НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки» спеціальності 125 «Кібербезпека»

на тему: Методи теорії ігор для вдосконалення механізмів нейтралізації кіберзагроз

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-06
(шифр групи)

Кононець Владислав Миколайович
(прізвище, ім'я, по батькові) (підпис)

Керівник д.т.н., професор каф. ІБ, заслужений діяч Качинський А.Б.
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент Професор кафедри штучного інтелекту НН ІПСА, д.т.н., професор, Данілов В.Я.
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2024 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2024 р.

ЗАВДАННЯ на дипломну роботу здобувачу вищої освіти

Кононець Владислав Миколайович
(прізвище, ім'я, по батькові)

Тема роботи: Методи теорії ігор для вдосконалення механізмів нейтралізації кіберзагроз,

керівник роботи Качинський Анатолій Броніславович, доктор технічних наук, заслужений діяч,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «31» травня 2024 р. № 2251-С

1. Термін подання здобувачем вищої освіти роботи 13 червня 2024 р.
2. Вихідні дані до роботи: попередні дослідження використання методів теорії ігор для вдосконалення механізмів нейтралізації загроз.
3. Зміст роботи: дослідження предметної області, нейтралізація загроз теоретико-ігровим підходом, програмна реалізація теоретико-ігрового підходу
4. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

Презентація до захисту дипломної роботи.

5. Дата видачі завдання: 22.09.2023

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання теми роботи, визначення завдань та мети	09.11.2023	Виконано
2	Узгодження структури дипломної роботи з керівником	14.02.2024	Виконано
3	Робота над першим розділом. Вивчення теоретичного підґрунтя теорії ігор	22.02.2024-07.03.2024	Виконано
4	Робота над другим розділом. Дослідження використання теорії ігор у кібернетичній безпеці	13.03.2024-03.04.2024	Виконано
5	Проходження переддипломної практики	15.04.2024-19.05.2024	Виконано
6	Робота над третім розділом. Розробка програми для пошуку оптимальних стратегій захисту	15.04.2024-29.05.2024	Виконано
7	Графічне та текстове представлення дипломної роботи. Формування висновків	22.05.2024-30.05.2024	Виконано
8	Формування презентації дипломної роботи	01.06.2024-10.06.2024	Виконано
9	Попередній захист дипломної роботи	13.06.2024	Виконано
10	Застосування рекомендацій	14.06.2024-21.06.2024	Виконано
11	Захист дипломної роботи	24.06.2024	Виконано

Здобувач вищої освіти _____ Кононець Владислав
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

Керівник роботи _____ Анатолій КАЧИНСЬКИЙ
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**

РЕФЕРАТ

Обсяг дипломної роботи 58 сторінок, 17 ілюстрацій, 6 таблиць, 2 додатки і 26 джерел літератури.

Об’єкт дослідження: процеси стратегічної взаємодії між захисниками та зловмисниками.

Предмет дослідження: методи та моделі теорії ігор, що застосовуються для аналізу та розробки стратегій нейтралізації кіберзагроз.

Мета дослідження: дослідження методів теорії ігор та їх застосування для підвищення ефективності механізмів нейтралізації кіберзагроз.

Методи дослідження: Аналіз літератури та джерел, математичне та комп’ютерне моделювання. Симуляція гри між зловмисником і захисником.

Отримані результати: оптимальні стратегії захисника та поточний стан захищеності системи від кібератак. Знайдено шлях з мінімальними втратами у разі кібератаки.

Результати роботи були представлені на Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики».

Ключові слова: теорія ігор, нейтралізація загроз, рівновага Неша, змішані стратегії, теоретико-ігровий підхід, матрична гра.

ABSTRACT

The volume of the thesis is 58 pages, 17 illustrations, 6 tables, 2 appendices and 26 sources of literature.

Object of research: processes of strategic interaction between defenders and attackers.

Subject of research: methods and models of game theory used to analyze and develop strategies to neutralize cyber threats .

Purpose of the study: to study the methods of game theory and their application to improve the effectiveness of mechanisms for neutralizing cyber threats.

Research methods: Analysis of literature and sources, mathematical and computer modeling. Simulation of a game between an attacker and a defender.

Results: The optimal strategies of the defender and the current state of the system's security against cyberattacks. A path with minimal losses in the event of a cyberattack was found.

The results were presented at the All-Ukrainian Scientific and Practical Conference of Students, Postgraduates and Young Scientists “Theoretical and Applied Problems of Physics, Mathematics and Computer Science”.

Keywords: game theory, threat neutralization, Nash equilibrium, mixed strategies, game theory approach, matrix game.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

TCP (Transmission Control Protocol) — протокол управління передачею.

IP (Internet Protocol) — міжмережевий протокол.

ECC — еволюційно стабільна стратегія.

IDS (Intrusion Detection System) — система виявлення атак (вторгнень).

ВМ — віртуальні машини.

DDoS (Distributed Denial of Service) — розподілена атака відмови ви обслуговуванні.

ПЗ — програмне забезпечення.

SaaS (Software as a Service) — програмне забезпечення як послуга.

SCADA (Supervisory Control and Data Acquisition) — диспетчерське управління та збір даних.

ВСТУП

Теорія ігор, як один з найсучасніших математичних інструментів, знаходить дедалі ширше застосування в різних галузях знань. Вона дозволяє моделювати та аналізувати складні ситуації взаємодії між різними сторонами, де кожна з них прагне досягти своїх цілей.

Одним з найбільш перспективних напрямків застосування теорії ігор є вдосконалення механізмів нейтралізації загроз. У сучасному світі загрози можуть мати різноманітний характер – від кібернетичних атак до терористичних актів, і ефективна протидія їм вимагає не лише технічних рішень, а й стратегічного підходу, який враховує поведінку потенційних загроз і реакції на них.

Актуальність роботи: з кожним роком зростає кількість та складність кіберзагроз, що вимагає сучасного та ефективного підходу для їх нейтралізації. Методи теорії ігор є одним з таких найсучасніших математичних інструментів, що дозволяє передбачати можливі дії зловмисників та оптимізувати ресурси для їх протидії.

Мета дослідження: дослідження методів теорії ігор та їх застосування для підвищення ефективності механізмів нейтралізації загроз.

У роботі буде розглянуто основні принципи теорії ігор, їх практичне впровадження та аналіз конкретних прикладів, де такі методи вже довели свою ефективність. Спеціальна увага буде приділена розробці моделі, яка дозволить оптимально визначити можливі дії агресорів і оптимізувати стратегії захисту для мінімізації ризиків.

Предмет дослідження: методи та моделі теорії ігор, що застосовуються для аналізу та розробки стратегій нейтралізації кіберзагроз.

Об'єкт дослідження: процеси стратегічної взаємодії між захисниками та агресорами у контексті забезпечення безпеки та нейтралізації кібернетичних загроз.

Представлення роботи: Представлено роботу, як доповідь на Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики».

Публікації: Опубліковано роботу на Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики».

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд теорії ігор

Теорія ігор є розділом математики, що досліджує процес ухвалення рішень у ситуаціях, коли результат визначається діями кількох учасників. Ключові поняття в теорії ігор охоплюють гру, рішення, виграш, рівновагу та домінування.

Гра являє собою ситуацію, де кілька учасників взаємодіють та приймають рішення. Вона може мати різні форми: послідовність рішень, діалог, конкуренцію або їх комбінацію. Основним аспектом гри є конфлікт між учасниками, що потребує подальшого розв'язання.

Дії, які обирають учасники гри, називаються рішеннями. Існує декілька типів рішень, а саме: реактивні, проактивні та змішані. Якщо говорити про реактивні рішення, то це дії які приймають учасники відповідно до дій опонентів, наприклад попередні атаки беруться до уваги, щоб протидіяти поточним атакам (рисунок 1.1). Відповідно проактивні рішення це дії, що приймають учасники залежно від своїх стратегій чи цілей. Тоді змішані рішення представляють дії, що учасники приймають з використанням випадкових чи інших внутрішніх факторів. Ключовим аспектом є взаємодія рішень з іншими учасниками та реакція на їхні дії. [1]

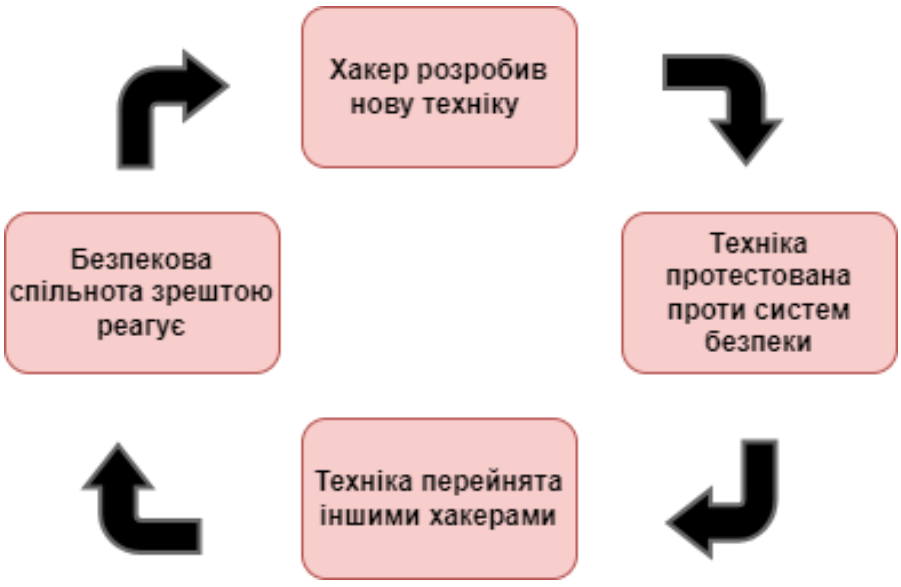


Рисунок 1.1 - Цикл реактивного підходу

Виграш – це підсумок гри для кожного з учасників. Він може бути поданий як абсолютна величина, чи як величина, що є співвідношенням до виграшу

іншого учасника. Виграш обумовлюється прийнятими рішеннями і може варіюватися в різних ситуаціях.

Рівновага — це ситуація, в якій жодна із сторін не може покращити свій виграш, змінюючи своє рішення односторонньо. Вона може бути динамічною, стратегічною і змішаною. Динамічна рівновага обумовлює стан, коли учасники приймають рішення послідовно, і будь-яке відхилення від цього порядку знижує виграш. Стратегічна рівновага виникає, коли жодна сторона не може змінити своє рішення, не погіршуючи при цьому свого виграшу. Змішана рівновага особлива тим, що сторони обирають різні рішення з певною ймовірністю.[1]

Домінування — це ситуація, коли одна зі стратегій гравця забезпечує більший виграш, ніж інша, незалежно від дій опонентів. Існує і протилежне поняття – нетранзитивність, що виникає коли певна стратегія може давати менші виграші порівняно з іншою, залежно від поведінки інших учасників.

1.1.1 Класифікація ігор

Класифікують ігри відповідно до обраного критерію. Ігри можуть відрізнятися за кількістю гравців, властивостями функцій виграшу, кількістю стратегій, а також можливостями взаємодії між учасниками гри.

Коли у грі приймають участь два гравці, то вона називається парною або грою двох осіб. Доволі часто зустрічається, що у грі приймає участь багато учасників, тоді вже гра називається множинною.

Відповідно до кількості стратегій виділяють скінченні та нескінченні ігри. У випадку, коли кожен учасник гри має скінченну кількість стратегій, гра називається скінченною. В протилежному випадку гра є нескінченною. У ситуації коли виграш одного учасника гри дорівнює програшу іншого – отримуємо гру з нульовою сумою. Гра з нульовою сумою характеризується протилежними інтересами сторін, тобто конфліктною ситуацією. Ігри з ненульовою сумою зустрічаються як за умов конфліктної поведінки гравців, так і за їх узгоджених дій.

Залежно від можливості поєднання інтересів учасників гри та домовленості між ними щодо вибору стратегій, ігри поділяються на кооперативні та

некооперативні. Кооперативні ігри передбачають можливість координувати дії гравців, тоді як у некооперативних іграх гравці не мають змоги або не бажають координувати свої дії.

Доволі часто розглядаються ігри з двома гравцями, в яких виграш одного учасника гри дорівнює програшу іншого, а сума виграшів обох учасників дорівнює нулю. Це називається грою двох осіб з нульовою сумою. Основною метою розв'язання задач цього класу є розробка рекомендацій щодо вибору оптимальних стратегій конфліктуючих сторін на основі методичних підходів теорії ігор. [2]

1.1.2 Застосування теорії ігор

Теорія ігор використовується у великій кількості галузей, таких як: економіка, інформатика, психологія, медицина та інші. Її методи допомагають нам вирішувати різні проблеми, що стосуються взаємодії між учасниками, та забезпечують оптимальне прийняття рішень.

Наприклад, у економіці вона допомагає зрозуміти поведінку споживачів та зрозуміти ринки чи певні аукціони. У комп'ютерних науках вона є в основі розробки штучного інтелекту і також певних алгоритмів. Якщо казати про соціальні науки, то теорія ігор у цьому аспекті дає уявлення про людську поведінку та соціальну динаміку. Без такого підходу не обійтись і у кібернетичній безпеці, де теорія ігор може застосовуватись для спостереження за природою кіберінциденту.

Не можна не зазначити, що теорія ігор використовується для управління та розподілу цінних ресурсів, як вода, нафта та інші природні багатства. Наприклад, водні конфлікти між країнами, які спільно використовують одну річку, можна аналізувати за допомогою теорії ігор, щоб знайти оптимальні стратегії співпраці та розподілу ресурсів. Концепції даного підходу застосовуються в мережевих протоколах і алгоритмах, зокрема в маршрутизації трафіку та балансуванні навантаження. Інтернет-протоколи, такі як TCP/IP, використовують принципи теорії ігор для ефективного розподілу мережевих ресурсів.

