НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕОРЕТИКО-ІГРОВІ МЕТОДИ В КІБЕРБЕЗПЕЦІ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»
спеціальність 125 «Кібербезпека»
Губа Владислав Анатолійович

Керівник: к.ф.-м.н., доцент
Черєвко Євген Володимирович

Рецензент: к.т.н., доцент
Бойко Віктор Дмитрович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека та захист інформації**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Губі Владиславу Анатолійовичу

1. Тема роботи: «Атаки на базові станції мобільного зв'язку: ключові проблеми та шляхи їх вирішення»
Керівник роботи: к.ф.-м.н, доцент Черєвко Євген Володимирович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання«15» вересня 2024 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз вимог до проєкту	25.02.2024 – 04.03.2024	
2	Аналіз конкурентів	01.03.2024 – 07.03.2024	
3	Розробка функціональних вимог	08.03.2024 – 14.03.2024	
4	Проєктування застосунку	16.03.2024 – 22.03.2024	
5	Реалізація проєкту	23.03.2024 – 29.03.2024	
6	Реалізація матриці імовірностей	1.04.2024 – 24.04.2024	
7	Аналіз результатів та висновки	26.04.2024 – 20.04.2024	
8	Оформлення пояснювальної записки	02.04.2024 – 20.04.2024	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Теоретико-ігрові методи в кібербезпеці” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 9 рисунків, 7 таблиці, 1 додаток, 16 літературних джерел за переліком посилань. Робота виконана на 44 сторінках загального тексту і 35 сторінках основного тексту.

Метою роботи є демонстрація застосування теорії ігор у кібербезпеці. Розроблено алгоритми для аналізу протидії кібератакам. Програмно реалізовано алгоритми аналізу стратегії для забезпечення безпеки та мінімізацію шкоди в програмному середовищі.

Результати роботи можуть бути використані при вибору оптимальної стратегії з метою виявлення найбільш ефективних методів захисту та протидії кібератакам. Можливими напрямками подальших досліджень є зміцнення кібербезпеки.

СТРАТЕГІЯ, КІБЕРЗАГРОЗА, КІБЕРАТАКА, КІБЕРБЕЗПЕКА, МЕТОДИ, МОДЕЛЮВАННЯ, АНТАГОНІСТИЧНА ГРА, АНАЛІЗ, ПРОТИДІЯ, КОМП’ЮТЕРНА СИСТЕМА.

ABSTRACT

Qualification work on the topic "Theoretical and game methods in cyber security" for obtaining the first (bachelor) level of higher education in the specialty 125 Cyber security, educational program: Cyber security, contains 9 figures, 7 tables, 1 appendix, 16 literary sources for the list of references. The work was completed on 44 pages of the general text and 35 pages of the main text.

The method of work is a demonstration of the application of game theory in cyber security. Algorithms have been developed to analyze countermeasures against cyber-attacks. Algorithms for the analysis of the security strategy and damage minimization in the software environment have been implemented in software.

The results of the work can be used when choosing the optimal strategy for identifying the most effective methods of protection and countermeasures against cyber attacks.

Possible areas of further research are strengthening cyber security.

STRATEGY, CYBER THREAT, CYBERATTACK, CYBERSECURITY, METHODS, SIMULATION, ANTAGONISTIC GAME, ANALYSIS, COUNTERMEASURE, COMPUTER SYSTEM.

ЗМІСТ

ВСТУП

З виростанням кіберзагроз та поширенням кібератак стає все більш важливим використання передових методів для забезпечення безпеки в онлайн середовищі. Одним з таких методів є використання теорії ігор у кібербезпеці.

Теорія ігор – це наука, яка вивчає взаємодію між різними учасниками в умовах, де кожен має свої власні цілі та обмеження. Вона використовується для аналізу різноманітних ситуацій, від економічних до політичних, і для визначення оптимальних стратегій для кожного учасника.

Теорія ігор, в контексті кібербезпеки, дозволяє розглядати ці взаємодії як стратегічні ігри, де кожна сторона прагне досягти своїх цілей, при цьому враховуючи дії опонентів. Це означає аналіз не лише можливих атак та заходів захисту, а й оцінку впливу рішень однієї сторони на поведінку інших, що є ключовим аспектом у визначенні оптимальних стратегій. Використання цих стратегій дозволяє розробляти більш ефективні та інтелектуальні підходи до кібербезпеки, що є критично важливим у сучасному цифровому світі. У цьому контексті, детальне вивчення теорії ігор у кібербезпеці відкриває шлях до розуміння та захисту від сучасних кіберзагроз.

Кібербезпека – це складний і безперервний процес протистояння хакерам та вірусам, які намагаються зламати системи захисту та отримати доступ до конфіденційної інформації. У цьому контексті теорія ігор має кілька переваг. По-перше, це дозволяє розглядати кібербезпеку як систему з взаємозалежними агентами, а не просто як набір окремих технічних проблем. По-друге, вона дозволяє виявляти та аналізувати ризики, які можуть виникнути внаслідок стратегічних дій різних сторін. Вона надає можливість розробляти більш динамічні та адаптивні стратегії захисту, що враховують змінюючийся ландшафт кіберзагроз.

Метою моєї дипломної роботи є донести важливість, актуальність та значущість дослідження і аналізу застосування теорії ігор у сфері кібербезпеки. Це включає глибоке розуміння того, як теорія ігор може бути використана для моделювання та аналізу складних взаємодій між атакуючими сторонами та захисниками у

кіберпросторі. Об'єктом мого дослідження є не лише сам процес цієї взаємодії, але й різні аспекти кібербезпеки, які можуть бути ефективно піддані моделюванню за допомогою теоретико-ігрових підходів. Це охоплює вивчення стратегій, тактик і прийомів, які застосовуються обома сторонами, з метою виявлення найбільш ефективних методів захисту та протидії кібератакам.

1 ТЕОРЕТИЧНІ АСПЕКТИ ТЕОРІЇ ІГОР

1.1 Основні поняття та методи теорії ігор

Теорія ігор є дисципліною, яка досліджує взаємодію між розумними агентами, які приймають рішення у ситуаціях конфлікту або співпраці. Вона застосовує математичні моделі для аналізу стратегій, які гравці обирають з метою оптимізації своїх вигод або корисності. Гравці, які взаємодіють у цих сценаріях, вважаються раціональними в тому сенсі, що вони мають певні цілі та обирають дії, які максимізують їхній виграш. Теорія ігор досліджує не лише сценарії з конфліктом, а й ситуації співпраці, де гравці мають спільні цілі і можуть співпрацювати для досягнення них.

Основні поняття теорії ігор включають поняття стратегії, корисності, рівноваги, інформованості та інші [1]. Ці поняття допомагають розуміти, як гравці приймають рішення та як їхні дії впливають на результати взаємодії. Теорія ігор також вивчає різноманітні типи ігор, включаючи ігри з нульовою сумою, кооперативні ігри, динамічні ігри тощо.

В контексті кібербезпеки, теорія ігор використовується для моделювання взаємодії між хакерами та захисниками, визначення оптимальних стратегій захисту та атаки, а також для розробки алгоритмів виявлення та реагування на кіберзагрози. Вона надає засоби для аналізу ризиків та прийняття обґрунтованих рішень у сфері кібербезпеки.

Теорія ігор є важливою галуззю економіки, математики, політики, військової стратегії, бізнесу та кібербезпеки, що досліджує прийняття рішень в умовах конкуренції та взаємодії між різними учасниками. Основні поняття та методи цієї теорії включають в себе[2]:

Гра - це ситуація, де кілька сторін взаємодіють і приймають рішення. Гра може приймати різні форми: бути послідовністю рішень, діалогом, конкуренцією або комбінацією цих елементів. Основним аспектом гри є конфлікт між сторонами, який потребує вирішення. [5]

Рішення - це дії, які сторони обирають у грі. Вони можуть бути проактивними, реактивними або змішаними. Проактивні рішення – це дії, що сторони здійснюють відповідно до своїх цілей і стратегій. Реактивні рішення – це дії у відповідь на дії інших сторін. Змішані рішення – це дії, що базуються на випадкових або інших внутрішніх факторах. Важливим аспектом рішень є їх взаємодія з іншими сторонами та їхні реакції на дії інших учасників. [5]

Виграш - це результат гри для кожної сторони. Він може бути визначений як абсолютна величина або відносно виграшу іншої сторони. Виграш залежить від рішень, які приймають сторони, і може варіюватися в різних ситуаціях. [5]

Рівновага - це стан, у якому жодна сторона не може односторонньо покращити свій виграш, змінюючи своє рішення. Рівновага може бути стратегічною, динамічною або змішаною. Стратегічна рівновага означає, що жодна сторона не може змінити своє рішення без втрати виграшу, динамічна рівновага означає, що сторони приймають послідовні рішення, а відхилення від цього порядку призводить до зниження виграшу. Змішана рівновага означає, що сторони приймають різні рішення з певною ймовірністю. [5]

Домінування - це ситуація, коли одне рішення є кращим для сторони незалежно від рішення іншої сторони. Домінування може бути стратегічним, динамічним або змішаним. Стратегічне домінування означає, що одне рішення краще для сторони в будь-якій ситуації, динамічне домінування означає, що одне рішення краще в будь-якому повторюваному рішенні, а змішане домінування означає, що одне рішення краще для сторони в середньому. [5]

Ігри з повторенням – це ситуаця, де гравці мають можливість вибирати стратегії не один раз, а декілька разів, і рішення приймаються на основі довгострокових наслідків. Для аналізу таких ігор використовуються такі концепції, як кредибельність стратегій та стратегії тит-за-тат.

