КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп'ютерних наук та кібернетики
Кафедра системного аналізу та теорії прийняття рішень

Кваліфікаційна робота
на здобуття ступеня магістра

за спеціальністю 124 Системний аналіз

на тему:

ДОСЛІДЖЕННЯ І РОЗВ'ЯЗАННЯ ГРИ «НАПАДНИК-ЗАХИСНИК» У СИСТЕМАХ ЗАХИСТУ

Виконав студент 2-го курсу магістратури
Сахневич Валерій Борисович

(підпис)

Науковий керівник:
асистент, кандидат фіз.-мат. наук
Іванов Сергій Миколайович

(підпис)

Засвідчую, що в цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Роботу розглянуто й допущено до захистуна засіданні кафедри системного аналізу та теорії прийняття рішень
«04» травня 2023 р.,
протокол № 11
Завідувач кафедри
О. Г. Наконечний _____
(підпис)

Київ – 2023

РЕФЕРАТ

Обсяг роботи 39 сторінок, 5 ілюстрацій, 21 таблиць, 12 джерел посилань.

ГРА «НАПАДНИК-ЗАХИСНИК», РІВНОВАГА НЕША, ЛІНІЙНЕ ПРОГРАМУВАННЯ, МАТРИЧНА ГРА, СИСТЕМА ЗАХИСТУ

Тема роботи: Дослідження та розв’язання гри «нападник-захисник» у системах захисту.

Об’єктом дослідження цієї роботи є взаємодія агентів нападник – захисник у системах захисту.

Предмет дослідження – алгоритми розв’язання гри «нападник-захисник» у системах захисту.

Метою роботи є дослідження взаємодії агентів нападник-захисник як матричної гри та пропонування алгоритму її розв’язання.

Результати роботи: виконано загальний огляд гри «нападник-захисник» та проведено дослідження наявних проблем складання платіжної матриці цієї гри у системах захисту.

За методами дослідження використовувалися: аналіз сучасної літератури, алгебраїчні обчислення і виведення формул для визначення коефіцієнтів платіжних матриць та розв’язання матричної гри методами лінійного програмування.

ЗМІСТ

ВСТУП

Оцінка сучасного стану об’єкта розробки. Гра «нападник-захисник» має вирішальне значення в системах захисту в різних областях, включаючи кібербезпеку, фізичну безпеку та навіть стратегічне планування. Ця гра представляє постійну боротьбу між тими, хто прагне скомпрометувати або зламати систему (зловмисники), і тими, хто прагне її захистити (захисники). Розуміння та аналіз цієї гри допомагає розробити ефективні стратегії захисту та зменшити ризики.

Проблемами гри «нападник-захисник» займалися: Jon Atli Benediktsson, Xiaoou Li, Jeffrey Reed, Charles A. Kamhoua, Christopher D. Kiekintveld, Charles A. Holt, Ricky Sahu, Angela M. Smith та багато інших. У працях цих авторів розглядалися проблеми гри «нападник-захисник» і досліджувалися способи складання платіжних матриць гри та її розв’язання [1,7].

Актуальність роботи та підстави для її виконання. У системах захисту однією з актуальних і складних задач є взаємодія нападника та захисника, яка може розглядатися як матрична гра. Важливість гри «нападник-захисник» у системах захисту визначається у наступному:

1. Оцінка ризику: гра «нападник-захисник» дозволяє організаціям оцінити потенційні ризики та вразливі місця в їхніх системах. Розуміючи тактику, прийоми та процедури, які використовують нападники, захисники можуть визначити слабкі місця та визначити пріоритети своїх зусиль для посилення захисту.
2. Розробка стратегії: гра дозволяє захисникам розробляти проактивні стратегії протидії потенційним атакам. Аналізуючи моделі та тактику минулих атак, захисники можуть передбачити майбутні загрози та вжити відповідних заходів протидії. Це включає впровадження заходів безпеки, виправлення вразливостей і розробку стійких систем.