1.2 Роль основних методів теорії ігор у кібербезпеці

Теорія ігор пропонує численні методи, що можуть бути застосовані у питаннях кібернетичної безпеки для аналізу, захисту та виявлення загроз. Розглянемо основні з них:

1. Модель нуль-сумової гри – метод, що застосовується для аналізу рішень у конфліктних ситуаціях, де один учасник намагається здійснити проникнення у систему, а інший робить усе можливе, щоб захистити її. Використовуючи такі моделі, можна робити аналіз дій кожного з учасників гри та визначати їх втрати та виграші, що у подальшому допоможе прийняти оптимальне рішення щодо кібернетичної безпеки.
2. Теоретико-ігровий аналіз задачі на найкоротший шлях – метод для виявлення потенційних шляхів атаки та формулювання ефективних маршрутів для захисту мережі. Цей метод базується на пошуку оптимального шляху в грі, коли гравці обирають свій шлях залежно від обмежень чи цілей.
3. Прийняття рішень та аналіз ризиків – підхід, що допомагає оцінити ризик та прийняти відповідні дії щодо нього. Зазвичай використовується для моделювання різноманітних сценаріїв атак, надання імовірнісної оцінки їх виникнення та формулювання найбільш ефективних стратегій захисту. Досить важливим фактором у цьому підході є правильне визначення ризиків, пов'язаних з потенційними атаками, для забезпечення найвищого рівня захисту від них.

Методи теорії ігор у сфері кібербезпеки були класифіковані так, як зображено у Таблиці 1.1.

Таблиця 1.1 – Класифікація методів теорії ігор у кібернетичній безпеці[3]

<table>
<tr><td colspan="3">Ігрові моделі</td><td>Питання застосування та безпеки</td></tr>
<tr><td>Кооперативні ігрові моделі</td><td colspan="2">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>

Кібербезпека виступає у ролі некооперативної динамічної ігрової моделі. Аналіз динамічної моделі є досить важливим, так як стратегії зловмисників не є статичною. Щоб досягти найкращого ефекту не менш важливим є аналіз такої моделі, бо саме динамічні моделі наближені до реальних проблем кібернетичної безпеки у реальному часі. Для аналізу кіберзахисту застосовується неповна інформаційно-ігрова модель [4].

1.3 Матричні ігри двох осіб

Матрична гра — це тип гри, в якій рішення гравців і їхні виграші представлені у вигляді матриці.

Коли множини S_1 і S_2 є скінченими (два гравці) нормальну форму гри можна представити у вигляді матриці A = (α_{ij}), де елементи рядків задають стратегії одного гравця, а елементи у стовпчиках задають стратегії іншого гравця відповідно. Елементи a_{ij} матриці A є платою другого гравця першому, якщо перший гравець обирає і-у стрічку, а другий – j-й стовпчик. Коли всі значення α_{ij} відомі, то можемо представити платіжну матрицю гри (таблиця 1.2). [5]

Таблиця 1.2 — Табличне представлення функції виграшу

	B_1	B_2	..	B_j	..	B_n	
A_1	a_{11}	a_{12}	..	a_{1j}	..	a_{1n}	α
A_2	a_{21}	a_{22}	..	a_{2j}	..	a_{2n}	α_1
..	..	..	..	..	..	..	..
A_i	a_{i1}	a_{i2}	..	a_{ij}	..	a_{in}	α_i
..	..	..	..	..	..	..	..
A_m	a_{m1}	a_{m2}	..	a_{mj}	..	a_{mn}	α_m
β	β_1	B_2	..	β_j	..	β_n	

1.3.1 Максимінно-мінімаксні стратегії

Очевидно, один гравець має на меті максимізувати плату, тобто свій виграш, а інший гравець має намір мінімізувати плату — свій програш. Гра такого плану називається матричною.

Перший гравець буде намагатись одразу обрати мінімальне значення виграшу по кожній стратегії:

$$\alpha_i = \min_j a_{ij}\,, i = \overline{1, m}. \tag{1.1}$$

А вже наступним кроком поміж цих виграшів буде шукати той, що забезпечує максимум:

$$\alpha_i = \max_i \alpha_1 = \max_i \min_j \alpha_{ij}\,. \tag{1.2}$$

Величина α буде нижньою чистою ціною гри — максимінною стратегією. Її реалізація першим гравцем при будь-яких стратегіях другого гравця, забезпечує йому виграш, що не менший за α. Іншими словами це забезпечений виграш першого гравця при будь-яких стратегіях другого гравця. [5]

Другий учасник, таким чином максимізує власний програш відповідно кожної стратегії:

$$\beta_j = \max_i a_{ij}\,, j = \overline{1, n}. \tag{1.3}$$

Поміж усіх стратегій обирає ту, за якої програш найменший:

$$\beta = \max_j \beta_j = \min_j \max_i a_{ij}\,. \tag{1.4}$$

У цьому випадку величина β є верхньою чистою ціною гри (мінімаксом). І це є гарантованим програшем другого гравця при будь-яких стратегіях першого

гравця. Оптимальним розв'язком такої гри є сідлова точка — це елемент a_{kl} матриці A, що задовольняє умові (1.5) для будь-яких i та j.

$$a_{il} \leq a_{kl} \leq a_{kj}. \tag{1.5}$$

1.3.2 Застосування змішаних стратегій

Буває так, що сідлової точки у матричній грі немає, тобто наступна умова не виконується:

$$\max_i \min_j \alpha_{ij} \leq \min_j \max_i a_{ij}\,. \tag{1.6}$$

Звідси виникає ситуація, коли максимінно-мінімаксні стратегії не є оптимальними. Таким чином, кожен учасник гри може покращити свій результат, обираючи інший підхід. Тоді оптимальний розв'язок знаходять шляхом використання змішаних стратегій.

Змішані стратегії атакуючого будуть представлені у вигляді:

$$S_A = (p_1, p_2, \dots, p_m). \tag{1.7}$$

Аналогічно змішані стратегії захисника:

$$S_B = (q_1, q_2, \dots, q_m). \tag{1.8}$$

Варто зазначити, що коли застосовуються змішані стратегії, то для будь-якої скінченної гри можливо знайти пару стійких оптимальних стратегій. [5]

1.3.3 Використання рівноваги Неша у матричній грі

Якщо розглядати матричні ігри двох осіб, то доречно ознайомитись із рівновагою Неша. Це концепція у теорії ігор, що названа на честь Джона Неша - американського математика. Вона описує стан у грі, при якому жоден з учасників гри не може покращити свій виграш, змінюючи свою стратегію, коли стратегії інших гравців залишаються незмінними. Іншими словами, можна сказати, що це є набором стратегій для всіх гравців, де кожна стратегія представляє собою найкращу реакцію на стратегії інших гравців.

Надамо формальне визначення рівноваги Неша [6]. Нехай маємо кінцеву матричну гру:

$$G = (N, (S_i)_{i \in N}, (u_i)_{i \in N}), \tag{1.9}$$

де N — множина гравців;

S_i — множина стратегій гравця i;

$u_i : S_1 \times S_2 \times \ldots \times S_N \rightarrow \mathbb{R}$ — функція виграшу гравця i.

Набір стратегій $(s_1^*, s_2^*, \ldots, s_N^*)$ є рівновагою Неша, коли для кожного гравця i і будь-якої стратегії $s_i \in S_i$ виконується наступне:

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*), \tag{1.10}$$

На сьогодні є досить багато досліджень алгоритмів пошуку рівноваги Неша в задачах кібербезпеки [7]. У одному з таких досліджень, віртуальні машини (ВМ) з урахуванням безпеки були запропоновані дослідниками з використанням теорії ігор в публічному хмарному середовищі, де для гри в безпеку в публічному хмарному середовищі було включено кілька рівноваг Неша, тобто захисник має протидії на кожну зі стратегій зловмисників [7].

Варто зауважити, що доказ існування рівноваги Неша є лише логічним, а не конструктивним. Не існує методів, що дозволяють реалізувати рівновагу Неша на практиці. Усі припущення не можуть бути використані без доказів, оскільки це може призвести до порушення безпеки.

1.4 Прийняття рішень в умовах конфлікту

Кібербезпека набуває все більшої важливості взагалі по всьому світу, оскільки, мобільні пристрої, комп'ютери, носії інформації та Інтернет значно впливають на наше повсякдення, бізнес-процеси і взагалі безпеку. Кіберконфлікти на сьогодні є все поширенішими та виразнішими, що підвищує потребу в осмисленні стратегій і рішень для управління такими конфліктами.

Одним з вагомих аспектів управління конфліктами у сфері кібербезпеки є створення оптимальної стратегії. Стратегія кібербезпеки повинна мати дії, що запобігають атакам, виявляють і реагують на інциденти, і, відповідно, дії відновлення після інциденту. Серед головних принципів стратегії кібербезпеки є принцип превентивної оборони, він передбачає приймання заходів попередньо для уникнення потенційних атак [8].

Стартегії у кібернетичній безпеці представляють собою різні складові, зокрема такі як:

- Запобігання атакам: використання міжмережевих екранів (фаєрволів), систем виявлення і запобігання вторгненням, регулярні оновлення, щоб усунути вразливості у програмному забезпеченні і, відповідно, тренінги для співробітників з питань безпеки, фішингових атак та інших видів кіберзагроз
- Виявлення загроз: використання засобів моніторингу мережевих трафіків, щоб виявляти підозрілу активність, програмні рішення для автоматичного виявлення підозрілої активності та регулярний аналіз лог-файлів, щоб виявити невідповідності.
- Відновлення після інциденту: регулярне створення резервних копій важливих даних і систем та внесення змін до політик і процедур безпеки на основі висновків з аналізу інциденту.
- Оцінка та управління ризиками: постійне стеження за новими загрозами і аналіз їхньої потенційної небезпеки, проведення оцінок вразливостей для виявлення слабких місць у системах.

1.5 Кіберзагрози та їх вплив на різні галузі

Кіберзагрози стали серйозною проблемою для різних галузей. Від банків і лікарень до енергетичних компаній і державних установ, кожна галузь стикається зі своїми викликами в сфері кібербезпеки. З розвитком цифрових технологій росте і ризик кібератак, загрожуючи безпеці даних і стабільності бізнес-процесів. Наслідки таких атак можуть включати фінансові втрати, шкоду репутації, зупинку важливих сервісів і навіть загрозу національній безпеці. Тому досить важливо розуміти характер кіберзагроз і їх вплив на різні галузі, щоб розробити ефективні захисні стратегії.

1.5.1 Поширеність кіберзагроз.

В останні роки поширеними є наступні види кіберзагроз [9]:

1. Фішингові атаки.
2. Використання вразливостей.
3. Атаки шкідливим програмним забезпеченням (ПЗ).
4. DDoS-атаки.

Класифікація є дещо умовною, бо атаки шкідливим програмним забезпеченням можуть комбінуватися з використанням вразливостей чи фішингом. Ознайомимося з деякими з них детальніше.

Фішинг навіть на сьогодні є найбільш поширенішоб формою кіберзлочинів. Кажучи про 2023 рік кожен день надсилається близько 3,5 мільярда фішингових електронних листів [9]. Доступ до них зловмисники зазвичай мають після минулих кібератак із витоком даних. Як можна побачити на рисунку 1.2, цілями для фішингових атак були і є соціальні мережі, електронна пошта, SaaS та фінансові установи.

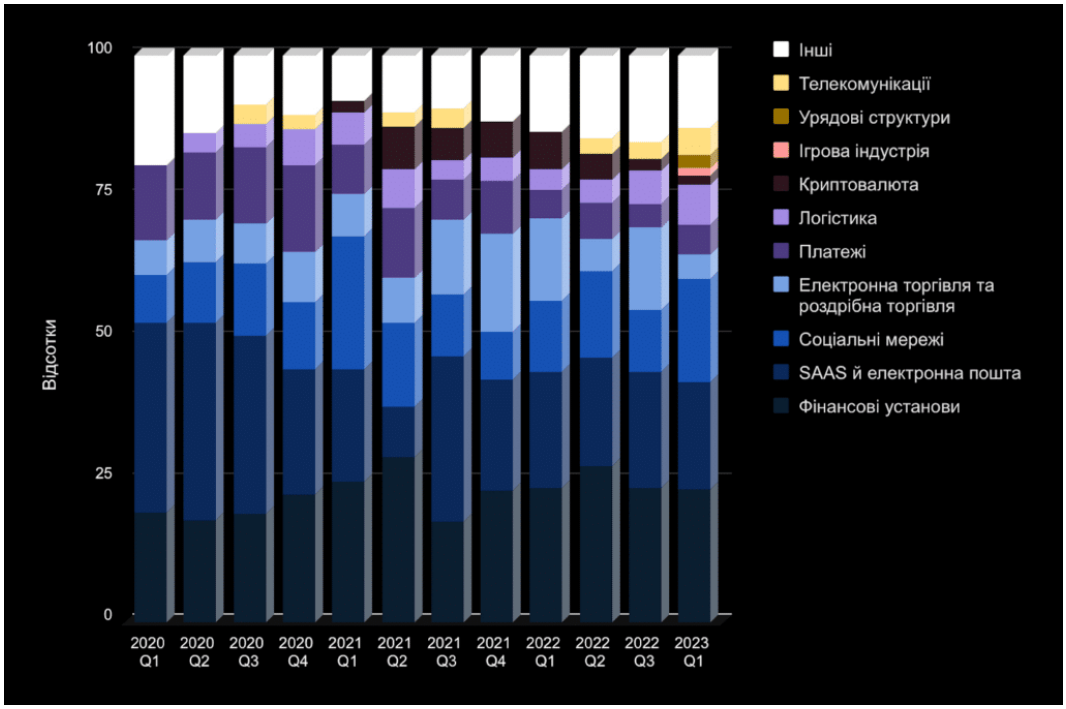


Рисунок 1.2 — Цілі фішингових атак 2020-2023 років [9]

Усе активніше здійснюються DDoS-атаки. Зловмисники атакують різні галузі і досить тяжко визначити одну або дві конкретні сфери. Тому на рисунку 1.3 зображено три найбільш цільові галузі даної загрози.