Динамічні ігри – ці ігри моделюють ситуації, де гравці приймають рішення в послідовному порядку, знаючи рішення, прийняте попередніми гравцями. Для аналізу таких ігор використовуються такі поняття, як рівновага в секвенціях, підгри і стратегії спостереження.

Рішення в умові неповної інформації – це методи, які досліджують взаємодію гравців, які не мають повної інформації про стратегії або виграші інших гравців. Такі ігри моделюються за допомогою дерев вибору або інших структур, і рішення приймаються на основі очікуваних виграшів.

Рівновага Неша – ситуація в грі, коли жоден гравець не може покращити свій виграш, змінюючи свою стратегію, за умови, що інші гравці не змінюють свої стратегії.

Кооперативні ігри – це ігри, де гравці можуть утворювати коаліції та домовлятися про спільні дії. Для аналізу таких ігор використовуються поняття ядра та різницевих векторів.

В теорії ігор матричні ігри використовуються як один із основних інструментів аналізу. Вони дозволяють досліджувати різні концепції, такі як рівноваги Неша, домінантні стратегії, оптимальні стратегії тощо.

Матричні ігри - це спосіб моделювання ситуацій, де учасники приймають рішення і отримують виграш або збитки залежно від того, які дії вони обирають, а також вибору дій інших учасників. У матриці представлені всі можливі комбінації дій учасників та відповідні виграші або втрати для кожного учасника. Це допомагає аналізувати, які дії можуть бути найбільш вигідними для кожного учасника в залежності від вибору інших учасників.

Для кожного гравця в матриці визначені виграші чи втрати, які він отримує, якщо він обирає певну дію, при умові, що інші гравці обирають свої варіанти дій. Це дозволяє аналізувати, які стратегії можуть бути найбільш вигідними для кожного учасника в залежності від дій інших учасників.

Матричні ігри знаходять застосування в різних областях, оскільки вони дозволяють моделювати взаємодію в умовах невизначеності та конкуренції. Наприклад:

В економіці матричні ігри використовуються для аналізу стратегій учасників ринку, встановлення оптимальних цінових політик, дослідження конкуренції між компаніями тощо.

В політиці вони застосовуються для аналізу виборчих стратегій політичних партій, міжнародних конфліктів, стратегій дипломатії тощо.

В бізнесі матричні ігри допомагають вирішувати конфліктні ситуації між бізнесами, встановлювати стратегії ціноутворення, аналізувати ризики та приймати стратегічні рішення.

В біології та екології вони використовуються для аналізу конкуренції між видами в екосистемах, взаємодії хижак-жертва та інших екологічних процесів.

В Соціальних науках матричні ігри допомагають розуміти поведінку та взаємодію між індивідами та групами.

Деякі приклади матричних ігор:

Гра в "дві монети" – два гравці одночасно кидають монети. Якщо випадає дві голови, перший гравець виграє 1 гривню, а другий програє 1 гривню. Якщо випадає дві решки, другий гравець виграє 1 гривню, а перший програє 1 гривню. Якщо випадає одна голова і одна решка, ніхто не виграє і не програє.

Гра в "дилему в'язня" – два підозрюваних у злочині заарештовані поліцією. Кожному з них пропонують зізнатися або заперечувати свою вину. Якщо обидва зізнаються, кожен отримує 4 роки в'язниці. Якщо один зізнається, а другий заперечує, то перший отримує 1 рік в'язниці, а другий - 10 років. Якщо обидва заперечують, кожен отримує по 2 роки в'язниці.

Аукціон – декілька учасників торгуються за товар, роблячи ставки. Переможцем стає той учасник, який запропонував найвищу ставку, що не перевищує його максимальну ціну.

Методи теорії ігор включають рішення різних видів ігрових ситуацій за допомогою математичних моделей, таких як рівноважні точки, аналіз домінантних стратегій, змішані стратегії тощо. Вони використовується для аналізу широкого кола проблем, включаючи економіку, політику, військову стратегію, бізнес та кібербезпеку.

1.2 Класифікація кібератака та кіберзагроза

Кібератаки – це зловмисні дії, спрямовані на використання комп'ютерних систем або мереж для злому, пошкодження або незаконного доступу до інформації. Існує багато типів кібератак, кожен зі своїми характеристиками та методами реалізації.

Кіберзагроза - це потенційна можливість виникнення події або ситуації, яка може викликати шкоду, порушити функціонування системи або загрожувати безпеці інформації. Це може бути будь-яка діяльність, яка має негативний вплив на інформаційну систему, комп'ютерні мережі, дані користувачів або інші цифрові ресурси. Кіберзагрози можуть включати атаки з використанням шкідливого програмного забезпечення, такі як віруси, черви, троянські програми, програми-вимагачі, шпигунські програми, а також соціальну інженерію, фішинг, DoS або DDoS атаки, кіберзлочинність і багато іншого. У сучасному світі кіберзагрози стали серйозним викликом для компаній, урядів і індивідуальних користувачів, і вимагають постійного моніторингу, захисту та реагування. Основними типами кібер загроз є:

Ось деякі з найпоширеніших видів кіберзагроз та їхні особливості [6]:

Фішинг: атака, в якій зловмисник видає себе за довірену сторону, зазвичай підробляючи електронні листи або веб-сторінки, щоб отримати конфіденційну інформацію, таку як паролі або номери кредитних карток. Фішинг може бути спрямований як на окремих користувачів, так і на організації. Інтерпретуємо як працює фішинг:

1. Зловмисники надсилають електронні листи або текстові повідомлення, які виглядають як законні повідомлення від відомої компанії або організації.
2. У повідомленні міститься посилання або кнопка, яку зловмисники хочуть, щоб ви натиснули.
3. Коли ви натискаєте на посилання або кнопку, ви переходите на фейковий веб-сайт, який виглядає як законний веб-сайт компанії або організації.
4. На фейковому веб-сайті вас просять ввести свою особисту інформацію, наприклад, пароль, номер кредитної картки або банківські реквізити.
5. Після того, як ви введете свою особисту інформацію, зловмисники можуть використовувати її для крадіжки вашої особистості, викрадення грошей з вашого банківського рахунку або здійснення інших шахрайських дій.

Віруси та черв'яки: шкідливі програми, які можуть самостійно поширюватися та пошкоджувати комп'ютерні системи. Вони можуть знищувати дані, порушувати роботу системи або використовувати комп'ютери для спаму чи атак на інші

системи. Черв'яки можуть поширюватися через мережу без участі користувача, тоді як віруси передаються через заражені файли, електронні листи тощо.

DDoS-атаки (атаки на відмову в обслуговуванні): атаки, спрямовані на перевантаження мережі або системи запитами, що порушують їх нормальну роботу. Це може призвести до недоступності веб-сайтів або мережевих послуг. Для проведення DDoS-атак зловмисники можуть використовувати ботнети або інші заражені комп'ютери.

Існує два основних типи атак DoS:

1. Атаки на основі обсягу – зловмисник надсилає велику кількість трафіку на цільову систему або мережу, щоб переповнити її пропускну здатність або ресурси. Це може бути зроблено за допомогою бот-мережі, яка складається з багатьох заражених комп'ютерів, або за допомогою спеціальних інструментів для генерування трафіку.
2. Атаки на основі запитів – зловмисник надсилає велику кількість запитів на цільову систему або мережу, щоб перевантажити її сервери або інші ресурси. Це може бути зроблено за допомогою інструментів для генерування запитів або за допомогою бот-мережі, яка надсилає багато запитів одночасно.

Атаки DoS можуть мати серйозні наслідки для організацій, такі як:

1. Фінансові втрати: Організації можуть втратити гроші через простої в роботі, втрату клієнтів або пошкодження репутації.
2. Пошкодження репутації: Атаки DoS можуть призвести до втрати довіри до організації з боку клієнтів, партнерів та інвесторів.
3. Втрата даних: У деяких випадках атаки DoS можуть призвести до втрати даних.
4. Атака, яка намагається зробити веб-сайт або службу недоступною, переповнюючи її трафіком.

