НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

НН Інститут прикладного системного аналізу

Кафедра математичних методів системного аналізу

До захисту допущено:

Завідувач кафедри

_____ Оксана ТИМОЩУК

«___»_____2023 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системний аналіз і управління»

спеціальності 124 «Системний аналіз»

на тему: «Відбиття атак у кіберпросторі (теорія ігор і захист комп систем)»

Виконав :
студент IV курсу, групи КА-93
Ничипорчук Дмитро Миколайович _____

Керівник:
Доцент, к.т.н. Барановська Л.В. _____

Консультант з економічного розділу:
доцент, к.е.н., доцент кафедри ТПЕ
Рощіна Надія Василівна _____

Консультант з нормоконтролю:
к.ф.-м.н. Статкевич В.М. _____

Рецензент:
НН ІПСА, к.т.н. Олександр БЕЗНОСИК _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент _____

Київ – 2023 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

НН Інститут прикладного системного аналізу

Кафедра математичних методів системного аналізу

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 124 "Системний аналіз"

Освітньо-професійна програма «Системний аналіз фінансового ринку»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Оксана ТИМОЩУК
«___»_____2023р.

ЗАВДАННЯ

на дипломну роботу студенту

Ничипорчуку Дмитру Миколайовичу

1. Тема роботи «Відбиття атак у кіберпросторі (теорія ігор і захист комп систем», керівник роботи доцент, к.ф.-м.н. Барановська Леся Валеріївна, затверджені наказом по університету від «___»_____ 2023 р. №_____

2. Термін подання студентом роботи

3. Вихідні дані до роботи: посилання будь-яких сайтів та онлайн книг

4. Зміст роботи: Дослідження предметної області, методи використання теорії ігор при відбитті кібератак, модель вирішення ситуації кібератаки на основі теоретико ігрового підходу, функціонально-вартісний аналіз програмного продукту

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний	Рощіна Н.В., доцент кафедри ТПЕ		

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Формулювання тематики (напряму) дослідження.	20.01.2023	Виконано
2	Аналіз актуальності задач стосовно тематики дослідження	20.04.2023	Виконано
3	Формулювання задач дослідження	30.04.2023	Виконано
4	Уточнення теми дипломної роботи	10.05.2023	Виконано
5	Збір статичних даних, попередній аналіз даних	15.05.2023	Виконано
6	Розробка програмного продукту для виконання обчислювальних експериментів	21.05.2023	Виконано
7	Оформлення пояснювальної записки у цілому	30.05.2023	Виконано
8	Підготовка презентації для захисту	05.06.2023	Виконано

Студент Дмитро НИЧИПОРЧУК

Керівник Леся БАРАНОВСЬКА

РЕФЕРАТ

Дипломна робота: 71 с.; 14 рисунків, 11 таблиць, 24 джерел, 2 додатки.

ВІДБИТТЯ АТАК У КІБЕРПРОСТОРІ (ТЕОРІЯ ІГОР ТА ЗАХИСТ КОМП'ЮТЕРНИХ СИСТЕМ).

Об'єкт дослідження – модель кібератаки як антагоністична гра в нормальній формі з нульовою сумою.

Предмет дослідження – знаходження оптимальних стратегій для захисту комп'ютерної системи при кібератаках.

Мета роботи – змоделювати кібератаку, описати її у вигляді гри, здійснити комп'ютерну реалізацію методу ітерацій для визначення оптимальних стратегій, спроможних відбити та захистити комп'ютерну мережу.

Актуальність: в наш час кібератаки являються дуже поширеними та постійно прогресують, щоб відбити та захиститись від них стає дедалі складніше. Теоретико-ігровий підхід полягає в застосуванні стратегій, які дозволяють запобігти кібератакам та зменшити їх наслідки. Прикладами використання теорії ігор є створення "ловушок" для кіберзлочинців та використання гри з нульовою сумою. У цьому випадку зловмисники не матимуть іншого вибору, як програти. Такий підхід може бути корисним, але не забезпечує 100% захисту від кіберзлочинців. Тому важливо поєднувати його з іншими методами та технологіями кібербезпеки.

Методи дослідження – метод ітерацій (метод Брауна-Робінсона), комп'ютерна реалізація його за допомогою мови програмування Python.

Отримані результати – побудовано модель гри «Кібератака», методом ітерацій знайдено рівновагу у змішаних стратегіях, побудовано програму на мові Python для комп'ютерної реалізації даного методу розв'язування.

ABSTRACT

The work consist: 71 pages; 14 figures, 11 tables, 24 sources, 2 appendices.

The theme: CYBER ATTACKS IN CYBERSPACE (GAME THEORY AND COMPUTER SYSTEM DEFENSE).

The object of the study is a model of a cyber attack as an antagonistic game in normal form with zero sum.

The subject of the research is finding optimal strategies for protecting the computer system against cyber attacks.

The purpose of the work is to simulate a cyber attack, describe it in the form of a game, implement a computer implementation of the iteration method to determine optimal strategies capable of repelling and protecting a computer network.

Relevance: nowadays, cyber-attacks are very common and are constantly progressing, so it becomes more and more difficult to repel and defend against them. The game-theoretic approach consists in applying strategies that allow one to prevent cyber-attacks and reduce their consequences. Examples of the use of game theory are the creation of "traps" for cybercriminals and the use of a zero-sum game. In this case, the attackers will have no choice but to lose. This approach can be useful, but does not provide 100% protection against cybercriminals. Therefore, it is important to combine it with other cyber security methods and technologies.

Research methods – the method of iterations (Brown-Robinson method), its computer implementation using the Python programming language.

The obtained results – the model of the game "Cyberattack" was built, the equilibrium in mixed strategies was found by the method of iterations, a Python program was built for the computer implementation of this solving method.

ЗМІСТ

ВСТУП

Теорія ігор в кібербезпеці є захоплюючою галузю, яка досліджує взаємодію між кібератаками та захисними стратегіями, використовуючи математичні моделі та концепції. У сучасному цифровому світі, де загрози кібербезпеки стають все більш складними і спритними, важливо мати ефективні методи інтелектуального аналізу, щоб протистояти цим загрозам. Цікавим фактом є те, що теорія ігор не тільки допомагає розробляти захисні стратегії, але і може бути використана для виявлення слабкі місць у системі, що дозволяє уникнути можливих кібератак, які можуть використовувати ці слабкі місця.

Теорія ігор - це наука, що досліджує взаємодію між різними учасниками в ситуації, де кожен з них має свої власні цілі та обмеження. Вона застосовується для вивчення різних ситуацій, від економічних до політичних, і для визначення оптимальних стратегій для кожного учасника.

Кібербезпека - це складний процес постійної боротьби з хакерами та вірусами, які намагаються зламати системи безпеки та отримати доступ до конфіденційної інформації. У цьому контексті теорія ігор може бути використана для вивчення того, як хакери діють та як можна вирішити цю проблему. Наприклад, вивчення стратегій хакерів може допомогти розробити більш ефективні методи захисту.

Тому в цій дипломній роботі буде проаналізовано приклади використання стратегічних ходів в захисті від різних типів кібератак та протидії і передбаченні їх у майбутньому.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Актуальність проблеми

З кожним роком кількість кібератак зростає, а їх наслідки можуть бути катастрофічними. Кіберзлочинці використовують різноманітні методи та технології, щоб отримати доступ до конфіденційної інформації, зламати системи управління та порушити роботу веб-сайтів. Україна не є винятком і також стала мішенню для кібератак з боку інших держав та кримінальних груп.

Що таке кібератака? Які види кібератак існують? Хто здійснює кібератаки? Які наслідки можуть бути від кібератак? Як захистити себе від кібератак? Ці питання стають дедалі більш актуальними, оскільки загроза кібератак стає все більш реальною. З появою нових технологій з'являються нові способи злому, тому необхідно постійно вдосконалювати заходи кібербезпеки, щоб захистити себе, свої дані, свої пристрої та свої бізнеси.

Кібератака - це злочин, який здійснюється через мережу Інтернет або інші електронні засоби з метою отримання конфіденційної інформації, злому системи управління або веб-сайту, а також з метою завдання шкоди компанії, установі або окремій людині.

Кібератаки можуть бути здійснювані різними особами - від зловмисників-одиначок до великих кримінальних груп та державних структур. Однією з найбільш відомих кібератак, яка здійснювалась державою, є кібератака на енергосистему України в грудні 2015 року, що призвела до відключення електроенергії в певних районах країни.

Також під час повномасштабного вторгнення відбувались масовані кібератаки різних типів і видів на всі види інфраструктури нашої держави (Рисунок 1.1).

Рисунок 1.1 Кібератаки, за перші чотири місяці повномасштабного вторгнення [1]

Наслідки кібератак можуть бути дуже серйозними - від втрати конфіденційної інформації та порушення роботи компанії до фінансових збитків та загрози для життя та здоров'я людей. Тому дуже важливо захистити свої дані та системи від кібератак.

Особливо важливою стала кібербезпека в умовах пандемії COVID-19, коли більшість компаній та установ перейшли на дистанційну роботу. Зловмисники використовують цю ситуацію, щоб проводити кібератаки на працівників, які працюють з власних домівок, та зламувати системи, що забезпечують роботу цих компаній та установ. [17]

Тому вирішення проблеми кібербезпеки є надзвичайно важливим завданням для української держави та всього світу. Необхідно підвищувати рівень кібербезпеки на всіх рівнях - від простих користувачів до великих корпорацій та урядів. Тільки так можна зменшити кількість кібератак та забезпечити безпеку віртуального простору.

1.2 Огляд теорії ігор

Теорія ігор - це галузь математики, яка вивчає прийняття рішень у ситуаціях, де результат залежить від дій не однієї, а кількох сторін. Основні поняття в теорії ігор включають гру, рішення, виграш, рівновагу та домінування.

Гра - це ситуація, в якій кілька сторін взаємодіють між собою і приймають рішення. Гра може мати різні форми: вона може бути послідовністю рішень, діалогом, конкуренцією, або комбінацією цих елементів. Головним елементом гри є конфлікт між сторонами, який потребує вирішення. [4]

Рішення - це дії, які сторони вибирають в грі. Рішення можуть бути проактивними, реактивними або змішаними. Проактивні рішення - це дії, які сторона приймає відповідно до своїх цілей і стратегії. Реактивні рішення - це дії, які сторона приймає відповідно до дій інших сторін. Змішані рішення - це дії, які сторона приймає з використанням випадкових або інших внутрішніх факторів. Важливим аспектом рішень є їх взаємодія з іншими сторонами та їх реакції на рішення інших сторін. [4]

Виграш - це результат гри для кожної сторони. Виграш може бути визначений як абсолютна величина, або як відношення до виграшу іншої сторони. Виграш залежить від рішень, які сторони приймають, і може бути різним в різних ситуаціях. [4]

Рівновага - це стан, в якому ні одна сторона не може односторонньо покращити свій виграш шляхом зміни свого рішення. Рівновага може бути стратегічною, динамічною або змішаною. Стратегічна рівновага відображає стан, в якому жодна сторона не може змінити своє рішення, не знижуючи свій виграш, а динамічна рівновага відображає стан, в якому сторони приймають послідовно рішення, а відхилення від цього порядку призводить до зниження

виграшу. Змішана рівновага відображає стан, в якому сторони приймають різні рішення з певною ймовірністю. [4]

Домінування - це ситуація, в якій одне рішення краще для сторони, незалежно від рішення іншої сторони. Домінування може бути стратегічним, динамічним або змішаним. Стратегічне домінування відображає стан, в якому одне рішення краще для сторони в будь-якій ситуації, динамічне домінування відображає стан, в якому одне рішення краще для сторони в будь-якому рішенні, що повторюється, а змішане домінування відображає стан, в якому одне рішення краще для сторони в середньому. [4]

Теорія ігор застосовується у багатьох галузях, таких як економіка, політика, менеджмент, соціологія та інші. Вона допомагає вирішувати різноманітні проблеми, пов'язані з взаємодією між сторонами, і забезпечує раціональне прийняття рішень. Наприклад, у економіці теорія ігор застосовується для аналізу конкуренції на ринку, прийняття рішень про інвестування та ризиковий менеджмент. У політиці вона допомагає вивчити стратегії виборів та взаємодію між державами. У менеджменті теорія ігор використовується для аналізу конфліктів між менеджерами та прийняття рішень про розподіл ресурсів. [19]

1.2.1 Основні поняття теорії ігор та їх застосування

Теорія ігор має багато методів, які можуть бути застосовані в кібербезпеці для аналізу, захисту та виявлення загроз. Ось детальніше про кілька з них [5]:

1. Модель нуль-сумової гри: Цей метод використовується для аналізу стратегій конфліктних ситуацій, де одна сторона намагається проникнути в систему, а інша сторона намагається захистити її. За допомогою

моделей нуль-сумових ігор можна аналізувати можливі варіанти дій атакуючих та обороняючих сторін, їх виграші та втрати, що допомагає приймати ефективні рішення щодо кібербезпеки.

2. Аналіз ризику та прийняття рішень: Теорія ігор допомагає в оцінці ризику та прийнятті рішень в кібербезпеці. Вона може використовуватися для моделювання різних сценаріїв атак, оцінки ймовірності їх виникнення та визначення найбільш оптимальних стратегій захисту. Особливо важливо визначити ризики, пов'язані з можливими атаками, щоб забезпечити максимальний рівень захисту.

3. Теорія розв'язування ігор: Цей метод використовується для розробки оптимальних стратегій захисту. Вона дозволяє аналізувати ігри з неповною інформацією, де сторони можуть приховувати свої дії та намагатися виявити дії опонента. Цей підхід допомагає розробляти стратегії, які забезпечують максимальний рівень безпеки в умовах невизначеності. Зокрема, важливо враховувати можливість використання нових технологій, які можуть створити нові загрози та вимагати нові методи захисту.

4. Аналіз гри на найкоротші шляхи (game-theoretic analysis of shortest path problems): Цей метод використовується для виявлення потенційних шляхів атаки та визначення оптимальних маршрутів для захисту мережі. Він базується на ідеї знаходження найкоротшого шляху в грі, де гравці вибирають маршрути залежно від своїх цілей та обмежень.

Ці методи теорії ігор допомагають кібербезпековим фахівцям аналізувати загрози, виявляти слабкі місця в системах та розробляти оптимальні стратегії захисту. Наприклад, важливо враховувати те, що кіберзлочинці постійно шукають нові способи проникнення в системи та викрадення даних, тому необхідно постійно підвищувати рівень кібербезпеки та вдосконалювати методи захисту. Також важливо враховувати те, що загрози можуть змінюватися з часом, тому необхідно постійно моніторити нові тренди та ризики та вчасно реагувати на них.

Теорія ігор корисна тим, що вона моделює поведінку кожного гравця, його стратегії і фіксує взаємодію між гравцями-суперниками.

У цій "ігровій" взаємодії протиборчих сил (чи то команд, чи то окремих осіб) кожна сила зацікавлена у виграші, або навпаки, в уникненні програшу. Взагалі, кібербезпека є незбалансованою грою, оскільки захисники мережі завжди знаходяться в невигідному становищі. Незважаючи на всі технології кібербезпеки, вони не знають, коли, де і як зловмисники завдадуть удару. На інформації наведеній вище, можна помітити, як кібербезпека пов’язана з теорією ігор, але розглянемо це ще на декількох прикладах.