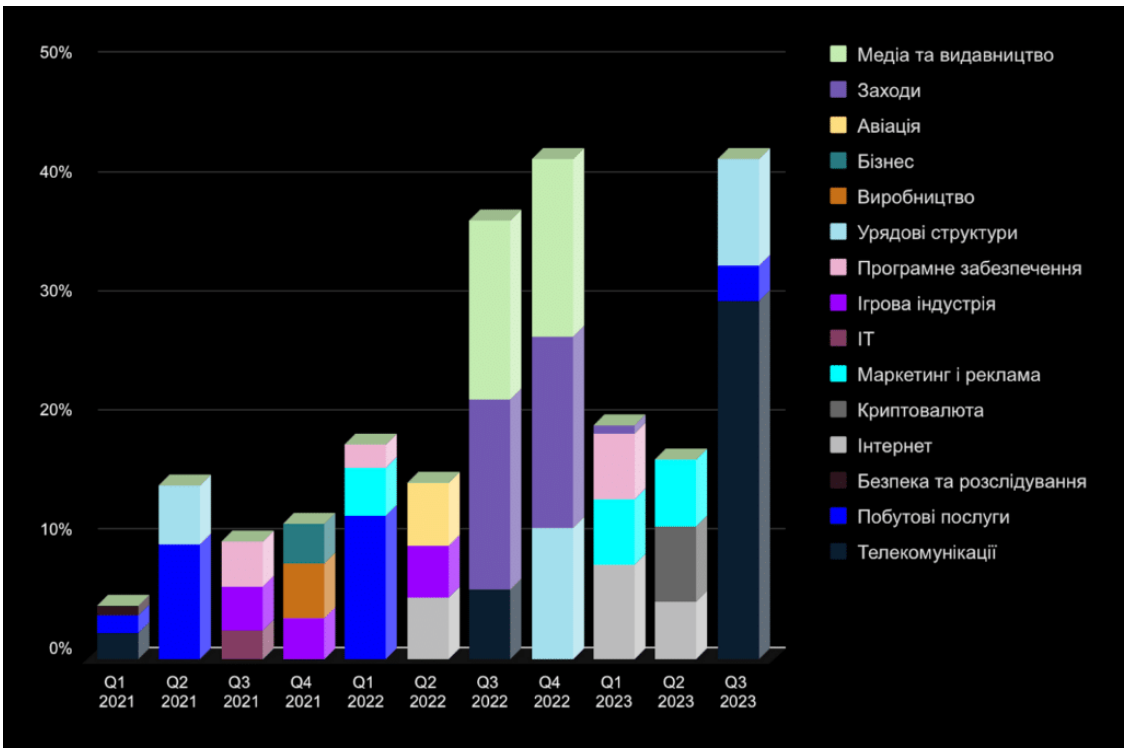


Рисунок 1.3 — Галузі, що були найбільш атакованими DDoS по кварталах 2021-2023 років [9]

1.5.2 Оцінка впливу кіберзагроз

Кіберзагрози часто взаємопов'язані та утворюють складні технологічні процеси або життєві цикли (Рисунок 1.4). Наприклад, зловмисники можуть використати викрадені дані для здійснення атак у подальшому, зокрема, атак з використанням програм-вимагачів. Кошти, що були отримані таким чином, направляються на фінансування інших шкідливих програм, ботнетів та інших атак.

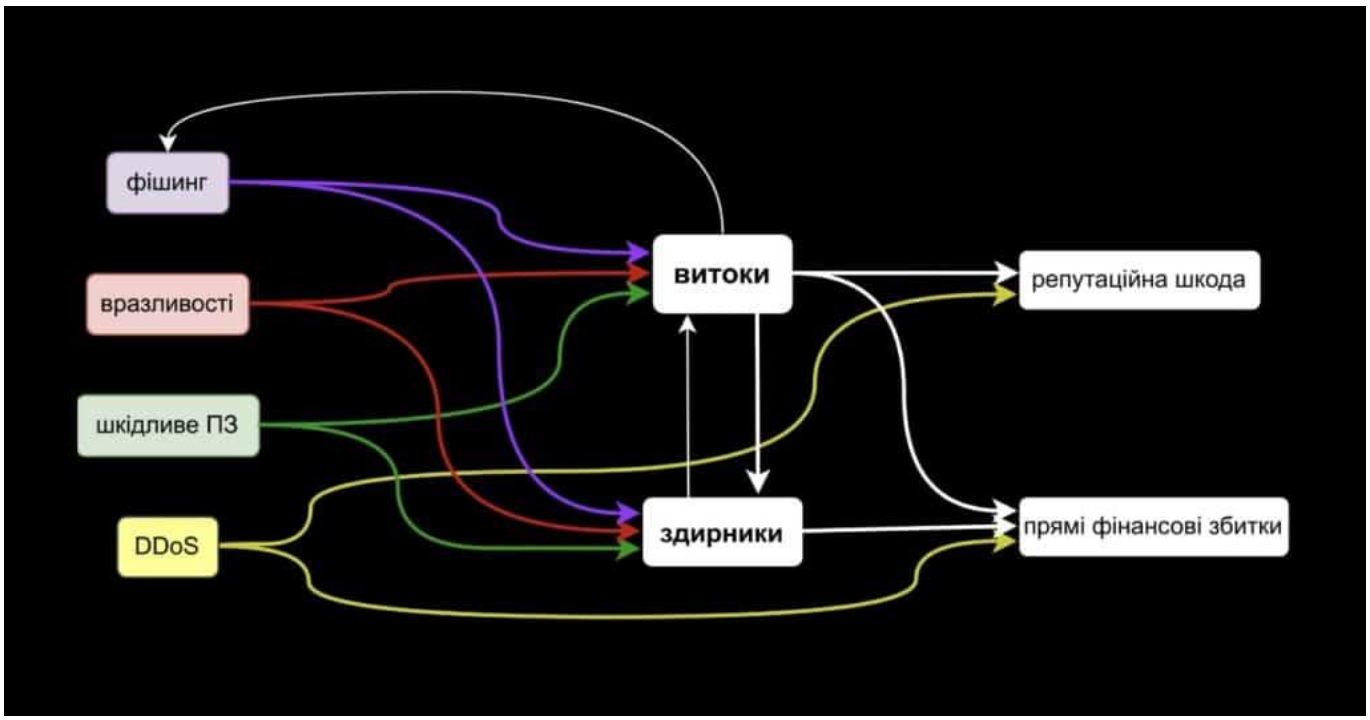


Рисунок 1.4 — Життєвий цикл кіберзагроз [9]

Необхідно усвідомлювати, що кожна така успішна атака стає частиною більшого ланцюга кіберзлочинності. Витоки даних надають джерело для нових атак, що ще більше ускладнює боротьбу з кіберзагрозами.

Станом на 2023 рік відбулися шокуючі за своїм масштабом кіберзлочини, які коштували компаніям і країнам мільярди доларів. Інформацію щодо цих злочинів та їх вплив на компанію подано у таблиці 1.3.

Таблиця 1.3 — Найбільші жертви кібератак та наслідки за 2023 рік

Жертва кібератаки	Наслідки
MOVEit	2393 організації та у рамках від 69 до 73,8 мільйона людей постраждало від витоку інформації
DarkBeam	Було вкрадено приблизно 4 млрд. електронних скриньок користувачів із їх паролями
23andMe	Потенційно викрадено мільйони наборів ДНК (точну кількість не визначено)

Кінець таблиці 1.3

Johnson Controls International	Більше 27 ТБ корпоративних даних було вкрадено та зашифровано віртуальні машини компанії VMWare ESXi
Barts Health NHS Data Breach	Витік даних, що становить 7 ТБ
Tampa General Hospital	Медичні дані близько 1,3 мільйона пацієнтів було викрадено

Доволі часто, щоб відновити дані, потрібно до одного тижня часу. Це навіть не залежить від методу їх повернення (віднова з резервної копії чи викуп). У середньому, 40% компаній відновлюють дані протягом даного терміну, у 30% випадків відновлення займає до одного місяця, а для 18% компаній необхідно від 1 до 3 місяців. Середня вартість відновлення для великої організації, без урахування викупів, за 2023 рік становить біля 1,82 млн. [9] Ця сума показує вартість простою, враховуючи, втрачений дохід, заробітні плати та інше.

Висновки до розділу 1

У сучасному цифровому світі кіберзагрози є все більш виразними й небезпечними, тому потрібно використовувати та шукати інноваційні та ефективні підходи їх нетралізації. Методи теорії ігор є одним з таких підходів для аналізу рішень та їх прийняття.

У коливаючому середовищі кіберзагроз, теорія ігор надає гнучкі інструменти, щоб адаптуватися до нових методів атак. Це допомагає підтримувати актуальність і ефективність захисних стратегій у темпі з часом.

2 НЕЙТРАЛІЗАЦІЯ ЗАГРОЗ ТЕОРЕТИКО-ІГРОВИМ ПІДХОДОМ

Нейтралізація загроз використовуючи методи теорії ігор є важливим інструментом в аналізі конфліктних ситуацій та прийнятті рішень у багатьох сферах, а саме: кібербезпека, економіка, військова справа та інші [10]. Основна ідея полягає у тому, щоб змоделювати ситуацію як гру між різними гравцями, де кожен гравець має свої цілі, стратегії та ресурси. Такий підхід не завжди має змогу повністю нейтралізувати атаку, але допомагає у зменшенні збитків після кібератаки.

Розглянемо приклад конфліктної ситуації, щоб продемонструвати як використовується даний підхід.

Приклад.

Нехай у керівника установи є m можливостей захистити дві вразливості, в свою чергу у внутрішнього порушника — n способів використання вразливостей. Припустимо, що $m > n$, тобто способів захисту більше. Тоді розглянемо стратегії керівника:

- $a_0 = (m, 0)$ — захищати тільки першу вразливість m способами.
- $a_1 = (m - 1, 1)$ — захищати першу вразливість $(\mathrm{m} - 1)$ способами, а іншу —одним.
- $a_m = (0, m)$ — захистити лише другу вразливість усіма доступними способами.

А для порушника у такому разі є такі стратегії:

- $b_0 = (n, 0)$ — застосувати тільки вразливість №1.
- $b_1 = (n - 1, 1)$ — застосувати вразливість №1 $(\mathrm{n} - 1)$ способами, а вразливість №2 — одним.
- $b_n = (0, n)$ — застосувати тільки другу вразливість усіма n способами.

Відповідно кожен виграш $U_{ij}, i = 1, \dots, m, j = 1, \dots, n$ має подане обчислення [10]:

$$U = \begin{cases} n + 1,\ m - i > n - j,\ i > j; \\ n - j + 1,\ m - i > n - j,\ i = j; \\ n - j - 1,\ m - i > n - j,\ i < j; \\ -m + i + j,\ m - i < n - j,\ i > j; \\ j + 1,\ m - i = n - j,\ i > j; \\ -m - 2,\ m - i < n - j,\ i < j; \\ -i - 1,\ m - i = n - j,\ i < j; \\ -m + i - 1,\ m - i < n - j,\ i = j; \\ 0,\ m - i = n - j,\ i = j; \end{cases}, \quad (2.1)$$

Нехай варіантів захисту у нас 4, а варіантів використати вразливість — 3, тоді маємо наступну матрицю виграшу (Таблиця 2.1).

Таблиця 2.1 — Матриця виграшу

	b_0	b_1	b_2	b_3	$\min_j U_{ij}$
a_0	4	2	1	0	0
a_1	1	3	0	-1	-1
a_2	-2	2	2	-2	-2
a_3	-1	0	3	1	-1
a_4	0	1	2	4	0

Доречно використати максимінний критерій (див. формулу 1.2):

$$\max_i (\min_j U_{ij}) = 0\,, \quad (2.2)$$

Звідси можна зробити висновок, що ефективною стратегією керівника компанії буде стратегія захисту однієї з вразливостей усіма способами, тобто (a_4, b_0) та (a_0, b_3).

2.1 Аналіз кіберзагроз методами теорії ігор

Теорія ігор є потужним інструментом для аналізу взаємодій між зловмисниками і захисниками в кіберпросторі. Вона дозволяє враховувати стратегічну поведінку обох сторін і знаходити оптимальні стратегії захисту. Її методи можуть бути використані у таких областях [11]:

1. моделювання діяльності зловмисника у мережах, де мережі аналізують, як складні системи;
2. IDS (системи виявлення вторгнень);
3. інвестиційні ігри або кількісна оцінка ризиків;
4. алгоритми розподілу ресурсів та розробка надійних протоколів взаємодії.

Теоретико-ігровий аналіз кібератак включає використання математичних моделей для оцінки стратегічної поведінки зловмисника та обирання оптимальної стратегії для зихисника, за якої загроза буде нейтралізована або збитки зменшені.

2.1.1 Аналіз та прогнозування поведінки зловмисників для формулювання стратегій захисту

Формулювання стратегій захисту вимагає вивчення поведінки зловмисника у конкретній ситуації. Найдоречніше для цього використовувати концепції з теорії ігор, щоб представити кібербезпеку як гру між учасниками, де кожен із них приймає рішення та відповідає на дії супротивника. Для боротьби та нейтралізації кіберзагроз використовуються наступні стратегії [11]:

- Стратегія обмеження збитків — вона зосереджена на тому, що неможливо забезпечити повний захист, тому потрібно акцентувати увагу на зменшенні збитків у разі кібератаки (Рисунок 2.1). Зазвичай використовують резервні копії даних чи відключають скомпрометовані системи.

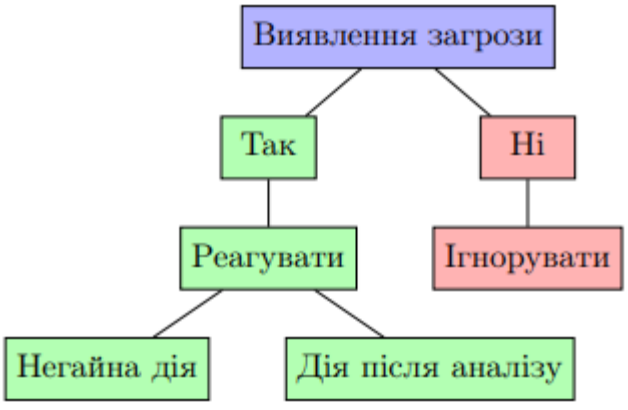


Рисунок 2.1 — Стратегія обмеження збитків

- Стратегія виявлення та реагування — у даній стратегії акцентується увага на ранньому детектуванні кіберзагрози та відповідному реагуванні на них (Рисунок 2.2). Зазвичай використовують системи моніторингу або аналізують журнали подій на випадок підозрілої активності. Якщо виявлена кіберзагроза, то захисник впроваджує план реагування і відновлення.