Вторгнення: незаконне проникнення в комп'ютерну систему або мережу з метою отримання несанкціонованого доступу до інформації або контролю над системою. Зловмисники можуть використовувати різні методи, такі як підбір паролів, використання вразливостей програмного забезпечення або викрадення автентифікаційних даних.

Ретельна атака (APT): складна та тривала атака, зазвичай виконувана державними або спонсорованими групами. Застосовується широкий спектр методів, таких як соціальний інжиніринг, експлуатація вразливостей, шпигунство та інші техніки, для отримання доступу до критичної інформації. APT-атаки можуть тривати місяцями або навіть роками, маючи різні цілі, від користувацьких даних до технологічних розробок.

Витік інформації: незаконне розкриття конфіденційної або чутливої інформації, що може статися через вразливості в системах безпеки, недбалість персоналу, крадіжку фізичних пристроїв або інші методи. Витік інформації може бути спричинений як внутрішніми, так і зовнішніми факторами.

Це може бути будь-яка інформація, яка вважається таємною, наприклад:

1. Особиста інформація – номери соціального страхування, номери кредитних карток, адреси, номери телефонів, дати народження.
2. Медична інформація – записи про стан здоров'я, історії хвороби, рецепти на ліки.
3. Фінансова інформація – банківські виписки, дані про кредитні картки, інвестиційні рахунки.
4. Торгові секрети – інформація про продукти, послуги, маркетингові плани або технології.
5. Урядова інформація – дані про національну безпеку, військові плани або дипломатичні відносини.

Витоки даних можуть бути викликані різними факторами, такими як:

1. Ненавмисні помилки: співробітники можуть випадково надіслати електронний лист з конфіденційною інформацією не тому адресату, залишити незахищений портативний комп'ютер або викинути папери, що містять конфіденційну інформацію.
2. Зловмисні дії: хакери можуть зламати комп'ютерні системи, щоб вкрасти дані, або шантажувати компанії, погрожуючи оприлюднити дані, якщо їм не виплатять викуп.
3. Внутрішні порушення: співробітники можуть вкрасти дані та продати їх на чорному ринку або використати для особистої вигоди.

4. Витоки даних можуть мати серйозні наслідки для осіб, організацій та урядів. Ось деякі з них:

5. Крадіжка особистості: шахраї можуть використовувати викрадену особисту інформацію, щоб відкрити нові рахунки, отримати кредити або вчинити інші злочини від вашого імені.

6. Фінансові втрати: організації можуть втратити клієнтів, понести шкоду репутації та сплатити штрафи за порушення законів про конфіденційність даних.

7. Пошкодження репутації: витік даних може призвести до втрати довіри до організації з боку клієнтів, партнерів та інвесторів.

8. Втрата контролю: уряди можуть втратити контроль над конфіденційною інформацією, що може загрожувати національній безпеці.

Атаки на розширення прав доступу: це атаки, які зловмисники використовують для отримання необмеженого доступу або вищих привілеїв в системі. Для цього можуть використовуватися програмні вразливості або методи соціального інжинірингу для здобуття потрібних даних. Такі атаки можуть бути націлені як на окремих користувачів, так і на організації.

Атаки типу "людина в середині" (MitM) – це тип кібератаки, при якій зловмисник перехоплює зв'язок між двома сторонами та вставляє себе в нього. Це дозволяє зловмиснику підслуховувати або змінювати дані, що передаються між двома сторонами.

Існує декілька способів здійснення атак MitM, ось деякі з них:

1. Перехоплення Wi-Fi – зловмисник може створити фейкову точку доступу Wi-Fi з ім'ям, схожим на законну точку доступу. Коли користувач підключається до фейкової точки доступу, зловмисник може перехоплювати весь його трафік.

2. Сніффінг – зловмисник може використовувати програмне забезпечення для сніфінгу, щоб перехоплювати весь трафік, що проходить через мережу.

3. Використання SSLStrip – зловмисник може використовувати інструмент під назвою SSLStrip, щоб перехоплювати HTTPS-трафік і перетворювати його на HTTP. Це дозволяє зловмиснику підслуховувати або змінювати дані, що передаються.

Атаки MitM можуть мати серйозні наслідки, такі як:

1. Крадіжка особистої інформації – зловмисник може вкрасти особисту інформацію, таку як паролі, номери кредитних карток або банківські реквізити.

2. Фінансові втрати – зловмисник може використовувати викрадену інформацію для здійснення шахрайських дій, таких як крадіжка коштів з банківських рахунків або використання кредитних карток для несанкціонованих покупок.

3. Втрата конфіденційної інформації – зловмисник може вкрасти конфіденційну інформацію, таку як торгові секрети або державні дані.

Кібершпіонаж – це несанкціоноване отримання конфіденційної інформації з використанням комп'ютерних технологій. Він відрізняється від звичайного злодійства тим, що має на меті отримати перевагу, наприклад:

1. Економічну: викрадення торгових секретів, інформації про дослідження та розробки або планів бізнесу.

2. Політичну: отримання інформації про урядові плани, дипломатичні відносини або національну безпеку.

3. Військову: викрадення інформації про військові технології, операції або розвідку.

Як правило кібершпіонаж це сокупність всіх вище перечислених кіберзагроз так, як зловмисники використовують різноманітні методи для здійснення шпіонажу.

1.3 Рішення в умовах конфлікту: стратегії та загрози в кібербезпеці

Кібербезпека стає все більш актуальною в сучасному світі, оскільки комп'ютери, мобільні пристрої та Інтернет суттєво впливають на наше щоденне життя, бізнес-процеси та навіть національну безпеку. Зростання кіберконфліктів вимагає глибшого розуміння стратегій та рішень для їх управління.

Одним з ключових аспектів управління в умовах кіберконфлікту є розробка ефективної стратегії. Стратегія кібербезпеки має включати заходи для запобігання атак, виявлення та реагування на інциденти, а також відновлення після їх виникнення. Принцип превентивної оборони є одним з ключових принципів такої стратегії, і він передбачає прийняття заходів заздалегідь для запобігання можливим атакам[4].

Стратегії в сфері кібербезпеки можуть включати різноманітні складові, такі як:

1. Розробка політики кібербезпеки: це включає в себе визначення мети, принципів та стандартів безпеки, які необхідно дотримуватися. Також важливо враховувати юридичні, регуляторні та етичні аспекти кібербезпеки.
2. Впровадження захисних механізмів: це охоплює розробку та впровадження технічних заходів безпеки, таких як мережеві брандмауери, антивірусне програмне забезпечення, шифрування даних та інші.
3. Розробка політики управління доступом: це означає встановлення правил і обмежень для доступу до інформації та ресурсів системи в залежності від рівня довіри та привілеїв користувачів.
4. Навчання та підвищення свідомості персоналу: розуміння принципів кібербезпеки та відповідальності кожного працівника є ключовим елементом стратегії. Персонал повинен бути навчений розпізнавати потенційні загрози та дотримуватися безпечних практик використання комп'ютерів та мереж.

Небезпеки в сфері кібербезпеки можуть походити з різних джерел. Ось деякі з них:

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

2. Соціальна інженерія: це методи маніпуляції людьми з метою отримання доступу до конфіденційної інформації або змушення їх виконувати шкідливі дії.
3. Фішинг: це вид шахрайства, при якому зловмисники використовують підроблені електронні листи або веб-сайти для того, щоб обманом отримати особисті дані користувачів, такі як паролі або номери кредитних карток.
4. Внутрішні загрози: це дії зловмисників, які мають легальний доступ до системи, наприклад, співробітників організації, які зловживають своїми привілеями.

Для ефективного управління ризиками в області кібербезпеки необхідно враховувати такі аспекти[4]:

1. Аналіз потенційних загроз та їх оцінка: це допомагає готуватися до можливих атак і виявляти нові загрози.
2. Розробка та вдосконалення планів реагування на інциденти: це включає розробку процедур для виявлення та ізоляції загроз, відновлення систем та процесів після атаки, а також аналіз причин та наслідків інциденту.
3. Постійне вдосконалення захисних механізмів: У динамічному світі кіберзагроз, де ризики постійно еволюціонують, критично важливо мати гнучкі захисні механізми, які відповідають актуальним загрозам та вимогам безпеки. Навчання персоналу: постійне навчання з питань кібербезпеки допомагає зберігати усвідомленість про потенційні загрози та використовувати безпечні практики.