Можна виділити дві широкі категорії застосування теорії ігор у сфері кібербезпеки. Перша категорія - аналіз захисту від кібератак. Друга категорія - оцінка кібербезпеки. Моделюючи поведінку захисту у вигляді ігор, можна передбачити дії кібератакувальника в аналізі кібератакизахисту. Він також аналізує можливі стани рівноваги між атакою та захистом. Стратегії контрзахисту можуть бути визначені в ідеалі на основі стану рівноваги [11].

Рівноважний стан кібератаки-захисту може бути ретельно вивчений. Прогнозування стратегій атаки та захисту може бути використано для раціоналізації кібернетичної безпеки та оцінки. Завдяки кількісним аспектам ігрового аналізу безпека та надійність розглядається як кількісна оцінка, яка дає обчислення кібернетичної безпеки та надійності[11].

Кібербезпека приймає некооперативну динамічну ігрову модель. Стратегії зловмисників при кібератаках не є статичною, і для досягнення ідеального ефекту дуже важливим є аналіз динамічної моделі, оскільки динамічні моделі дуже близькі до реальних проблем кібербезпеки в реальному часі. А для аналізу кіберзахисту використовується неповна інформаційно-ігрова модель, яка показано в Таблиці 1.1. Таким чином, можна сказати, що теорія ігор є незамінним інструментом в сфері кібербезпеки, який допомагає вивчати характер кіберінцидентів, передбачати дії зловмисників та розробляти ефективні стратегії захисту[12].

Таблиця 1.1 Класифікація методів теорії ігор у сфері кібернетичної безпеки.[12]

<table>
<tr><td colspan="3">Ігрові моделі</td><td>Питання застосування та безпеки</td></tr>
<tr><td colspan="2">Кооперативні ігрові моделі</td><td>Статистичні ігрові моделі</td><td>Мобільні бездротові ad hoc моделі</td></tr>
<tr><td rowspan="5">Некооперативні ігрові моделі</td><td colspan="2" rowspan="2">Статистичні ігрові моделі</td><td>Виявлення несанкціонованого проникнення</td></tr>
<tr><td>Оптимізація безпеки</td></tr>
<tr><td rowspan="3">Динамічні ігрові моделі</td><td rowspan="2">Повні інформаційні ігрові моделі</td><td>Механізм безпекового стимулювання</td></tr>
<tr><td>Оптимізація безпеки</td></tr>
<tr><td>Не повні інформаційні ігрові моделі</td><td>Аналіз кібератаки-захист</td></tr>
</table>

1.2.2 Рішення в умовах конфлікту: стратегії та небезпечні ситуації в кібербезпеці

Кібербезпека стає все більш актуальною темою в сучасному світі, оскільки комп'ютери, мобільні пристрої та Інтернет мають величезний вплив на наше повсякденне життя, бізнес-процеси та навіть національну безпеку. Кіберконфлікти стають все більш поширеними, і відповідно до цього зростає необхідність у розумінні стратегій та рішень для управління цими конфліктами.

Однією з ключових аспектів рішень в умовах конфлікту в кібербезпеці є розробка ефективної стратегії. Стратегія в кібербезпеці повинна передбачати заходи для запобігання атакам, виявлення і реагування на інциденти, а також відновлення після інциденту. Одним з ключових принципів стратегії в

кібербезпеці є принцип превентивної оборони, що означає прийняття заходів заздалегідь для запобігання можливим атакам [13].

Стратегії в кібербезпеці можуть включати в себе різноманітні елементи, такі як:

1. Розробка політики кібербезпеки: це включає визначення цілей, принципів та стандартів безпеки, які повинні бути виконані. Також необхідно враховувати правові, регуляторні та етичні аспекти кібербезпеки.

2. Постановка захисних механізмів: це включає в себе розробку і впровадження технічних заходів безпеки, таких як вогнепрогаління, антивірусне програмне забезпечення, шифрування даних тощо.

3. Розробка політики управління доступом: це означає визначення правил і обмежень щодо доступу до інформації і ресурсів системи залежно від рівня довіри та привілеїв користувачів.

4. Навчання та свідомість персоналу: розуміння принципів кібербезпеки та відповідальності кожного співробітника є важливим елементом стратегії. Персонал повинен бути навчений виявляти потенційні загрози та дотримуватися безпечних практик використання комп'ютерів та мереж.

Небезпечні ситуації в кібербезпеці можуть виникати з різних джерел. Ось деякі з них:

1. Хакерські атаки: це можуть бути спроби несанкціонованого доступу до системи, викрадення чутливої інформації, пошкодження даних або розповсюдження шкідливого програмного забезпечення.

2. Соціальний інжиніринг: це метод маніпулювання людьми з метою отримання доступу до конфіденційної інформації або виконання шкідливих дій.

3. Фішинг: це спосіб шахрайства, при якому зловмисник використовує підроблені електронні повідомлення або веб-сайти, щоб залучити користувачів надати особисті дані, такі як паролі або номери кредитних карток.

4. Внутрішня загроза: це можуть бути дії зловмисників, які мають легальний доступ до системи, наприклад, співробітники організації, які зловживають своїми привілеями.

Для ефективного управління небезпечними ситуаціями в кібербезпеці необхідно враховувати такі аспекти, як [13]:

1. Визначення можливих загроз та їх оцінка: це допомагає підготуватися до можливих атак та виявляти нові загрози.

2. Розробка та вдосконалення планів реагування на інциденти: це включає в себе розробку процедур виявлення та ізоляції загроз, відновлення систем та процесів після атаки, а також аналіз причин і наслідків інциденту.

3. Постійне оновлення захисних механізмів: оскільки загрози в кіберпросторі постійно еволюціонують, важливо мати захисні механізми, які відповідають найновішим загрозам та вимогам безпеки.

4. Навчання персоналу: постійне навчання з питань кібербезпеки допомагає підтримувати свідомість про потенційні загрози та використовувати безпечні практики.

Усвідомлення стратегій та небезпечних ситуацій в кібербезпеці є ключовим для ефективного захисту інформації та систем в умовах сучасного кіберпростору. Постійна підготовка, вдосконалення стратегій та виявлення нових загроз допомагають зменшити ризик і забезпечити надійний рівень кібербезпеки. Окрім того, важливо пам'ятати про те, що кібербезпека є процесом, який потребує постійного вдосконалення та оновлення, оскільки загрози в кіберпросторі постійно зростають та еволюціонують.

1.3 Кібератаки: типи та характеристики

Кібератаки — це зловмисний процес, який використовує комп'ютерні системи або мережі для злому, пошкодження або незаконного доступу до інформації. Існує безліч типів кібератак, кожен з яких має свої характеристики і способи реалізації. Ось деякі з найпоширеніших типів кібератак та їх характеристики[16, 18]:

1. Фішинг: це атака, в якій зловмисник виступає в ролі довіреної сторони, зазвичай шляхом підробки електронної пошти або веб-сторінок, щоб отримати конфіденційну інформацію, таку як паролі, номери кредитних карток тощо. Фішинг може бути спрямований на окремих користувачів або на цілі організації.
2. Віруси і черв'яки: це шкідливі програми, які можуть самостійно розповсюджуватися та пошкоджувати комп'ютерні системи. Вони можуть знищувати дані, перешкоджати роботі системи або використовувати комп'ютери для спаму чи атак на інші системи. Черв'яки можуть розповсюджуватися через мережу без участі користувача, тоді як віруси поширюються через забраковані файли, електронні листи тощо.
3. Деніал-сервіс (DDoS) атаки: це атаки, які спрямовані на переповнення мережі або системи запитами, що перевантажують їх і перешкоджають нормальному функціонуванню. Це може призводити до недоступності веб-сайтів або мережевих послуг. Для проведення DDoS-атак зловмисники можуть використовувати ботнети або інші комп'ютерні системи, які були заражені їхніми програмами.
4. Вторгнення: це процес незаконного проникнення в комп'ютерну систему або мережу з метою отримання несанкціонованого доступу до інформації або контролю над системою. Зловмисник може використовувати різні методи, такі як підбір паролів, використання вразливостей програмного

забезпечення або викрадення автентифікаційних даних. Це може бути спрямовано на окремих користувачів або на організації.

5. Ретельна атака (advanced persistent threat, APT): це складна та тривала атака, яка зазвичай виконується державними або спонсорованими групами. Вони використовують різні методи, включаючи соціальний інжиніринг, враження вразливостей, шпигунство та інші техніки, щоб отримати доступ до важливої інформації. APT-атаки можуть тривати місяці або навіть роки, і їхні цілі можуть бути дуже різними, від відомостей про користувачів до важливих технологічних розробок.

6. Витік інформації: це незаконне витікання конфіденційної або чутливої інформації. Це може статися через вразливості в системах безпеки, недбалість персоналу, викрадення фізичних пристроїв або інші методи. Витік інформації може статися через внутрішній або зовнішній фактори.

7. Розширення прав доступу: це атаки, які спрямовані на надання зловмиснику вищих привілеїв або прав доступу в системі. Вони можуть використовувати вразливості в програмному забезпеченні або використовувати соціальний інжиніринг для отримання необхідних даних. Розширення прав доступу може бути спрямоване на окремих користувачів або на організації.

Це лише кілька типів кібератак, існує багато інших варіацій та комбінацій цих атак. Зловмисники постійно розвивають нові методи та техніки, тому важливо підтримувати свої системи оновленими та захищеними для запобігання кібератакам. Щоб підтримувати високий рівень безпеки, користувачі можуть використовувати різні методи захисту, такі як антивірусні програми, файрволи, шифрування трафіку та інші техніки. Також важливо забезпечувати надійний пароль та використовувати двохфакторну автентифікацію, щоб ускладнити завдання зловмисникам.

1.3.1 Аналіз загроз та вразливостей, що використовуються в кібератаках

Останнім часом кількість кібератак на комп'ютерні системи та мережі невпинно збільшується, а вразливості стають все більшими і різноманітними. За даними статистики, у 2019 році було зафіксовано понад 20 разів більше попереджень про загальні вразливості та експлойти (CVE), ніж у 1999 році. З метою боротьби з цими загрозами, сучасні організації використовують десятки елементів управління, які потребують постійної тонкої настройки, щоб охопити весь спектр потенційних загроз. Однак, відділи безпеки вже не можуть залатати всі можливі проломи або налаштувати всі елементи керування вручну [10].

На жаль, старі погрози повертаються у новому вигляді, наділені більшою силою та досконалістю. Одним з прикладів може бути відома шкідлива програма Emotet. Вперше виявлена у 2014 році, Emotet адаптувалася до нових умов та налаштувань зловмисників, щоб уникнути виявлення та видалення. У 2018 та 2019 роках вона стала найактивнішою шкідливою загрозою, а потім зникла з радарів. Останнє її відродження відбулося в липні 2020 року, коли ботнети Emotet почали надсилати електронні листи зі шкідливими URL-адресами або вкладеннями [10].

Аналіз загроз та вразливостей, які використовуються в кібератаках, є важливим елементом для збереження безпеки та захисту від зловмисників. Кібератаки можуть мати різні форми та мету, але їх завдання все одне - завдати шкоди комп'ютерній системі або мережі, отримати незаконний доступ до конфіденційної інформації або скомпрометувати систему, щоб отримати підвищені привілеї [17].

Щоб зменшити ризики кібератак, важливо проводити індивідуальний аналіз загроз та вразливостей. Кожна організація має свої особливості та ризики, тому потрібно проводити дослідження кожної з них окремо. Після

ідентифікації загроз та вразливостей, організації можуть прийняти заходи для зниження ризиків кібератак [17].

Деякі загрози та вразливості, які використовуються в кібератаках, включають використання слабких паролів або недостатньої аутентифікації користувачів, використання застарілих програм або операційних систем з відомими вразливостями, недостатній захист мережі, такий як відсутність файрволів або недостатня мережева сегрегація, недостатній захист даних, таких як відсутність шифрування або недостатня фізична безпека та соціальний інжиніринг, який використовується для обману користувачів та отримання конфіденційної інформації[.

Щоб підтримувати високий рівень безпеки, користувачі можуть використовувати різні методи захисту, такі як антивірусні програми, файрволи, шифрування трафіку та інші техніки. Також важливо забезпечувати надійний пароль та використовувати двофакторну автентифікацію, щоб ускладнити завдання зловмисникам.

Зловмисники постійно розвивають нові методи та техніки кібератак, тому важливо підтримувати свої системи оновленими та захищеними. Для досягнення цієї мети, організації повинні регулярно оновлювати програмне забезпечення та оперативні системи, щоб захистити свої системи від відомих вразливостей. Організації повинні також забезпечити належний захист мережі та даних, щоб запобігти несанкціонованому доступу до конфіденційної інформації.

Загальна безпека кіберпростору залежить від того, наскільки ефективно організації та користувачі можуть захистити свої системи від кібератак. Тому важливо підтримувати постійне дослідження загроз та вразливостей та вживати заходів, щоб запобігати кібератакам.

1.3.2 Оцінка впливу кібератак на різні галузі та сектори

Кібератаки можуть мати значний вплив на різні галузі та сектори, і їх наслідки можуть бути різними залежно від конкретного випадку і рівня захищеності систем. Незабаром ми розглянемо більше галузей, на які можуть впливати кібератаки, але перед цим, нагадаємо, що оцінка впливу кібератак на різні галузі полягає в оцінці потенційного ризику, який може виникнути у випадку успішної атаки.

Ось огляд впливу кібератак на деякі галузі та сектори [1]:

1. Фінансовий сектор: Кібератаки на банки, фінансові установи та платіжні системи можуть призвести до фінансових втрат, порушення конфіденційності клієнтської інформації, крадіжки особистих даних та порушення довіри в систему фінансових послуг.

2. Енергетичний сектор: Кібератаки на енергетичні системи можуть призвести до перебоїв у постачанні електроенергії, відключення роботи енергетичних мереж, порушення нормальної експлуатації та потенційних загроз безпеці.

3. Транспортний сектор: Кібератаки на транспортну інфраструктуру, таку як авіакомпанії, залізниці, морські порти або автомобільні системи, можуть призвести до перебоїв у роботі, відмови систем керування, порушення графіків та вплинути на безпеку пасажирів.

4. Медичний сектор: Кібератаки на медичні установи можуть призвести до порушення роботи інформаційних систем, крадіжки конфіденційних медичних даних, переривання надання медичних послуг та загрози безпеці пацієнтів.

5. Виробничі компанії: Кібератаки на виробничі підприємства можуть призвести до зупинки виробництва, крадіжки комерційних та технічних даних, пошкодження обладнання, втрати конкурентної переваги та впливу на господарську діяльність.

6. Інформаційна та комунікаційна галузь: Кібератаки на інформаційні технології, мережі зв'язку та інтернет-провайдерів можуть призвести до відключення послуг зв'язку, порушення доступу до інтернету, крадіжки даних, пошкодження репутації та порушення приватності користувачів.