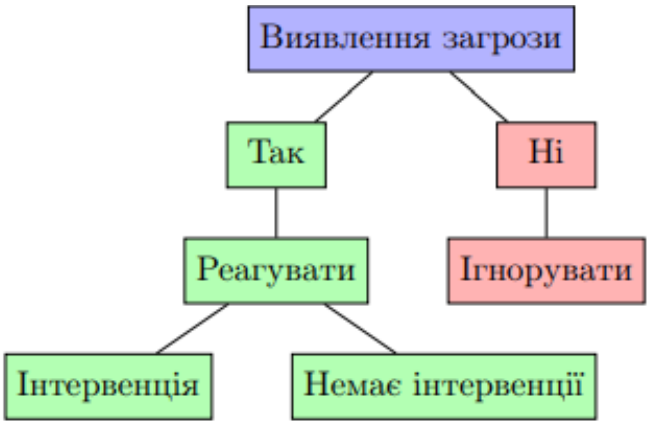


Рисунок 2.2 — Стратегія виявлення та реагування

- Fortress Strategy [12] (Стратегія Фортеці) — усі дії в даній стратегії направлені на надання найвищого рівня безпеки мережі чи системи (Рисунок 2.3). Серед таких дій є впровадження потужних фаєрволів та сучасне програмне забезпечення, що шифрує дані та виявляє вторгнення.

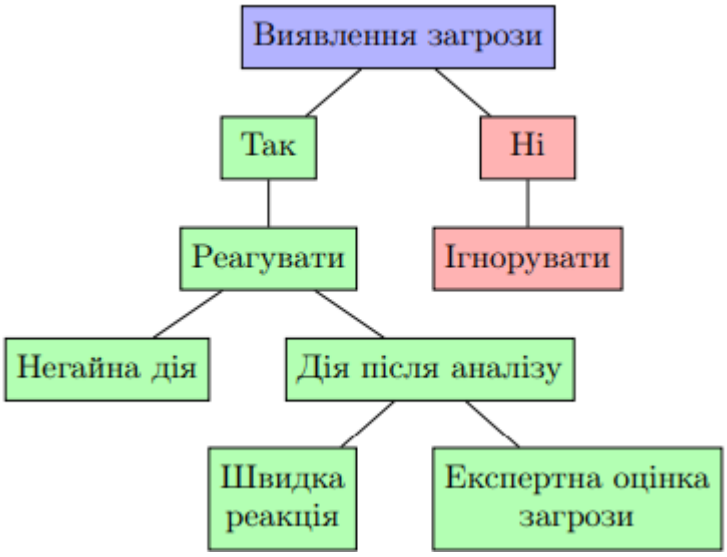


Рисунок 2.3 — Fortress Strategy

2.1.2 Використання ігрових моделей для вирішення проблем безпеки

Для вивчення дій захисника і зловмисника та моделювання взаємодії між ними використовуються різні типи ігор. У таблиці 2.1 представлені теоретико-ігрові моделі, проблеми безпеки або приватності та ключові рішення, отримані на основі відповідних моделей.

Таблиця 2.2 —Теоретико-ігрові моделі для вирішення проблем безпеки

Ігрова модель	Проблеми з безпекою	Рішення
Дилема в’язня	Егоїстична поведінка агентів у мережі [13, 14], конфіденційність у мобільних соціальних мережах [15]	Рівновага Неша
Статична гра з нульовою сумою	Глушіння та прослуховування [16], атаки на відмову в обслуговуванні [17], трояни.	Рівновага Неша
Гра Штакельберга	Кіберфізична безпека, цілісність і доступність даних [18].	Рівновага Штакельберга
Коаліційна гра	Егоїзм при пересиланні пакетів [18], прослуховуванні [19].	Алгоритм формування коаліції
Стохастична гра з нульовою сумою	Кіберфізична безпека, безпечна маршрутизація, стеганографія [20].	Рівновага (сідлова точка), Рівновага Неша
Байєсова гра	Траєкторія конфіденційності [20], атака відмова в обслуговуванні, стійкість.	Рівновага Байєса-Неша
Динамічна гра	Безпечна маршрутизація [21], кіберфізична безпека.	Сідлова точка (рівновага)
Повторювана гра	Пересилка некоректних пакетів	Стратегія на основі переконань

Кінець таблиці 2.2

Марківська гра	Конфігурація системи виявлення вторгнень (IDS) [22], захист інфраструктури Smart-grid, питання довіри в соціальній мережі.	Марківська рівновага
Еволюційна гра	Довіра в автономних багатокористувацьких мережах [23].	Еволюційно стабільна стратегія (ECC)

Якщо використовувати моделювання для різних кіберзагроз та їх реалізацій, можна зазначити основні кроки дій (Рисунок 2.4):

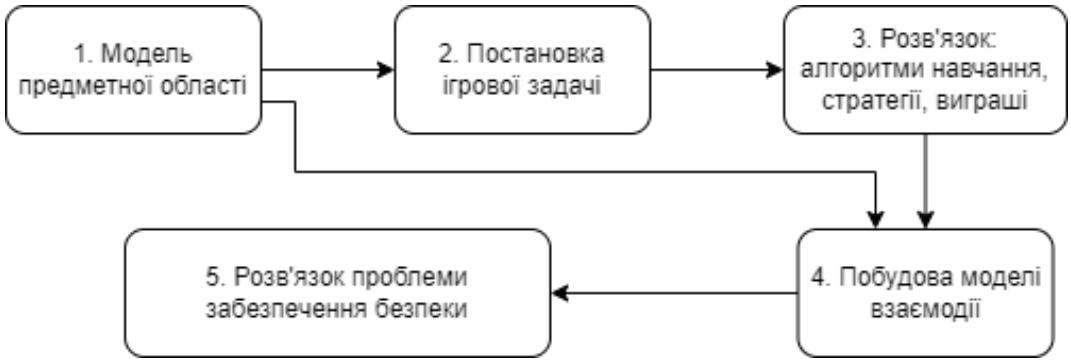


Рисунок 2.4 — Схема кроків дій ігрового підходу

2.2 Переваги та недоліки теоретико-ігрового підходу

Розглядаючи переваги методів теорії ігор, можна виділити те, що такий підхід є логічним та структурованим. Це дозволяє систематично аналізувати конфліктні ситуації між захисниками і зловмисниками. Не можна не сказати і про передбачення можливої поведінки супротивників на основі інтересів та цілей, що покращує підготовку до атак. І нарешті, теоретико-ігровий підхід допомагає ефективно розподілити обмежені ресурси для захисту, максимізуючи ефективність захисних заходів.

Звісно що серед переваг є і недоліки даного підходу:

1. Через те що найбільш вивченими є ігри двох учасників, то кожен раз при аналізі проблем безпеки зводять задачу до гри двох осіб. Проте,

це значно знижує реалістичність, якщо проводиться моделювання складніших процесів.

2. Використання матричних (статичних) ігор є не дуже реалістичним у багатьох ситуаціях через те, що багато процесів постійно змінюються з часом і це вимагає належного моделювання. Тому використання статичних матричних ігор є недоречним у дослідженні складніших систем.
3. Якщо моделювати стратегії, зазвичай визначається фіксована кількість станів, в яких можливе перебування гри. Така скінченна гра має розв’язок, але переходячи до практики, кількість таких станів є нескінченною, тому потрібні додаткові дослідження. Варіант з моделюванням гри вимагає поліпшення для того, щоб представляти реальність складніших систем.

2.3 Покращення засобів нейтралізації кіберзагроз

Покращити засоби нейтралізації кіберзагроз за допомогою методів теорії ігор наразі намагаються шляхом систематичного аналізу та оптимізації стратегій як для атакуючих, так і для захисників. Наприклад, використання еволюційних ігор допомагає у створенні фаєрволів, які можуть динамічно адаптувати свої правила фільтрації на основі аналізу поточних атак. Якщо розглядати інтелектуальні системи виявлення загроз, то застосування байєсових ігор може посприяти розробці систем виявлення загроз, що можуть враховувати невизначеність та ризики, підвищуючи точність виявлення аномалій у мережевому трафіку.

Використання коаліційних ігор для розробки спільних стратегій захисту між компаніями дозволить ефективніше реагувати на глобальні загрози. Шляхом розгляду статичних і динамічних ігор намагаються досягти оптимізації розподілу ресурсів на захист, зокрема, бюджетів на кібербезпеку, часу фахівців і технічних засобів.

Дослідження теоретико-ігрового підходу у галузі кібербезпеки наразі є перспективними, тому варто зазначити декілька з них.

Розумні будинки надають зручність, ефективність і безпеку, але також приносять нові виклики у сфері кібербезпеки. Одним з таких досліджень [24] розглядаються витрати та вигоди, пов'язані з різними стратегіями інвестування в кібербезпеку для користувачів «розумних будинків» в контексті кібератак. За допомогою еволюційної теорії ігор проводиться моделювання гри, що складається з трьох груп: користувачів «розумних будинків», зацікавлених сторін і зловмисників (Рисунок 2.5). У подальшій своїй роботі дослідники планують дослідити питання захисту розумних будинків, використовуючи теорію поведінкових ігор та моделювання за методом Монте-Карло. Це майбутнє дослідження забезпечить комплексне розуміння того, як забезпечити конфіденційність і безпеку людей які живуть в розумних будинках.

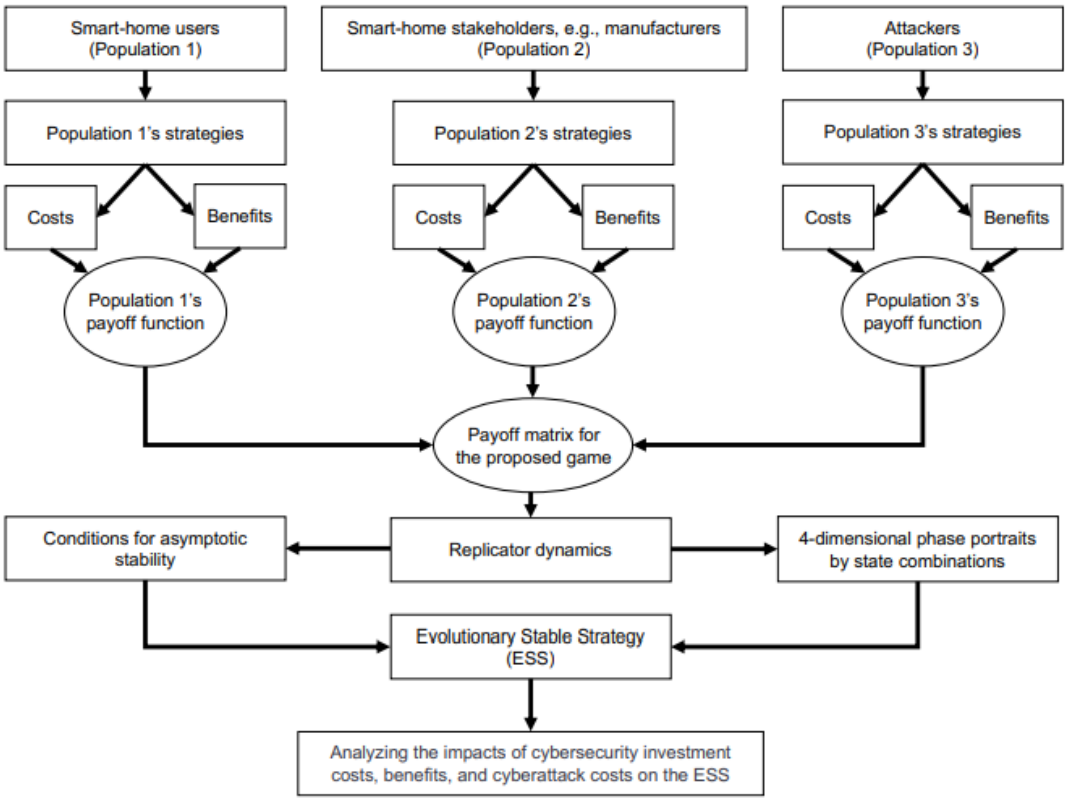


Рисунок 2.5 — Блок-схема запропонованого у дослідженні підходу[24]

Пошук економічно ефективних шляхів підвищення або покращення безпеки кіберінфраструктури є не менш важливим. Наразі є дослідження [25], що розглядає проблему розподілу ресурсів у кіберпросторі та пропонує сформулювати це як теоретико-ігрову задачу, беручи до уваги концепцію загальних знань і проблему невизначеної спостережливості.

Останнім часом конфіденційність стала критично важливою проблемою, оскільки мобільні додатки, мережі та Інтернет стрімко розвиваються. Для вирішення проблем конфіденційності в розподіленому режимі, на думку дослідників, теорія ігор є природним і потужним математичним апаратом. Тому застосовуючи наведені у таблиці 3.2 моделі і рішення, вони намагаються вирішити певні проблеми конфіденційності.[26]

Таблиця 2.3 — Короткий огляд ігрових моделей конфіденційності

Проблема конфіденційності	Ключова мета	Ігрова модель	Рішення
Криптографія	Гарантувати, що учасники продовжують користуватися визначеною послугою	Статична гра для двох гравців; Динамічна гра; Гра в екстенсивній формі; Повторювана гра; Стохастична гра для двох гравців з нульовою сумою	Рівновага Неша; Ідеальна байєсівська рівновага; Байєсівська рівновага Неша; Обчислювальна рівновага Неша; е-наближена рівновага Неша; Рівновага Неша без загроз
Анонімність	Прагнення брати участь у системі, не будучи відстеженим	Досконала і повна послідовна гра; Повторювана гра; Байєсівська гра	Підгра досконалої рівноваги; Рівновага Неша; Рівновага Баєса-Неша
Обмін інформацією	Захист конфіденційності інформації в процесі обміну інформацією	Кооперативна гра; Еволюційна гра; Стратегічна гра; Гра для двох гравців з нульовою сумою; Марковська гра	Механізм Вікрі-Кларка-Гровса; Рівновага Неша; Рівновага Маркова

Кінець таблиці 2.3

Конфіденційність	Обмежити доступ або накласти обмеження на певні види інформації	Сигнальна гра; Статична гра для двох гравців; Повторювана гра	Байєсівська рівновага; Рівновага Неша; Досконала рівновага підгри

Висновки до розділу 2

Використання методів теорії ігор для нейтралізації кіберзагроз є доволі перспективним підходом на сьогодні. Такий підхід дозволяє розглядати ігрові моделі для вирішення питань безпеки. Аналізуючи поведінку зловмисників, можна розробити стратегії боротьби з кібератаками та нейтралізації кіберзагроз.