Розуміння стратегій та потенційних небезпечних ситуацій в кібербезпеці є ключовим для ефективного захисту інформації та систем у сучасному кіберпросторі. Постійна підготовка, вдосконалення стратегій та виявлення нових загроз допомагають зменшити ризик і забезпечити надійний рівень кібербезпеки. Крім того, важливо пам'ятати, що кібербезпека є процесом, який потребує постійного вдосконалення та оновлення, оскільки загрози в кіберпросторі постійно зростають і еволюціонують.

2 МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ З ВИКОРИСТАННЯМ ТЕОРЕТИКО-ІГРОВИХ МЕТОДІВ

2.1 Моделювання взаємодії атакуючого та захисника у кібербезпеці

Моделювання кіберзагоз з застосуванням теоретико-ігрових методів є не лише корисним, але й необхідним інструментом для покращення кібербезпеки. Вони дозволяють імітувати поведінку атакуючих та захисників під час кібератаки, що дає краще розуміння динаміки кіберзагроз та факторів, які впливають на їх успіх. Також можна використовувати для тестування та оцінки нових методів кіберзахисту, перш ніж вони будуть впроваджені в реальних системах. Ще можна використовувати для кількісної оцінки ризиків, пов'язаних зрізними кіберзагрозами, для навчання захисників тому, як реагувати на різні типи кібератак й для стимулювання інновації в галузі кібербезпеки, заохочуючи дослідників до розробки нових та креативних методів захисту. Це все може допомогти краще підготуватися до кібератак та розробити більш ефективні стратегії захисту.

Для класифікації застосування теорії ігор у вирішенні проблем безпеки можна використовувати різні підходи. Одна з ранніх системних досліджень у цьому напрямку аналізувала проблему виявлення вторгнень у формі розширеної гри. Вона описує два варіанти: кооперативну гру системи виявлення, де сенсори формують коаліції для підвищення ймовірності виявлення вторгнень, та скінченну некооперативну гру між атакуючим та системою захисту.

Напрямки дослідження можна класифікувати за предметною областю застосування. До визначених областей належать [9]:

1. Системи виявлення вторгнень.
2. Прийняття рішень після виявлення атаки.
3. Моделювання зловмисної діяльності у мережах, де мережі розглядаються як складні системи.
4. Кількісна оцінка ризиків, включаючи інвестиційні ігри.
5. Алгоритми розподілу ресурсів та розробка стійких протоколів взаємодії.
6. Приватність, довіра та зручність використання.

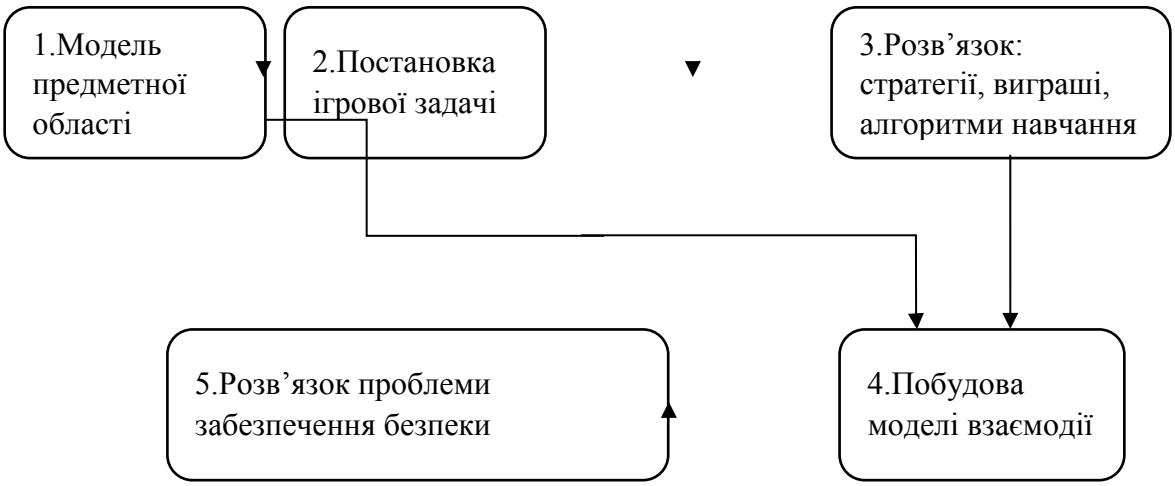
Цей підхід має очевидні переваги та практичну спрямованість. Однак, серед недоліків можна виділити ad-hoc схему і те, що різні області застосування можуть використовувати однакові ігрові моделі. Інші огляди можуть класифікувати дослідження на основі моделей теорії ігор, які застосовуються для вирішення проблем безпеки (Таблиця 2.1). Важливо пам'ятати, що використання теорії ігор для вирішення проблем у сфері безпеки є значущим і перспективним напрямком, який може принести велику користь нашому світу [3].

Таблиця 2.1 Матриця вибору методів в кіберзпеці [3]

Інформованість	Досконала	Недосконала	
	Динамічна постановка	Статистична 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 вторгнень 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 в двох гравців у якій кожний гравець намагається покращити своє знання про тип свого суперника.

2.2 Використання ігротеорії для моделювання кібератак.

Моделюючи кібератаки за допомогою теорії ігор, можна виділити декілька головних кроків, які детально описані на (Рисунку 2.1):



На Рисунку 2.1 представлена схема застосування ігрового підходу до кібербезпеки, описаного в [7, 8].

1. Моделювання предметної області є першим етапом дослідження будь-якого процесу. Він починається зі створення моделі, яка може належати до різних класів, таких як динамічні системи (неперервні, дискретні), що описуються диференціальними рівняннями (з запізненнями, імпульсним керуванням), лінійні стаціонарні системи, мультиагентні системи тощо. Після побудови моделі обирається інструментарій для її аналізу.

2. Постановка ігрової задачі - це другий етап. На цьому етапі визначаються всі ігрові характеристики: гравці, стратегії, рівень інформованості та виграші. Ставиться завдання ігрового аналізу, яке може включати формалізацію ігрової моделі, пошук рівноваги, визначення найкращих стратегій та розробку оптимальних правил, щоб результат гри відповідав заданим критеріям.

3. Розкриття стратегій, виграшів та алгоритмів навчання - третій етап. Тут вирішується завдання ігрового аналізу, включаючи пошук рівноваги, розв'язання гри (тобто обчислення найкращої поведінки гравців у кожній ситуації), визначення алгоритмів навчання, які наближаються до точки рівноваги в умовах обмеженої інформованості. Алгоритми навчання стають критично важливими

через обмежену доступність інформації в реальних системах та розподілений характер систем захисту.

4. Побудова моделі взаємодії - четвертий етап. На основі отриманих стратегій поведінки гравців та використовуючи моделі предметної області, створюється модель конфлікту для визначення важливих характеристик, таких як обчислення числових параметрів захищеності (вразливості) існуючої системи протидії. На цьому етапі стає можливим вимірювання якості системи захисту або її вразливості до певних типів атак.

5. Розв'язання проблеми забезпечення безпеки - п'ятий та останній етап. Обчислення характеристик вразливості до різних атак дозволяє сформулювати задачу забезпечення безпеки системи як задачу теорії ігор: яким вимогам має відповідати система захисту, щоб гарантувати певний виграш у випадку атаки. Для розв'язання цієї задачі застосовуються різні методи та алгоритми, які підвищують рівень захисту системи від кібератак.

Важливо зазначити, що теорія ігор має кілька ключових переваг, які сприяють її успішному застосуванню в сфері безпеки.

По-перше, вона базується на математичному апараті. Сучасні рішення з безпеки часто використовують евристики, запропоновані фахівцями на основі їхнього досвіду. Теорія ігор дозволяє застосовувати розвинений математичний апарат для моделювання ситуацій прийняття рішень агентами в умовах конфлікту і невизначеності. Це дає змогу розглядати кожну ситуацію з ширшої перспективи та проводити більш об'єктивний аналіз можливих наслідків [10].

По-друге, теорія ігор гарантує результат. Якщо захисний механізм побудований на основі аналітично розв'язаної гри і дотримуються припущення, за яких гра була визначена, то стратегія гарантує певний рівень безпеки незалежно від дій інших учасників. Таким чином, застосування теорії ігор дозволяє забезпечити стійкість до будь-яких атак і підвищити ефективність захисних механізмів [10].

Третє, ігрові моделі дозволяють створити систему взаємодії, де кожен гравець максимізує свій виграш, тим самим сприяючи загальній системі захисту. Розподілені захисні механізми виявляються більш ефективними, ніж централізоване управління, яке має численні недоліки та часто стає мішенню

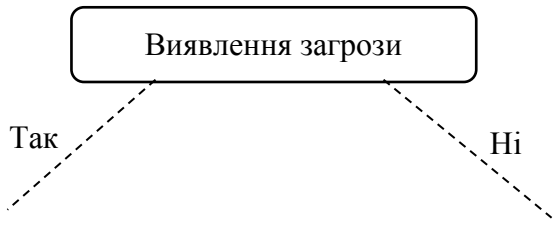
атак. Ігрові моделі дозволяють створити систему, де кожен гравець максимізує свій виграш, тим самим сприяючи загальній системі захисту. Перспективним напрямком у цій сфері є агентно-орієнтовані системи [10].