3. Адаптивність: зловмисники постійно вдосконалюють свої методи, використовуючи нові вразливості та новітні технології. Гра «нападник-захисник» допомагає захисникам адаптуватися та ефективно реагувати на ці зміни. Усвідомлюючи нові загрози, захисники можуть постійно оновлювати свій захист, контролювати систему та розробляти нові методи протидії атакам.
4. Red teaming: гра «нападник-захисник» часто передбачає проведення вправ «red teaming», під час яких незалежні команди моделюють реальні атаки на систему, щоб виявити вразливі місця. Ці вправи допомагають захисникам оцінити стан безпеки своєї системи, підтвердити існуючі засоби захисту та виявити потенційні слабкі місця, які потрібно усунути.
5. Реагування на інцидент і відновлення: у разі успішної атаки гра «нападник-захисник» допомагає реагувати у відповідь на інцидент і відновлення. Аналізуючи вектори атак і використовувані методи, захисники можуть визначити ступінь порушення, зупинити збитки та вжити заходів для запобігання майбутнім атакам.
6. Постійне вдосконалення: гра «зловмисник-захисник» — це ітеративний процес, який сприяє постійному вдосконаленню систем захисту. Захисники можуть вчитися на минулих атаках, ділитися інформацією, співпрацювати зі спільнотою безпеки та розробляти нові інструменти та методи для посилення свого захисту.

Мета й завдання роботи. Метою цієї роботи є дослідження взаємодії агентів нападник-захисник як матричної гри та пропонування алгоритму її розв’язання. Для досягнення мети необхідно розв’язати такі задачі:

1. Дослідити взаємодію агентів нападник-захисник у протекційних системах як матричної гри.
2. Запропонувати алгоритм знаходження коефіцієнтів матричної гри «нападник-захисник та її розв‘язання.

Об’єкт, предмет дослідження. Об’єктом дослідження цієї роботи є взаємодія агентів нападник – захисник у системах захисту.

Предмет дослідження – алгоритми розв’язання гри «нападник-захисник» у системах захисту.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ МАТРИЧНИХ ІГОР

1.1 Основні відомості матричних ігор

Гра складається щонайменше з трьох елементів: набору гравців, набору дій для гравців, функції виграшу, яка описує, скільки виграшу або корисності кожен гравець може отримати. Ігри можна розділити на різні типи на основі відмінностей у цих елементах. Ігри з двома гравцями досліджувалися набагато ширше, ніж ігри з трьома або більше гравцями. Гра вважається нульовою, якщо сума виграшів гравців завжди дорівнює нулю. Одночасні ігри – це ігри, в яких усі гравці виконують дії одночасно, після чого не потрібно виконувати жодних дій, тобто гра закінчується негайно. Навіть якщо гравці не рухаються одночасно, гру все одно можна розглядати як одночасну гру, якщо гравці, які приймають рішення пізніше, абсолютно не знають про дії попередніх гравців: вони навіть не можуть зробити жодного висновку про дії попередніх гравців з того, що вони зробили. Навпаки, гра є послідовною, якщо деякі гравці виконують дії після інших гравців, і вони мають певні відомості про попередні дії, зроблені іншими гравцями[1].

При грі з ненульовою сумою гравець має розв’язати задачу на максимум, тобто обрати з тих можливостей, які в нього є, ту, яка дає йому максимальний виграш або, якщо гра включає в собі випадкові ходи, то гравець має обрати ту можливість, яка дає максимум математичного сподівання виграшу.

Таким чином, для вивчення характерних особливостей стратегічних ігор, треба перейти до ігор з участю двох або більше гравців.

Розглянемо основні відомості гри «нападник-захисник».

Стратегічна гра для двох гравців із нульовою сумою визначається як трійка $(\mathcal{N}, \mathcal{A}, \mathcal{R})$, де,

1. $\mathcal{N} = \{1, 2\}$ – набір гравців, де гравець 1 є захисником мережі, а гравець 2 – атакуючим[1].

2. $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ – простір дій гри, де $\mathcal{A}_1$ і $\mathcal{A}_2$ – простір дій першого та другого гравця відповідно. Профіль дій, що вказує на спільну дію двох суперників $(a_1,\ a_2)$, визначає винагороду, яку отримають обидва гравці[1].

3. $\mathcal{R} = \{\mathcal{R}_1; \mathcal{R}_2\}$, де $R_1 + R_2 = 0$. $\mathcal{R}_1 : \mathcal{A} \to \mathbb{R}^2$– функція винагороди для першого гравця, а $\mathcal{R}_2$ – функція винагороди для другого гравця[1].

Розглянемо цю гру детальніше. Кожен гравець має лише один хід. Перший з них обирає число з перших m натуральних чисел, а другий обирає число з n натуральних чисел, при цьому другий гравець не знає, який вибір зробив перший гравець. Потім ці два числа порівнюються і один з гравців платить іншому суму, яка залежить від виборів, які вони зробили і визначається правилами гри. Такі ігри в подальшому будемо називати матричними[4].

