. P. H. van Beckum, and W. P. M. van Swaaij. A Numerical Model of Gas-Fluidized Beds. Chem. Eng. Sei. 1992.

38. Корнієнко Б.Я. Особливості моделювання процесів переносу у дисперсних системах. *Вісник Національного технічного університету України «Київський політехнічний інститут».* Серія: Хімічна інженерія, екологія та ресурсозбереження. 2011. № 2(8). С. 5-9.

39. The official GNS3 Documentation. *GNS3*. 2017. URL: https://www.gns3.com/ support/docs.

40. Сергієнко І.В. Інформатика в Україні: Становлення, розвиток, проблеми. Київ: Наукова думка, 1999. 354 с.

41. Korniyenko B. The classification of information technologies and control systems. *International scientific journal*. 2016. № 2. P. 78 - 81.

42. Корнієнко Б.Я., Максімов Ю.О., Марутовська Н.М. Прикладні програми управління інформаційними ризиками. *Захист інформації*. 2012. № 4 (57). С.60 – 64, doi.org/10.18372/2410-7840.14.3493 (ukr).

43. Корнієнко Б.Я, Юдін О.К., Снігур О.С. Безпека аутентифікації у web-ресурсах. *Захист інформації*. 2012. № 1 (54). С. 20 -25, doi.org/10.18372/2410-7840.14.2056 (ukr).

44. Основная Конфигурация NAT ASA: Webserver в DMZ в Версии 8.3 ASA и позже. *CISCO*. 2018. URL: http://www.cisco.com/cisco/web/support/RU/111/1118/ 1118943_asa-config-dmz-00.html.

45. Межсетевые экраны следующего поколения Cisco ASA серии 5500 и 5500X для Интернет-периметра. *CISCO*. 2018. URL: http://www.cisco.com/web/RU/ downloads/broch/data_sheet_c78-701808.pdf.

46. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПБ.: Питер, 2005. 561 с.

47. Основы маршрутизации и коммутации. *Amazon AWS*. 2018. URL: https://static-course-assets.s3.amazonaws.com/RSE503/ru/index.htm l# 9.1.1.1.

48. Обзор продуктов и решений Cisco Systems (Издание VI). *Lanwan. 2018.* URL: http://catalog.lanwan.ru/Obzor_routers_ and_ servers_Cisco.pdf.

49. Стресс-тест сети: DoS с исользованием Hping3. *Codeby.* 2018. URL: https://codeby.net/bezopasnost/stress-test-seti-dos-s-ispolzovaniem-hping3-i-spufingo m-ip-v-kali-linux.

50. Как использовать сканер безопасности Zenmap на Linux. *Codeby.* 2018. URL: https://codeby.net/bezopasnost/kak-ispolzovat-skaner-bezopasnosti-nmap-na-linux.

51. Wireshark User Guide. *Wireshark.* 2018. URL: https://www.wireshark.org/docs/ wsug_html.

52. IRisk Equatuion A White paper by Chris Clymer, Ken Stasiak, Matt Neely, Stephen Marchewitz. *Securestate*. 2018. URL: https://securestate.en/iRisk-Equation-Whitepaper.pdf .

53. Common Vulnerability Scoring System v3.0: User Guide. *First.* 2018. URL: https://www.first.org/cvss/user-guide.

54. Cisco IOS Software Command Authorization Bypass. *CISCO*. 2018. URL: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-2012 0328pai.

55. Cisco Web Security Appliance Administrative Interfaces Access Control Bypass Vulnerability. *CISCO*. 2018. URL: https://tools.cisco.com/security/center/content/ CiscoSecurityAdvisory/cisco-sa-20170719-wsa5 .

56. Эксплойт EternalBlue. *Habrahabr*. 2018. URL: https://habrahabr.ru/company/ panda/blog/329044 .

57. Meltdown. *Meltdown.* 2018. URL: https://meltdownattack.com/meltdown.pdf .

58. Spectre Attacks: Exploiting Speculative Execution. *Spectreattack*. 2018. URL: https://spectreattack.com/spectre.pdf.

59. Росенко А.П. Теоретические основы анализа и оценки влияния внутрених угроз на безопасность конфиденциальной информации: монография. М.: Гелиос АРВ, 2008. 154с.

60. Korniyenko B.Y., Galata L.P. Design and research of mathematical model for information security system in computer network. *Наукоємні технології*. 2017. № 2 (34). С. 114 - 118.

61. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. *Sciences of Europe*. 2016. V. 2., № 2 (2). P. 61 -63.

62. Korniyenko B., Yudin A., Galata L. Risk estimation of information system. *Wschodnioeuropejskie Czasopismo Naukowe*. 2016. № 5. P. 35 - 40.

63. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources. *Information Technologies and Security" (ITS 2018)*: CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference, Kyiv, Ukraine, November 27, 2018. Vol-2318. P. 176-187, urn:nbn:de:0074-2318-4.

64. Корнієнко Б.Я., Галата Л.П. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. *Моделювання та інформаційні технології*. 2018. Вип. 83. С. 34-41.

65. Корнієнко Б.Я., Галата Л.П. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. *Наукоємні технології*. 2017. № 4 (36). С. 316 - 322.

66. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. *Advanced Trends in Information Theory (IEEE ATIT -2019):* Conference Proceedings of 2019 IEEE Inernational Conference, Dezember 18 – 20, 2019, Kyiv, Ukraine. P. 244-248.

67. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. *Information Technologies and Security" (ITS 2019)*: CEUR Workshop Proceedings, Selected Papers of the XIX International

Scientific and Practical Conference, Kyiv, Ukraine, November 28, 2019. Vol-2577. P.281-291.

68. Galata L.P., Korniyenko B.Y. Research of the Training Ground for the Protection of Critical Information Resources by iRisk Method. *Mechanisms and Machine Science.* 2020. Springer International Publishing. Volume 70. P. 227-237. DOI https://doi.org/10.1007/978-3-030-13321-4. ISBN 978-3-030-13321-4

69. Korniyenko B., Galata L. Implementation of the Information Resources Protection Based on the CentOS Operating System. *Electrical and Computer Engineering*: Proceedings of 2019 IEEE 2nd Ukraine Conference, Lviv, Ukraine. 2019. IEEE. P. 1007-1011.

70. Корников В. В., Серёгин И. А., Хованов Н. В. Многокритериальное оценивание финансовых рисков в условиях неопределённости: Учеб. Пособие. СПб.: Изд-во С.-Петерб. ун-та, 2002. 96 с.

71. Михайлов М. В. Построение множества согласованных допустимых векторов весовых коэффициентов в методе сводных показателей. Деп. ВИНИТИ, Ш 3645-В96. М., 1996. 12 с.

72. Городецкий С. Ю. ННГУ. Модели и методы конечномерной оптимизации. Часть2. Нелинейное программирование и многоэкстремальная оптимизация: учебный курс. Учебно-исследовательская лаборатория "Математические и программные технологии для современных компьютерных систем (Информационные технологии)". 2003. 157 с.

73. Герасимова Л.В., Погожев И.Б. Комплексная оценка качества проектов и выбор оптимального варианта по методу академика А.Н. Крылова. *Стандарты и качество*. 1972. №8. С.37-39.

74. Постников В. М. Спиридонов С. Б. Методы выбора весовых коэффициентов локальных критериев. *Наука и Образование. МГТУ им. Н. Э. Баумана*. Электрон. 2015. № 06. С. 267-287.

75. Ногин В. Д. Обобщённый принцип Эджворта-Парето и границы его применимости. *Экономика и математические методы*. Москва: Наука, 2005. С. 128-134.

76. Biggs M.C. Constrained Minimization Using Recursive Quadratic Programming. *Towards Global Optimization*. 1975. North-Holland. P. 341-349.

77. Han S.P. A Globally Convergent Method for Nonlinear Programming. Optimization Theory and Applications. 1977. Vol. 22. 297 p.

78. Hock W. and Schittkowski K. A Comparative Performance Evaluation of 27 Nonlinear Programming Codes. Computing. 1983. Vol. 30. 335 p.

79. Powell M.J.D. The Convergence of Variable Metric Methods for Nonlinearly Constrained Optimization Calculations. Nonlinear Programming 3. Academic Press. 1978. 308 p.

80. Powell M.J.D. A Fast Algorithm for Nonlinearly Constrained Optimization Calculations. Numerical Analysis: Lecture Notes in Mathematics. Springe Verlag, 1978. Vol. 630. 232 p.

81. Gill P.E., Murray W., Saunders M.A. and Wright M.H. Procedures for optimization Problems with a Mixture of Bounds and General Linear Constraints. *ACM Trans. Math. Software.* 1984. Vol. 10. P. 282-298.