За останній час стає все більше досліджень застосування теоретико-ігрового підходу у кібернетичній безпеці. Такі дослідження розглядають не лише соціальну сферу нашого життя, а ще й економічну та правову. Усі вони направлені на покращення засобів нейтралізації кіберзагроз або на зменшення збитків після кібератак, що дає нам зрозуміти — ріст у цьому напрямку принесе неабиякі успіхи.

Звісно, у використанні методів теорії ігор є свої недоліки у недостатній реалістичності моделей. Інколи це може призводити до прийняття помилкових рішень або дій. І дуже важливим аспектом є вдосконалення таких моделей та дослідження теоретико-ігрового підходу, щоб зробити безпечнішим кіберпростір

3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТЕОРЕТИКО-ІГРОВОГО ПІДХОДУ

Завдання полягає у тому, щоб використати методи теорії ігор для того щоб у подальшому нейтралізувати кіберзагрозу або зменшити збитки після можливої кібератаки. Для цього потрібно обрати тип гри, задати множину гравців, задати можливі кіберзагрози та варіанти реагування на них.

Щоб реалізувати такий підхід необхідно сформулювати саму задачу, отримати необхідні значення з оцінок експертів та розрахувати платежі матриці виграшу. Далі, використовуючи теорію ігор, потрібно знайти оптимальний шлях — тобто ефективну стратегію захисту.

3.1 Формулювання задачі: потреби та вимоги

У задачі розглядається виробнича система, яка може ідентифікувати 7 типів кіберзагроз, а саме: крадіжка інтелектуальної власності, злом облікових даних співробітників, зараження SCADA, злом бездротових пристроїв, захоплення виробничих машин, зараження мережі, інсайдерська атака. Таким чином, будь-які спроби завдати шкоди та атакувати ці вразливості будуть розглядатися як дії зловмисника. У свою чергу виробнича система, як захисник, має п'ять різних дій, щоб реагувати на дії зловмисника. Дані дії можуть належати до основних чотирьох типів захисної реакції, а саме: уникнути, передати відповідальність, пом'якшити або прийняти ризик. І останньою п’ятою дією є бездіяльність, яка є прийнятим типом реакції для захисника.

Таким чином, взаємодія між системою та зловмисником моделюється як матрична гра двох гравців з нульовою сумою. Дана гра є одночасною стохастичною грою, тобто обидва гравці обирають свої дії одночасно, або якщо один гравець грає раніше, інший гравець не зможе дізнатися про свій хід, доки не зробить свій вибір. Крім того, це гра з повною інформацією та раціональними гравцями, що означає, що обидва гравці знають наслідки своїх дій і обидва намагаються отримати максимальну вигоду від гри. Виходячи з визначення гри, оскільки це гра з нульовою сумою максимальний виграш для захисника полягає в тому, щоб мінімізувати шкоду для системи.

Узагальнимо системну інформацію. Система стикається із сьома різними типами кіберзагроз, A = $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ = {крадіжка інтелектуальної власності, злом облікових даних співробітників, зараження SCADA, злом бездротових пристроїв, захоплення виробничих машин, зараження мережі, інсайдерська атака}. Для протидії ним, пропонуються п'ять різних механізмів реагувань, тобто D = $\{d_1, d_2, d_3, d_4, d_5\}$ = {уникнути ризику, передати ризик, зменшити ризик, прийняти ризик, нічого не робити}. Крім того, рівень втрат виробництва відповідно до кожної дії атаки становить s = {80, 150, 200, 500, 0}, тоді як загальний обсяг виробництва становить: T = 1000. Якщо атака успішна, то вартість відновлення системи до початкового стану становить r = {140, 50, 100, 300, 120, 200, 500}. І, нарешті, матриця ефективності, яка описує поведінку кожного захисного механізму, що стикається з будь-якою із загроз, має наступний вигляд:

$$E = \begin{bmatrix} 0.8 & 0.1 & 0.1 & 0.3 & 0 \\ 0.95 & 0.1 & 0.1 & 0.3 & 0 \\ 0.1 & 0.7 & 0.5 & 0.9 & 0 \\ 0.1 & 0.85 & 0.95 & 0.7 & 0 \\ 0.2 & 0.7 & 0.8 & 0.9 & 0 \\ 0.4 & 0.85 & 0.95 & 0.1 & 0 \\ 0.05 & 0.8 & 0.2 & 0.2 & 0 \end{bmatrix} \quad (3.1)$$

Потрібно представити функцію винагороди (матрицю платежів) для моделювання мотивації нападників через концепцію винагороди та витрат, яка присвоює значення (γ_{ij}) кожній комбінації атакуючих та захисних дій.

Іншими словами, якщо зловмисник і захисник застосовують дії і та j відповідно, то (γ_{ij}) — це сума, яку виграє зловмисник, а захисник втрачає. Функція винагороди у такому випадку потрібна складається з трьох частин: вартості утримання захисного механізму, вартості виробничих втрат і вартості відновлення системи до початкового стану після атаки. Для формування цієї функції необхідно розглянути характеристику виробничих систем з точки зору кібербезпеки.

3.2 Розробка гри «Кіберзагрози»

Коли задачу вже сформовано і усі вимоги та потреби знайдено, можна переходити до моделювання такої гри. Маючи уявлення як дана задача працює математично, досить легко перейти до програмної реалізації.

3.2.1 Математичний підхід до задачі

На основі даних що маємо, першим кроком потрібно обчислити функцію винагороди (платежі матриці). Як було зазначено, дана функція буде складатися з трьох частин: вартості утримання захисного механізму, вартості виробничих втрат і вартості відновлення системи до початкового стану після атаки. Розглянемо кожну частину окремо.

Перші частина функції (рівняння 3.2) — вартість утримання оборонного механізму. Нехай $\mathrm{s} = \{s_1, s_2, \dots, s_m\}$ множина, яка включає вартість реалізації та підтримки кожної з оборонних стратегій. Дивлячись на функцію з точки зору теорії ігор, коли захисний механізм ефективний, на цьому елементі не повинно бути додатної суми. Отже, кожен такий елемент із додатньою сумою є виграшем для зловмисника [31].

$$s_j - \left(s_i \times e_{ij}\right) \tag{3.2}$$

Кожен механізм захисту може бути ефективним повністю або частково для однієї або декількох дій атаки і може бути описаний у вигляді матриці (рівняння 3.3).

$$E = \begin{array}{c} \\ a_1 \\ \vdots \\ a_n \end{array} \begin{array}{c} \begin{array}{ccc} d_1 & \dots & d_m \end{array} \\ \begin{bmatrix} e_{11} & \cdots & e_{m1} \\ \vdots & \ddots & \vdots \\ e_{n1} & \cdots & e_{nm} \end{bmatrix} \end{array}, \qquad 0 \le e_{ij} \le 1 \tag{3.3}$$

У цій матриці, якщо елемент e_{ij} дорівнює 1, то це означає, що стратегія захисту j є повністю ефективною для запобігання загрози i з боку зловмисника. Відповідно, якщо елемент дорівнює 0, це означає, що ефективність захисту j для запобігання дії i дорівнює нулю і його не можна розглядати як стратегію захисту від кібератаки з боку нападника. Чим більше маємо число, тим більший ефект захисна стратегія може мати для запобігання певному типу атаки.

Друга частина функції винагороди пов'язана з сумою грошей, яку виробник втратить внаслідок атаки. У виробничих системах найважливішими атрибутами є цілісність, доступність та узгодженість виробництва, і однією з головних цілей будь-якого зловмисника є його порушення. Якщо T — загальний обсяг виробництва, а p_i - рівень втрат виробництва для типу атаки i, який можна представити у вигляді $\mathrm{p} = \{p_1, p_2, \dots, p_n\}, 0 \leq p \leq 1$, то обчислити втрати виробництва, з урахуванням усіх типів захисних механізмів внаслідок різних дій атакуючого, можна шляхом множення загального обсягу виробництва та темпу втрат на неефективність різних механізмів.

$$T \times p_i \times \left(1 - e_{ij}\right) \tag{3.4}$$

Третя частина функції — вона є вартістю відновленням атакованої виробничої системи та поверненням її до належного (стабільного) стану. Вартість відновлення можна описати як множину $\mathrm{r} = \{r_1, r_2, \dots, r_n\}$, в якій кожен з елементів демонструє вартість відновлення внаслідок конкретної атаки [29].

$$r_i \times \left(1 - e_{ij}\right) \tag{3.5}$$

Функція винагороди може бути представлена у вигляді матриці $m \times n$, якщо це гра для двох гравців, в якій гравець у рядку є зловмисником, а гравець у стовпці — захисником.

$$\Gamma = \begin{bmatrix} \gamma_{11} & \cdots & \gamma_{1m} \\ \vdots & \ddots & \vdots \\ \gamma_{n1} & \cdots & \gamma_{nm} \end{bmatrix} \tag{3.6}$$

Враховуючи вищеописане, можна описати обрахунок кожного елемента даної матриці наступною формулою:

$$\gamma_{ij} = s_j - \left(s_i \times e_{ij}\right) + T \times p_i \times \left(1 - e_{ij}\right) + r_i \times \left(1 - e_{ij}\right), \forall\, i, j \tag{3.7}$$

Підставивши значення, які маємо, до формули 3.7 будемо мати наступну матрицю платежів:

$$E = \begin{bmatrix} 64 & 351 & 396 & 518 & 240 \\ 14 & 315 & 360 & 490 & 200 \\ 882 & 315 & 550 & 140 & 900 \\ 792 & 142.5 & 50 & 390 & 800 \\ 960 & 381 & 264 & 162 & 1120 \\ 228 & 67.5 & 25 & 720 & 300 \\ 1501 & 330 & 1360 & 1600 & 1500 \end{bmatrix} \quad (3.8)$$

Оскільки сідлова точка відсутня, то шукаємо розв'язки задачі у змішаних стратегіях. Математичну модель гравця А записуємо у вигляді:

$$\begin{gathered} Z = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 \to min \\ 64x_1 + 14x_2 + 882x_3 + 792x_4 + 960x_5 + 228x_6 + 1501x_7 \geq 1 \\ 315x_1 + 315x_2 + 142.5x_3 + 381x_4 + 67.5x_5 + 67.5x_6 + 330x_7 \geq 1 \\ 396x_1 + 360x_2 + 550x_3 + 50x_4 + 264x_5 + 25x_6 + 1360x_7 \geq 1 \\ 518x_1 + 490x_2 + 140x_3 + 390x_4 + 162x_5 + 720x_6 + 1600x_7 \geq 1 \\ 240x_1 + 200x_2 + 900x_3 + 800x_4 + 1120x_5 + 300x_6 + 1500x_7 \geq 1 \\ x_i \geq 0 \end{gathered} \quad (3.9)$$

Аналогічно для гравця В:

$$\begin{gathered} Z = y_1 + y_2 + y_3 + y_4 + y_5 \to max \\ 64y_1 + 351y_2 + 396y_3 + 518y_4 + 240y_5 \leq 1 \\ 14y_1 + 315y_2 + 360y_3 + 490y_4 + 200y_5 \leq 1 \\ 882y_1 + 315y_2 + 550y_3 + 140y_4 + 900y_5 \leq 1 \\ 792y_1 + 142.5y_2 + 50y_3 + 390y_4 + 800y_5 \leq 1 \\ 960y_1 + 381y_2 + 264y_3 + 162y_4 + 1120y_5 \leq 1 \\ 228y_1 + 67.5y_2 + 25y_3 + 720y_4 + 300y_5 \leq 1 \\ 1501y_1 + 330y_2 + 1360y_3 + 1600y_4 + 1500y_5 \leq 1 \\ y_i \geq 0 \end{gathered} \quad (3.10)$$

Далі можна вирішити систему нерівностей 3.10 симплекс-методом [30], оскільки дана задача вже має канонічну форму. Отримаємо оптимальний план $z_{max} = \frac{1489}{556140}$, $x_1 = 0$, $x_2 = \frac{719}{278070}$, $x_3 = 0$, $x_2 = \frac{17}{185380}$, $x_5 = 0$.

Щоб отримати ймовірності вибору стратегій скористаємося формулою:

$$p_i = y_i \times \partial \quad (3.11)$$

А ціну гри (∂) визначаємо для цього за формулою:

$$\partial = \frac{1}{z_{max}} \quad (3.12)$$

3.2.2 Програмна реалізація моделі

Для програмної реалізації використовувалась мова програмування Python 3.11. Робота з матрицями була реалізована розширенням мови Python — numpy. А симплекс-метод імпортовано з відкритої бібліотеки SciPy, у якій є метод linprog, для вирішення задачі лінійного программування.

Розрахунки значень матриці витрат були проведені відповідно формули 3.7, як показано на рисунку 3.1.

```
def calculate_payment_matrix():
    s = np.array([80, 150, 200, 500, 0])
    p = np.array([0.1, 0.15, 0.8, 0.5, 1, 0.1, 1])
    T = 1000
    r = np.array([140, 50, 100, 300, 120, 200, 500])
    E = np.array([
        [0.8, 0.1, 0.1, 0.3, 0],
        [0.95, 0.1, 0.1, 0.3, 0],
        [0.1, 0.7, 0.5, 0.9, 0],
        [0.1, 0.85, 0.95, 0.7, 0],
        [0.2, 0.7, 0.8, 0.9, 0],
        [0.4, 0.85, 0.95, 0.1, 0],
        [0.05, 0.8, 0.2, 0.2, 0]
    ])

    # Ініціалізуємо матрицю виплат
    Gamma = np.zeros((7, 5))

    # Обчислюємо матрицю виплат за формулою
    for i in range(7):
        for j in range(5):
            Gamma[i, j] = (s[j] - (s[j] * E[i, j]) +
                           T * p[i] * (1 - E[i, j]) +
                           r[i] * (1 - E[i, j]))
    return np.round(Gamma, decimals: 3)
```

Рисунок 3.1 — Вхідні значення задачі та розрахунок платежів матриці

Розв’язання прямої і двоїстої задачі лінійного програмуванняя зроблено імпортованим симплекс методом із зазначеними параметрами, як показано на рисунку 3.2.

```
# Обчислення результатів
matrix = np.array(matrix)
c = [-1 for _ in range(matrix.shape[1])]
b = [1 for _ in range(matrix.shape[0])]

defender = linprog(c, matrix, b, method='highs')
attacker = linprog(b, -matrix.T, c, method='highs')
game_price = round(1 / -defender.fun, 2)
```

Рисунок 3.2 — Розв’язання прямої та двоїстої задачі симплекс-методом

Відповідно, щоб розв’язати двоїсту задачу потрібно транспонувати матрицю платежів та змінити місцями вектор обмеження нерівності та коефіцієнти лінійної цільової функції.