Наведемо приклад матричної гри. Гравець G1 вибирає число з множини $\{1,\ 4,\ 9\}$, а гравець G2 – з $\{\ 10,\ 11,\ 12, 13\}$. При цьому гравець G2 не знає, який вибір зробив гравець G1. Після того, як обидва гравці зробили свій вибір, гравець G2 платить G1 суму, яка визначена в таблиці 1.1:

Таблиця 1.1 – Приклад матричної гри

G2 / G1	10	11	12	13
10	6	4	11	8
11	8	-7	1	-4
12	-8	2	-5	0

Тобто, якщо гравець G1 обере, наприклад, 1, а G2 обере 9, то гравець G2 платить гравцю G1 11 євро. Якщо ж гравець G1 обере 4, а G2 – 16, то гравець G1 платить гравцю G2 4 євро.

Матрична гра описується платіжною матрицею:

$$\begin{pmatrix} 6 & 4 & 11 & 8 \\ 8 & -7 & 1 & -4 \\ -8 & 2 & -5 & 0 \end{pmatrix}.$$

1.2 Нормальна форма гри і домінування

Наведемо означення.

Означення 1.1 Нехай $D_1, \dots, D_n$ – множини. Декартовим добутком цих множин називається:

$$D = D_1 \times \dots \times D_n = \{(d_1, \dots, d_n) | d_1 \in D_1, \dots, d_n \in D_n\}$$ [2].

Нехай $M = \{1, \dots, n\}$ – множина гравців, $D_1, \dots, D_n$ – множина стратегій гравців. Будемо говорити, що $D = D_1 \times \dots \times D_n$ – множина профілів стратегій[2].

Довільний елемент $d_i \in D_i$ називається стратегією i – ого гравця, а довільний елемент $d \in D$ – профілем стратегій гравців[2].

Множину всіх профілів стратегій для всіх гравців, крім i – ого гравця позначимо так: $D_{-i} = \underset{j \neq i}{\times} D_j$, а профіль стратегій всіх гравців, крім i – ого гравця - $d_{-i} = (d_1, \dots, d_{i-1}, d_{i+1}, \dots, d_n)$ [2].

Функція виграшу i – ого гравця присвоює кожному профілю стратегій $d \in D$ якийсь виграш $u_i: D \to R$. Функція $u_i: D \to R^n = (u_1, \dots u_n)$ називається профілем функції виграшів гравців[2].

Означення 1.2 Набір $T = \langle M, D, u \rangle$ називається грою у нормальній формі[2].

Отже, щоб задати гру в нормальній формі, необхідно навести множину гравців, множину можливих стратегій кожного з гравців та їх виграші[2].

Означення 1.3 Нехай $T = \langle M, D, u \rangle$ – гра у нормальній формі. Тоді $d^* \in D$ називається рівновагою Неша, якщо $\forall i, \forall d_i' \in D_i$ виконується:

$$u_i(d_i^*, d_{-i}^*) \geq u_i(d_i', d_{-i}')$$ [2].

Фактично, рівновага Неша – це такий профіль стратегій, що жоден окремо взятий гравець не захоче змінювати свою стратегію, якщо інші гравці теж не змінювали свої стратегії[2].

Дуже важливим питанням в будь-яких іграх є оптимальна стратегія, тобто, чи можна довести що певна стратегія є раціональною[3].

Введемо деякі поняття[3]:

Нехай є матриця А, будемо говорити, що i-ий рядок **домінує** k-ий рядок, якщо $a_{ij} \geq a_{kj}$ для всіх j, і $a_{ij} > a_{kj}$ принаймні для одного j [3].

Аналогічно для стовпців[3]:

j-ий стовпчик домінує l-ий стовпчик, якщо $a_{ij} \leq a_{il}$ для всіх i, і $a_{ij} < a_{il}$ принаймні для одного і [3].

Сформулюємо наступну теорему[3].

Теорема 1

Нехай А – матрична гра, і нехай рядки $i_1,\ i_2, \dots,\ i_k$ матриці А домінуються. Тоді перший гравець має таку оптимальну стратегію x, що

$x_{i_1} = x_{i_2} = \cdots = x_{i_k} = 0$; крім того, будь-яка оптимальна стратегія для гри, яка отримується в результаті видалення домінованих рядків, також буде оптимальною стратегією для початкової гри[3].