82. Корнієнко Б. Інформаційні технології оптимального управління виробництвом мінеральних добрив: монографія. Київ: Аграр Медіа Груп, 2014. 154 с.

83. Korniyenko B.Y., Ladieva L. R., Galata L.P. Mathematical Model of Heat Transfer Process of Production of Granulated Fertilizers in Fluidized Bed. *ARPN Journal of Engineering and Applied Sciences.* 2021. Volume 16, Issue 20. P. 2126-2131.

84. Korniyenko, B., Ladieva, L., Galata, L. Control system for the production of mineral fertilizers in a granulator with a fluidized bed. *2020 2nd IEEE International Conference on Advanced Trends in Information Theory:* ATIT 2020 – Proceedings. 2020. P. 307–310, 9349344.

85. Астахов А.А. Особенности обеспечения информационной безопасности промышленных систем. *CISA-2006*. No3. С. 76-79.

86. Пищик Б.Н. Безопасность АСУ ТП. *Вычислительные технологии*. 2013. Том 18, спец. выпуск. С. 170-175.

87. Демидович Д.И. Современные технологии защиты информации в АСУ ТП. *56-я научная конференция аспирантов, магистрантов и студентов БГУИР*, 2020. Минск. С.12-17.

ДОДАТОК 1

Програмна реалізація розрахунку критеріїв оптимальності, програмна реалізація розробленої математичної моделі

ПРОГРАМНА РЕАЛІЗАЦІЯ РОЗРАХУНКУ КРИТЕРІЇВ ОПТИМАЛЬНОСТІ

Matlab-скрипт

```
function [] = thesis_script()
    % Lower bounds
    lb = [];
    % Upper bounds
    ub = [];
    % Start point
    x0 = [1; 1; 0; 0];

    iterValues = [];
    funValues = [];
    x1Values = [];
    x2Values = [];
    x3Values = [];
    x4Values = [];

    % Optimization options parameters
    options = optimset('LargeScale', 'off', 'Display', 'iter', 'OutputFcn',
@OutFcn, 'TolCon', 0.001, 'MaxFunEvals', 500); %'MaxFunEvals', 100
    % Optimization function call
    [x, fval, exitflag, output] = fmincon(@objfun, x0, [], [], [], [], lb,
ub, @confun, options);
    x % minimum point
    fval % function value in minimum point
    % constraints
    [c, ceq] = confun(x)
```

```
    %figure;
    plot(iterValues, funValues, 'r');
    legend('criterion value');

    figure;

    hold on;

    plot(iterValues, x1Values, 'g');
    plot(iterValues, x2Values, 'b');
    plot(iterValues, x3Values, 'm');
    plot(iterValues, x4Values, 'c');

    hold off;

    legend('p1', 'p2', 'p3', 'p4');

    % criterion 1
    function f = objfun(x)
        x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);
        c1 = 0.2; c2 = 0.7; c3 = 0.1; c4 = 0.3;
        l1 = 20; l2 = 3; l3 = 4; l4 = 5;
        % target function
        f = (c1 * l1 * (1 - x1) + c2 * l2 * (1 - x2) + c3 * l3 * (1 - x3) +
c4 * l4 * (1 - x4)) / (c1 * l1 + c2 * l2 + c3 * l3 + c4 * l4);
    end

    % criterion 2
    function f = objfun1(x)
        x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);
        c1 = 0.2; c2 = 0.7; c3 = 0.1; c4 = 0.3;
        % target function
```

```
        f = (c1  * (1 - x1) + c2  * (1 - x2) + c3 * (1 - x3) + c4 * (1 - x4))
/ (c1 + c2 + c3 + c4);
    end


    % criterion 3
    function f = objfun2(x)
        x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);
        c1 = 0.2; c2 = 0.7; c3 = 0.1; c4 = 0.3;
        % target function
        f = (c1.^2  * (1 - x1) + c2.^2  * (1 - x2) + c3.^2 * (1 - x3) + c4.^2
* (1 - x4)) / (c1.^2 + c2.^2 + c3.^2 + c4.^2);
    end


    function [c, ceq] = confun(x)
       x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);
       % Non-equality constraints, <= 0
       c = [-x1, x1 - 0.3, -x2 + 0.4, x2 - 0.6, -x3 + 0.6, x3 - 0.5, -x4 +
0.9, x4 - 0.6];
       % Equality constraints
       ceq = [-0.040 * x1 + 0.015 * x2 + 0.010 * x3 + 0.015 * x4 - 1,
           0.225 * x1 - 0.250 * x2 - 0.025 * x3 + 0.050 * x4 - 1,
           0.625 * x1 - 0.160 * x2 - 0.855 * x3 + 0.390 * x4 - 1,
           -0.00 * x1 + 0.075 * x2 + 0.200 * x3 - 0.275 * x4 - 1];
    end


    function stop = OutFcn(x, optimvalues, state)
       stop = false;
       PlotIter(x, optimvalues);
    end


    function PlotIter(x, optimvalues)
       x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);


       iterValues(end + 1) = optimvalues.iteration;
```

```
        funValues(end + 1) = optimvalues.fval;
        x1Values(end + 1) = x1;
        x2Values(end + 1) = x2;
        x3Values(end + 1) = x3;
        x4Values(end + 1) = x4;
    end

end
```

ПРОГРАМНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ МАТЕМАТИЧНОЇ МОДЕЛІ

Python-скрипт

```
import numpy as np
import matplotlib.pyplot as plt

def frk(x, fx, n, hs):
    k1 = []
    k2 = []
    k3 = []
    k4 = []
    xk = []
    for i in range(n):
        k1.append(fx[i](x)*hs)
    for i in range(n):
        xk.append(x[i] + k1[i]*0.5)
    for i in range(n):
        k2.append(fx[i](xk)*hs)
    for i in range(n):
        xk[i] = x[i] + k2[i]*0.5
    for i in range(n):
        k3.append(fx[i](xk)*hs)
    for i in range(n):
        xk[i] = x[i] + k3[i]
```

```
    for i in range(n):
        k4.append(fx[i](xk)*hs)
    for i in range(n):
        x[i] = x[i] + (k1[i] + 2*(k2[i] + k3[i]) + k4[i])/6
    return x

def f1(x):
    #return -0.040 * x[0] + 0.225 * x[1] + 0.625 * x[2] + 0.000 * x[3]
    return -0.040 * x[0] + 0.225 * x[1] + 0.575 * x[2] - 0.125 * x[3]

def f2(x):
    #return 0.015 * x[0] - 0.250 * x[1] - 0.160 * x[2] + 0.075 * x[3]
    return 0.015 * x[0] - 0.250 * x[1] - 0.200 * x[2] + 0.145 * x[3]

def f3(x):
    #return 0.010 * x[0] - 0.025 * x[1] - 0.855 * x[2] + 0.200 * x[3]
    return 0.010 * x[0] - 0.025 * x[1] - 0.875 * x[2] + 0.180 * x[3]

def f4(x):
    #return 0.015 * x[0] + 0.050 * x[1] + 0.390 * x[2] - 0.275 * x[3]
    return 0.015 * x[0] + 0.050 * x[1] + 0.500 * x[2] - 0.200 * x[3]

def impl():
    f = [f1, f2, f3, f4]
    x = [1, 0, 0, 0]
    hs = 1
    p0 = []
    p1 = []
    p2 = []
    p3 = []
    t1 = np.arange(0.0, 51.0, 1.0)
    print('****************************************')
    print('*  t  *   p0   *   p1   *   p2   *   p3  *')
```

```
    print('*****************************************')
    for i in range(51):
        x = frk(x, f, 4, hs)
        p0.append(x[0])
        p1.append(x[1])
        p2.append(x[2])
        p3.append(x[3])
        ti = str(i)
        if i < 10:
            ti = '0'+ti
        print('*  %s * %.4f * %.4f * %.4f * %.4f' % (ti, x[0], x[1], x[2],
x[3]))
    print('*****************************************')
    lines = plt.plot(t1, p0, 'r', t1, p1, 'b', t1, p2, 'g', t1, p3, 'y')
    plt.axis([0, 50, 0, 1])
    plt.title('Graph')
    plt.xlabel('Time, t')
    plt.ylabel('Probability, Pi(t), i=0,1,2,3')
    plt.grid(True)
    plt.setp(lines, linewidth=3.0)
    plt.show()

if __name__ == '__main__':
    impl()
```

ДОДАТОК 2

Список публікацій здобувача, відомості про апробацію та впровадження результатів дисертації

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації у виданнях, що входять до міжнародної наукометричної бази даних (Scopus)