Ще одна галузь, яка може постраждати від кібератак, - це сфера міжнародних відносин та дипломатії. Кібератаки можуть вплинути на діяльність державних органів, дипломатичних місій, консульських служб та інших установ, які займаються міжнародними відносинами (Рисунок 1.2).

Рисунок 1.2 Основні сектори які зазнали ворожих атак за повномасштабне вторгнення. [1]

Важливо зазначити, що кожна організація повинна провести власну оцінку ризику, щоб визначити конкретні наслідки, які можуть статися у їхньому випадку і розробити ефективні стратегії захисту. Також, важливо пам'ятати, що кібербезпека - це процес, а не одноразова подія, і вимагає постійної уваги та підтримки. Регулярне оновлення програмного забезпечення, зміна паролів, резервне копіювання даних та інші запобіжні заходи можуть значно зменшити ризики від кібератак.

1.4 Висновки до розділу 1

У даному розділі ми розібралися, що таке кібератаки та які види їх існує. Також дослідили вплив кібератак на державу та різні галузі і сектори. Було визначено поняття теорії ігор та основні принципи, що лежать в її основі. Детально розібрано основні методи захисту та протидії від кібератак, а також виявлено, що теоретико-ігровий підхід може бути дуже корисним у захисті комп'ютерних мереж. На основі наших досліджень можна зробити висновок, що кібербезпека є дуже важливою сферою в сучасному світі, тому її необхідно приділяти велику увагу та розвивати її засобами як науки, так і практики.

РОЗДІЛ 2

МЕТОДИ ВИКОРИСТАННЯ ТЕОРІЇ ІГОР ПРИ ВІДБИТТІ КІБЕРАТАК

2.1 Використання теорії ігор для аналізу кібератак

Різні підходи можуть бути використані для класифікації застосування теорії ігор для розв’язання проблем в області безпеки. Одна з перших робіт, у якій проблема розглядалась системно, досліджувала проблему виявлення вторгнення у вигляді гри у розширеній формі. Вона описує дві постановки: кооперативну гру системи виявлення, в якій сенсори утворюють коаліції для підвищення ймовірності виявлення вторгнення, та скінчену некооперативну гру атакуючого та системи захисту.

Напрямки дослідження можуть бути класифіковані за предметною областю застосування. До виділених областей можуть належати [23]:

1. системи виявлення вторгнень;
2. прийняття рішень після виявлення атаки (вторгнення);
3. моделювання зловмисної діяльності у мережах, де мережі розглядаються як будь-яка складна мережева система;
4. кількісна оцінка ризиків, включаючи інвестиційні ігри;
5. алгоритми розподілу ресурсів та побудова стійких протоколів взаємодії;
6. приватність, довіра та зручність використання.

Цей підхід має очевидні переваги та практичну орієнтованість. Серед недоліків можна відзначити ad-hoc схему та те, що різні області застосування можуть використовувати одні й ті самі ігрові моделі. Інші огляди можуть будувати класифікацію на основі моделей теорії ігор, які використовуються для розв’язання проблем безпеки (Таблиця 2.1). Однак, не слід забувати, що застосування теорії ігор для розв’язання проблем в області безпеки - це

важливе та цікаве дослідження, яке може принести багато користі для нашого світу [12].

Таблиця 2.1 Матриця вибору методів в кіберзпеці [12]

Інформованість	Досконала	Недосконала	
	Динамічна постановка	Статична постановка	Динамічна постановка
Повна	Гра виявлення вторгнення у постановці матричної гри двох учасників Штакельберга (що означає наявність лідера який приймає рішення першим, інший гравець будує свою стратегію знаючи цю обставину).	Ігри інвестування у безпеку та розподілу ресурсів у матричній постановці. Гра інформаційного протиборства двох гравців. Оцінка ризиків у мережах для гри двох гравців з нульовою сумою.	Стохастичні ігри. Проблема визначення оптимальної стратегії адміністратора для балансування ризиків в мережі за умов атаки. Обчислення оптимальної протидії. Марковські ігри. Використання Q-навчання у ситуації невідомою перехідної матриці.
Неповна	Виявлення вторгнення в Ad hoc мережі. Формулювання у вигляді сигнальної гри двох гравців. Гра за умов невідомих функцій виграшу гравців. Навчання за різними схемами. Багатокрокові Байєсівські ігри у безпровідних мережах для моделювання атак глушіння.	Інформаційна гра безпеки між експертом та декількома “наївними” агентами за умов обмеженості інформації про ризики інших. Байєсівські ігри двох гравців.	Багатокрокова Байєсівська гра двох гравців у якій кожний гравець намагається покращити своє знання про тип свого суперника.

2.1.1 Застосування методів теорії ігор для моделювання кібератак

При моделюванні різних методів кібератак на основі теорії ігор можна виділити кілька основних кроків (Рисунок 2.1):

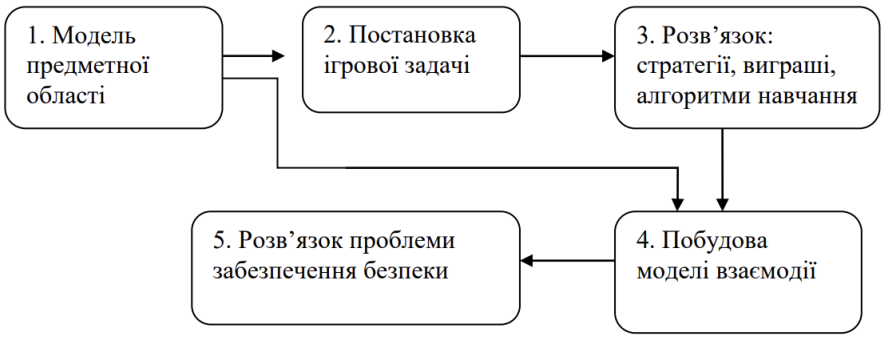


Рисунок 2.1 Схема застосування ігрового підходу [20, 21]

1. Моделювання предметної області є першим етапом дослідження будь-якого процесу. Цей етап починається з побудови моделі, що належить до різних класів, таких як динамічні системи (неперервні, дискретні), що описуються диференціальними рівняннями (з запізненнями, імпульсним керуванням), лінійні стаціонарні системи, мульти-агентні системи тощо. Після побудови моделі, вибирається інструментарій аналізу.

2. Постановка ігрової задачі - другий етап. На цьому етапі визначаються всі ігрові характеристики: гравці, стратегії, інформованість та виграші. Ставиться задача ігрового аналізу, яка може полягати у формалізації ігрової моделі, пошуку рівноваги, визначенні найкращих стратегій та розробці оптимальних правил, за яких результат гри буде відповідати заданим критеріям.

3. Розв'язок: стратегії, виграші та алгоритми навчання - третій етап. На цьому етапі розв'язується задача ігрового аналізу, включаючи пошук рівноваги, розв'язання гри (тобто обчислення найкращої поведінки гравців у кожній точці), визначення алгоритмів навчання, які наближаються до точки рівноваги за умов обмеженої інформованості. Пошук алгоритмів навчання особливо важливий з огляду на обмеженість інформованості у реальних системах та розподіленість систем захисту.

4. Побудова моделі взаємодії - четвертий етап. На базі отриманих стратегій поведінки гравців та з використанням моделей предметної області

будується модель конфлікту з метою визначення важливих характеристик, наприклад обчислення числових параметрів захищеності (вразливості) існуючої системи протидії. На цьому етапі виникає можливість вимірювання параметрів якості системи захисту або вразливості до певного типу атак.

5. Розв'язок проблеми забезпечення безпеки - п'ятий та останній етап. Обчислення характеристик вразливості до тих чи інших атак дає змогу поставити проблему про забезпечення безпеки системи, як задачу теорії ігор: яким параметрам має задовольняти система захисту, щоб гарантувати певний виграш за умов атаки. При розв'язанні цієї задачі використовуються різні методи та алгоритми, що дозволяють збільшити рівень захисту системи від кібератак.

Важливо зазначити, що теорія ігор має декілька ключових переваг, що сприяють її успішному використанню в сфері безпеки.

По-перше, вона базується на математичному апараті. Сучасні рішення з безпеки використовують евристики, запропоновані спеціалістами на основі власного досвіду. Теорія ігор дозволяє залучати для прийняття рішень розвинений математичний апарат, який призначений для моделювання ситуацій прийняття рішень агентами за умов конфлікту і невизначеності. Застосування теорії ігор дозволяє розглядати кожну ситуацію з більш широкої перспективи та проводити більш об'єктивний аналіз можливих наслідків[24].

Друге, теорія ігор гарантує результат. Якщо захисний механізм побудований на основі аналітично розв'язаної гри і виконуються припущення (за яких гра була визначена), то стратегія гарантує певний рівень безпеки за будь-яких дій інших учасників. Таким чином, використання теорії ігор дозволяє забезпечити стійкість до будь-яких атак і підвищити ефективність захисних механізмів[24].

Третє, ігрові моделі дозволяють створити систему взаємодії, де кожен гравець максимізує свій виграш і, тим самим, сприяє загальній системі захисту. Розподілені захисні механізми є більш ефективними, ніж централізоване керування, оскільки останнє має багато недоліків і часто стає

ціллю атак. Ігрові моделі дозволяють створити систему взаємодії, де кожен гравець максимізує свій виграш і, тим самим, сприяє загальній системі захисту. Інший перспективний напрямок, який може бути корисний у цій області – агентно-орієнтовані системи[24].

Нарешті, розробка оптимальних механізмів є важливою складовою теорії ігор. Вона досліджує задачі створення правил гри, за яких гравці ведуть себе потрібним чином. В рамках цього підходу можливе створення протоколів, які заохочують кооперацію між користувачами та дозволяють їм об’єднуватися для відбиття атаки. Застосування теорії ігор дозволяє розглядати більш широкий спектр можливих рішень та їх наслідків, що полегшує прийняття важливих рішень в галузі безпеки.

2.1.2 Визначення стратегій захисту та протидії кібератакам

Стратегії боротьби і уникнення кібератак на основі теорії ігор використовують концепції та методи з теорії ігор для аналізу і прогнозування поведінки зловмисників та розробки ефективних стратегій захисту. Мета полягає у тому, щоб розглядати кібербезпеку як гру між атакуючою стороною (зловмисником) і захисною стороною (жертвою атаки або оборонюючоюся організацією), де кожна сторона приймає рішення, враховуючи можливі дії та відповіді противника. Основні стратегії боротьби і уникнення кібератак на основі теорії ігор включають[23]:

1. Стратегія максимального захисту (Fortress Strategy)(Рисунок 2.2.): Ця стратегія полягає в тому, щоб зосередити всі зусилля на забезпеченні найвищого рівня безпеки для системи або мережі. Це може включати в себе встановлення сильних брандмауерів, використання сучасного програмного забезпечення для виявлення вторгнень та шифрування всіх даних. Мета полягає в тому, щоб створити такі умови, в яких зловмисники відмовляться

від атаки через високі витрати або низьку ймовірність успіху.

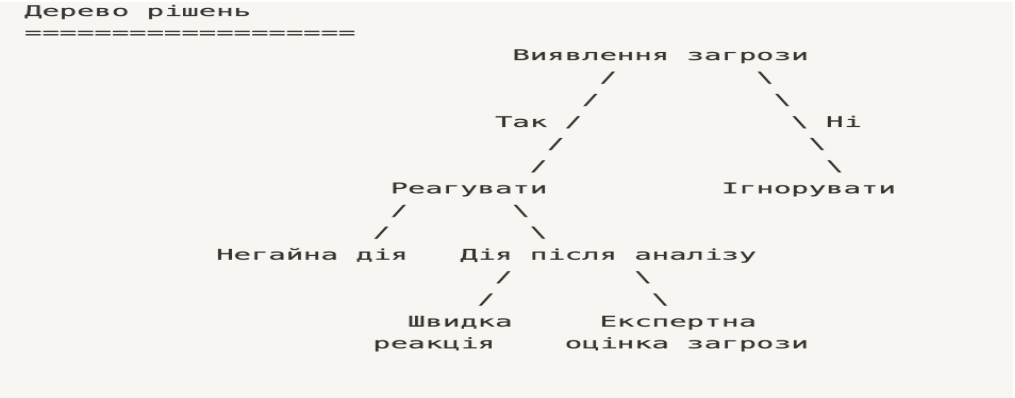


Рисунок 2.2 Дерево рішень для стратегії максимального захисту

2. Стратегія обмеження шкоди (Damage Limitation Strategy)(Рисунок 2.3): Ця стратегія передбачає, що втілення повного захисту неможливе, тому основна мета полягає в обмеженні шкоди в разі атаки. Це може бути досягнуто шляхом впровадження резервних копій даних, виявлення та відключення компрометованих систем, швидкого відновлення після інциденту та мінімізації впливу на бізнес-процеси.

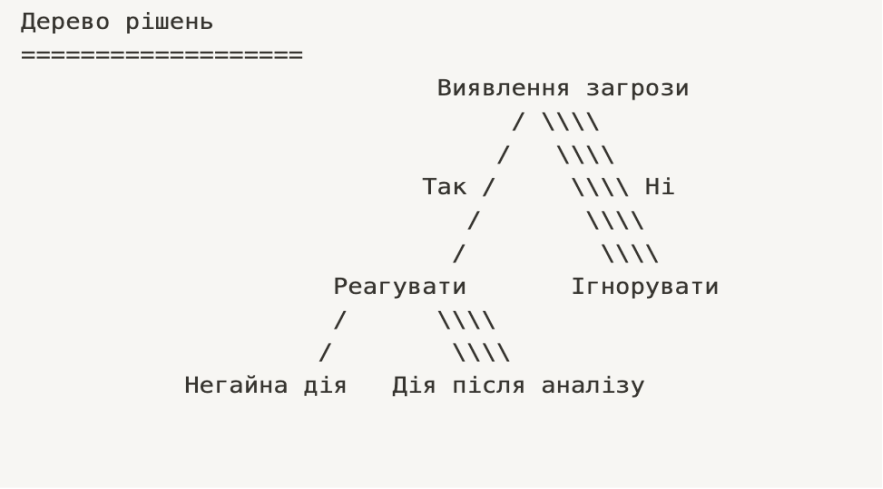


Рисунок 2.3 Дерево рішень для стратегії обмеження шкоди

Якщо загрозу було виявлено, можна вибрати між реагуванням негайно, тобто здійсненням дії без подальшого аналізу, або дією після аналізу, коли спочатку проводиться оцінка загрози, а вже потім здійснюється реагування.

При реагуванні негайно можуть бути застосовані автоматичні заходи захисту, наприклад, блокування IP-адрес. А дія після аналізу має бути забезпечена експертами, які проводять оцінку загрози та вибір методів захисту. При цьому важливо забезпечити максимальну швидкість реагування на загрозу, щоб зменшити шкоду від кібератак і збільшити ефективність захисту системи.

3. Стратегія детекції та реагування (Detection and Response Strategy) (Рисунок 2.4): Ця стратегія зосереджена на ранньому виявленні атаки та швидкому реагуванні на неї. Вона включає в себе використання систем моніторингу, аналізу журналів подій та інших методів для виявлення незвичайної активності та аномалій. Після виявлення атаки захисна сторона має розроблені плани реагування та відновлення для ефективного управління інцидентом.