Аналогічно формулюється теорема і для домінування стовпчиків[3].

Загальний результат цих теорем – всі доміновані рядки і стовпчики можуть бути видалені і це дозволяє розглядати меншу матрицю.[3]

В прикладі, наведеному раніше, можна побачити, що кожний елемент першого рядка більший, ніж відповідний елемент другого рядка і також більший, ніж відповідний елемент третього рядка. Тому, незалежно від того, яке число обирає гравець G2, гравцю G1 краще вибрати 1, ніж 4 чи 9. Це означає, що 1 буде найбільш оптимальним вибором для гравця G1[3].

Точно так же кожний елемент другого стовпчика менший, ніж відповідний елемент інших стовпчиків. Тому, для G2 найбільш оптимальним є вибір числа 4 [3].

Розглянемо іншу матрицю, наприклад таку:

$$\begin{pmatrix} 8 & 9 & 9 & 4 \\ 6 & 5 & 8 & 7 \\ 3 & 4 & 8 & 6 \\ 8 & 9 & 9 & 4 \end{pmatrix}.$$

Перший і четвертий рядок однакові, тому видалимо четвертий:

$$\begin{pmatrix} 8 & 9 & 9 & 4 \\ 6 & 5 & 8 & 7 \\ 8 & 9 & 9 & 4 \end{pmatrix}.$$

Другий рядок домінує третій, тому відкинемо третій рядок:

$$\begin{pmatrix} 8 & 9 & 9 & 4 \\ 6 & 5 & 8 & 7 \end{pmatrix}.$$

Третій стовпчик домінує четвертий, тому відкинемо третій.

$$\begin{pmatrix} 8 & 9 & 4 \\ 6 & 5 & 7 \end{pmatrix}.$$

Далі спростити матрицю неможливо, оскільки $8 > 6$, $4 < 7$; $8 < 9$, $6 > 5$; $8 > 4$, $6 < 7$; $9 > 4$, $5 < 7$.

РОЗДІЛ 2 ОПИС ГРИ «НАПАДНИК-ЗАХИСНИК»

2.1 Опис та подання гри «нападник-захисник»

Гра «Нападник-захисник» - це гра, в якій кілька захисників намагаються захистити ресурс або частину території, тоді як кілька нападників намагаються знищити або захопити той самий ресурс або територію, які захищаються. Таку гру можна застосувати до багатьох різних сценаріїв, таких як тероризм і боротьба з тероризмом, кібербезпека, промислова організація, конкуренція та вихід на територію фірми, пенальті, міжнародні та громадянські війни. Ігри «Нападник-захисник» зазвичай представлені у вигляді матриць виграшів і дерев рішень, але можуть набувати більш складних форм, якщо застосовувати різні інструменти [6].

Як зазначалося раніше, усі ігри мають три основні елементи: набір гравців, набір стратегій, наданих кожному гравцеві, і набір виграшів, що відповідають кожному кортежу стратегій. Тому ігри «нападник-захисник» складаються з кількох гравців; зокрема, набір «нападаючих» і набір «захисників». Кожен гравець має набір стратегій; ці стратегії визначаються типом гравця, який діє, нападаючий чи захисний. Виграш кожного гравця визначається його успіхом у атаці чи захисті території чи ресурсу. Через взаємозалежний характер ігор виграші кожного гравця залежать як від стратегій, які вони виконують, так і від стратегій, які також виконують інші гравці[6].

Розглянемо простий приклад гри «нападник-захисник».

Гравці. У грі «нападник-захисник», яку ми спочатку проаналізуємо, є лише два гравці: армія «атакуючого» та армія «захисника».

Стратегії. Армія захисника захищає місто, яке має два головних входи: один вхід через легкий перевал, а інший вхід через жорсткий перевал. Тому армія-захисник може захистити або легкий шлях, або важкий шлях. Так само армія нападників може атакувати місто як з легкого, так і з важкого шляху. Загалом обидва гравці мають ідентичні набори стратегій, які містять по дві

стратегії: важкий шлях або легкий шлях. Щоб зберегти термінологію простою, ми позначатимемо легкий шлях «легким», а важкий шлях — «важким».

Загалом, стратегічна ситуація ефективно показана простою схемою на рисунку 1 нижче.