1. Galata L.P., Korniyenko B.Y., Yudin A.K. Research of the simulation polygon for the protection of critical information resources. *Information Technologies and Security (ITS 2017):* CEUR Workshop Proceedings, Selected Papers of the XVII International Scientific and Practical Conference*,* Kyiv. 2017. Vol. 2067. P. 23-31.
2. Korniyenko B., Galata L., Ladieva L. Security estimation of the simulation polygon for the protection of critical information resources. *Information Technologies and Security (ITS 2018):* CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference, Kyiv. 2018. Vol. 2318. P. 176-187.
3. Korniyenko B., Galata L. Implementation of the Information Resources Protection Based on the CentOS Operating System. *Proceedings of 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering*, Lviv. 2019. P. 1007-1011.
4. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. *Information Technologies and Security (ITS 2019)*: CEUR Workshop Proceedings, Selected Papers of the XIX International Scientific and Practical Conference*,* Kyiv. 2019. Vol. 2577. P. 281-291.
5. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. *2019 IEEE Inernational Conference on Advanced Trends in Information Theory:* IEEE ATIT - Conference Proceedings, Kyiv. 2019. P. 244-248.

6. Galata L.P., Korniyenko B.Y. Research of the Training Ground for the Protection of Critical Information Resources by iRisk Method. *Mechanisms and Machine Science.* 2020. Vol. 70. P. 227-237.
7. Korniyenko, B., Ladieva, L., Galata, L. Control system for the production of mineral fertilizers in a granulator with a fluidized bed. *2020 2nd IEEE International Conference on Advanced Trends in Information Theory:* ATIT 2020 – Proceedings. 2020. P. 307–310, 9349344.
8. Korniyenko B.Y., Ladieva L. R., Galata L.P. Mathematical Model of Heat Transfer Process of Production of Granulated Fertilizers in Fluidized Bed. *ARPN Journal of Engineering and Applied Sciences.* 2021. Volume 16, Issue 20. P. 2126-2131.

Публікації у наукових фахових виданнях України

9. Korniyenko B. Y., Galata L. P. Design and research of mathematical model for information security system in computer network. *Наукоємні технології.* 2017. Т. 2, №34. С. 114-118.
10. Корнієнко Б.Я., Галата Л.П. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. *Наукоємні технології.* 2017. Т.4, №36. С. 316-322.
11. Корнієнко Б.Я., Галата Л.П. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. *Моделювання та інформаційні технології: зб. наук. пр. Нац. акад. наук України, Ін-т пробл. моделювання в енергетиці ім. Г. Є. Пухова.* 2018. Вип. №83. С. 34-42.
12. Korniyenko B., Galata L. Modeling of information security system in computer network. *Безпека інформаційних систем і технологій.* 2019. Т.1, №1. С. 36-41.
13. Галата Л.П., Корнієнко Б.Я., Заболотний В.В. Математична модель протидії загрозам у системі захисту критичних інформаційних ресурсів. *Наукоємні технології.* 2019. Т.3, №43. С. 300-306.
14. Корнієнко Б.Я., Галата Л.П. Метод IRISK для оцінки рівня захищеності імітаційного полігону захисту критичних інформаційних ресурсів. *Вісник Університету «Україна».* Серія: Інформатика, обчислювальна техніка та кібернетика. 2019. Т.2, №23. С. 288-296.

15. Галата Л.П., Корнієнко Б.Я. Дослідження системи захисту інформації корпоративної мережі на основі GNS3. *Наукоємні технології.* 2020. Т.2, №46. С. 172-179.
16. Корнієнко Б.Я., Ладієва Л.Р., Галата Л.П. Оптимальна система управління виробництвом мінеральних добрив у грануляторі із пседозрідженим шаром. *Новітні технології.* 2021. Т.2, № 12. С. 18-28.

Патент на корисну модель

17. Спосіб забезпечення управління доступом у захищених багатомашинних автоматизованих системах із виявлення загроз: пат. 132248 Україна: МПК(2019.01), G06F 13/00, G06F 21/00, H04L 9/00. № u 2018 03740; заявл. 06.04.2018; опубл. 25.02.2019, Бюл. № 4, 4 с.