Робимо перевірку, чи збігаються значення двоїстої задачі, що отримали з симплекс-методу із значеннями імпортованого методу linprog та отримуємо той самий результат (Рисунок 3.3).

```
Оптимальне значення функції: 0.002677383392670 91
Оптимальні змінні:
y1: 0.0
y2: 0.0025856798647822493
y3: 0.0
y4: 9.170352788866068e-05
y5: 0.0
```

Рисунок 3.3 — Значення оптимального плану двоїстої задачі

Фінальним результатом є імовірнісне значення успішності стратегій захисника та атакуючого і ціна гри (Рисунок 3.4), звідки яким можна дізнатись на захист від якої кіберзагрози акцентувати більше уваги та як зменшити втрати до мінімуму у разі кібератаки.

```
Імовірності успішності стратегій захисника:
p_y1 = 0.0
p_y2 = 0.965751
p_y3 = 0.0
p_y4 = 0.034251
p_y5 = 0.0

Імовірності успішності стратегій зловмисника:
p_x1 = 0.0
p_x2 = 0.0
p_x3 = 0.0
p_x4 = 0.0
p_x5 = 0.852924
p_x6 = 0.0
p_x7 = 0.147079

Ціна гри: 373.5
```

Рисунок 3.4 — Фінальний вивід програми

У даній задачі бачимо, зловмисник відмовляється від використання дій a_1, a_2, a_3, a_4, a_6 у довгостроковій перспективі і приймає стратегію використання a_5 та a_7 з ймовірністю 85% та 15% відповідно. Аналогічно, захисник в кінцевому підсумку відмовляється від стратегій d_1, d_3, d_5 і слідує лише стратегіям d_2 та d_4 з ймовірністю 97% і 3% відповідно. Зрештою, глобальна корисність, тобто мінімальна сума, яку втратить захисник після кібератаки буде становити 373.50. І для нього не існує кращої стратегії для мінімізації своїх збитків.

За допомогою багатоплатформної графічної бібліотеки інтерфейсів Tkinter, створено графічну програму із зазначеними вище методами та формулами, для демонстрації теоретико-ігрового підходу.

3.3 Тестування програми

Після запуску програма містить вікно у якому можливо задати свою матрицю платежів з нуля або ж обрати варіант створення обчисленої матриці платежів відповідно вхідних даних (Рисунок 3.5).

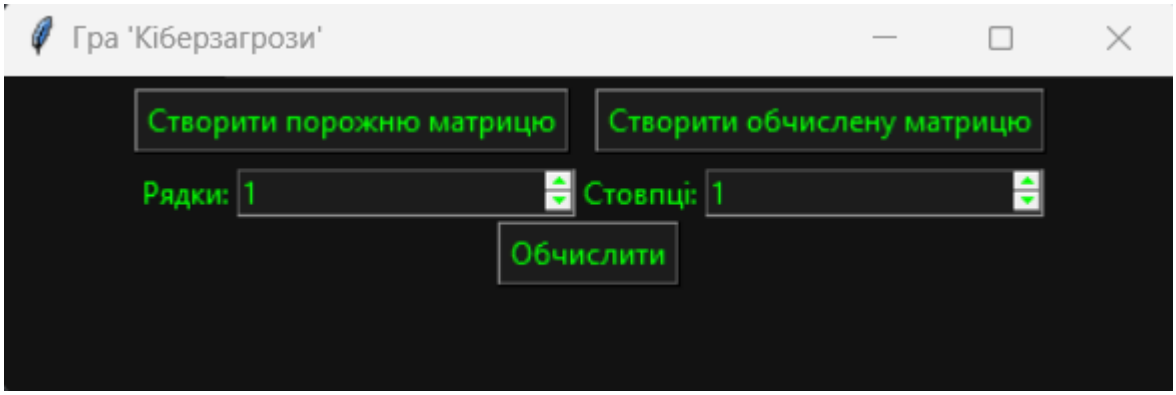


Рисунок 3.5 — Вікно після запуску програми

Якщо обрати кнопку «Створити порожню матрицю», то отримаємо вікно із зазначеними рядками та стовпцями матриці. Наприклад якщо матриця платежів матиме розмірність 3×4, то вікно прийме вигляд як показано на рисунку 3.6.

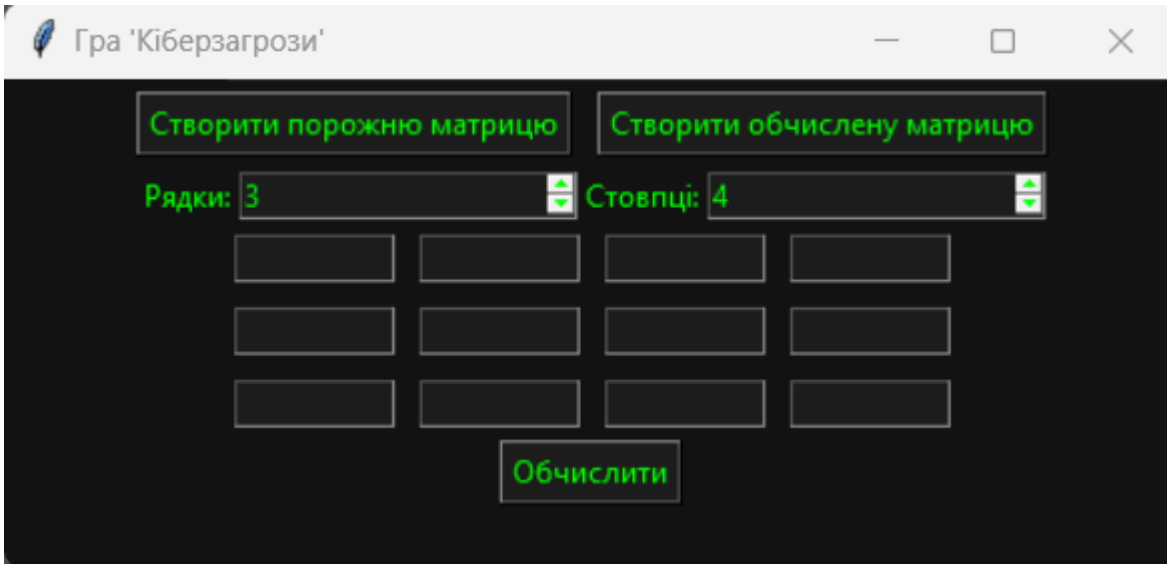


Рисунок 3.6 – Створення матриці 3×4

У випадку, коли у нас є вхідні дані, які потрібно обрахувати за формулою 3.7, щоб отримати функцію винагороди (платежі матриці) — натискаємо кнопку «Створити обчислену матрицю». На рис. 3.7 показано, що створена матриця у результаті обчислень має ті самі значення, що матриця 3.8.

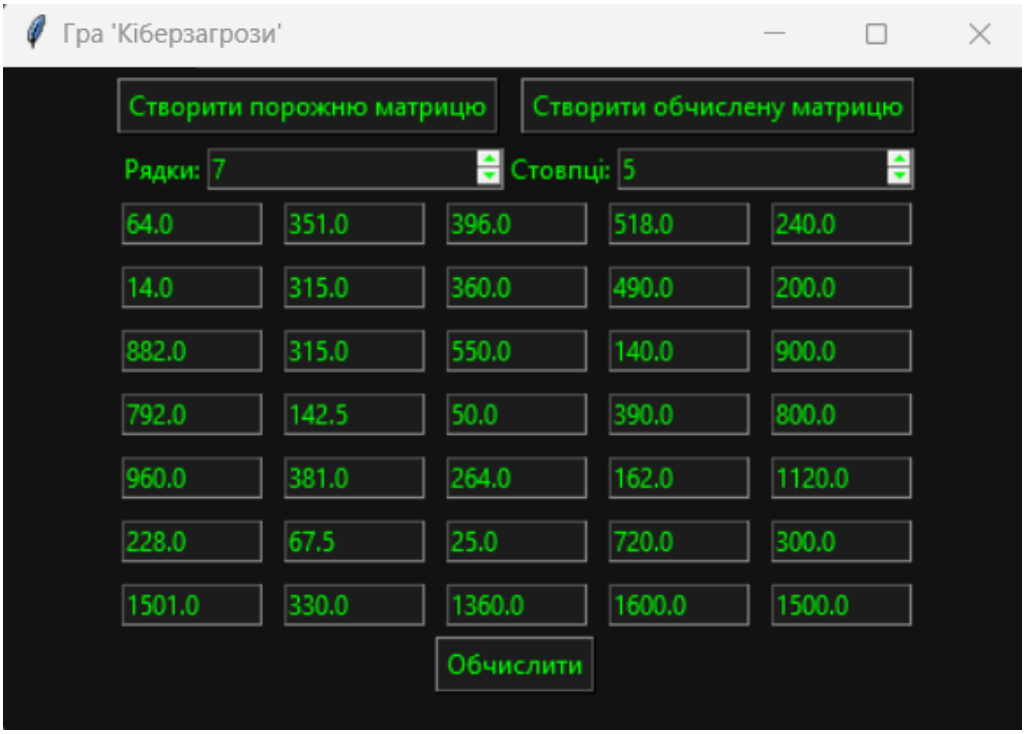


Рисунок 3.7 — Вікно після натискання кнопки «Створити обчислену матрицю»

Коли значення матриці задані після натискання кнопки «Обчислити» ми отримуємо ймовірність успіху стратегій захисника та зловмисника, з яких можемо робити висновки (Рисунок 3.8), на захист від якої загрози потрібно приділити більше уваги чи коштів. І, відповідно, яким найменшим значенням втрат зможе обійтись виробництво у разі кібератаки.

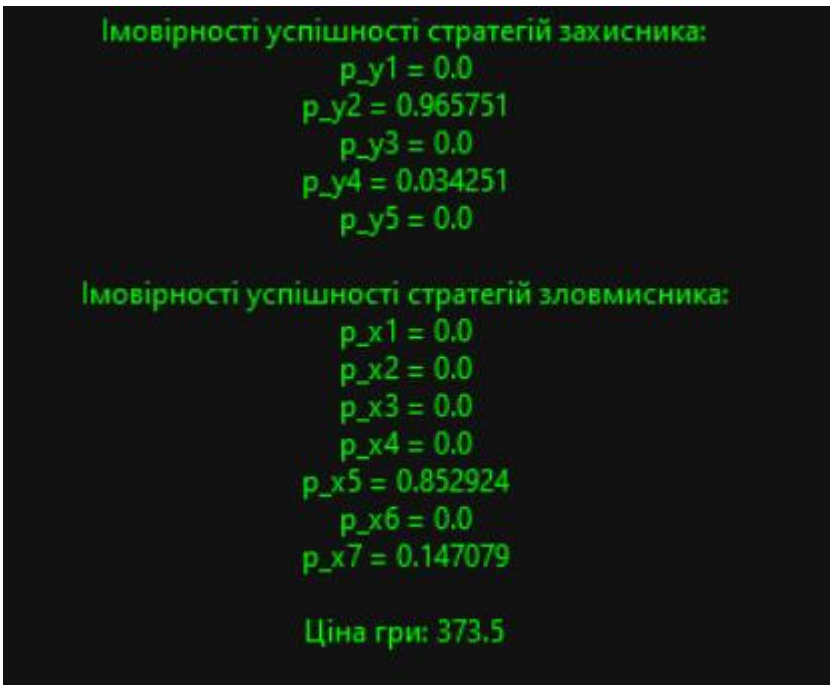


Рисунок 3.8 — Розв’язок гри з нульовою сумою та її ціна

Висновки до розділу 3

Програмна реалізація теоретико-ігрового підходу до пошуку оптимального шляху нейтралізації кіберзагроз демонструє ефективність використання методів теорії ігор для захисту виробничих систем. За допомогою моделювання взаємодії між зловмисником та захисником як матричної гри з нульовою сумою, вдалося обчислити оптимальні стратегії для обох сторін. Захисник визначає найбільш ефективні дії для мінімізації втрат. Використання симплекс-методу для вирішення задачі лінійного програмування дозволяє знайти розв'язки у змішаних стратегіях, що сприяє точнішій оцінці ризиків і потенційних збитків.

Випробування програми підтвердили, що теоретико-ігровий підхід може допомогти у визначенні пріоритетних захисних стратегій та мінімізації економічних втрат у разі кібератак. Такий підхід може бути корисним для підприємств, які прагнуть оптимізувати свої стратегії кібербезпеки та ефективніше розподіляти ресурси для захисту критичних виробничих систем.

ВИСНОВКИ

За результатами даної роботи можна зробити наступні висновки:

1. Розглянуті методи теорії ігор дозволили виділити методи, що можуть бути застосовані у вирішенні питань кібернетичної безпеки серед яких основними є: пошук рівноваги Неша, максимінна та мінімаксна стратегії, розв’язок матричної гри з нульовою сумою.

2. Виділено види найпоширеніших кібератак та їх вплив на різні галузі, серед них є: фішингові атаки, використання вразливостей, атаки шкідливим ПЗ, DDoS-атаки.

3. Досліджено використання різних методів теорії ігор та їх застосування для виявлення загроз або для вдосконалення механізмів їх нейтралізації. Дослідження виявили, що моделювання ігор між захисником та зловмисником допомагає у підвищенні ефективності стратегій захисту та оптимізації використання ресурсів для кібербезпеки.

4. Опираючись на теоретичні знання та дослідження, розроблено програму для знаходження оптимальної стратегії для нейтралізації кіберзагроз або пом’якшення збитків після їх реалізації. Програма використовує розглянуті методи, щоб віднайти найефективніший хід дій для захисника, базуючись на ефективності захисту для протидії кібератакам.