Нарешті, розробка оптимальних механізмів є важливою складовою теорії ігор. Вона досліджує створення правил гри, за яких гравці діють бажаним чином. У цьому підході можна створювати протоколи, які заохочують кооперацію між користувачами та дозволяють їм об’єднуватися для відбиття атак. Теорія ігор дозволяє розглядати ширший спектр можливих рішень та їх наслідків, що полегшує прийняття важливих рішень у сфері безпеки.

2.3 Формування стратегії кібербезпеки для захисту від кібернетичних атак.

Стратегії боротьби та уникнення кібератак, засновані на теорії ігор, застосовують концепції та методи цієї теорії для аналізу і прогнозування поведінки зловмисників, а також для розробки ефективних захисних стратегій. Мета полягає в тому, щоб розглядати кібербезпеку як гру між атакуючою стороною (зловмисником) і захисною стороною (жертвою атаки або обороняючоюся організацією), де кожна сторона приймає рішення, враховуючи можливі дії та реакції противника. Основні стратегії боротьби та уникнення кібератак, засновані на теорії ігор, включають[9]:

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 встановлення потужних брандмауерів, використання сучасного програмного забезпечення для виявлення вторгнень і шифрування всіх даних. Мета полягає в тому, щоб створити умови, за яких зловмисники відмовляться від атаки через високі витрати або низьку ймовірність успіху.



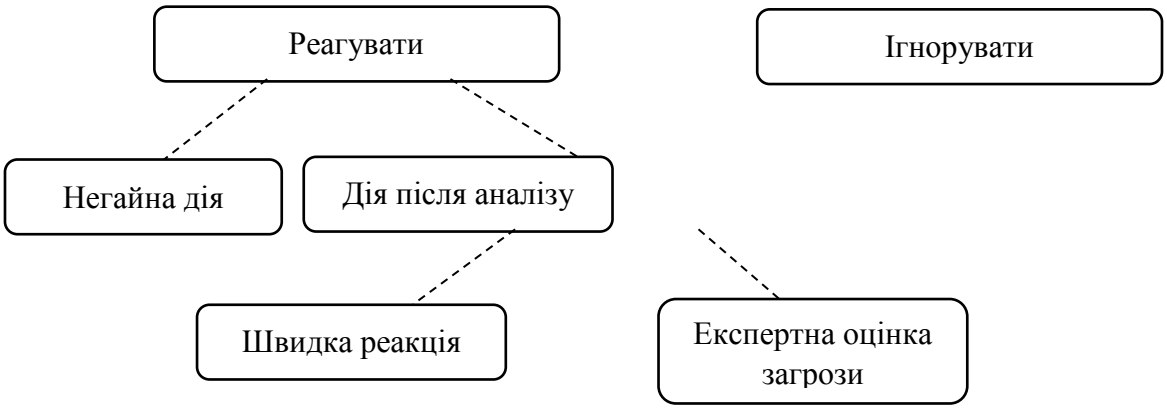


Рисунок 2.2 Схема прийняття рішень, що веде до максимального захисту від кібератак.

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

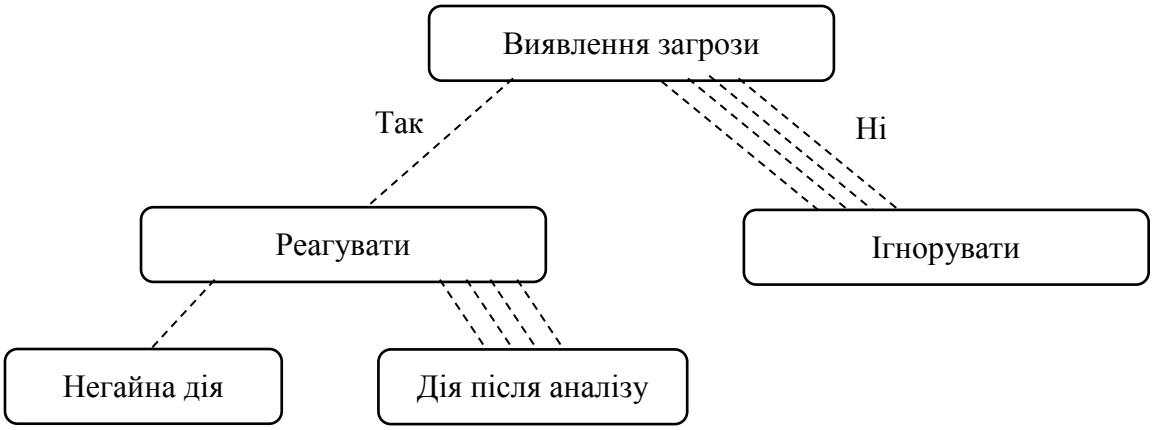


Рисунок 2.3 Схема прийняття рішень, що веде до стратегії обмеження шкоди від кібератак.

Якщо загрозу виявлено, можна вибрати між негайним реагуванням, тобто діями без подальшого аналізу, або реагуванням після аналізу, коли спочатку проводиться оцінка загрози, а потім здійснюються дії. При негайному реагуванні можуть застосовуватися автоматичні заходи захисту, наприклад, блокування IP-адрес. Реагування після аналізу передбачає участь експертів, які оцінюють загрозу та обирають методи захисту. Важливо забезпечити максимальну

швидкість реагування на загрозу, щоб мінімізувати шкоду від кібератак і підвищити ефективність захисту системи.

3. Стратегія виявлення та реагування (Detection and Response Strategy) (Рисунок 2.4): Ця стратегія спрямована на раннє виявлення атаки та оперативне реагування на неї. Вона включає використання систем моніторингу, аналізу журналів подій та інших методів для виявлення незвичайної активності та аномалій. Після виявлення атаки захисна сторона повинна мати розроблені плани реагування та відновлення для ефективного управління інцидентом.

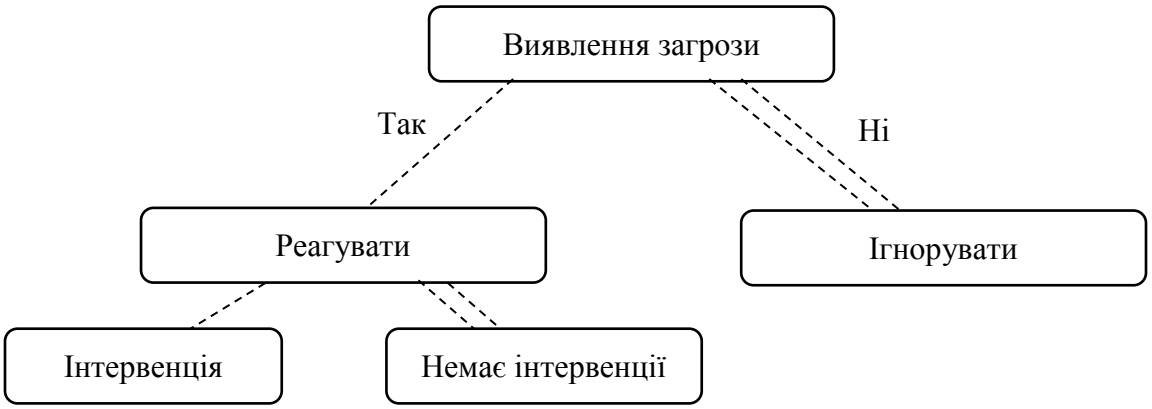


Рисунок 2.4 Схема прийняття рішень щодо виявлення та реагування на кібератаки.

4. Стратегія психологічного тиску (Psychological Pressure Strategy): Ця стратегія передбачає використання психологічних методів для відволікання уваги атакуючих або створення непередбачуваних ситуацій. Наприклад, можна використовувати фальшиві слабкі місця або підроблені дані, щоб збентежити зловмисників, змусити їх робити помилки, або спрямувати їхню увагу на інші системи, відволікаючи атаки від основної 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 у кіберпросторі, враховуючи можливі дії та відповіді противника. Наприклад, можна виявляти прогалини в безпеці, використовуючи інформацію про діяльність зловмисників, і застосовувати ці знання для покращення захисту.

Також можна розглянути використання штучного інтелекту для аналізу та прогнозування поведінки зловмисників і виявлення потенційних загроз. Крім

того, варто розглянути застосування технологій блокчейн для забезпечення безпеки даних і підвищення стійкості до кібератак.