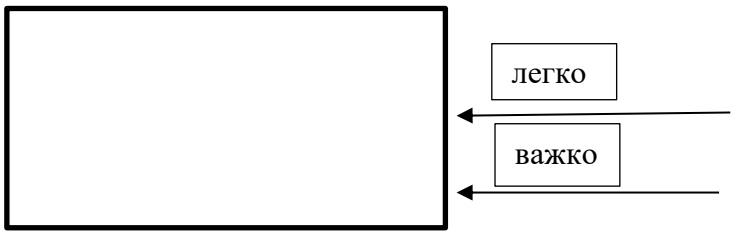

Рисунок 2.1 - Зловмисники можуть атакувати легким шляхом (легкий) або важким шляхом (важкий), а захисник також може захищатися або легким шляхом (легкий), або важким шляхом (важкий)

Результати та виплати. Враховуючи, що є два гравці, кожен з яких має по дві стратегії, є чотири унікальні результати гри. Це: (легко, легко); (легко, важко); (важко, легко); і (важко, жорстко), де стратегія, яка реалізувалася захисниками, є першим елементом у дужках, а стратегія, яку застосовували атакуючі, є другим елементом[6].

Виплати для кожного гравця залежать від стратегії, яку реалізує інший гравець. Виплати, розподілені за кожним результатом, такі[6].

Якщо нападаючий атакує легким шляхом, а захисник захищає легкий шлях, тоді обидві армії зустрінуться і будуть битися. Враховуючи те, що обидві армії обирають легкий шлях, обидві армії однаково підібрані, тому існує 50-50 шансів на перемогу певної армії. Виплата результату (легко, легко) становить (1, 1)[6].

Якщо нападаючий атакує легким проходом, а захисник захищає важкий шлях, тоді армії не зустрінуться, і атакуючий може зайняти позицію, щоб захопити місто без серйозної конфронтації. Армія оборони втрачає контроль над містом і програє штурм. Виплата за результат (важкий, легкий) становить (0, 2) [6].

Якщо атакуючий атакує по важкому шляху, а захисник захищає легкий шлях, то, знову ж таки, армії не зустрінуться. Однак армія нападаючих проходить важкий шлях, що означає, що вони втрачають половину (або значну кількість) армії через втрати та голод тощо. Враховуючи кількість втрат, які зазнали нападники, вони не в такому становищі, щоб захопити місто. Як наслідок, армія, що обороняється, може перегрупуватися та захистити місто. Отже, виграш за результат (легкий, важкий) дорівнює (1, 1) [6].

Нарешті, якщо атакуючий атакує важким шляхом, а захисник захищає важкий шлях, тоді обидві армії зустрічаються. Однак, оскільки нападник зазнав втрат, вони легко переможені захисником. Виплата результату (важко, важко) становить (2, 0) [6].

Отже, було визначено всі елементи, необхідні для простої гри. Зокрема, є асиметрична гра, яку можна налаштувати кількома різними способами. Розглядаються два різні способи: один, коли захисник бачить, що нападник наближається, і вибирає маршрут для захисту, а інший, коли атакуючий і захисник не знають, де один одного збираються атакувати чи захищати. Перша гра є грою з досконалою інформацією та описується за допомогою дерева рішень, а інша є грою з недосконалою інформацією та описується з використанням матриці виграшів [6].

Гра 1. Нехай гравці рухаються послідовно: спочатку атакуючий рухається першим, захисник бачить нападника, що наближається, і вибирає для захисту певний шлях. Ця гра представлена деревом рішень нижче[6].

Унікальна досконала рівновага Неша (SPNE) підгри цієї гри очевидна та визначається формулою (легко, легко/важко). На це вказують червоні стрілки. Незалежно від того, що вибере атакуючий, той, хто захищається, завжди хоче координувати свої дії з нападаючим. Знаючи це, нападаючий раціонально вибере атакувати легким шляхом, а захисник захищатиме легкий шлях. Результат не такий вже й цікавий[6].