5. Тестування програми показало, що даний підхід стане у нагоді будь-якої компанії чи організації, що зберігає конфіденційні дані та хоче забезпечити мінімальні втрати виробництва, з урахуванням усіх типів захисних механізмів.

6. Використання програми є доречним і у випадку інвестицій у захисний механізм, щоб акцентувати увагу на ефективних механізмах захисту і вдосконаленні менш ефективних.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Alireza Zarreh, Can Saygin, HungDa Wan, Yooneun Lee, Alejandro Bracho. A game theory based cybersecurity assessment model for advanced manufacturing systems. – 2018 – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S2351978918308382?via%3Dihub

2. A Comprehensive Guide to Types of Games in Game Theory [Електроний ресурс] – 2024 – Режим доступу до ресурсу: https://medium.com/@systementcorp/a-comprehensive-guide-to-types-of-games-in-game-theory-18b779ef0343

3. О.П. Ігнатенко. Теоретико-ігровий підхід до проблеми безпеки мереж. – 2017 – Режим доступу до ресурсу: http://dspace.nbuv.gov.ua/handle/123456789/144500

4. G. Owen, Game Theory, New York: Academic Press, 3rd ed., 2001, p. 46.

5. Конспект лекції з теорії ігор. Режим доступу до ресурсу: https://financial.lnu.edu.ua/wp-content/uploads/2019/09/ME-lektsiia-11.pdf

6. Рівновага Неша [Електроний ресурс] – 2021 – Режим доступу до ресурсу: https://www.wikiwand.com/uk/

7. Cyber-Security and the Game Theory [Електроний ресурс] – 2022 – Режим доступу до ресурсу: https://dev.to/dev180memes/cyber-security-and-the-game-theory-58ia

8. В.А. Савченко, О.Й. Мацько. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу. – 2019 – Режим доступу до ресурсу: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2309

9. Прогноз кіберзагроз 2024 [Електроний ресурс] – 2023 – Режим доступу до ресурсу: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua

10. С.М. Шевченко, Ю.Д. Жданова, П.М. Складанний, С.В. Бойко. Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. – 2023 – Режим доступу до ресурсу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/539

11. Quanyan Zhu, Tansu Alpcan, Emmanouil Panaousis, Milind Tambe, William Casey "Decision and Game Theory for Security". 490p.

12. Mario Draper. Fortress Policy and Strategy. – 2018 – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-3-319-70386-2_6

13. Charles Kamhoua, Niki Pissinou. Mitigating selfish misbehavior in multi-hop networks using stochastic game theory – 2010 – Режим доступу до ресурсу: https://doi.org/10.1109/lcn.2010.5735709

14. Alan Busovaca, Niki Pissinou, Kia Makki. Belief-free equilibrium of packet forwarding game in ad hoc networks under imperfect monitoring. – 2010 – Режим доступу до ресурсу: https://doi.org/10.1109/pccc.2010.568229

15. Xiaohui Liang, Xu Li, Tom H. Luan, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. Morality-driven data forwarding with privacy preservation in mobile social networks. – 2012 – Режим доступу до ресурсу: http://dx.doi.org/10.1109/TVT.2012.2202932

16. Munnujahan Ara, Hugo Reboredo, Samah A. M. Ghanem, Miguel R. D. Rodrigues. A zero-sum power allocation game in the parallel Gaussian wiretap channel with an unfriendly jammer. – 2012 – Режим доступу до ресурсу: https://doi.org/10.1109/iccs.2012.6406109

17. T. Spyridopoulos, G. Karanikas, T. Tryfonas, G. Oikonomou. A game theoretic defence framework against DoS/DDoS cyber attacks. – 2013 – Режим доступу до ресурсу: https://doi.org/10.1016/j.cose.2013.03.014

18. Charles A. Kamhoua, Luke Kwiat, Kevin A. Kwiat, Joon S. Park, Ming Zhao, Manuel Rodriguez. Game Theoretic Modeling of Security and Interdependency in a Public Cloud. – 2014 – Режим доступу до ресурсу: https://doi.org/10.1109/cloud.2014.75

19. Walid Saad, Zhu Han, Tamer Basar, Merouane Debbah, Are Hjorungnes. Physical layer security: Coalitional games for distributed cooperation. – 2009 – Режим доступу до ресурсу: https://doi.org/10.1109/wiopt.2009.5291619

20. Niki Pissinou, Sitthapon Pumpichet, Xinyu Jin, Charles A. Kamhoua, Kevin Kwiat. Modeling cooperative, selfish and malicious behaviors for Trajectory Privacy Preservation using Bayesian game theory. – 2009 – Режим доступу до ресурсу: https://doi.org/10.1109/lcn.2013.6761339

21. Zhu Ji, Wei Yu, K.J. Ray Liu. A Belief Evaluation Framework in Autonomous MANETs under Noisy and Imperfect Observation: Vulnerability Analysis and Cooperation Enforcement. – 2010 – Режим доступу до ресурсу: https://doi.org/10.1109/tmc.2010.87

22. Dan Shen, Genshe Chen, Erik Blasch, George Tadda. Adaptive Markov Game Theoretic Data Fusion Approach for Cyber Network Defense. – 2007 – Режим доступу до ресурсу: https://doi.org/10.1109/milcom.2007.4454758

23. Charles A. Kamhoua, Niki Pissinou, Kia Makki. Game Theoretic Modeling and Evolution of Trust in Autonomous Multi-Hop Networks: Application to Network Security and Privacy. – 2011 – Режим доступу до ресурсу: https://doi.org/10.1109/icc.2011.5962511

24. N’guessan Y.-R. Douha, Masahiro Sasabe, Yuzo Taenaka and Youki Kadobayashi. An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users against Cyberattacks. – 2023 – Режим доступу до ресурсу: https://doi.org/10.3390/app13074645

25. В.М. Горбачук, Г.В. Голоцуков, М.С. Дунаєвський, А.А. Сирку, С.-Б. Сулейманов. Теоретико-ігрові та оптимізаційні моделі і методи підвищення безпеки кіберінфраструктур. – 2022 – Режим доступу до ресурсу: https://doi.org/10.34229/2786-6505-2022-2-6

26. Cuong T. Do, Nguyen H. Tran and Choongseon Hong, A. Kamhoua, Kevin A. Kwiat, and Erik Blasch. Game Theory for Cyber Security and Privacy. – 2017 – Режим доступу до ресурсу: http://dx.doi.org/10.1145/3057268

ДОДАТОК А

“game_theory.py”

```
import numpy as np
import tkinter as tk
from tkinter import messagebox
from scipy.optimize import linprog


def calculate_matrix_cost():
    s = np.array([80, 150, 200, 500, 0])
    p = np.array([0.1, 0.15, 0.8, 0.5, 1, 0.1, 1])
    T = 1000
    r = np.array([140, 50, 100, 300, 120, 200, 500])
    E = np.array([
        [0.8, 0.1, 0.1, 0.3, 0],
        [0.95, 0.1, 0.1, 0.3, 0],
        [0.1, 0.7, 0.5, 0.9, 0],
        [0.1, 0.85, 0.95, 0.7, 0],
        [0.2, 0.7, 0.8, 0.9, 0],
        [0.4, 0.85, 0.95, 0.1, 0],
        [0.05, 0.8, 0.2, 0.2, 0]
    ])

    # Ініціалізуємо матрицю виплат
    Gamma_matrix = np.zeros((7, 5))

    # Обчислюємо матрицю виплат за формулою
    for i in range(7):
        for j in range(5):
            Gamma_matrix[i, j] = (s[j] - (s[j] * E[i, j]) +
                                  T * p[i] * (1 - E[i, j]) +
                                  r[i] * (1 - E[i, j]))
    return np.round(Gamma_matrix, 3)


def probabilities():
    try:
        # Отримання введеної матриці з поля вводу
```

```
matrix = []
for i in range(len(matrix_entries)):
    row_player = []
    for j in range(len(matrix_entries[0])):
        entry_value = matrix_entries[i][j].get()
        # Перетворення значення строки в число
        row_player.append(float(entry_value))
    matrix.append(row_player)

# Обчислення результатів
matrix = np.array(matrix)
c = [-1 for _ in range(matrix.shape[1])]
b = [1 for _ in range(matrix.shape[0])]

defender = linprog(c, matrix, b, method='highs')
attacker = linprog(b, -matrix.T, c, method='highs')
game_price = round(1 / -defender.fun, 2)

defender_optimal_strategies = []
defender_non_optimal_strategies = []
attacker_optimal_strategies = []
attacker_non_optimal_strategies = []

if defender.success:
    for i, var in enumerate(defender.x):
        prob = round(var * game_price, 6)
        if prob > 0:
            defender_optimal_strategies.append(f"p_y{i + 1} = {prob}")
        else:
            defender_non_optimal_strategies.append(f"p_y{i + 1} = {prob}")
else:
    result_label.config(text="Рішення для захисника не знайдено.")
    return

if attacker.success:
    for i, var in enumerate(attacker.x):
        prob = round(var * game_price, 6)
        if prob > 0:
```

```
                attacker_optimal_strategies.append(f"p_x{i + 1} = {prob}")
            else:
                attacker_non_optimal_strategies.append(f"p_x{i + 1} = {prob}")
        else:
            result_label.config(text="Рішення для зловмисника не знайдено.")
            return

        result_text = ""

        if defender_optimal_strategies:
            result_text += "Оптимальне застосування стратегій забезпечить безпеку системи: " + ", ".join(defender_optimal_strategies) + ".\n"
        if defender_non_optimal_strategies:
            result_text += "Реалізація таких стратегій захисника не є оптимальним рішенням: " + ", ".join(defender_non_optimal_strategies) + ".\n"

        result_text += "\n"

        if attacker_optimal_strategies:
            result_text += "Варто прийняти до уваги та підвищити захист проти таких загроз: " + ", ".join(attacker_optimal_strategies) + ".\n"
        if attacker_non_optimal_strategies:
            result_text += "Реалізація таких стратегій зловмисника не є оптимальним рішенням: " + ", ".join(attacker_non_optimal_strategies) + ".\n"
        result_text += f"\nЦіна гри: {game_price}"

        # Вивід результатів у консоль
        print(result_text)

        result_label.config(text=result_text)
    except Exception as e:
        messagebox.showerror("Помилка", f"Помилка: {e}")


def update_matrix_entries(matrix=None):
    try:
        # кількість рядків та стовпців зі спінбоксів
        rows = int(rows_spinbox.get())
        columns = int(columns_spinbox.get())
```

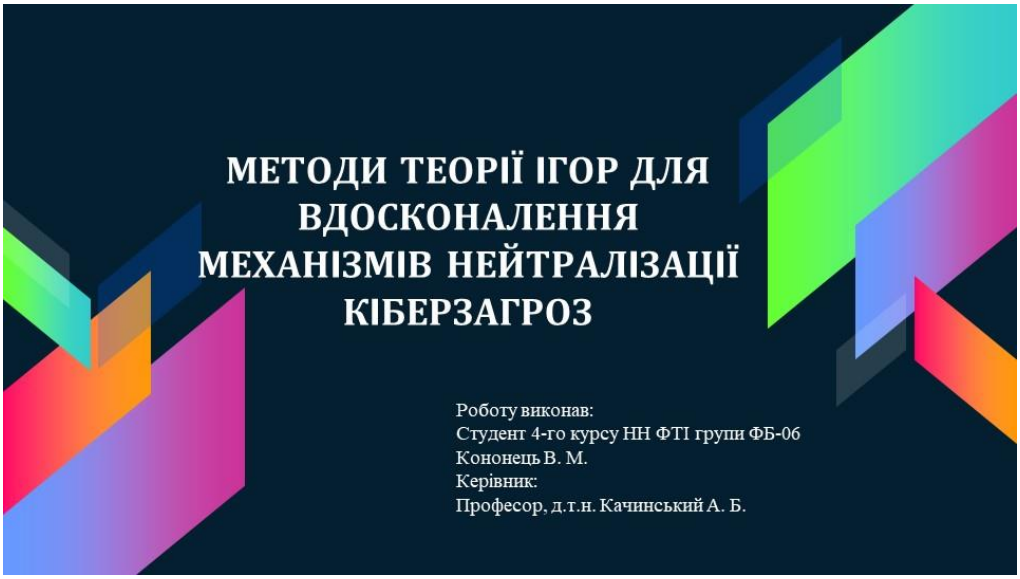
```
        # очищення попередніх полів введення
        for row in matrix_entries:
            for entry in row:
                entry.destroy()

        # створення нових полів введення
        matrix_entries.clear()
        for i in range(rows):
            row_entries = []
            for j in range(columns):
                entry = tk.Entry(matrix_frame, width=10, bg="#1c1c1c", fg="#00ff00",
insertbackground="#00ff00")
                entry.grid(row=i, column=j, padx=5, pady=5)
                if matrix is not None:
                    entry.insert(0, str(matrix[i, j]))
                row_entries.append(entry)
            matrix_entries.append(row_entries)
    except ValueError:
        messagebox.showerror("Помилка", "Введіть коректне ціле число для
кількості рядків та стовпців.")


def create_empty_matrix():
    update_matrix_entries()


def create_calculated_matrix():
    payment_matrix = calculate_matrix_cost()
    rows_spinbox.delete(0, tk.END)
    rows_spinbox.insert(0, payment_matrix.shape[0])
    columns_spinbox.delete(0, tk.END)
    columns_spinbox.insert(0, payment_matrix.shape[1])
    update_matrix_entries(payment_matrix)


def main():
```