Рисунок 2.4 Дерево рішень для стратегії детекції та реагування

4. Стратегія психологічного тиску (Psychological Pressure Strategy): Ця стратегія передбачає використання психологічних методів для відволікання атакуючої сторони або створення непередбачуваних ситуацій. Наприклад, можуть бути використані фальшиві слабкі місця або підроблені дані, щоб збентежити зловмисників та змусити їх зробити помилки, або залучити увагу до інших систем, що відволікають атаки від головної цілі.

Ці стратегії використовуються в контексті теорії ігор для аналізу поведінки сторін, розрахунку можливих варіантів та прийняття рішень.

Організація може розробити більш ефективні стратегії захисту своїх систем та даних в кіберпросторі, враховуючи можливі дії та відповіді противника. Наприклад, можна виявити пробіли в безпеці із використанням інформації про діяльність зловмисників та використовувати цю інформацію для покращення захисту.

Також можна розглянути можливість використання штучного інтелекту для аналізу та прогнозування поведінки зловмисників та виявлення потенційних загроз. Крім того, можна розглянути використання технологій блокчейн для забезпечення безпеки даних та підвищення стійкості до кібератак.

2.2 Проблеми та перспективи данного підходу

Застосування ігрового підходу до розв’язання проблем безпеки має багато варіантів залежно від обраної схеми ігрової взаємодії користувачів. Наприклад, при моделюванні ігор між одним нападником і системою захисту можуть використовуватись ігри двох учасників. Якщо ж ситуація розгортається у часі, можна використовувати динамічну постановку. Важливо також враховувати рівень інформованості учасників, що визначає використання ігор з досконалою або недосконалою, повною або неповною інформованістю.

Однак сучасні підходи мають свої недоліки, які потребують подальшого дослідження:

1. Найбільш дослідженими є ігри двох учасників, тому при розгляді проблем безпеки часто намагаються звести задачу до цього типу. Але це може призвести до втрати реалістичності при моделюванні більш складних процесів.

2. Матричні (статичні) ігри, які використовують через їх простоту, малореалістичні. Майже всі реальні процеси змінюються у часі і вимагають відповідного моделювання, що може зробити матричні ігри непридатними для дослідження більш складних систем.

3. При моделюванні стратегій, як правило, фіксується певна скінченна кількість станів, у яких може знаходитись гра. Відповідна скінчена гра може бути розв’язана, але на практиці кількість таких станів нескінченна, що потребує додаткових досліджень. Таким чином, підхід із моделюванням ігор потребує подальшого вдосконалення, щоб відображати реальність складних систем безпеки.

Майбутні напрямки досліджень.

У сучасному світі безпека є однією з найбільш актуальних проблем. З цією метою, сьогодні відбуваються дослідження в області кібербезпеки. Виділимо найбільш перспективні напрямки досліджень, у яких буде розвиватись теоретико-ігровий підхід.

1. Соціальні мережі. Останнім часом соціальні мережі, такі як Фейсбук і Твіттер, стали найпоширенішим засобом комунікації. Це призвело до того, що соцмережі накопичили гігантські обсяги приватних даних, які можуть бути об’єктом атаки. Іншою ціллю можуть бути фірми, які перенесли свою діяльність у Фейсбук. Вже спостерігаються скоординовані атаки з негативними відгуками та зниженням рейтингу. Тому, дослідники працюють над розвитком нових методів захисту від цих загроз [18].

2. Хмарні обчислення. Хмарні обчислення (Cloud computing) це нова парадигма, яка дозволяє отримувати доступ до програмних, обчислювальних та інформаційних ресурсів у вигляді мережевих сервісів. З розвитком та ускладненням хмарних сервісів виникає проблема побудови ефективних алгоритмів забезпечення їх безперешкодної роботи. Користувачі отримують доступ на основі принципу pay-as-you-use до найбільш сучасної інфраструктури не витрачаючи коштів на її створення та підтримку. Провайдери в свою чергу максимізують використання своїх потужностей та

можуть балансувати навантаження через мережі для досягнення рівномірної загрузки. Теорія ігор, яка вже має історію успішного застосування до розв’язання задач маршрутизації, планування, керування потоками даних і перевантаженнями, є головним напрямком аналітичного моделювання хмарних систем [18].

3. Інтернет речей. Це технологія, яка об’єднує в одну мережу всі розумні прилади, що уже в недалекому майбутньому будуть забезпечувати людське життя. За оцінками, понад два мільярди нових приладів буде під’єднано до глобальної мережі у наступні 10 років. Проникнення розумних речей у наше життя стає тотальним і тому і загрози, які при цьому виникають також є тотальними. Вже фіксуються появи вірусів, що здатні брати під свій контроль кавоварки, тостери та інші прилади. Тому, дослідники працюють над розробкою технологій, які будуть забезпечувати безпеку використання розумних речей [18].

4. Блокчейн. Це технологія, на основі якої будуються криптовалюти і деякі нові сервіси. Одною з ключових проблем є забезпечення ефективного та безпечного “майнингу” (тобто обчислення підтвердження нових операцій або одиниць валюти). Теорія ігор моделює процес майнингу як взаємодію автономних агентів, що конкурують за ресурси. Враховуючи сучасну вартість криптовалюти біткоін атака на механізми обчислення може бути надзвичайно прибутковою [18].

Схоплюючи все вищезгадане, можна сказати, що застосування теоретико-ігрового підходу до проблем безпеки, хоча і продовжується два десятиліття, все ще є новим підходом з багатьма нерозв’язаними проблемами. Складність ігор з багатьма учасниками за умов конфлікту і невизначеності стимулює дослідників до створення нових моделей і методів, які допоможуть створити новий, безпечний і ефективний кіберпростір. Розвиток та застосування теорії ігор у вищезгаданих напрямках досліджень є важливим кроком до забезпечення безпеки в цифровому світі.

2.3 Висновки до розділу 2

Застосування теорії ігор у кібербезпеці є новим та перспективним підходом, який може допомогти вирішити проблеми безпеки в цифровому світі. Використання теорії ігор дозволяє моделювати складні процеси та враховувати різні стани та можливі дії учасників конфлікту, що допомагає зрозуміти та передбачити можливі напади та атаки.

Цей підхід вже успішно використовується у дослідженнях соціальних мереж, хмарних обчислень, Інтернету речей та блокчейну. У соціальних мережах, наприклад, використання теорії ігор допомагає вивчати взаємодії між користувачами, що може бути корисним для попередження кібератак та забезпечення безпеки приватних даних. У хмарних обчисленнях, теорія ігор використовується для побудови алгоритмів забезпечення безперешкодної роботи сервісів та балансування навантаження. У Інтернеті речей, теорія ігор допомагає зрозуміти можливі загрози та розробляти технології, які забезпечують безпеку використання розумних речей.

Однак існують недоліки теорії ігор, зокрема, недостатня реалістичність моделей. Це може призвести до неправильних висновків та помилкових дій при захисті від кібератак. Тому важливим є подальший розвиток та вдосконалення теорії ігор, що дозволить створити новий, безпечний та ефективний кіберпростір.

Розвиток та застосування теорії ігор у вищезгаданих напрямках досліджень є важливим кроком до забезпечення безпеки в цифровому світі. Використання теорії ігор може допомогти зменшити ризики кібератак, забезпечити безпеку використання розумних речей, збільшити ефективність хмарних сервісів та забезпечити безпеку приватних даних у соціальних мережах. Продовження досліджень у галузі теорії ігор дозволить досягти нових результатів та створити безпечний та ефективний кіберпростір для користувачів по всьому світу.

РОЗДІЛ 3
МОДЕЛЬ ВИРІШЕННЯ СИТУАЦІЇ КІБЕРАТАКИ НА ОСНОВІ ТЕОРЕТИКО-ІГРОВОГО ПІДХОДУ

3.1 Моделювання гри «Кібератака»

Завдання цієї роботи полягає в застосуванні теорії ігор для відбиття кібератаки на систему. Мета полягає в знаходженні оптимальної стратегії захисту, яка дозволить зменшити можливі наслідки кібератаки та зберегти цілісність системи. Розглядається антагоністична гра у нормальній формі. Щоб сформулювати гру, необхідно описати множину гравців, описати стратегії та визначити виграші гравців.

Для досягнення цієї мети необхідно вивчити можливі варіанти атак та їх наслідки для системи. Потрібно провести аналіз потенційних загроз та визначити вектори атак, які можуть бути спрямовані на систему.

Після вивчення можливих варіантів атак потрібно проаналізувати можливі стратегії захисту та їх наслідки. Можна розглядати різні варіанти захисту, такі як встановлення антивірусних програм, файрволів, систем безпеки, а також різні методи контролю доступу до системи.

Далі, застосовуючи теоретико-ігровий підхід до вирішення цією проблеми, необхідно знайти оптимальну стратегію захисту системи від кібератаки. Можна використовувати різні методи теорії ігор, наприклад, алгоритми пошуку рівноваги Неша, методи мінімаксу та інші.

Отже, завдання з використанням теорії ігор для відбиття кібератаки на систему складається з кількох етапів, включаючи вивчення можливих варіантів атак, аналіз можливих стратегій захисту та застосування теорії ігор для знаходження найкращої стратегії захисту.

Загалом використання апарату теорії ігор у вирішенні проблеми кібератак можна розглядати гру, в якій присутні два учасники:

1. зловмисник, який намагається скомпрометувати цільову систему
2. захисник, який представлений власником інформаційної системи.

Зловмисник може використовувати відомі вектори атак та окремі атаки, щоб здійснити свої погрози або привести ігрову ситуацію до відомої стратегії з визначеним виграшем. Захисник повинен реалізовувати та використовувати відомі методи захисту в рамках своєї інформаційної системи для протидії найбільш імовірним атакам для даної інформаційної системи.

Зловмисник має виграти, щоб порушити цілісність, конфіденційність та доступність інформації, що обробляється у атакованій інформаційній системі. Захисник, натомість, має виграти, щоб запобігти цим діям. Гра має нульову суму, оскільки виграш зловмисника призводить до втрат захисника. Гра описується як гра в нормальній формі, для якої пара "інформаційна атака-метод захисту" буде представляти собою зміст матриці платежів для даної гри [15] (Таблиця 3.1).

Таблиця 3.1 Приклад платіжної гри в матричній формі

Стратегії гравця 1	Стратегії гравця 2						
		B_1	B_2	…	B_j	…	B_n
	A_1	α_{11}	α_{12}	…	α_{1j}	…	α_{1n}
	A_2	α_{21}	α_{22}	…	α_{2j}	…	α_{2n}
	…	…	…	…	…	…	…
	A_i	α_{i1}	α_{i2}	…	α_{ij}	…	α_{in}
	…	…	…	…	…	…	…
	A_m	α_{m1}	α_{m2}	…	α_{mj}	…	α_{mn}

Отже, в цій грі зловмисник (гравець 1) та захисник (гравець 2) використовують свої власні стратегії, щоб досягти своїх цілей. Зловмисник використовує відомі вектори атак та окремі атаки, тоді як захисник реалізовує та використовує відомі методи захисту в рамках своєї інформаційної системи. Виграшем для зловмисника є порушення цілісності, конфіденційності та

доступності інформації, тоді як захисник має за мету недопущення вказаних дій.

3.2 Математичне рішення задачі

Один з відомих чисельних методів рішення в теорії ігор - так званий метод ітерацій. Цей метод демонструє накопичення досвіду шляхом багатьох повторень конфлікту [2 - 4].

Його ідея полягає в тому, щоб розігрувати "умовну гру", де гравці (А та В) по черзі обирають свої стратегії один проти одного, прагнучи виграти якомога більше (програти якомога менше). Кожен з гравців намагається слідкувати за діями супротивника і відповісти на них найбільш вигідним для себе способом.

Гра імітується з ряду "партій". Починається вона з того, що один з гравців (А) робить свій вибір, допустимо, він грає стратегію A_i. Перший хід гравцеві А доцільно вибрати за принципом $Arg_i\{max_i\, min_j\,(a_{ij})\}$ (обираємо той рядок, що забезпечує нижню ціну гри). Супротивник (В) відповідає на цей хід своїм вибором - він обирає зі своїх стратегій B_j, яка найвигідніша для нього, тобто обертає свій програш при стратегії A_i в мінімум - $Arg_j\{min_j\,(a_{ij})\}$ (обирає j - стовпчик, що забезпечує мінімальний програш при вибраній гравцем А стратегії).

Далі настає черга А реагувати на дії гравця В – гравець А відповідає гравцеві В такою своєю стратегією A_k, яка дає максимальний виграш при стратегії B_j гравця В – $Arg_i\{max_i(a_{ij})\}$.

Після цього черга йде до гравця В, який відповідає своєю стратегією, що мінімізує його програш. Він обирає стратегію, яка дає йому мінімальний

програш відносно накопиченого виграшу гравця A, як сумарного виграшу при застосуванні стратегій A_i , A_k

$$a'_{k1} = a_{i1} + a_{k1}, a'_{k2} = a_{i2} + a_{k2}, \dots, a'_{km} = a_{im} + a_{km}$$

Таким чином, на кожній ітерації гравці використовують оптимальні стратегії для максимізації свого виграшу та мінімізації програшу свого опонента. Цей процес продовжується до досягнення кінцевого результату, коли гравці отримують оптимальні виграші та програші.

Хід гри зручно відобразити в таблиці (Таблиця 3.2.). В таблиці представлені, окрім описаних, також нижня оцінка ціни гри U, що обчислюється як найменший середній виграш гравця A :$U_n = \frac{min_k a'_{ik}}{N}$, а також верхня оцінка ціни гри W, як найбільший середній програш гравця B : $U_n = \frac{max_k a'_{ki}}{N}$, ν =(U+W)/2 - наближена оцінка ціни гри, як середнє арифметичне між U та W. [2]

Таблиця 3.2 Модель задачі ітераційного методу

№ гри	Стратегія гравця A	Накопичуваний виграш гравця A				Стратегія гравця B	Накопичуваний програш гравця B				U	W	ν
1	A_i	a_{i1}	a_{i2}	…	a_{im}	B_j	a_{1j}	a_{2j}	…	a_{nj}	U_1	W_1	ν_1
2	A_k	a_{k1}'	a_{k2}'	…	a_{km}'	B^1	a_{1l}'	a_{2l}'	…	a_{nl}'	U_2	W_2	ν_2
…	…	…	…	…	…	…	…	…	…	…	…	…	…
N	A_p	a_{p1}'	a_{p2}'	…	a_{pm}'	B_t	a_{1t}'	a_{2t}'	…	a_{nt}'	U_N	W_N	ν_N

Правило зупину методу ітерацій буде виглядати наступним чином.

Нехай задано число ε >0. Процес ітерацій зупинимо на кроці n, коли вперше виконається нерівність W(n) – U(n) ≤ ε. В цьому разі ціна гри стане

рівною ν ≈ (W(n) + U(n))/2, змішані стратегії гравців знаходимо за формулами статистичного визначення ймовірностей :

$$S_A^*(p_1^*, p_2^*, ..., p_m^*), S_B^*(q_1^*, q_2^*, ..., q_n^*$$

$$p_1^* = \frac{n_{A_1}}{N}, \quad p_2^* = \frac{n_{A_2}}{N}, \quad p_m^* = \frac{n_{A_m}}{N},$$

$$q_1^* = \frac{n_{B_1}}{N}, \quad q_2^* = \frac{n_{B_2}}{N}, \quad q_n^* = \frac{n_{B_n}}{N},$$

де n_{A_1} n_{A_1} - загальна кількість використання гравцем А стратегії A_i та відповідно гравцем В стратегії B_j .