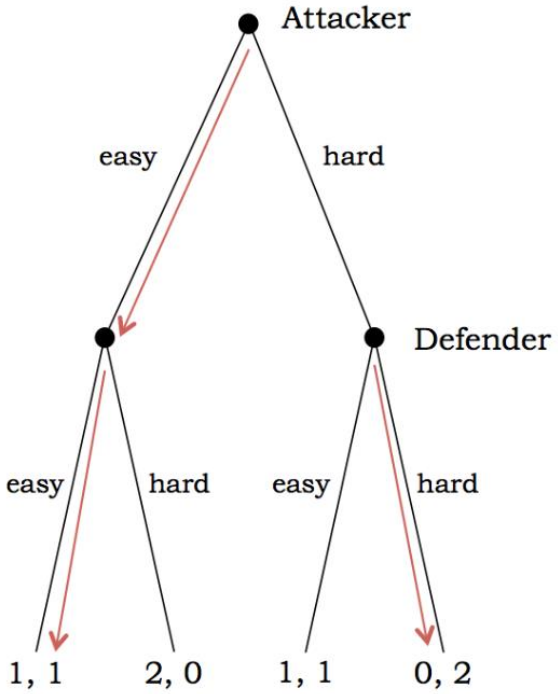

Рисунок 2.2 - Дерево рішень у грі «нападник-захисник» із ідеальною інформацією про те, де нападник рухається першим, а захисник відповідає[6].

Якщо захисник рухався першим, а нападаючий відповідав, тоді захисник повинен завжди захищати легкий шлях, а нападаючий буде байдужим щодо нападу на легкий або важкий шлях. Тому існує дві однаково дійсні ідеальні рівноваги Неша підгри: (легка, легка / легка) і (легка, важка / легка). Незважаючи на це, у захисника завжди є стимул захищатися легким шляхом, оскільки він знає, що нападаючий ідеально йому відповідає[6].

У всіх обговорених підіграх рівноваги Неша всі виграші (1, 1) [6].

Гра 2. недосконала інформація. Більш реалістичним є сценарій, коли атакуючий не знає, де збирається захищатися той, хто захищається, а той, хто захищається, не знає, де атакуючий збирається атакувати. Це гра з недосконалою інформацією, і вона знову представлена деревом рішень, як показано нижче. Єдина відмінність полягає в тому, що між вузлами прийняття рішень захисника існує пунктирна лінія: захисник не знає, який хід зробив атакуючий [6].

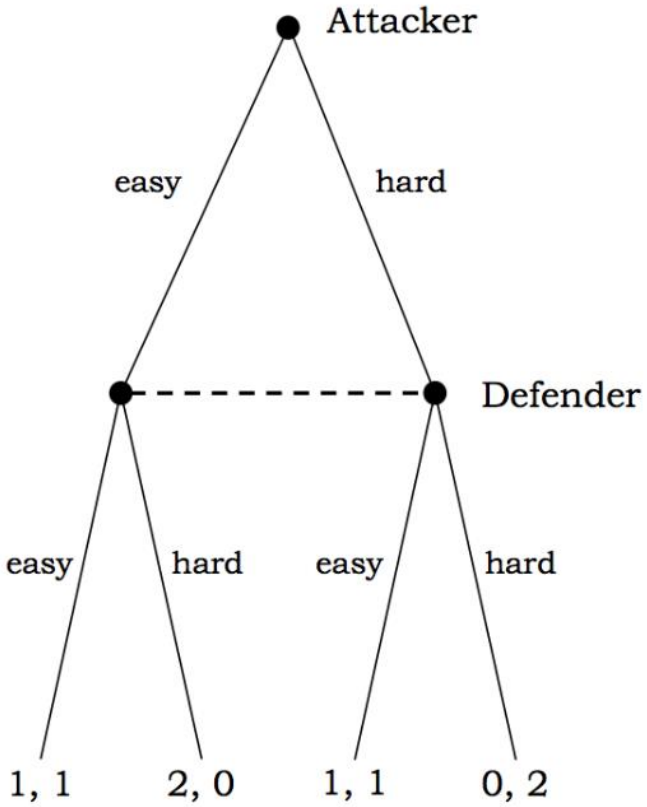

Рисунок 2.3 - Дерево рішень у грі «зловмисник-захисник» з недосконалою інформацією[6]

Нападник і захисник мають обмежену інформацію; зокрема, захисник не знає, звідки підійде нападник. Гру можна перетворити на матрицю виграшів наступного вигляду(табл. 2.1) [6]

Таблиця 2.1 – Матриця виграшу, що представляє гру нападник-захисник з недосконалою інформацією.

		Нападник	
		Легко	Важко
Захисник	Легко	1; 1	1,1
	Важко	0; 2	2; 0

У цій ситуації захисник знову хоче координувати дії з атакуючим, але стратегія нападаючих, спрямована на атаку легким шляхом, слабко домінує над стратегією нападу на важкий шлях. Таким чином, існує єдина чиста стратегія рівноваги Неша, коли нападник атакує легким шляхом, а захисник захищає легкий шлях, що призводить до виграшу (1, 1) [6].