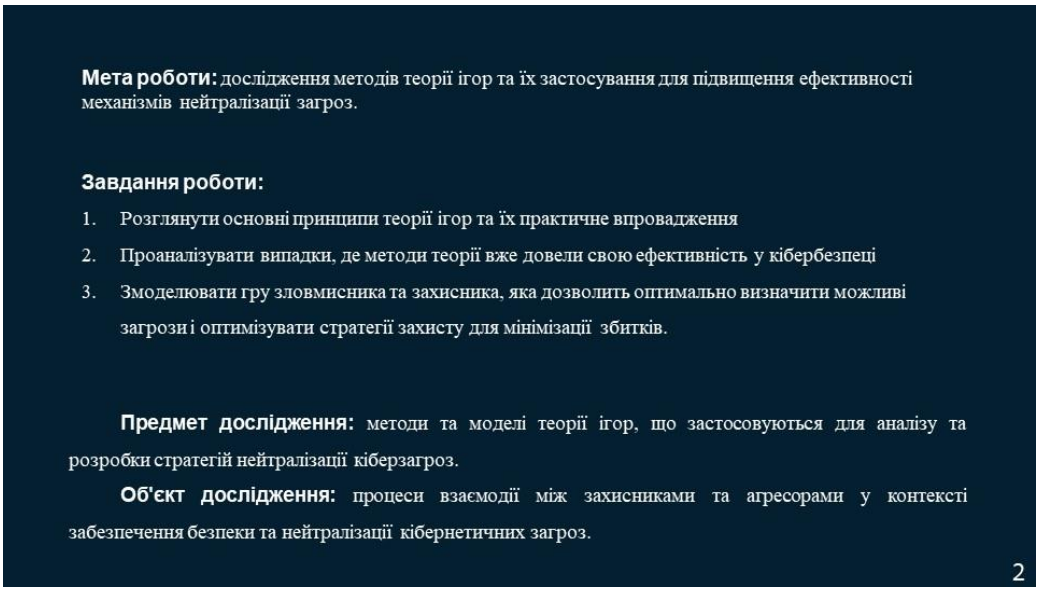
```
    global matrix_entries, rows_spinbox, columns_spinbox, matrix_frame,
result_label

    # Створення вікна
    root = tk.Tk()
    root.title("Гра 'Кіберзагрози'")
    root.configure(bg="#121212")

    # Фрейм для кнопок створення матриці
    create_matrix_frame = tk.Frame(root, bg="#121212")
    create_matrix_frame.pack()

    # Кнопка для створення порожньої матриці
    create_empty_matrix_button = tk.Button(create_matrix_frame, text="Створити
порожню матрицю", command=create_empty_matrix, bg="#1c1c1c",
fg="#00ff00")
    create_empty_matrix_button.grid(row=0, column=0, padx=5, pady=5)

    # Кнопка для створення матриці з обчисленими значеннями
    create_calculated_matrix_button = tk.Button(create_matrix_frame,
text="Створити обчислену матрицю", command=create_calculated_matrix,
bg="#1c1c1c", fg="#00ff00")
    create_calculated_matrix_button.grid(row=0, column=1, padx=5, pady=5)

    # Фрейм для розмірності матриці
    dimensions_frame = tk.Frame(root, bg="#121212")
    dimensions_frame.pack()

    # Напис і спінбокс для вибору кількості рядків
    rows_label = tk.Label(dimensions_frame, text="Рядки:", bg="#121212",
fg="#00ff00")
    rows_label.grid(row=0, column=0)
    rows_spinbox = tk.Spinbox(dimensions_frame, from_=1, to=10, bg="#1c1c1c",
fg="#00ff00")
    rows_spinbox.grid(row=0, column=1)

    # Напис і спінбокс для вибору кількості стовпчиків
    columns_label = tk.Label(dimensions_frame, text="Стовпці:", bg="#121212",
fg="#00ff00")
```

```
    columns_label.grid(row=0, column=2)
    columns_spinbox = tk.Spinbox(dimensions_frame, from_=1, to=10,
bg="#1c1c1c", fg="#00ff00")
    columns_spinbox.grid(row=0, column=3)

    # Фрейм для матриці
    matrix_frame = tk.Frame(root, bg="#121212")
    matrix_frame.pack()

    # Поля введення для матриці
    matrix_entries = []

    # Фрейм для кнопки "Обчислити"
    calculate_frame = tk.Frame(root, bg="#121212")
    calculate_frame.pack()

    # Кнопка "Обчислити"
    calculate_button = tk.Button(calculate_frame, text="Обчислити",
command=probabilities, bg="#1c1c1c", fg="#00ff00")
    calculate_button.pack()

    # Фрейм для результатів
    result_frame = tk.Frame(root, bg="#121212")
    result_frame.pack()

    # Результат гри
    result_label = tk.Label(result_frame, text="", bg="#121212", fg="#00ff00")
    result_label.pack()

    # Запуск GUI
    root.mainloop()


if __name__ == "__main__":
    main()
```

ДОДАТОК Б

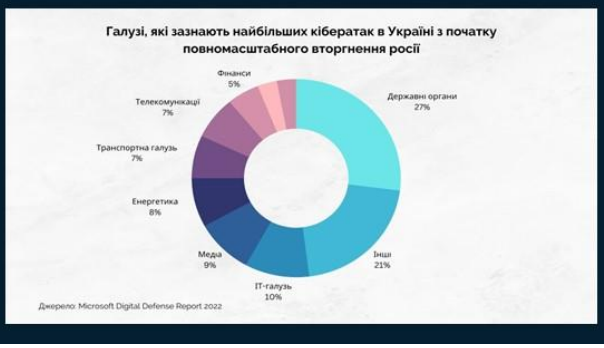
Слайди презентації:





Актуальність теми

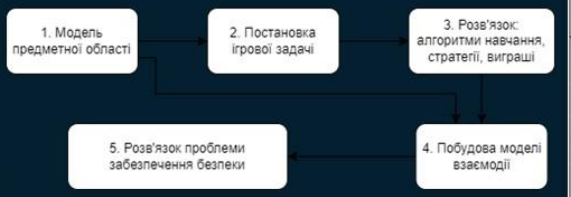
У сучасному цифровому світі, де кіберзагрози стають все більш виразними й небезпечними, пошук ефективних методів їх нейтралізації стає завданням пріоритетним для багатьох сфер: від корпоративних систем до національної безпеки.



3

Методи використання

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



Ігрові моделі			Питання застосування та безпеки
Кооперативні ігрові моделі	Статистичні ігрові моделі		Мобільні бездротові ad hoc моделі
Некооперативні ігрові моделі	Статистичні ігрові моделі		Виявлення несанкціонованого проникнення
			Оптимізація безпеки
	Динамічні ігрові моделі	Повні інформаційні ігрові моделі	Механізм безпекового стимулювання
			Оптимізація безпеки
		Не повні інформаційні ігрові моделі	Аналіз кібератак-захист

4

Наявні дослідження та їх результат

Дослідники Fultz і Grossklags (2009) використовують статичну некооперативну гру для того щоб виконати підбір моделі гри , щоб у подальшому аналізувати стимули зловмисників. Розуміння стимулів зловмисників може допомогти дослідникам знайти спосіб зупинити ці атаки та відповісти на них.

Mohi та ін. змушують вузли співпрацювати за допомогою статичної байєсівської гри для двох гравців, в якій гравцями є бездротові пристрої WSN та пристрій моніторингу (IDS). Байєсівська гра допомагає бездротовим вузлам здобути «репутацію», якщо вони працюють добре. Дослідники виявили, що IDS також може покращити свою роботу, використовуючи знання про низку минулих подій у грі. (2009)

Bedi та ін. (2011) фокусується на протоколі керування передачею (TCP/TCP-friendly) потоків. Як статичні, так і динамічні ігри з ненульовою сумою застосовуються для досягнення оптимальної дії для запобігання шахрайському трафіку, одночасно допускаючи відповідний трафік.

5

Постановка задачі

A = $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ = {крадіжка інтелектуальної власності, злом облікових даних співробітників, зараження SCADA, злом бездротових пристроїв, захоплення виробничих машин, зараження мережі, інсайдерська атака}

D = $\{d_1, d_2, d_3, d_4, d_5\}$ = {уникнути ризику, передати ризик, зменшити ризик, прийняти ризик, нічого не робити}

s = {80, 150, 200, 500, 0} вартість реалізації та підтримки кожної з оборонних стратегій

r = {140, 50, 100, 300, 200, 500} — вартість відновлення системи до стабільного стану

p = {0.1, 0.15, 0.8, 0.5, 1, 0.1, 1} — рівень втрат виробництва відповідно певної атаки

T = 1000

$$E = \begin{bmatrix} 0.8 & 0.1 & 0.1 & 0.3 & 0 \\ 0.95 & 0.1 & 0.1 & 0.3 & 0 \\ 0.1 & 0.7 & 0.5 & 0.9 & 0 \\ 0.1 & 0.85 & 0.95 & 0.7 & 0 \\ 0.2 & 0.7 & 0.8 & 0.9 & 0 \\ 0.4 & 0.85 & 0.95 & 0.1 & 0 \\ 0.05 & 0.8 & 0.2 & 0.2 & 0 \end{bmatrix}$$

6

Розв'язання задачі

Щоб сформувати функцію виграшу та обчислити платежі матриці, розглянемо характеристику виробничих систем з точки зору кібербезпеки.

1) Вартість утримання захисного механізму
2) Сума втрат у разі атаки
3) Вартість відновлення системи внаслідок конкретної атаки

$$\Gamma = \begin{bmatrix} \gamma_{11} & \cdots & \gamma_{1m} \\ \vdots & \ddots & \vdots \\ \gamma_{n1} & \cdots & \gamma_{nm} \end{bmatrix}$$

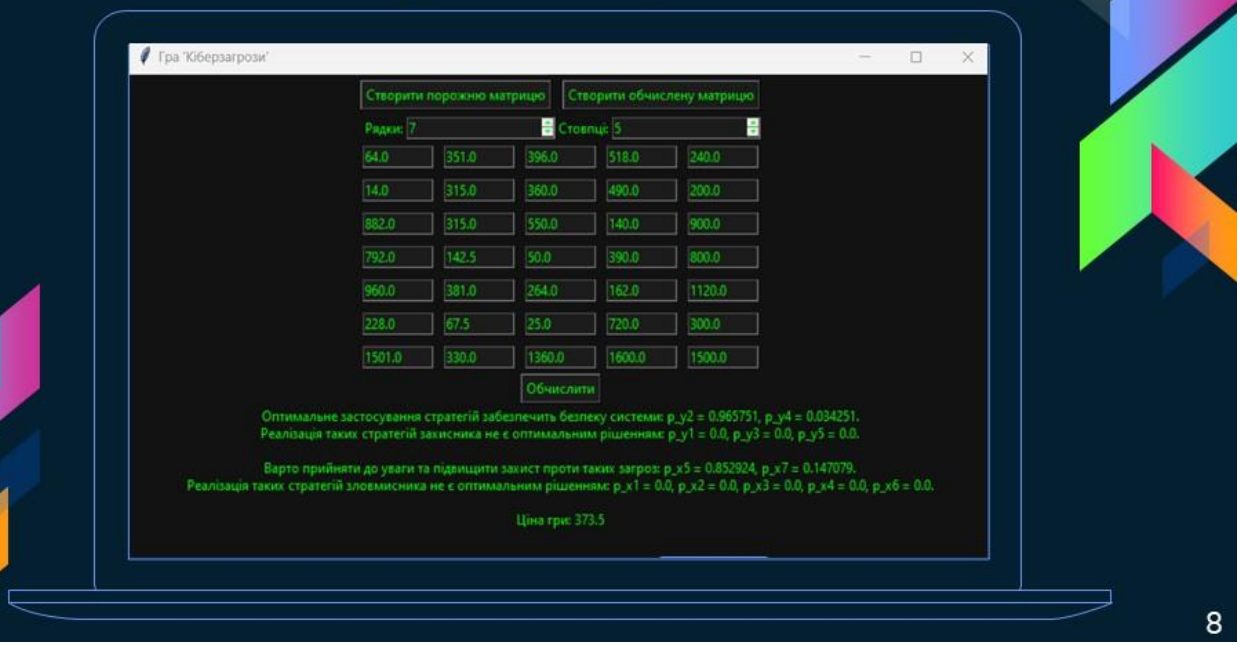
$$\gamma_{ij} = s_j - (s_i \times e_{ij}) + T \times p_i \times (1 - e_{ij}) + r_i \times (1 - e_{ij}), \forall\, i,j$$

$$\begin{gathered} Z = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 \to min \\ 64x_1 + 14x_2 + 882x_3 + 792x_4 + 960x_5 + 228x_6 + 1501x_7 \geq 1 \\ 315x_1 + 315x_2 + 142.5x_3 + 381x_4 + 67.5x_5 + 67.5x_6 + 330x_7 \geq 1 \\ 396x_1 + 360x_2 + 550x_3 + 50x_4 + 264x_5 + 25x_6 + 1360x_7 \geq 1 \\ 518x_1 + 490x_2 + 140x_3 + 390x_4 + 162x_5 + 720x_6 + 1600x_7 \geq 1 \\ 240x_1 + 200x_2 + 900x_3 + 800x_4 + 1120x_5 + 300x_6 + 1500x_7 \geq 1 \\ x_i \geq 0 \end{gathered}$$

$$\begin{gathered} Z = y_1 + y_2 + y_3 + y_4 + y_5 \to max \\ 64y_1 + 351y_2 + 396y_3 + 518y_4 + 240y_5 \leq 1 \\ 14y_1 + 315y_2 + 360y_3 + 490y_4 + 200y_5 \leq 1 \\ 882y_1 + 315y_2 + 550y_3 + 140y_4 + 900y_5 \leq 1 \\ 792y_1 + 142.5y_2 + 50y_3 + 390y_4 + 800y_5 \leq 1 \\ 960y_1 + 381y_2 + 264y_3 + 162y_4 + 1120y_5 \leq 1 \\ 228y_1 + 67.5y_2 + 25y_3 + 720y_4 + 300y_5 \leq 1 \\ 1501y_1 + 330y_2 + 1360y_3 + 1600y_4 + 1500y_5 \leq 1 \\ y_i \geq 0 \end{gathered}$$

7

Результат гри



8

Висновки

- Розглянуто приклади методів теорії ігор, та зроблено висновок, що кооперативні та некооперативні ігрові моделі допомогають у вирішенні питань безпеки.
- Результати аналізу використання теорії ігор показали, що для моделювання та аналізу можливих стратегій зловмисника, теоретико-ігровий підхід є ефективним для захисту від кіберзагроз і це доводять дослідження, які вже принесли вагомий внесок у вдосконалення механізмів нейтралізації кіберзагроз.
- Була змодельована матрична гра з нульовою сумою (як приклад можливих кіберзагроз для системи), з якої знайдено оптимальні стратегії захисника та зловмисника у змішаних стратегіях, і обчислено ціну такої гри з найменшими втратами для захисника у разі кібератаки.

9