Взагалом модель будь-якої матричної гри з нульовою сумою може бути приведено до задач лінійного програмування та до певних математичних моделей [2].

Припустимо шо платіжна матриця гри нам відома та оптимальні стратегії гравців будем знаходити в змішаних стратегіях описаних вище.

Якщо ми розглядаємо гру з перспективи гравця А, то його оптимальна стратегія повинна гарантувати йому виграш, що не менше ніж ν, незалежно від того, яку стратегію обере гравець В, а при оптимальній стратегії гравця В виграші обох гравців будуть дорівнювати ν.

Припустимо, що гравець А застосовує свою оптимальну змішану стратегію S_A^* (яка нам поки невідома), а гравець В використовує будь-яку чисту стратегію B_j . В такому випадку середній виграш гравця А буде розраховуватись наступним чином:

$$a_j = p_1 a_{1j} + p_2 a_{2j} + ... + p_m a_{mj}$$

Але кожне із чисел a_j не може бути менше ν відповідно до теореми теорії ігор про активні стратегії (*Теорема про активні стратегії.* Якщо один з гравців дотримується своєї оптимальної змішаної стратегії, то його виграш не менше ціни гри, незалежно від того, що робить інший гравець.)[2]. Звідси одержуємо в загальному випадку n нерівностей

$$\begin{cases} p_1 a_{11} + p_2 a_{21} + \ldots + p_m a_{m1} \geq v, \\ p_1 a_{12} + p_2 a_{22} + \ldots + p_m a_{m2} \geq v, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p_1 a_{1n} + p_2 a_{2n} + \ldots + p_m a_{mn} \geq v, \end{cases} \quad (3.1)$$

Ця система нерівностей визначає математичну модель матричної гри, рішення якої приведе до шуканого результату.

3.3 Комп’ютерна реалізація

Для застосування алгоритмів ітераційної парадигми, повернемось до математичної моделі (3.1).

Взагалом в цій системі $\{a_{ij}\}$ - це платіжна матриця гри , υ – виграш, який має нижню та верхню границі: $\alpha \leq \upsilon \leq \beta$, а p_i – змішані стратегії гравця. Так як гравець прагне отримати максимально можливий виграш у грі, то побудуємо наступний алгоритм його дій [8].

Алгоритм простого перебору.

1) Приймемо $\upsilon = \beta$.

2) Підставимо поточне значення υ в систему (3. 3), та шляхом простого перебору на полі допустимих значень $p_i(\sum_{i=1}^{n} p_i)$ перевіряємо виконуваність

системи. Якщо так, то той набір p_i є рішенням для гравця, а поточне значення υ є його виграшом. Кінець алгоритму. Рішення отримане. [8]

Якщо ні, то переходимо до п. 3.

3) Відступимо на крок Δβ (його можна обрати заздалегідь), тобто поточне значення виграшу приймемо υ = β - Δβ. Якщо β ≥ α переходимо до п. 2, якщо ні – кінець алгоритму. Рішення не можливе[8]

Представимо матрицю з тестовими даними для цього (Таблиця 3.3.)

Таблиця 3.3. Матриця з тестового розрахунку

	B			
A	6	9	11	6
	13	6	8	10
	9	7	6	12
	6	11	8	7
	11	8	7	9

Проведемо попередні дослідження: MAX_MIN = 7 MIN_MAX = 11.

Сідлова точка відсутня, тому зводимо до задачі лінійного програмування в змішаних стратегіях.[7]

$$S_A = (p_1, p_2, p_3, p_4, p_5),\ S_B = (q_1, q_2, q_3, q_4)$$

Математична модель для гравця А:

$$L(x) = x_1 + x_2 + x_3 + x_4 + x_5 \rightarrow min$$
$$6x_1 + 13x_2 + 9x_3 + 6x_4 + 11x_5 \geq 1$$
$$9x_1 + 6x_2 + 7x_3 + 11x_4 + 8x_5 \geq 1$$
$$11x_1 + 8x_2 + 6x_3 + 68 + 7x_5 \geq 1$$
$$6x_1 + 10x_2 + 12x_3 + 7x_4 + 9x_5 \geq 1$$
$$x_i \geq 0$$

Математична модель для гравця В:

$$L(x) = y_1 + y_2 + y_3 + y_4 \rightarrow max$$
$$6y_1 + 9y_2 + 11y_3 + 6y_4 \leq 1$$
$$13y_1 + 6y_2 + 8y_3 + 10y_4 \leq 1$$
$$9y_1 + 7y_2 + 6y_3 + 12y_4 \leq 1$$
$$6y_1 + 11y_2 + 8y_3 + 7y_4 \leq 1$$
$$11y_1 + 8y_2 + 7y_3 + 9y_4 \leq 1$$
$$y_i \geq 0$$

Вхідний файл містить матрицю :

6	9	11	6
13	6	8	10
9	7	6	12
6	11	8	7
11	8	7	9

Результати обрахунків зображено нижче (Рисунки 3.1 – 3.3)

Рисунок 3.1 Результат поточного виграшу для гравця А

```
P values :
[0.25527555 0.26758283 0.17465398 0.29703272 0.00545492]
```

Рисунок 3.2 Результат обчислень стратегій для А

```
Q values :
[0.11818894 0.3364585  0.27712003 0.26823252]
```

Рисунок 3.3 Результат обчислень стратегій для В

Загальними висновками з рішення цієї задачі є те, що гравцю А не вигідно використовувати стратегію 5, оскільки ймовірність p5 = 0.05. Також можна зробити висновок, що для гравця В невигідно використовувати стратегію 1, оскільки ймовірність q1 = 0.11.

3.4 Висновки до розділу 3

Ми розглянули метод ітерацій (метод Брауна-Робінсона) та вирішили за допомогою нього антагоністичну матричну гру в нормальній формі, яка змодельована для двох гравців (нападника та захисника) в області захисту комп’ютерних мереж. Метод передбачає розігрування "умовної гри", в якій гравці по черзі обирають свої стратегії один проти одного, прагнучи виграти якомога більше (програти якомога менше). Гравці використовують оптимальні стратегії для максимізації свого виграшу та мінімізації програшу

свого опонента. Цей процес продовжується до досягнення кінцевого результату, коли гравці отримують оптимальні виграші та програші.

Метод на основі теорії ігор дозволяє знайти оптимальний розподіл бюджету між різними захисними механізмами, що максимізує ефективність відбиття кібератак, враховуючи обмеження бюджету і ризику безпеки. Гра має нульову суму, оскільки виграш зловмисника призводить до втрат захисника. Під час гри зловмисник та захисник використовують свої власні стратегії, щоб досягти своїх цілей. Зловмисник використовує відомі вектори атак та окремі атаки, тоді як захисник реалізовує та використовує відомі методи захисту в рамках своєї інформаційної системи. Виграшем для зловмисника є порушення цілісності, конфіденційності та доступності інформації, тоді як захисник має за мету недопущення вказаних дій.

Метод ітераційних алгоритмів на основі теорії ігор - це чудовий інструмент для вирішення задач захисту інформаційних систем від кібератак. Він дозволяє знайти оптимальну стратегію захисту, яка забезпечить максимальний захист від кібератак при обмеженому бюджеті та ризику безпеки. Крім того, метод дозволяє аналізувати можливості та потенційні загрози кібербезпеки, що дозволяє розробляти більш ефективні стратегії захисту та вдосконалювати інформаційну безпеку в цілому.

РОЗДІЛ 4
ФУНКЦІОНАЛЬНО-ВАРТІСНИЙ АНАЛІЗ ПРОГРАМНОГО ПРОДУКТУ

В заданому розділі буде проведено оцінювання основних характеристик для майбутнього програмного продукту, що спеціалізується на дослідженні демографічного стану.

Дана реалізація буде сприяти проведенню усіх необхідних досліджень, що дасть змогу якісно дослідити питання не лише в Україні, проте у всьому світі.

Також в даному дослідженні показано різні варіанти реалізації для забезпечення найбільш коректної та оптимальної стратегії вибору, що має вплив на економічні фактори та сумісність з майбутнім програмним продуктом. Для цього застосовувався апарат функціонально-вартісного аналізу.

Функціонально-вартісний аналіз (ФВА) передбачає собою технологію, що дозволяє оцінити реальну вартість продукту або послуги незалежно від організаційної структури компанії. ФВА проводиться з метою виявлення резервів зниження витрат за рахунок ефективніших варіантів виробництва, кращого співвідношення між споживчою вартістю виробу та витратами на його виготовлення. Для проведення аналізу використовується економічна, технічна та конструкторська інформація.

Алгоритм функціонально-вартісного аналізу включає в себе визначення послідовності етапів розробки продукту, визначення повних витрат (річних) та кількості робочих часів, визначення джерел витрат та кінцевий розрахунок вартості програмного продукту.

4.1 Постановка задачі проектування

У роботі застосовується метод ФВА для проведення техніко-економічного аналізу розробки системи прогнозу стійкості фінансових показників. Оскільки рішення стосовно проектування та реалізації компонентів, що розробляється, впливають на всю систему, кожна окрема підсистема має її задовольняти. Тому фактичний аналіз представляє собою аналіз функцій програмного продукту, призначеного для збору, обробки та проведення аналізу даних по компанії.

Технічні вимоги до програмного продукту є наступні:

- функціонування на персональних комп’ютерах із стандартним набором компонентів;
- зручність та зрозумілість для користувача;
- швидкість обробки даних та доступ до інформації в реальному часі;
- можливість зручного масштабування та обслуговування;
- мінімальні витрати на впровадження програмного продукту.

4.2 Обґрунтування функцій програмного продукту

Головна функція F_0 – розробка можливого програмного продукту, яка дозволяє аналізувати різні характеристики, що безпосередньо впливають на стійкість підприємства. Беручи за основу цю функцію, можна виділити наступні:

F_1 – вибір самої програми.

F_2 – якісний аналіз даних.

F_3 – графічні показники.

Кожна з цих функцій має декілька варіантів реалізації:

Функція F_1:

а) Eviews.

б) R.

Функція F_2.

а) Застосування вбудованих функцій.

б) Створення своїх обчислень значень.

Функція F_3:

а) Використання шаблонних графіків.

б) Створення своїх.

Варіанти реалізації основних функцій наведені у морфологічній карті системи (рис. 4.1).

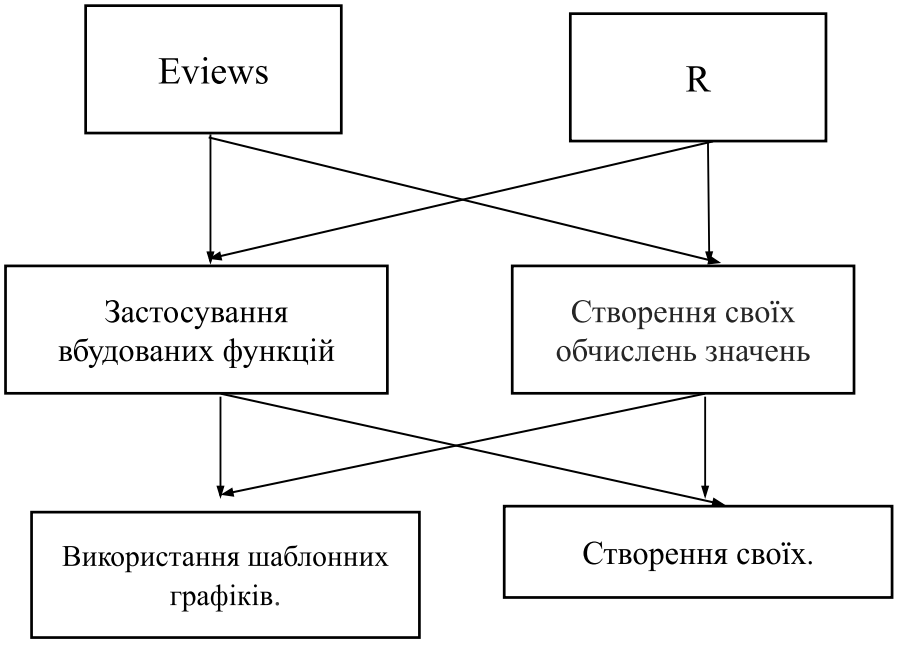


Рисунок 4.1 – Морфологічна карта

Морфологічна карта відображає множину всіх можливих варіантиів основних функцій. Позитивно-негативна матриця показана в таблиці 4.1.

Таблиця 4.1 - Позитивно-негативна матриця

Функції	Варіанти реалізації	Переваги	Недоліки
F_1	*А*	Загальнодоступна програма, доступність багатьох бібліотек	Необхідність повної реалізації алгоритму
	Б	Доступна в реалізації програма для різних обчислень	На написання коду необхідно мати базові навички та вміння
F_2	*А*	Доступність та легкість при написанні	Іноді не відповідає задачі яку треба розв’язати
	Б	Ідеально описують усі необхідні характеристики	Достатньо затратно реалізовувати свої алгоритми для подальшої реалізації
F_3	*А*	Загально прийнята реалізація	Іноді не відповідає очікуваним значенням
	Б	При виконанні власних досліджень краще може передавати висновки	Необхідно достатньо багато часу для написання програми для побудови та знаходження всього необхідного в задачі.

На основі аналізу позитивно-негативної матриці робимо висновок, що при розробці програмного продукту деякі варіанти реалізації функцій варто відкинути, тому, що вони не відповідають поставленим перед програмним продуктом задачам. Ці варіанти відзначені у морфологічній карті.

Функція F_1:

Перевагу даємо загальнодоступності. Для спрощення роботи по написанню коду варіант Б має бути відкинутий.

Функція F_2:

Програма допускає обрання обох варіантів. Можливо використати варіанти А чи Б.

Функція F_3:

Реалізація першого варіанту є сприйнятливою для програми. Це варіант А.

Таким чином, будемо розглядати такий варіанти реалізації ПП:

$$F_1\text{а} - F_2\text{а} - F_3\text{а}$$
$$F_1\text{а} - F_2\text{б} - F_3\text{а}$$

Для оцінювання якості розглянутих функцій обрана система параметрів, описана нижче.

4.3 Обґрунтування системи параметрів програмного продукту

На основі даних, розглянутих вище, визначаються основні параметри вибору, які будуть використані для розрахунку коефіцієнта технічного рівня.

Для того, щоб охарактеризувати програмний продукт, будемо використовувати наступні параметри:

- *X1* – швидкодія мови програмування;

- *X2* – об’єм пам’яті для обчислень та збереження даних;
- *X3* – час навчання даних;
- *X4* – потенційний об’єм програмного коду.

Гірші, середні і кращі значення параметрів вибираються на основі вимог замовника й умов, що характеризують експлуатацію програмного продукту як показано у таблиці 4.2.