Публікації у збірниках матеріалів конференцій

18. Галата Л.П., М.С. Мариняк. Оцінка та менеджмент ризиків корпоративної мережі. *ПОЛІТ. Сучасні проблеми науки. Комп'ютерні технології:* тези доповідей XV міжнародної науково-практичної конференції молодих учених і студентів, Київ. 2015. С. 4.
19. Галата Л.П., Козюберда О.В. Моделювання безпеки комп'ютерної системи. *Комп'ютерні системи та мережні технології (CSNT-2015):* Збірник тез VIII Міжнародної науково-технічної конференції, Київ. 2015. С. 15-16.
20. Галата Л.П., Колесник Н.І. Дослідження моделей безпеки комп'ютерних систем. *ПОЛІТ. Сучасні проблеми науки. Комп'ютерні технології*: тези доповідей XVI міжнародної науково-практичної конференції молодих учених і студентів, Київ. 2016. С. 14.
21. Yudin O.K., Kornienko B.Y., Галата Л.П. Risk estimation of information system. *Wschodnioeuropejskie Czasopismo Naukowe.* 2016. № 5.3. P. 35 – 40.
22. Galata L.P., Kozuberda O.W. Modeling of security and risk assessment in information and communication system. *Sciences of Europe.* 2016. V. 2, No 2 (2). P. 61-63.
23. Корнієнко Б.Я., Галата Л.П., Удовенко Б.В. Імітаційне моделювання системи захисту інформації комп`ютерної мережі. *Інтелектуальні системи прийняття рішень та*

проблеми обчислювального інтелекту (ISDMCI'2016): Збірка наукових праць міжнародної наукової конференції, Херсон. 2016. С. 77 - 79.

24. Галата Л.П., Пасічник П.В. Захист інформаційно-комунікаційної мережі на основі розширеної моделі OSI. *ПОЛІТ. Сучасні проблеми науки. Комп'ютерні технології*: тези доповідей XVII міжнародної науково-практичної конференції молодих учених і студентів. Київ: НАУ. 2017. С. 6.
25. Galata L. Modeling of information security system in computer network. *VII Miedzynarodowa konferencja studentow oraz doktorantow "Inzynier XXI wieku",* Series: Monogrpah, Projekt interdyscyplinarny projektem XXI wieku, Bielsko-Biala. 2017. Poland: ATH. Tom 2. P. 75-82.
26. Korniyenko B., Galata L., Yudin A. Research of the simulation polygon for the protection of critical information resources. *Информационные технологии и безопасность: Материалы XVII Международной научно-практической конференции ИТБ-2017*, Київ. 2017. С. 35-51.
27. Korniyenko B.Y., Galata L.P.,. Borysenko O.V. Research and analysis of the information security mathematical models. *Materials of the XIV International scientific and practical Conference Cutting-edge science*, Sheffield. UK: Science and education LTD, 2018. P. 51-52.
28. Корнієнко Б.Я., Галата Л.П., Борисенко О.В. Математичне моделювання системи захисту інформаційних ресурсів. *Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту*: Матеріали міжнародної наукової конференції, Херсон. 2018. С. 69-71.
29. Корнієнко Б.Я., Галата Л.П. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів. *Прикладні системи та технології в інформаційному суспільстві*: зб. тез доповідей і наук. повідомл. учасників II Міжнародної науково-практичної конференції, Київ. 2018. С. 77-80.
30. Корнієнко Б.Я., Галата Л.П. Визначення методу аналізу ризиків для імітаційного полігону захисту критичних інформаційних ресурсів. *Прикладні системи та технології в інформаційному суспільстві*: зб. тез доповідей і наук. повідомл. учасників II Міжнародної науково-практичної конференції, Київ. 2018. С. 80-83.