Існує (технічно) нескінченна кількість змішаних стратегій рівноваги Неша. Нехай p — ймовірність того, що захисник вибере легкий шлях, а q — ймовірність того, що атакуючий вибере легкий шлях[6].

Якщо захисник вважає, що $q > 0,5$, то він має обрати легкий шлях. І навпаки, якщо захисник вважає, що $q < 0,5$, то він має обрати легкий шлях. Якщо $q = 0,5$, то захиснику байдуже, яку стратегію йому слід прийняти[6].

Аналогічно, якщо зловмисник вірить, що захисник однозначно вибере легкий шлях $p = 1$, тоді він байдужий до вибору легкого або важкого шляху. Якщо, з іншого боку, $p < 1$, то зловмисник однозначно повинен вибрати легкий шлях. Криві найкращого відгуку можна побачити на осях нижче; всі рівноваги Неша показані фіолетовим кольором, де перетинаються криві найкращого відгуку[6].

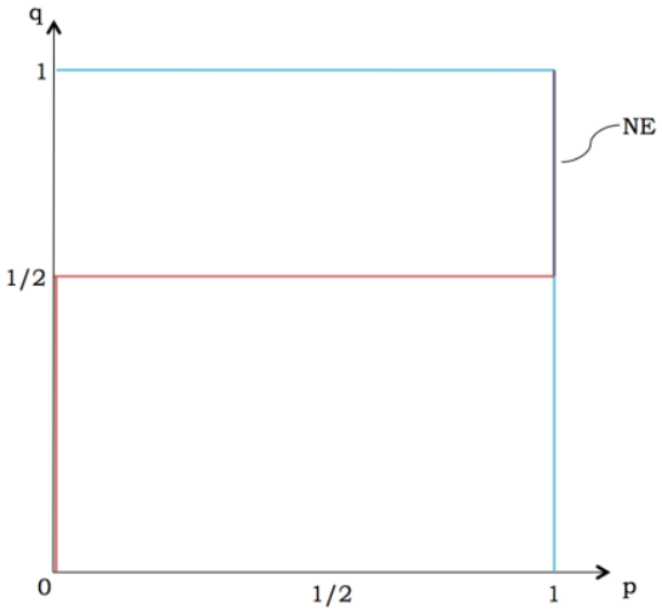

Рисунок 2.4 - Найкращі функції відповіді для нападника та захисника та повний набір рівноваг Неша змішаної стратегії[6]

2.2 Гра «нападник-захисник» у мережі

Розглянемо діаграму атаки з N вузлів, представлений у вигляді графа $G(\mathcal{V}, \mathcal{E})$, де $N = |\mathcal{V}|$. Кожний вузол представляє вразливість, пов'язану з хостом або механізмом в мережі. Ребро $e_{u,v} \in \mathcal{E}$, яке з'єднує два вузли u і v, вказує на можливість використання вразливості у вузлі v через уразливість у другому вузлі - u. Кожен вузол в графі має значення w_v, яке відображає його важливість для адміністратора(захисника) мережі. Вузли з вищим значенням є важливішими для мережі, яка містить важливі бази даних та цінну інформацію для військової групи. Тому припустимо, що вузли високої вартості дуже привабливі для супротивників і мережевих зловмисників. Зловмисник хоче максимізувати свою очікувану винагороду шляхом правильного вибору вузла-жертви серед всіх вузлів, $\mathcal{V}$. Припустимо, що зловмисник знає значення, пов'язані з кожним вузлом. Це припущення виправдане, оскільки зловмисники зазвичай можуть отримати деяку внутрішню інформацію щодо структури мережі та можуть досліджувати вузли за допомогою інструментів сканування мережі[1] (Lyon, 2009).