2.4 Сильні та слабкі сторони ігрового підходу

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

Проте існують певні недоліки у сучасних підходах, які потребують додаткового розгляду:

1. Найбільш дослідженими є ігри двох учасників, тому при аналізі проблем безпеки часто намагаються звести задачу до цього формату. Однак такий підхід може призвести до втрати реалістичності у моделюванні складних процесів.
2. Матричні (статичні) ігри, що користуються популярністю через їх простоту, можуть бути нереалістичними. Більшість реальних процесів змінюються у часі, тому потребують відповідного моделювання, що може зробити матричні ігри непридатними для дослідження складних систем.
3. У звичайному моделюванні стратегій зазвичай обмежується певною скінченною кількістю можливих станів, в яких може перебувати гра. Хоча така скінчена гра може бути розв'язана, насправді кількість таких станів є нескінченною, що вимагає додаткових досліджень. Таким чином, підхід до моделювання ігор потребує подальшого вдосконалення, щоб адекватно відображати реальність складних систем безпеки.

Майбутні напрямки досліджень в області безпеки привертають значну увагу в сучасному світі. Серед них виділяються перспективні напрямки, де теоретико-ігровий підхід має потенціал для подальшого розвитку.

1. Соціальні мережі. Останнім часом соціальні мережі, такі як Фейсбук і Твіттер, стали ключовим засобом комунікації, накопичуючи значні обсяги приватних даних. Це робить їх об'єктом потенційних кібератак, а також можливим місцем для координації негативних дій, спрямованих на користувачів та компанії. Дослідники зосереджуються на розробці нових методів захисту від цих загроз [6].

2. Хмарні обчислення. Хмарні обчислення — це нова парадигма, що надає доступ до програмних та обчислювальних ресурсів через мережеві сервіси. З розвитком цих сервісів виникають проблеми побудови ефективних алгоритмів, що забезпечують їх надійну роботу. Теорія ігор, яка вже успішно застосовувалася у вирішенні різних задач, стає головним напрямком для аналітичного моделювання хмарних систем [6].

3. Інтернет речей — це технологія, що об'єднує всі "розумні" пристрої в одну мережу, яка, за прогнозами, в недалекому майбутньому стане невід'ємною частиною людського життя. Протягом наступних 10 років понад два мільярди нових пристроїв будуть підключені до цієї глобальної мережі. Це широке впровадження "розумних" речей призводить до загроз, які також стають широко поширеними. Вже спостерігається випадки появи вірусів, які можуть контролювати кавоварки, тостери та інші побутові пристрої. Тому вчені працюють над розробкою технологій, що забезпечать безпеку використання "розумних" речей [6].

4. Щодо блокчейну, ця технологія, на якій ґрунтується багато криптовалют та нових сервісів, стикається з ключовою проблемою ефективного та безпечного "майнінгу" — процесу обчислення, що підтверджує нові операції або одиниці валюти. Теорія ігор розглядає майнінг як процес взаємодії між автономними агентами, які змагаються за доступ до ресурсів. З урахуванням сучасної вартості криптовалюти біткоін, атака на механізми обчислення може бути надзвичайно прибутковою [6].

Узявши до уваги зазначене вище, можна сказати, що застосування теорії ігор у вирішенні проблем безпеки, хоч і триває вже два десятиліття, все ще є новим підходом з численними нерозв'язаними проблемами. Складність ігор з багатьма

учасниками в умовах конфлікту і невизначеності стимулює дослідників до створення нових моделей і методів, що допоможуть створити новий, безпечний та ефективний кіберпростір. Розвиток та застосування теорії ігор у зазначених напрямках досліджень є важливим кроком до забезпечення безпеки в цифровому світі. Використання теорії ігор може допомогти знизити ризики кібератак, підвищити безпеку розумних пристроїв, збільшити ефективність хмарних сервісів та забезпечити захист приватних даних у соціальних мережах. Продовження досліджень у цій галузі дозволить досягти нових результатів і створити безпечний та ефективний кіберпростір для користувачів у всьому світі.

3 МОДЕЛЮВАННЯ СТРАТЕГІЙ КІБЕРЗАГРОЗ ТА РОЗРОБКА СТРАТЕГІЇ ЗАХИСТУ ЗА ДОПОМОГОЮ ТЕОРІЇ ІГОР

31. Моделювання ігор кіберзагроз

Завдання цієї роботи полягає в застосуванні теорії ігор для запобігання кіберзагроз на систему. Мета полягає в знаходженні оптимальної стратегії захисту, яка дозволить зменшити можливі наслідки кіберзагрози та зберегти цілісність системи. Розглядається антагоністична гра у нормальній формі. Для формулювання гри необхідно описати множину гравців, їхні стратегії та виграші.

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

Після дослідження можливих варіантів атак слід оцінити різні стратегії захисту та їхні наслідки. Розглядаються такі варіанти захисту, як встановлення антивірусних програм, файрволів, систем безпеки та впровадження методів контролю доступу до системи.

Далі, застосовуючи теоретико-ігровий підхід, необхідно визначити оптимальну стратегію захисту системи від кіберзагроз. Можна використовувати різні методи теорії ігор, наприклад, алгоритми пошуку рівноваги Неша, методи мінімаксу та інші.

Отже, завдання із застосування 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 теорії ігор у вирішенні проблеми кібератак можна розглядати як гру з двома учасниками:

1. Зловмисник, який намагається скомпрометувати цільову систему.
2. Захисник, представлений власником інформаційної системи.

Зловмисник може використовувати відомі вектори атак та окремі атаки для досягнення своїх цілей або для приведення ситуації до відомої стратегії з

визначеним виграшем. Захисник повинен впроваджувати та використовувати відомі методи захисту в межах своєї інформаційної системи для протидії найбільш ймовірним атакам.

Зловмисник прагне порушити цілісність, конфіденційність та доступність інформації в атакованій системі. Захисник, навпаки, намагається запобігти цим діям. Гра має нульову суму, оскільки виграш зловмисника означає втрати для захисника. Ця гра описується як гра в нормальній формі, де пара "інформаційна атака-метод захисту" представляє зміст матриці виплат для цієї гри (Таблиця 3.1).

Таблиця 3.1Матричне представлення прикладу платіжної гри

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) і захисник (гравець 2) застосовують свої стратегії для досягнення своїх цілей. Зловмисник використовує відомі вектори атак і окремі атаки, тоді як захисник впроваджує та застосовує відомі методи захисту в межах своєї інформаційної системи. Для зловмисника виграшем є порушення цілісності, конфіденційності та доступності інформації, тоді як мета захисника — запобігти цим діям.

3.2 Аналітичне рішення задачі за допомогою математичних методів

Один із відомих чисельних методів у теорії ігор - так званий метод ітерацій. Цей метод демонструє накопичення досвіду через багаторазові повторення конфлікту [13 - 1].

Його суть полягає в розігруванні "умовної гри", де гравці (А і В) по черзі обирають свої стратегії один проти одного, прагнучи виграти якомога більше (або програти якомога менше). Кожен гравець намагається стежити за діями супротивника і реагувати на них найбільш вигідним для себе чином.

Гра імітується через серію "партій". Починається вона з того, що один з гравців (А) робить свій вибір, припустимо, він грає стратегію A_i. Перший хід гравцеві А доцільно обрати за принципом $Arg_i\{max_i\, min_j(a_{ij})\}$, вибираючи той рядок, який забезпечує найнижчу ціну гри. Супротивник (В) відповідає на цей хід своїм вибором - він обирає зі своїх стратегій B_j, яка є для нього найвигіднішою, тобто зводить його програш при стратегії A_i до мінімуму - $Arg_j\{min_j(a_{ij})\}$, обираючи стовпчик, що забезпечує мінімальний програш при вибраній гравцем А стратегії.

Далі наступає черга гравця А реагувати на дії гравця В. Гравець А відповідає гравцеві В 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 А, тобто сумарного виграшу при застосуванні стратегій A_i та 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, щоб максимізувати свій виграш і мінімізувати програш свого опонента. Цей процес триває до досягнення кінцевого результату, коли обидві сторони отримують свої оптимальні виграші та програші.

Хід гри зручно відобразити в таблиці (Таблиця 3.2.). У цій таблиці, крім описаних елементів, також представлені нижня оцінка ціни гри U, яка обчислюється як найменший середній виграш гравця A: $U_n = \frac{min_k a_{ik}^{/}}{N}$, і верхня оцінка ціни гри W, яка визначається як найбільший середній програш гравця B: $U_n = \frac{max_k a_{ik}^{/}}{N}$. Оцінка ν = (U + W) / 2 представляє наближену оцінку ціни гри, як середнє арифметичне між U та W [13].

Таблиця 3.2 Табличне представлення моделі задачі для 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^{l}	$a_{1l}^{/}$	$a_{2l}^{/}$	…	$a_{nl}^{/}$	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

Умова зупинки ітераційного методу буде наступною.