31. Galata L.P., Korniyenko B.Y. Analyzing information risks of the simulation polygon for protection of the critical information resources, *The Eighth World Congress "AVIATION IN THE XXI-st CENTURY" Safety in Aviation and Space Technologies*, Київ. 2018. С. – 2.3.18-2.3.21.
32. Галата Л.П. Інформаційно-комунікаційні мережі на основі розширеної моделі OSI. *Інформаційні технології та взаємодії*: матеріали V міжнародної науково-практичної конференції, Київ. 2018. С. 375-376.
33. Korniyenko B.Y., Galata L.P., Ladieva L.R. Security estimation of the simulation polygon for the protection of critical information resources. *Информационные технологии и безопасность*: Материалы XVIII Международной научно-практической конференции ИТБ-2018, Київ. 2018. Вип.18. С. 183-196.
34. Korniyenko B.Y., Zabolotnyi V.V., Galata L.P. System of protection of critical information resources of technological process. *Prospects of world science:* Materials of the XV International scientific and practical Conference, Sheffield. Science and education LTD, 2019. P. 59-60.
35. Korniyenko B.Y., Galai Y.O., Galata L.P. Construction and testing of information protection system of corporate network. *Nauka: teoria i praktyka – 2019:* Materiały XV Międzynarodowej naukowi-praktycznej konferencji. Przemyśl: Nauka i studia, 2019. Volume 7. P. 53-55.
36. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. *Информационные технологии и безопасность*: Материалы XIX Международной научно-практической конференции ИТБ-2019, Київ. 2019. С. 86-92.
37. Korniyenko B.Y., Ladieva L.R., Galata L.P. System of automated control of the process of production of mineral fertilizers in the fluidized bed. *Science without borders – 2020:* Materials of the XVI International scientific and practical Conference, Sheffield. Science and education LTD, 2020. P. 24-27.
38. Корнієнко Б.Я., Ладієва Л.Р., Галата Л.П. Математична модель теплообміну процесу виробництва гранульованих мінеральних добрив у псевдорозрідженому шарі.

Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту: матеріали міжнар. наук. конф., Херсон. 2020. С. 77-79.

39. Korniyenko B., Ladieva L., Galata L. Mathematical model of heat transfer process of production of granulated fertilizers in fluidized bed. *Математичне та імітаційне моделювання систем. МОДС 2020:* тези доповідей П'ятнадцятої міжнародної науково-практичної конференції. Чернігів: ЧНТУ, 2020. С. 84 -87.
40. Korniyenko B., Galata L., Ladieva L. Optimization of critical information resources protection system. *Інформаційні технології і безпека*: матеріали XX Міжнародної науково-практичної конференції ІТБ-2020, Київ. 2020. Випуск 20. С. 28-29.
41. Корнієнко Б.Я., Фесенко С.А., Галата Л.П. Оптимальна система управління виробництвом мінеральних добрив у грануляторі із пседозрідженим шаром. *Автоматика 2020*: матеріали XXVI Міжнародної конференції з автоматичного керування, Київ. 2020. С. 87-88.
42. Заболотний В.В., Корнієнко Б.Я., Галата Л.П. Оцінка ризиків в системах захисту інформації критичних ресурсів. *Science without borders*: Materials of the XVII International scientific and practical Conference, Sheffield. Science and education LTD, 2021. P 66-71.

Апробація результатів дисертаційної роботи. Основні наукові положення, результати, рекомендації та висновки дисертаційної роботи доповідались та обговорювались на науково-технічних конференціях: VIII Міжнародна науково-практична конференція «Комп'ютерні системи та мережні технології» (м. Київ, квітень 2015 року); Міжнародна науково-практична конференція «Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту» (с. Залізний Порт, травень 2016, 2018, 2020 років); Miedzynarodowa konferencja studentow oraz doktorantow "Inzynier XXI wieku" (м. Бєльсько-Бяла, грудень 2017, 2018 років); Міжнародна науково-практична конференція «Информационные технологии и безопасность» (м. Київ, листопад 2017, 2018, 2019, 2020 років); XIV International scientific and practical Conference Cutting-edge science – 2018 (м. Шеффілд, травень

2018 року); II Міжнародна науково-практична конференція «Прикладні системи та технології в інформаційному суспільстві» (м. Київ, жовтень 2018 року); The Eighth World Congress “AVIATION IN THE XXI-st CENTURY” Safety in Aviation and Space Technologies (м. Київ, жовтень 2018 року); V Міжнародна науково-практична конференція «Інформаційні технології та взаємодії» (м. Київ, листопад 2018 року); IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (м. Львів, липень 2019 року); XV International scientific and practical Conference Prospects of world science – 2019 (м. Шеффілд, серпень 2019 року); XV Międzynarodowej naukowi-praktycznej konferencji «Nauka: teoria i praktyka - 2019» (м. Перемишль, серпень 2019 року); IEEE Inernational Conference on Advanced Trends in Information Theory (м.Київ, 2019, 2020 років); XVI International scientific and practical Conference Science without borders (м. Шеффілд, квітень 2020, 2021 років); П’ятнадцята міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2020» (м. Чернігів, червень 2020 року); XXVI Міжнародна конференція з автоматичного керування (м. Київ, жовтень 2020 року).