Таблиця 4.2 – Основні параметри програмного продукту

Назва Параметра	Умовні позначення	Одиниці виміру	Значення параметра		
			гірші	середні	кращі
Швидкодія мови програмування	X1	оп/мс	9000	13000	18000
Об’єм пам’яті	X2	Мб	512	128	32
Час попередньої обробки даних	X3	мс	10	5	3
Потенційний об’єм програмного коду	X4	кількість рядків коду	10000	5000	1300

За даними таблиці 4.3 будуються графічні характеристики параметрів (рис. 4.2 – рис. 4.5).

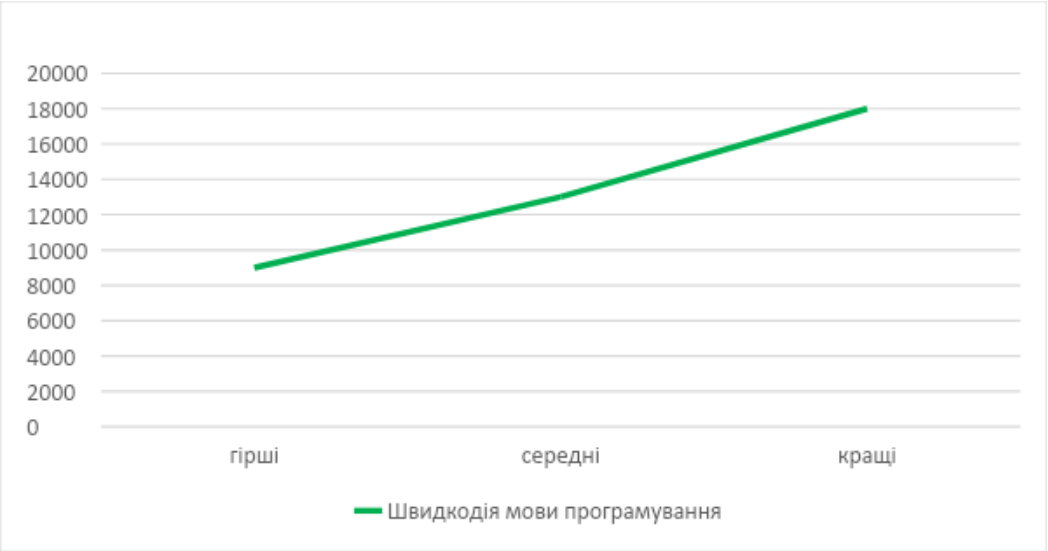


Рисунок 4.2 – X1, швидкодія мови програмування

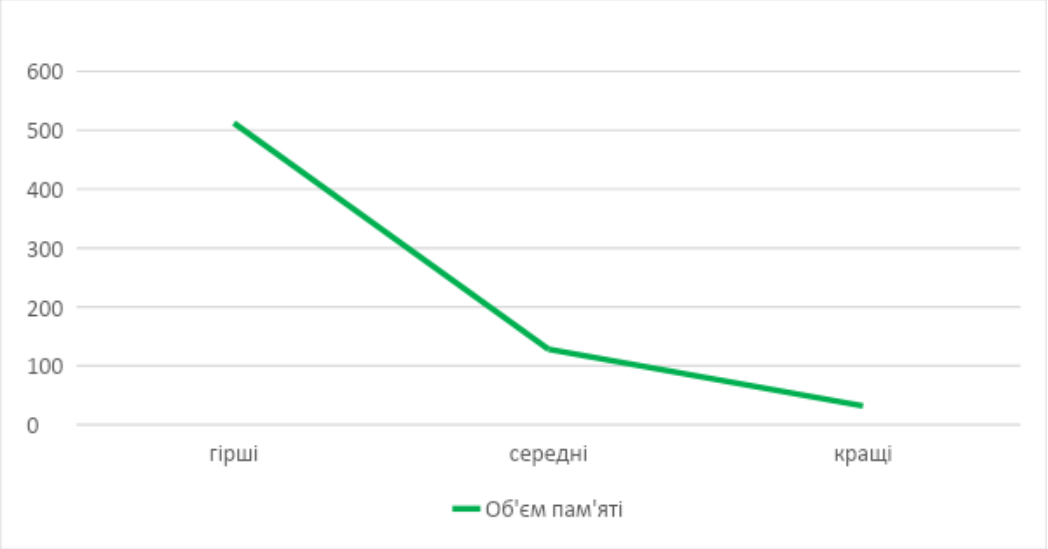


Рисунок 4.3 – X2, об’єм пам’яті

Рисунок 4.4 – X3, час попередньої обробки даних

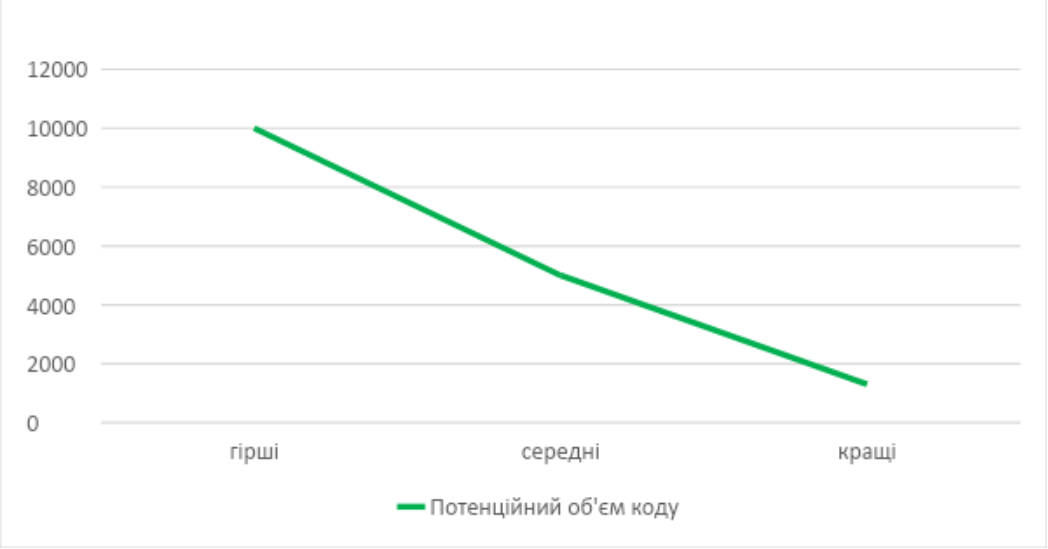


Рисунок 4.5 – X4, потенційний об’єм програмного коду

4.4 Аналіз експертного оцінювання параметрів

Після детального обговорення й аналізу кожний експерт оцінює ступінь важливості кожного параметру для конкретно поставленої цілі – розробка програмного продукту, який дає найбільш точні результати при знаходженні

параметрів моделей адаптивного прогнозування і обчислення прогнозних значень.

Значимість кожного параметра визначається методом попарного порівняння. Оцінку проводить експертна комісія із 7 людей. Визначення коефіцієнтів значимості передбачає:

- визначення рівня значимості параметра шляхом присвоєння різних рангів;
- перевірку придатності експертних оцінок для подальшого використання;
- визначення оцінки попарного пріоритету параметрів;
- обробку результатів та визначення коефіцієнту значимості.

Результати експертного ранжування наведені у таблиці 4.4.

Таблиця 4.4 – Результати ранжування параметрів

Позначення параметра	Назва параметра	Одиниці виміру	Ранг параметра за оцінкою експерта							Сума рангів R_i	Відхилення Δ_i	Δ_i^2
			1	2	3	4	5	6	7			
X1	Швидкодія мови програмування	Оп/мс	1	1	1	1	1	1	2	8	-9,7	95,0625
X2	Об’єм пам’яті	Mb	3	2	3	2	3	2	1	16	-1,75	3,0625
X3	Час попередньої	мс	2	3	2	3	2	3	6	22	4,25	18,0625

	обробки даних											
X4	Потенційний об’єм програмного коду	Кількість рядків коду	4	4	4	4	4	4	1	25	7,25	52,5625
	Разом		10	10	10	10	10	10	10	71	0	168,75

Для перевірки степені достовірності експертних оцінок, визначимо наступні параметри:

а) сума рангів кожного з параметрів і загальна сума рангів:

$$R_i = \sum_{j=1}^{N} r_{ij} R_{ij} = \frac{Nn(n+1)}{2} = 98, \quad (4.1)$$

де N – число експертів;

n – кількість параметрів.

б) середня сума рангів:

$$T = \frac{1}{n} R_{ij} = 17,75 \quad (4.2)$$

в) відхилення суми рангів кожного параметра від середньої суми рангів:

$$\Delta_i = R_i - T. \quad (4.3)$$

Сума відхилень по всім параметрам повинна дорівнювати 0;

г)загальна сума квадратів відхилення:

$$S = \sum_{i=1}^{N} \Delta_i^2 = 168,75. \quad (4.4)$$

Порахуємо коефіцієнт узгодженості:

$$W = \frac{12S}{N^2\left(n^3-n\right)} = \frac{12\cdot 211}{7^2\left(4^3-4\right)} = 0,69 > W_k = 0,67. \qquad (4.5)$$

Ранжування можна вважати достовірним, тому що знайдений коефіцієнт узгодженості перевищує нормативний, котрий дорівнює 0,67.

Скориставшись результатами ранжирування, проведемо попарне порівняння всіх параметрів і результати занесемо у таблицю 4.5.

Таблиця 4.5 – Попарне порівняння параметрів.

Параметри	Експерти							Кінцева оцінка	Числове значення
	1	2	3	4	5	6	7		
X1 і X2	>	<	>	<	>	>	>	>	1,5
X1 і X3	=	<	=	=	>	=	=	=	1
X1 і X4	=	<	<	<	<	=	>	<	0,5
X2 і X3	=	=	=	=	>	>	=	=	1
X2 і X4	>	>	>	>	>	>	>	>	1,5
X3 і X4	>	=	>	=	=	>	>	>	1,5

Числове значення, що визначає ступінь переваги *i*–го параметра над *j*–тим, a_{ij} визначається по формулі:

$$a_{ij} = \{1.5 \text{ при } X_i > X_j \; 1.0 \text{ при } X_i = X_j \; 0.5 \text{ при } X_i < X_j . \qquad (4.6)$$

З отриманих числових оцінок переваги складемо матрицю А=$\| a_{ij} \|$.

Для кожного параметра зробимо розрахунок вагомості $K_{ві}$ за наступними формулами:

$$K_{\text{ві}} = \frac{b_i}{\sum_{i=1}^{n} b_i}, \quad (4.7)$$

$$b_i = \sum_{i=1}^{N} a_{ij} \quad (4.8)$$

Відносні оцінки розраховуються декілька разів доти, поки наступні значення не будуть незначно відрізнятися від попередніх (менше 2%). На другому і наступних кроках відносні оцінки розраховуються за наступними формулами:

$$K_{\text{ві}} = \frac{b_i'}{\sum_{i=1}^{n} b_i'}, \quad (4.9)$$

$$b_i' = \sum_{i=1}^{N} a_{ij} b_j \quad (4.10)$$

.Як видно з таблиці 4.6, різниця значень коефіцієнтів вагомості не перевищує 2%, тому більшої кількості ітерацій не потрібно.

Таблиця 4.6 – Розрахунок вагомості параметрів

Параметри x_i	Параметри x_j				Перша ітер.		Друга ітер.		Третя ітер	
	X1	X2	X3	X4	b_i	$K_{\text{ві}}$	b_i^1	$K_{\text{ві}}^1$	b_i^2	$K_{\text{ві}}^2$
X1	1	1,5	1	0,5	4,00	0,25	16,00	0,25	64,00	0,24
X2	0,5	1,5	1	1,5	4,50	0,28	20,25	0,31	91,13	0,35
X3	0,5	1	1	1,5	4,00	0,25	16,00	0,25	64,00	0,24
X4	1,5	0,5	0,5	1	3,50	0,22	12,25	0,19	42,88	0,16
Всього:					16,00	1,00	64,50	1,00	262,00	1,00

4.5 Аналіз рівня якості варіантів реалізації функцій

Визначаємо рівень якості кожного варіанту виконання основних функцій окремо.

Абсолютні значення параметрів *X2* (Об'єм пам'яті), *X3* (час попередньої обробки даних) та *X4* (потенційний об'єм програмного коду) відповідають технічним вимогам умов функціонування даного ПП.

Абсолютне значення параметра *X1* (швидкість роботи мови програмування) обрано не найгіршим.

Коефіцієнт технічного рівня для кожного варіанта реалізації ПП розраховується так:

$$K_K(j) = \sum_{i=1}^{n} K_{\text{в}i,j} B_{i,j}, \qquad (4.11)$$

де n – кількість параметрів;

$K_{\text{в}i}$ – коефіцієнт вагомості i–го параметра;

B_i – оцінка i–го параметра в балах.

Розрахунок показників рівня якості варіантів реалізації основних функцій ПП наведений у таблиці 4.7.

Таблиця 4.7 – Розрахунок показників рівня якості варіантів реалізації основних функцій ПП

Основні функції	Варіант реалізації функції	Параметри	Абсолютне значення параметра	Бальна оцінка параметра	Коефіцієнт вагомості параметра	Коефіцієнт рівня якості
F1	A	X1	9000	6	0,24	1,44

F2	А	X2	32	3	0,35	1,05
	Б	X2	64	5	0,35	1,75
F3	А	X3	1000	9	0,24	2,16

За даними з таблиці 4.7 за формулою:

$$K_K = K_{\text{ТУ}}\left[F_{1k}\right] + K_{\text{ТУ}}\left[F_{2k}\right] + \ldots + K_{\text{ТУ}}\left[F_{zk}\right], \qquad (4.12)$$

визначаємо рівень якості кожного з варіантів:

$$K_{K1} = 1{,}35 + 0{,}98 + 13{,}68 = 16{,}01;$$

$$K_{K2} = 1{,}35 + 1{,}89 + 13{,}68 = 16{,}92.$$

Як видно з розрахунків, кращим є другий варіант, для якого коефіцієнт технічного рівня має найбільше значення.

4.6 Економічний аналіз варіантів розробки ПП

Для визначення вартості розробки ПП спочатку проведемо розрахунок трудомісткості.

Всі варіанти включають в себе два окремих завдання:

1. Розробка проекту програмного продукту;

2. Розробка програмної оболонки;

Завдання 1 за ступенем новизни відноситься до групи А, завдання 2 – до групи Б. За складністю алгоритми, які використовуються в завданні 1 належать до групи 1; а в завданні 2 – до групи 3.

Для реалізації завдання 1 використовується довідкова інформація, а завдання 2 використовує інформацію у вигляді даних.

Проведемо розрахунок норм часу на розробку та програмування для кожного з завдань.