Нехай задано число ε > 0. Процес ітерацій зупиняється на кроці n, коли вперше виконується нерівність W(n) − U(n) ≤ ε. У цьому випадку ціна гри буде приблизно рівною ν ≈ (W(n) + U(n)) / 2. Змішані стратегії гравців визначаються за формулами статистичного визначення ймовірностей:

$$S_A^*(p_1^*, p_2^*, \dots, p_m^*), S_B^*(p_1^*, p_2^*, \dots, p_n^*)$$

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

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

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

Загалом, модель будь-якої матричної гри з нульовою сумою може бути зведена до задач лінійного програмування та певних математичних моделей [13].

Припустимо, що платіжна матриця гри відома, а оптимальні стратегії гравців будемо знаходити в змішаних стратегіях, описаних вище.

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

За умови, що гравець А використовує свою оптимальну змішану стратегію S_A^*, яка наразі нам невідома, гравець В обирає будь-яку чисту стратегію B_j. У такому випадку середній виграш гравця А розраховуватиметься наступним чином:

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

Але кожне із чисел a_j не може бути менше ν відповідно до теореми про активні стратегії з теорії ігор. Теорема про активні стратегії стверджує, що якщо один з гравців дотримується своєї оптимальної змішаної стратегії, то його виграш не менше ціни гри, незалежно від дій іншого гравця. Звідси в загальному випадку одержуємо n нерівностей:

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

Дана система нерівностей описує математичну модель матричної гри, знаходження оптимального рішення якої дасть шуканий результат.

3.3 Програмне втілення

Загалом, в цій системі {a – це платіжна матриця гри, υ – виграш}, який має нижню та верхню межі: α ≤ υ ≤ β, а p – змішані стратегії гравця. Оскільки гравець прагне отримати максимально можливий виграш у грі, побудуємо наступний алгоритм його дій.

1. Перевіримо чи є сідлова точка в матриці, якщо вона є тоді матрична задача розвязана, це буде означати, що виявилена стратегічна рівновага, при якій жоден з гравців не може покращити свій результат, змінюючи свою стратегію односторонньо. Така точка гарантує, що обидві сторони, дотримуючись своїх оптимальних стратегій, досягнуть стабільного результату, і гра досягне рівноважного стану. Знаходження сідлової точки значно спрощує аналіз та управління системою, оскільки дозволяє визначити чіткі та ефективні дії для кожного учасника гри. В таких умовах можна впевнено використовувати знайдені стратегії для протидії кіберзагрозам і забезпечення максимального рівня безпеки. .
2. Якщо не знаходимо сідлову точку, це означає, що стратегічна рівновага, при якій жоден з гравців не може покращити свій результат, змінюючи свою стратегію односторонньо, відсутня. У такому випадку повинні використовувати змішані стратегії, щоб досягти рівноваги. Це передбачає розробку і застосування ймовірнісних підходів, де гравці вибирають свої стратегії на основі ймовірностей, а не однієї конкретної стратегії.

Застосування змішаних стратегій включає аналіз та оптимізацію ймовірнісного розподілу стратегій кожного гравця, щоб мінімізувати ризики і максимізувати виграші в умовах невизначеності. Це складніший процес, але він дозволяє знайти

більш гнучкі та ефективні рішення, які можуть забезпечити стабільність і безпеку системи навіть в умовах відсутності чистої стратегії з сідловою точкою. Складемо тестову платіжну матрицю ймовірностей успіху противника, ці ймовірності можна отримати за допомогою статистичних досліджень (Таблиця 3.3.)

Таблиця 3.3. Тестова платіжна матриця ймовірностей

B_J / A_I	B1	B2	B3	B4	B5
A1	0,9	0,7	0,5	0,4	0,2
A2	0,4	0,8	0,6	0,8	0,4
A3	0,3	0,6	0,4	0,3	0,3
A4	0,5	0,3	0,9	0,5	0,4

Тепер для зручності обчислень помножимо усі елементи матриці на 10, очевидно що це не впливатиме на розподіл мішаних стратегій:

B_J / A_I	B1	B2	B3	B4	B5
A1	9	7	5	4	2
A2	4	8	6	8	4
A3	3	6	4	3	3
A4	5	3	9	5	4

Проведемо дослідження: MAX_MIN = 4 MIN_MAX = 4.

Сідлова точка знайдена задача виконана оптимальна точка перший рядок, п’ятий стовпчик і число 4.

Як відреагувала програма на сідлову точку (Рисунок 3.1)

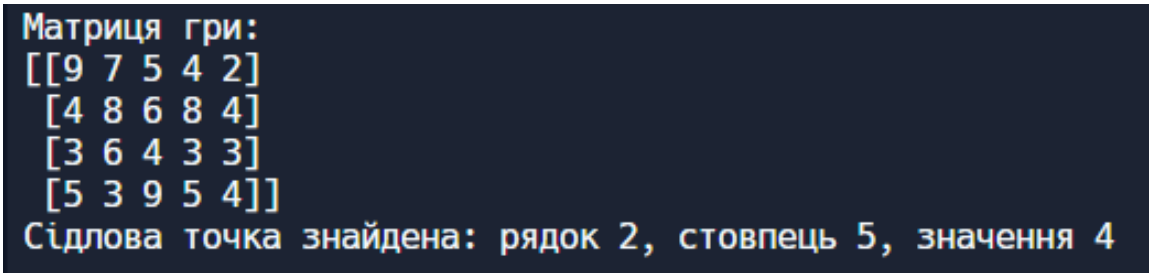


Рисунок 3.1 Результат в терміналі якщо знайїдена сідлова тоска

Розглянемо ще одну тестову платіжну матрицю з данними (Таблиця 3.4.)

Таблиця 3.4. Тестова платіжна матриця ймовірностей

B_J A_I	B1	B2	B3	B4	B5
A1	0,3	0,7	0,8	0,3	0,7
A2	0,1	0,4	0,5	0,4	0,2
A3	0,6	0,1	0,9	0,7	0,4
A4	0,8	0,3	0,1	0,5	0,2

Також для зручності обчислень помножимо усі елементи матриці на 10, очевидно що це не впливатиме на розподіл мішаних стратегій:

B_J A_I	B1	B2	B3	B4	B5
A1	3	7	8	3	7
A2	1	4	5	4	2
A3	6	1	9	7	4
A4	8	3	1	5	2

Проведемо дослідження: MAX_MIN = 3 MIN_MAX = 7.

За відсутності сідлової точки використовуємо лінійне програмування в змішаних стратегіях.[15]

Задача пошуку стратегій гравця А:

$$f = x_1 + x_2 + x_3 + x_4 \to min$$
$$3_1 + 1_2 + 6_3 + 8_4 \geq 1$$
$$7_1 + 4_2 + 1_3 + 3_4 \geq 1$$
$$8_1 + 5_2 + 9_3 + 1_4 \geq 1$$
$$3_1 + 4_2 + 7_3 + 5_4 \geq 1$$
$$7_1 + 2_2 + 4_3 + 2_4 \geq 1$$
$$x_1 \geq 0; x_2 \geq 0; x_3 \geq 0; x_4 \geq 0;$$

Задача пошуку стратегій гравця B:

$$f = y_1 + y_2 + y_3 + y_4 + y_5 \to max$$
$$3_1 + 7_2 + 8_3 + 3_4 + 7_5 \leq 1$$
$$1_1 + 4_2 + 5_3 + 4_4 + 2_5 \leq 1$$
$$6_1 + 1_2 + 9_3 + 7_4 + 4_5 \leq 1$$
$$8_1 + 3_2 + 1_3 + 5_4 + 2_5 \leq 1$$
$$y_1 \geq 0; y_2 \geq 0; y_3 \geq 0; y_4 \geq 0; y_5 \geq 0;$$

Файл який містить інформацію про матрицю під назвою “matrix.txt”

3	7	8	3	7
1	4	5	4	2
6	1	9	7	4
8	3	1	5	2

Результати програми зображено нижче (Рисунки 3.2 – 3.5)

```
Матриця гри:
[[3 7 8 3 7]
 [1 4 5 4 2]
 [6 1 9 7 4]
 [8 3 1 5 2]]
Сідлова точка не знайдена. Розв'язування гри у мішаних стратегіях...
```

Рисунок 3.2 Програма показує в терміналі нашк матрицю та та шукає сідлову точку.

Рисунок 3.3 Результати стратегій для гравця А

Рисунок 3.4 Результати стратегій для гравця В

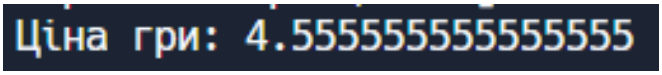


Рисунок 3.5 Результати ціни гри

Розтлумачимо стратегію гравця А:

p1=0,555555556; p2=0; p3=0,333333333; p4=0,111111111;

Це означає, що стратегії повинні бути застосовані у кількостях, пропорційних цим ймовірностям. Якщо було N атак, то першу стратегію застосовано $N * p_1$, другу — $N * p_2$ (у нашому випадку жодного разу) тощо.