Крім того, результати дисертаційної роботи були обговорені на науково-технічних семінарах кафедри комп’ютеризованих систем захисту інформації, науково-практичних конференціях молодих учених і студентів «ПОЛІТ. Сучасні проблеми науки», які проводилися в Національному авіаційному університеті.

ЗАТВЕРДЖУЮ
в.о. проректора Національного авіаційного університету з наукової роботи
_____ О. В. Радченко
«19» 05 2021 р.

ЗАТВЕРДЖУЮ
Директор
ТОВ «НВЦ «ІНФОЗАХСИТ»
_____ Я. В. Калінін
«17» 06 2021 р.

АКТ ВПРОВАДЖЕННЯ

результатів дисертаційної роботи Галати Л.П. «Інформаційна технологія захисту критичних ресурсів виробництва мінеральних добрив»

Ми, що підписалися нижче, від ТОВ «НВЦ «ІНФОЗАХСИТ» м.Київ директор Калінін Я.В. та від Національного авіаційного університету асистент кафедри комп'ютеризованих систем захисту інформації Галата Л.П. підтверджуємо, що наукові результати отримані Галатою Лілією Павлівною в її дисертаційній роботі «Інформаційна технологія захисту критичних ресурсів виробництва мінеральних добрив», а саме: математична модель протидії впливу внутрішніх та зовнішніх загроз, імітаційний полігон захисту критичних інформаційних ресурсів, метод оптимізації системи захисту та система автоматичного управління:

- передано у використання ТОВ «НВЦ «ІНФОЗАХСИТ» для впровадження системи захисту та управління критичних інформаційних ресурсів в проекті імітаційного полігону;
- містять практичну цінність та наукову новизну.

Застосування інформаційної технології захисту критичних інформаційних ресурсів значно підвищить оперативність і ефективність управління та дозволить досягти потрібного рівня захищеності при обмеженнях вартості системи захисту і впливу на продуктивність систем.

_____ Л.П. Галата

Директор
ТОВ «НВЦ «ІНФОЗАХСИТ»
_____ Я.В. Калінін

УЗГОДЖЕНО
Проректор Національного авіаційного університету
з навчальної роботи
_____ А. В. Полухін
«16» 03 2021 р.

ЗАТВЕРДЖУЮ
в.о. проректора Національного авіаційного університету з наукової роботи
_____ О. В. Радченко
«18» 03 2021 р.

АКТ ВПРОВАДЖЕННЯ
результатів дисертаційної роботи асистента кафедри КСЗІ Галати Л.П. в навчальний процес Національного авіаційного університету

Ми, що нижче підписалися, *завідувач кафедри комп'ютеризованих систем захисту інформації С.В. Казмірчук, вчений секретар кафедри комп'ютеризованих систем захисту інформації О.О.Мелешко, доцент кафедри комп'ютеризованих систем захисту інформації А.В. Ільєнко*
склали цей акт про те, що результати наукових досліджень *за темою дисертаційної роботи Галати Лілії Павлівни «Інформаційна технологія захисту критичних ресурсів виробництва мінеральних добрив»* використовуються у навчальному процесі *Факультету кібербезпеки, комп'ютерної та програмної інженерії НАУ на кафедрі комп'ютеризованих систем захисту інформації*

Найменування впровадженого результату	Форма впровадження і досягнутий фактичний ефект
Інформаційна технологія захисту критичних ресурсів виробництва мінеральних добрив: математична модель протидії впливу внутрішніх та зовнішніх загроз, імітаційний полігон захисту критичних інформаційних ресурсів, метод оптимізації системи захисту, математична модель процесу виробництва та система автоматичного управління.	Матеріали дисертаційної роботи впроваджені у вигляді лабораторних та розрахунково-графічних робіт з дисциплін «Безпека інформаційно-комунікаційних систем та мереж», «Проектування систем безпеки ІКСМ» та «Інформаційно-комунікаційні системи та мережі». Впровадження вказаних методично-навчальних матеріалів дозволило перейти до комплексного вивчення студентами способів підвищення ефективності та надійності функціонування сучасних інформаційних систем на основі розробки інформаційної технології захисту критичних ресурсів виробництва мінеральних добрив.

Завідувач кафедри
комп'ютеризованих систем захисту інформації _____ С.В. Казмірчук

Вчений секретар кафедри
комп'ютеризованих систем захисту інформації _____ О.О.Мелешко

Доцент кафедри
комп'ютеризованих систем захисту інформації _____ А.В.Ільєнко