Загальна трудомісткість обчислюється як

$$Т_О = Т_Р \cdot К_П \cdot К_{СК} \cdot К_М \cdot К_{СТ} \cdot К_{СТ.М}, \qquad (5.13)$$

де $Т_Р$ – трудомісткість розробки ПП;

$К_П$ – поправочний коефіцієнт;

$К_{СК}$ – коефіцієнт на складність вхідної інформації;

$К_М$ – коефіцієнт рівня мови програмування;

$К_{СТ}$ – коефіцієнт використання стандартних модулів і прикладних програм;

$К_{СТ.М}$ – коефіцієнт стандартного математичного забезпечення

Для першого завдання, виходячи із норм часу для завдань розрахункового характеру степеню новизни А та групи складності алгоритму 1, трудомісткість дорівнює: $Т_Р$ =90 людино-днів. Поправочний коефіцієнт, який враховує вид нормативно-довідкової інформації для першого завдання: $К_П$ = 1.6. Поправочний коефіцієнт, який враховує складність контролю вхідної та вихідної інформації для всіх семи завдань рівний 1: $К_{СК}$ = 1. Оскільки при розробці першого завдання використовуються стандартні модулі, врахуємо це за допомогою коефіцієнта $К_{СТ}$ = 0.8. Тоді загальна трудомісткість програмування першого завдання дорівнює:

$Т_1 = 60 \cdot 1.6 \cdot 0.8 = 76.8$ людино-днів.

Проведемо аналогічні розрахунки для подальших завдань.

Для другого завдання (використовується алгоритм третьої групи складності, степінь новизни Б), тобто $Т_Р$ =30 людино-днів, $К_П$ =0.7,$К_{СК}$ = 1,$К_{СТ}$ =0.8:

$Т_2 = 30 \cdot 0.7 \cdot 0.8 = 16.8$ людино-днів.

Складаємо трудомісткість відповідних завдань для кожного з обраних варіантів реалізації програми, щоб отримати їх трудомісткість:

$T_I = (76.8 + 16.8 + 4.8 + 16.8) \cdot 8 = 921.6$ людино-годин.

$T_{II} = (76.8 + 16.8 + 6.91 + 16.8) \cdot 8 = 938.48$ людино-годин.

Найбільш високу трудомісткість має варіант II.

В розробці беруть участь два програмісти з окладом 20000 грн., один аналітик в області даних з окладом 22000. Визначимо середню зарплату за годину за формулою:

$$СЧ = \frac{М}{T_m \cdot t} грн., \quad (5.14)$$

де М – місячний оклад працівників;

T_m – кількість робочих днів тиждень;

t – кількість робочих годин в день.

$$СЧ = \frac{20000+22000}{2 \cdot 21 \cdot 8} = 125 грн. \quad (5.15)$$

Тоді, розрахуємо заробітну плату за формулою:

$$СЗП = С_ч \cdot Т_i \cdot КД, \quad (5.16)$$

де $С_ч$– величина погодинної оплати праці програміста;

$Т_i$ – трудомісткість відповідного завдання;

$К_Д$ – норматив, який враховує додаткову заробітну плату.

Зарплата розробників за варіантами становить:

I. $С_{ЗП} = 125 \cdot 921.6 \cdot 1.2 = 138\ 240{,}00$ грн.

II. $С_{ЗП} = 125 \cdot 938.48 \cdot 1.2 = 140772{,}00$ грн.

Відрахування на єдиний соціальний внесок становить 22%:

I. $С_{ВІД} = С_{ЗП} \cdot 0.22 = 138\ 240{,}00 \cdot 0.22 = 27648{,}00$ грн.

II. $С_{ВІД} = С_{ЗП} \cdot 0.22 = 140772{,}00 \cdot 0.22 = 30969{,}84$ грн.

Тепер визначимо витрати на оплату однієї машино-години. ($С_М$)

Так як одна ЕОМ обслуговує одного програміста з окладом 20000 грн., з коефіцієнтом зайнятості 0,2 то для однієї машини отримаємо:

$С_Г = 12 \cdot М \cdot К_З = 12 \cdot 20000 \cdot 0,2 = 48000$ грн.

З урахуванням додаткової заробітної плати:

$С_{ЗП} = С_Г \cdot (1 + К_З) = 48000 \cdot (1 + 0.2) = 57600$ грн.

Відрахування на соціальний внесок:

$С_{ВІД} = С_{ЗП} \cdot 0.22 = 57600 \cdot 0,22 = 12672,00$ грн.

Амортизаційні відрахування розраховуємо при амортизації 25% та вартості ЕОМ – 50000 грн.

$С_А = К_{ТМ} \cdot К_А \cdot Ц_{ПР} = 1.15 \cdot 0.25 \cdot 50000 = 14375,99$ грн.,

де $К_{ТМ}$ - коефіцієнт, який враховує витрати на транспортування та монтаж приладу у користувача;

$К_А$- річна норма амортизації;

$Ц_{ПР}$ - договірна ціна приладу.

Витрати на ремонт та профілактику розраховуємо як:

$С_Р = К_{ТМ} \cdot Ц_{ПР} \cdot К_Р = 1.15 \cdot 50000 \cdot 0.05 = 2875$ грн.,

де $К_Р$- відсоток витрат на поточні ремонти.

Ефективний годинний фонд часу ПК за рік розраховуємо за формулою:

$Т_{ЕФ} = (Д_К – Д_В – Д_С – Д_Р) \cdot t_З \cdot К_В = (365 – 104 – 12 – 16) \cdot 8 \cdot 0.9 =$

$= 1677.6$ годин,

де $Д_К$ - календарна кількість днів у році;

$Д_В$, $Д_С$ - відповідно кількість вихідних та святкових днів;

$Д_Р$ - кількість днів планових ремонтів устаткування;

t -кількість робочих годин в день;

$К_В$0 коефіцієнт використання приладу у часі протягом зміни.

Витрати на оплату електроенергії розраховуємо за формулою:

$С_{ЕЛ} = Т_{ЕФ} \cdot N_С \cdot К_З \cdot Ц_{ЕН} = 1677.6 \cdot 0.3 \cdot 0.5 \cdot 4.87 = 1225.49$ грн.,

де $N_С$ - середньо-споживча потужність приладу;

$К_З$- коефіцієнтом зайнятості приладу;

$Ц_{ЕН}$ - тариф за 1 КВт-годин електроенергії.

Накладні витрати розраховуємо за формулою:

$С_Н = Ц_{ПР} \cdot 0.67 = 50000 \cdot 0,67 = 33500$ грн.

Тоді, річні експлуатаційні витрати будуть:

$$С_{ЕКС} = С_{ЗП} + С_{ВІД} + С_А + С_Р + С_{ЕЛ} + С_Н, \quad (5.17)$$

$С_{ЕКС} = 57600 + 12672,00 + 14375,99 + 2875 + 1225.49 + 33500 =$ 122248.48 грн.

Собівартість однієї машино-години ЕОМ дорівнюватиме:

$С_{М\text{-}Г} = С_{ЕКС} / Т_{ЕФ} = 107533.76 / 1677.6 = 64.09$ грн/год.

Оскільки в даному випадку всі роботи, які пов‘язані з розробкою програмного продукту ведуться на ЕОМ, витрати на оплату машинного часу, в залежності від обраного варіанта реалізації, складає:

$$С_М = С_{М-Г} \cdot T, \quad (5.18)$$

I. $С_М = 64.09 \cdot 921.6 = 59065.34$ грн.

II. $С_М = 64.09 \cdot 938.48 = 60147.18$ грн.

Накладні витрати складають 67% від заробітної плати:

$$С_Н = С_{ЗП} \cdot 0,67, \quad (5.19)$$

I. $С_Н = 138\ 240,00 \cdot 0,67 = 92620,80$ грн.

II. $С_Н = 140772,00 \cdot 0,67 = 94317,24$ грн.

Отже, вартість розробки ПП за варіантами становить:

$$С_{ПП} = С_{ЗП} + С_{ВІД} + С_М + С_Н, \quad (5.20)$$

I. $С_{ПП} = 138\ 240,00 + 27648,00 + 59065.34 + 92620,80 = 317583.14$ грн.

II. $С_{ПП} = 140772,00 + 30969,84 + 60147.18 + 94317,24 = 326206.26$ грн.

4.7 Вибір кращого варіанту ПП техніко-економічного рівня

Розрахуємо коефіцієнт техніко-економічного рівня за формулою:

$$К_{ТЕР_j} = К_{К_j}/С_{Ф_j}, \quad (5.21)$$

$К_{ТЕР1} = 4{,}25/ 317583.14 = 1{,}338 \cdot 10^{-5}$,

$К_{ТЕР2} = 3{,}74/ 326206.26 = 1.14 \cdot 10^{-5}$.

Як бачимо, найбільш ефективним є перший варіант реалізації програми з коефіцієнтом техніко-економічного рівня $К_{ТЕР1} = 1{,}30 \cdot 10^{-5}$

Після виконання функціонально-вартісного аналізу програмного комплексу що розроблюється, можна зробити висновок, що з альтернатив, що залишились після першого відбору двох варіантів виконання програмного комплексу оптимальним є перший варіант реалізації програмного продукту. У нього виявився найкращий показник техніко-економічного рівня якості $К_{ТЕР} = 1{,}30 \cdot 10^{-5}$.

4.8 Висновки до розділу 4

В даній частині було проведено повний функціонально-вартісний аналіз програмного продукту. Також було знайдено оцінку основних функцій програмного продукту.

В результаті виконання функціонально-вартісного аналізу програмного комплексу що розроблюється, було визначено та проведено оцінку основних функцій програмного продукту, а також знайдено параметри, які його характеризують.

На основі аналізу вибрано варіант реалізації програмного продукту.

ВИСНОВКИ

В процесі дослідження кібербезпеки, ми провели широкий аналіз різних типів кібератак та кіберзагроз, щоб отримати наочне уявлення про те, які проблеми існують в цьому секторі. Ми також дослідили різні теоретико-ігрові підходи в секторі кібербезпеки, щоб зрозуміти, як ці підходи можуть бути застосовані до боротьби з кіберзагрозами.

В залежності від типу кібератак і вразливостей системи, можуть існувати десятки тисяч варіантів атак. Ми пройшлися по основних варіантах атак, від DDoS до SQL ін'єкцій, щоб зрозуміти, які техніки використовуються кіберзлочинцями та як їх можна уникнути.

Ми також дослідили різні теорії ігор та їх застосування в секторі кібербезпеки. Наші дослідження виявили, що метод ітерацій (метод Брауна-Робінсона) може бути корисним при визначенні оптимальної стратегії для протидії кібератакам.

Базуючись на нашому досвіді та дослідженнях, ми розробили програму для пошуку оптимальної стратегії для боротьби з кіберзлочинцями. Наша програма використовує різні техніки, щоб знайти найбільш ефективний план дій для протидії кібератакам.

Наші дослідження та програма можуть бути дуже корисні для будь-якої компанії або організації, яка має ділитися важливою інформацією та зберігає конфіденційні дані в мережі. Використання наших досліджень та програми може допомогти зменшити можливість кібератак та збільшити рівень кібербезпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Державна служба спеціального зв'язку та захисту інформації України. URL:https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak
2. Corchyn L. C., Marini M. A. Handbook of Game Theory and Industrial Organization,Volume I, Theory. Edward Elgar Publishing Limited, 2018.
3. Corchyn L. C., Marini M., A. Handbook of Game Theory and Industrial Organization,Volume II, Applications. – Edward Elgar Publishing Limited, 2018.
4. Frahm G. Rational Choice and Strategic Conflict. The Subjectivistic Approach to Game and Decision Theory. – Berlin/Boston: « Walter de Gruyter GmbH», 2019.
5. Bauso D. Game Theory: Models, Numerical Methods and Applications. Foundations and Trends in Systems and Control, vol. 1, no. 4, 2014.
6. Clark R. Meaningful Games: Exploring Language with Game Theory. The MIT Press, 2012. - 376 p.
7. Lee K. D., Hubbard S. Data Structures and Algorithms with Python. Springer, 2015. – 363 p.
8. Теоретико-ігровий підхід до проблеми безпеки мереж О.П. Ігнатенко Проблеми програмування 2017. URL: http://dspace.nbuv.gov.ua/handle/123456789/144500
9. Ігнатенко О.П., Молчанов О.А. Еволюційні ігри в TCP мережах з політиками обмеження швидкості. Проблеми програмування. 2016. № 4. С. 33–47
10. Itzik Kotler, CTO & Co-Founder, SafeBreach: Threat analysis: how the rapid evolution of reporting can change security 2020. URL: https://www.safebreach.com/resources/threat-analysis-how-the-rapid-evolution-of-reporting-can-change-security/

11. Game-theoretic approach to the network security problem. PROBLEMS IN PROGRAMMING. 2017. No. 3. p. 149–160. URL: https://doi.org/10.15407/pp2017.03.149.
12. G. Owen, Game Theory, New York: Academic Press, 3rd ed., 2001, p. 46.
13. В.А. Савченко, О.Й. Мацько: Управління ризиками кібербезпеки на основі теоретико-ігрового підходу, 2019, 16ст
14. The WASC Threat Classification v2.0. 2010. 172p. URL: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf
15. Костевич Л.С., Лапко А.А, Теория игр. Исследование операций. – Минск: Вышэйшая школа, 1982. 229 с.
16. Ярочкин В.И. Безопасность информационных систем. Ось, 2015 — 320 с.
17. Нестеров С. А. Анализ и управление рисками в сфере информационной безопасности: Учебный курс. — СПб.: СПбГПУ, 2007. — 47 с. Отчет «Исследование текущих тенденций в области информационной безопасности бизнеса». URL: http://media.kaspersky.com/.
18. Peter W. Singer and Allan Friedman: "Cybersecurity and Cyberwar: What Everyone Needs to Know"
19.- Роберт Гіббонс: "Game Theory for Applied Economists"
20. Roy, Sankardas, et al. A survey of game theory as applied to network security. System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, 2010.
21. Liang, Xiannuan, and Yang Xiao. Game theory for network security. IEEE Communications Surveys & Tutorials 15.1 (2013): 472-486.
22. Thomas J. Mowbray: "Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions". Indianapolis, Ind. : John Wiley & Sons, c2014. 323p