У звичайних дробах це виглядає так:

$$p_1 = \frac{5}{9}, p_2 = 0, p_3 = \frac{1}{3}, p_4 = \frac{1}{9},$$

Отже, якщо атак було, наприклад, N = 90, то:

Першу стратегію потрібно застосувати – $90 \times \frac{5}{9} = 50$ разів.

Третю стратегію потрібно застосувати – $90 \times \frac{1}{3} = 30$ разів.

Четверту стратегію потрібно застосувати – $90 \times \frac{1}{9} = 10$ разів.

Таким чином, використовуючи кожну стратегію відповідно до її ймовірності, забезпечує оптимальний розподіл зусиль відповідно до обчислених пропорцій.

Ми застосували метод ітерацій для розв'язання антагоністичної матричної гри в нормальній формі, змодельованої для двох гравців (нападника та захисника) в контексті захисту комп'ютерних мереж. Цей метод передбачає поетапне проведення "умовної гри", де гравці почергово обирають свої стратегії, намагаючись максимізувати свій виграш та мінімізувати програш. Гравці використовують оптимальні стратегії для досягнення цих цілей. Процес триває

до досягнення кінцевого результату, коли обидва гравці досягають оптимальних виграшів та програшів.

Метод, заснований на теорії ігор, дозволяє знайти оптимальний розподіл бюджету між різними захисними механізмами для максимізації ефективності відбиття кібератак, враховуючи обмеження бюджету та ризики безпеки. Оскільки виграш зловмисника призводить до втрат захисника, гра є грою з нульовою сумою. Під час гри зловмисник і захисник застосовують власні стратегії для досягнення своїх цілей. Атакуюча сторона застосовує відомі вектори атак та окремі методи нападу, натомість сторона захисту використовує відомі методи захисту в межах своєї інформаційної системи. Виграш зловмисника полягає у порушенні цілісності, конфіденційності та доступності інформації, тоді як метою захисника є запобігання цим діям.

Ітераційні алгоритми, засновані на теорії ігор, є потужним інструментом для вирішення завдань захисту інформаційних систем від кібератак. Вони дозволяють знайти оптимальну стратегію захисту, яка забезпечить максимальний захист від кібератак при обмеженому бюджеті та ризиках безпеки. Крім того, цей метод дає змогу аналізувати можливості та потенційні загрози кібербезпеки, що допомагає розробляти більш ефективні стратегії захисту та вдосконалювати інформаційну безпеку загалом.

ВИСНОВОК

В ході дипломної роботи було продемонстровано важливість і актуальність застосування теорії ігор у кібербезпеці. Розроблені алгоритми та методи на основі теорії ігор показали свою ефективність у моделюванні та аналізі стратегій захисту і атак. Проведені експериментальні дослідження підтвердили, що застосування теоретико-ігрових підходів дозволяє розробляти більш інтелектуальні та адаптивні системи захисту, здатні протистояти сучасним кіберзагрозам.

Застосування теорії ігор у кібербезпеці відкриває нові перспективи для подальших досліджень та вдосконалення методів захисту інформаційних систем. Подальший розвиток цієї галузі дозволить створювати ще більш ефективні та інноваційні стратегії для забезпечення безпеки в цифровому середовищі, що є критично важливим у сучасному світі.

На основі свого досвіду та проведених досліджень, я розробив програму для пошуку оптимальної стратегії боротьби з кіберзлочинністю. Ця програма застосовує різні техніки для визначення найефективнішого плану дій у протидії кібератакам.

Мої дослідження та програма можуть бути надзвичайно корисними для будь-якої компанії або організації, яка обробляє важливу інформацію та зберігає конфіденційні дані в мережі. Використання результатів допоможе зменшити ризик кібератак і підвищити рівень кібербезпеки. Крім того, програма сприяє ефективнішому розподілу ресурсів, дозволяючи компаніям фокусуватися на найбільш критичних аспектах захисту.

Впровадження рішення забезпечить комплексний захист інформаційних систем, знижуючи ймовірність витоків даних і підвищуючи стійкість до атак. Це особливо важливо у сучасному цифровому світі, де загрози стають все більш витонченими та частими. Цей підхід також дозволяє здійснювати постійний моніторинг та вдосконалення захисних заходів, що є ключовим для підтримання високого рівня безпеки у довгостроковій перспективі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Von Neumann and Morgenstern: Theory of Games and Economic Behavior.
2. Bauso D. Game Theory: Models, Numerical Methods and Applications. Foundations and Trends in Systems and Control, vol. 1, no. 4, 2014.
3. G. Owen, Game Theory, New York: Academic Press, 3rd ed., 2001, p. 46.
4. В.А. Савченко, О.Й. Мацько: Управління ризиками кібербезпеки на основі теоретико-ігрового підходу, 2019, 16ст.
5. Frahm G. Rational Choice and Strategic Conflict. The Subjectivistic Approach to Game and Decision Theory. – Berlin/Boston: « Walter de
6. Gruyter GmbH», 2019.
7. Peter W. Singer and Allan Friedman: "Cybersecurity and Cyberwar: What Everyone Needs to Know".
8. 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.
9. Liang, Xiannuan, and Yang Xiao. Game theory for network security. IEEE Communications Surveys & Tutorials 15.1 (2013): 472-486.
10. Quanyan Zhu, Tansu Alpcan, Emmanouil Panaousis, Milind Tambe, William Casey "Decision and Game Theory for Security: 7th International Conference, GameSec 2016". 489p.
11. Stefan Rass, Stefan Schauer: "Game Theory for Security and Risk Management: From Theory to Practice", 2018, 418p
12. Теоретико-ігровий підхід до проблеми безпеки мереж О.П. Ігнатенко Проблеми програмування 2017. URL: http://dspace.nbuv.gov.ua/handle/123456789/144500
13. 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-evoluti on-of-reporting-can-change-security/

14. Corchyn L. C., Marini M. A. Handbook of Game Theory and Industrial Organization,Volume I, Theory. Edward Elgar Publishing Limited, 2018.
15. Corchyn L. C., Marini M., A. Handbook of Game Theory and Industrial Organization,Volume II, Applications. – Edward Elgar Publishing Limited, 2018.
16. Lee K. D., Hubbard S. Data Structures and Algorithms with Python. Springer, 2015. – 363 p.

ДОДАТКИ

```
import numpy as np
from scipy.optimize import linprog


def read_matrix_from_file(filename):
    with open(filename, 'r') as file:
        matrix = []
        for line in file:
            row = list(map(int, line.strip().split()))
            matrix.append(row)
        return np.array(matrix)


def find_saddle_point(matrix):
    min_in_rows = np.min(matrix, axis=1)
    max_in_cols = np.max(matrix, axis=0)

    for i in range(len(min_in_rows)):
        for j in range(len(max_in_cols)):
            if min_in_rows[i] == max_in_cols[j] ==
matrix[i][j]:
                return (i + 1, j + 1, matrix[i][j])
    return None


def solve_mixed_strategies(matrix):
    c = [1] * len(matrix)
    A = -np.transpose(matrix)
    b = [-1] * len(matrix[0])
    res = linprog(c, A_ub=A, b_ub=b, bounds=(0, None),
method='highs')
    player1_strategy = res.x / res.x.sum()
    game_value = 1 / res.fun

    c = [-1] * len(matrix[0])
    A = matrix
    b = [1] * len(matrix)
    res = linprog(c, A_ub=A, b_ub=b, bounds=(0, None),
method='highs')
    player2_strategy = res.x / res.x.sum()

    return player1_strategy, player2_strategy, game_value


def main(filename):
    matrix = read_matrix_from_file(filename)
    print("Матриця гри:")
    print(matrix)

    saddle_point = find_saddle_point(matrix)
```

```
    if saddle_point:
        print(
            f"Сідлова точка знайдена: рядок {saddle_point[0]},
стовпець {saddle_point[1]}, значення {saddle_point[2]}"
        )
    else:
        print(
            "Сідлова точка не знайдена. Розв'язування гри у
мішаних стратегіях..."
        )
        p1_strategy, p2_strategy, game_value =
solve_mixed_strategies(matrix)
        natural_game_value = round(game_value)
        print(f"Стратегія гравця A: {p1_strategy}")
        print(f"Стратегія гравця B: {p2_strategy}")
        print(f"Ціна гри: {game_value}")


if __name__ == "__main__":
    # Назва файлу з матрицею гри
    filename = 'matrix.txt'
    main(filename)
```