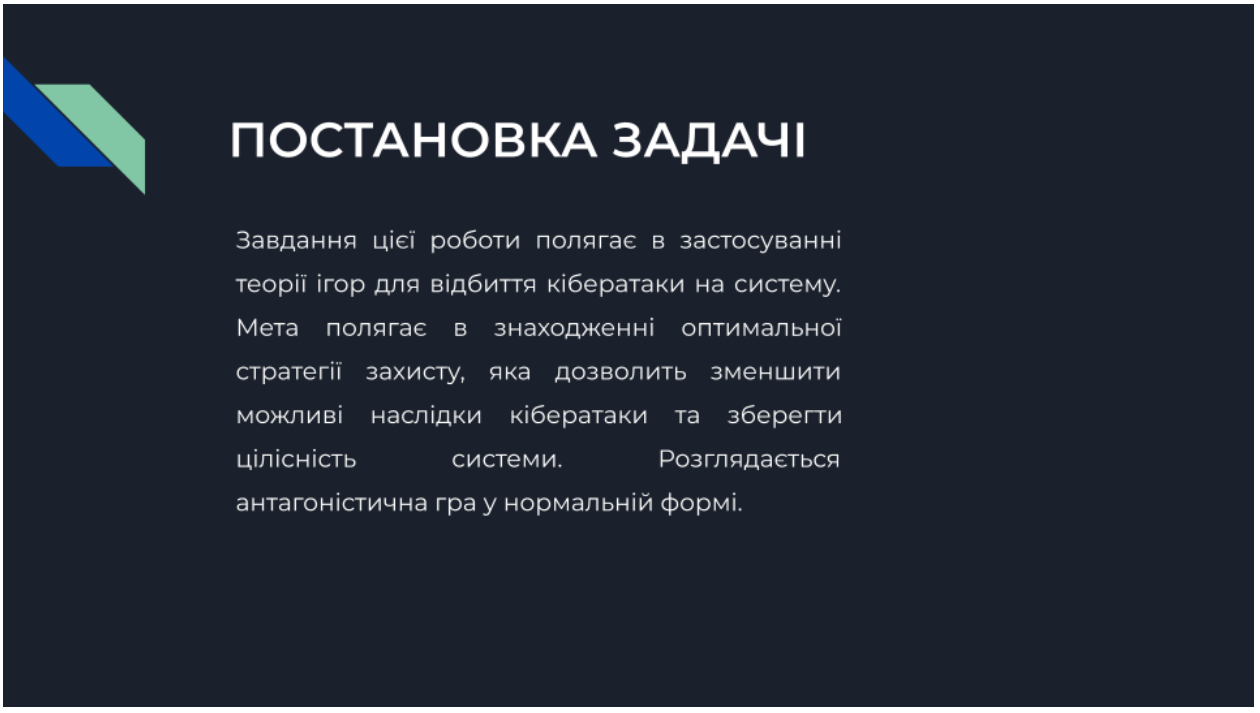
23. Quanyan Zhu, Tansu Alpcan, Emmanouil Panaousis, Milind Tambe, William Casey "Decision and Game Theory for Security: 7th International Conference, GameSec 2016". 489p.
24. Stefan Rass, Stefan Schauer: "Game Theory for Security and Risk Management: From Theory to Practice", 2018, 418p

ДОДАТОК А
ЛІСТИНГ ПРОГРАМНОГО КОДУ

```
import numpy as np
import datetime as dt

def get_cost_matrix(filename):
   matrix = list()
   with open(filename, "tr") as matrix_file:
       for line in matrix_file:
           numbers = line.split(" ")
           current_row = list()
           for number in numbers:
               current_row.append(int(number))
           matrix.append(current_row)
   return np.array(matrix)

def calc_p_vals(matrix):
   beta = get_min_max(matrix)
   alpha = get_max_min(matrix)
   main_itr_step = 0.1
   v = beta
   while alpha <= v <= beta:
       n_iterations = 2000000
       for iter_index in range(n_iterations):
           p_random_vals = build_random_p_values(matrix.shape[0])
             if not are_ineq_satisfied(matrix, p_random_vals, lambda p_dot_a:
p_dot_a >= v):
               continue
           return p_random_vals, v
       v -= main_itr_step
   return None



def get_max_min(game_matrix):
   rows_mins = np.min(game_matrix, axis=1)
   return np.max(rows_mins)

def get_min_max(game_matrix):
   columns_maxs = np.max(game_matrix, axis=0)
   return np.max(columns_maxs)

def build_random_p_values(size):
   result = np.zeros(shape=size)
   high_border = 1.0
   for i in range(size-1):
       new_random_p = np.random.uniform(0, high_border, 1)
       result[i] = new_random_p
       high_border -= new_random_p
       result[-1] = high_border
```

```
    return result

def are_ineq_satisfied(matrix, x_val, inequality):
    for column_index in range(matrix.shape[1]):
        column = matrix[:, column_index]
        x_dot_a = np.dot(column, x_val)
        if not inequality(x_dot_a):
            return False
    return True

matrix = get_cost_matrix("matrix")
p_vals, v_val = calc_p_vals(matrix)
finish = dt.datetime.now()
print("V : ")
print(v_val)
print("P values : ")
print(p_vals)
```

ДОДАТОК Б
СЛАЙДИ ПРЕЗЕНТАЦІЇ



АКТУАЛЬНІСТЬ ТЕМИ

З кожним роком кількість кібератак зростає, а їх наслідки можуть бути катастрофічними. Кіберзлочинці використовують різноманітні методи та технології, щоб отримати доступ до конфіденційної інформації, зламати системи управління та порушити роботу веб-сайтів. Україна не є винятком і також стала мішенню для кібератак з боку інших держав та кримінальних груп. Тому для досягнення безпеки потрібно постійно вдосконалюватись та вивчати нові методи протидії кібератакам не тільки на технічному а й стратегічному рівні.

МЕТОДИ ВИКОРИСТАННЯ

При моделюванні різних методів кібератак на основі теорії ігор можна виділити кілька основних кроків

Моделювання гри “Кібербезпека”

Один з відомих чисельних методів рішення в теорії ігор - так званий метод ітерацій. Цей метод демонструє накопичення досвіду шляхом багатьох повторень конфлікту. Гра має нульову суму, оскільки виграш зловмисника призводить до втрат захисника. Гра описується як гра в нормальній формі, для якої пара "інформаційна атака-метод захисту" буде представляти собою зміст матриці платежів для даної гри Виграшем для зловмисника є порушення цілісності, конфіденційності та доступності інформації, тоді як захисник має за мету недопущення вказаних дій.

Стратегії гравця 1	Стратегії гравця 2						
	B_1	B_2	…	B_j	…	B_n
A_1	α_{11}	α_{12}	…	α_{1j}	…	α_{1n}
A_2	α_{21}	α_{22}	…	α_{2j}	…	α_{2n}
…	…	…	…	…	…	…
A_i	α_{i1}	α_{i2}	…	α_{ij}	…	α_{in}
…	…	…	…	…	…	…
A_m	α_{m1}	α_{m2}	…	α_{mj}	…	α_{mn}

Хід гри

На кожній ітерації гравці використовують оптимальні стратегії для максимізації свого виграшу та мінімізації програшу свого опонента. Цей процес продовжується до досягнення кінцевого результату, коли гравці отримують оптимальні виграші та програші.

№ гри	Стратегія гравця A	Накопичуваний виграш гравця A				Стратегія гравця B	Накопичуваний програш гравця B				U	W	v
1	A_i	a_{i1}	a_{i2}	…	a_{im}	B_j	a_{1j}	a_{2j}	…	a_{nj}	U_1	W_1	v_1
2	A_k	a_{k1}'	a_{k2}'	…	a_{km}'	B^1	a_{11}'	a_{21}'	…	a_{n1}'	U_2	W_2	v_2
…	…	…	…	…	…	…	…	…	…	…	…	…	…
N	A_p	a_{p1}'	a_{p2}'	…	a_{pm}'	B_t	a_{1t}'	a_{2t}'	…	a_{nt}'	U_N	W_N	v_N

Тестові вхідні дані

	B			
A	6	9	11	6
	13	6	8	10
	9	7	6	12
	6	11	8	7
	11	8	7	9

Проведемо попередні дослідження: MAX_MIN = 7 MIN_MAX = 11.

Вхідний файл містить матрицю :

6	9	11	6
13	6	8	10
9	7	6	12
6	11	8	7
11	8	7	9

Сідлова точка відсутня, тому зводимо до задачі лінійного програмування в змішаних стратегіях.
Sa=(p1,p2,p3,p4,p5), Sв=(q1,q2,q3,q4)

Результати гри

```
V :
8.400000000000016
```

Результат поточного виграшу для гравця А

```
P values :
[0.25527555 0.26758283 0.17465398 0.29703272 0.00545492]
```

Результат обчислень стратегій для гравця А

```
Q values :
[0.11818894 0.3364585  0.27712003 0.26823252]
```

Результат обчислень стратегій для гравця В

Загальними висновками з рішення цієї задачі є те, що гравцю А не вигідно використовувати стратегію 5, оскільки ймовірність p5 = 0.05. Також можна зробити висновок, що для гравця В невигідно використовувати стратегію 1, оскільки ймовірність q1 = 0.11.

Висновок

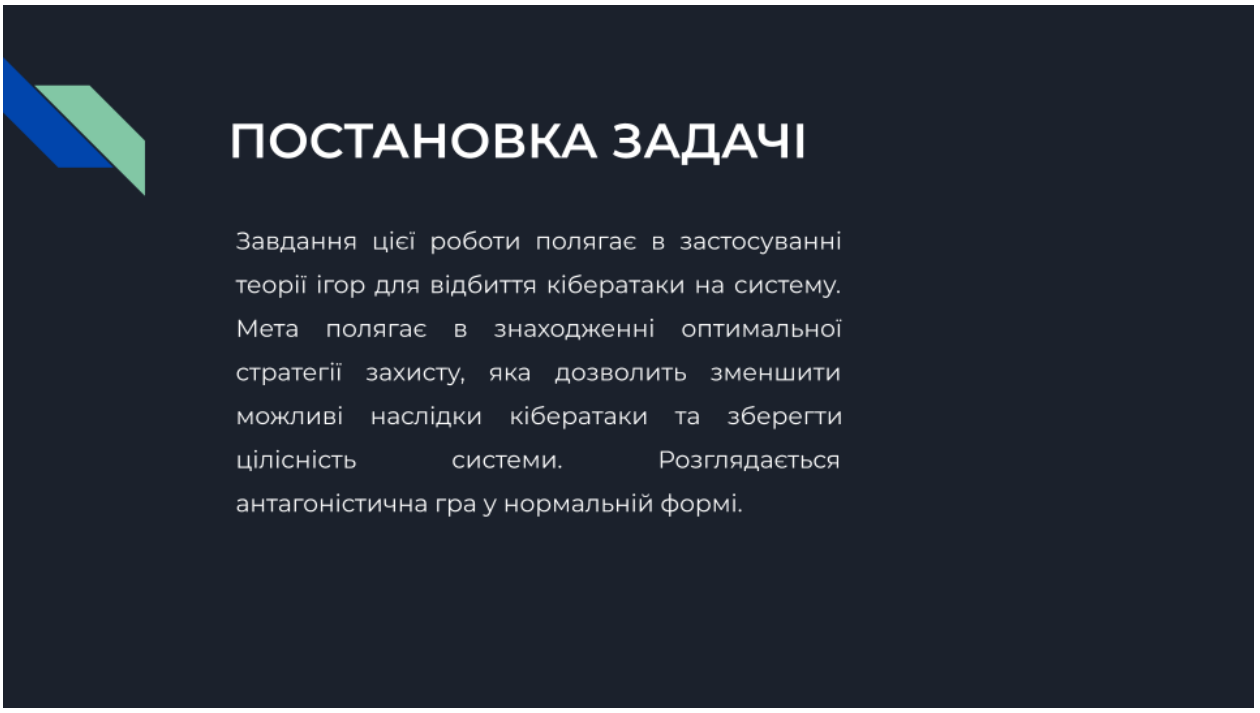
- За результатами дослідження ми виявили, що використовувати теорію ігор для моделювання та аналізу можливих стратегій зловмисника є доволі ефективним підходом для захисту не тільки з технічної точки зору, а й з аналітичної
- Змоделювали платіжну гру в матричній формі з нульовою сумою, як одну із можливих кібератак на систему, та розв'язали її методом ітерацій (Методом Брауна-Робінсона)
- Порівняли найкращі стратегії для вибору для обох учасників гри та вибрали найкращі

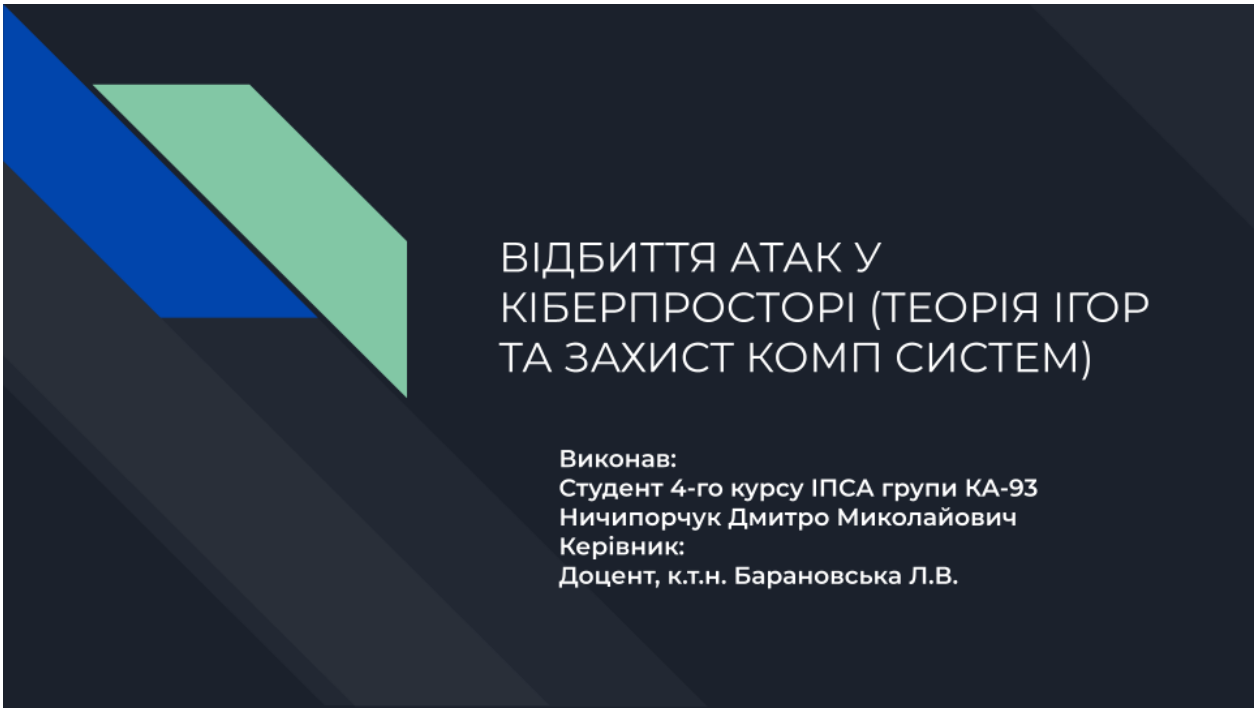
Перспективи досліджень

У сучасному світі безпека є однією з найбільш актуальних проблем. З цією метою, сьогодні відбуваються дослідження в області кібербезпеки. Виділимо найбільш перспективні напрямки досліджень, у яких буде розвиватись теоретико-ігровий підхід.

1. Соціальні мережі.
2. Хмарні обчислення.
3. Інтернет речей.
4. Блокчейн


ДЯКУЮ ЗА УВАГУ!


ПОСТАНОВКА ЗАДАЧІ
Завдання цієї роботи полягає в застосуванні теорії ігор для відбиття кібератаки на систему. Мета полягає в знаходженні оптимальної стратегії захисту, яка дозволить зменшити можливі наслідки кібератаки та зберегти цілісність системи. Розглядається антагоністична гра у нормальній формі.


ВІДБИТТЯ АТАК У КІБЕРПРОСТОРІ (ТЕОРІЯ ІГОР ТА ЗАХИСТ КОМП СИСТЕМ)
Виконав:
Студент 4-го курсу ІПСА групи КА-93
Ничипорчук Дмитро Миколайович
Керівник:
Доцент, к.т.н. Барановська Л.В.

.