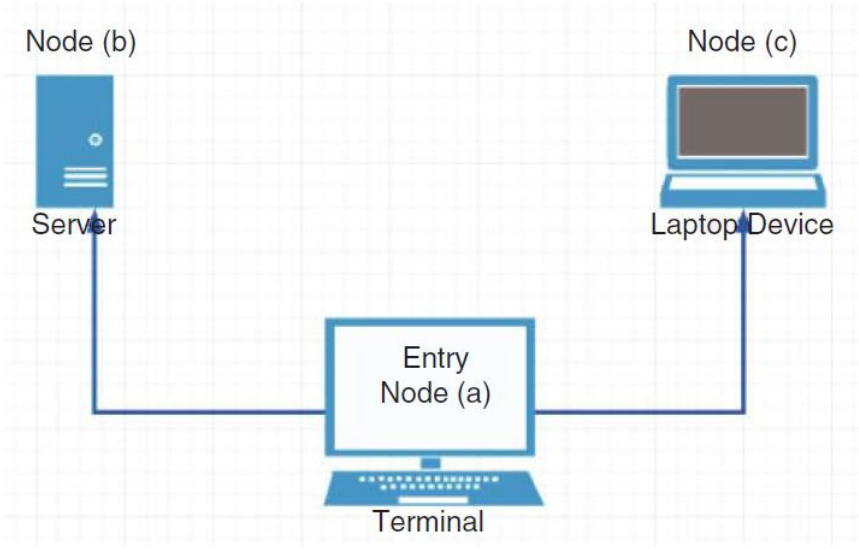

Рисунок 2.5 - Модель гри[1]

На рнсунку 2.5 зображено модель цієї гри. Маємо три вузли. $a \in \mathcal{V}$ - вузол входу в мережу. Вузол a має два ребра, $e_{a,b}$ і $e_{a,c}$, що з'єднують його з вузлом b і с відповідно. Припустимо, що захисник не знає точного місцезнаходження

нападника. Захисник знає, що зловмисники можуть проникнути в мережу через точки входу. Оскільки записи в мережі можуть легко забезпечити розподіл $f_a(.)$ за набором точок входу, де $\mathcal{V}_e \subset \mathcal{V}$ позначає набір точок входу. Тобто, захисник знає ймовірність того, що зловмисник проникне в мережу через точку входу $u \in \mathcal{V}_e$, яка дорівнює $f_a(u)$, так що $\sum_{u \in \mathcal{V}_e} f_a(u) = 1$.

Дії захисника: він виділяє набір з k приманок на шляху зловмисника, щоб його обдурити. Розміщені привабливі приманки вздовж його/її шляху відвернуть зловмисника від досягнення реальних вузлів. Приманкирозміщені як підроблені сервіси по різних ребрах, що з'єднують вразливості мережі. Якщо зловмисник скористався приманкою, розміщеною в $e_{u,v}$, щоб отримати доступ до вузла v від u, захисник відстежує нове місцезнаходження зловмисника, і фальшива служба(приманка) розкриє важливу інформацію про методи злому зловмисника. Це відстеження є дуже важливим для захисника, для здійснення своїх майбутніх захисних дій. Припустимо, що зловмисник атакує з вузла входу a, як показано на рисунку 2.5. Захисник розміщує одну приманку, і йому потрібно вирішити, на якому ребрі зробити це. При цьому, він не впевнений, що зловмисник знаходиться на вузлі a, він також розглядає дію без розміщення як можливий вибір, щоб уникнути витрат на розподіл. Загалом, захисник має 2 варіанти: розмістити приманку на ребрах $e_{a,b}$ і $e_{a,c}$ або не розміщувати приманку.

Дії нападника: він вирішує, який вузол атакувати наступним. Нападник може скористатись вразливістю у вузлі b чи c. Оскільки він хоче залишатися непомітним, існує ціна за атаку. Отже, зловмисник може вирішити повністю відступити за деяких обставин, щоб уникнути таких витрат.

Функція винагороди: рахисник матиме фіксовані витрати за розміщення нової приманки в ребрі мережі. Нехай P_c позначає вартість розміщення приманки. Вартість атаки нападника позначається як A_c . Вартість атаки відображає ризик, прийнятий зловмисником. Якщо захисник розмістив приманку на тому ж ребрі, яку використовує зловмисник, захисник отримує винагороду за захоплення, позначимо її Cap. Якщо зловмисник скористався

іншим безпечним ребром, то він отримує успішну нагорода за атаку, позначимо Esc. Таким чином, як винагорода за захоплення, так і винагорода за успішну атаку зважуються за значенням захищеного або атакуваного вузла, w_v. Почнемо з вираження матриці винагороди для гри, зображеної на рисунку 2.5, а потім представляємо загальну матрицю винагороди[1]

$$R_1 = \begin{bmatrix} -P_c + A_c + Cap * w_b & -P_c + A_c - Esc * w_c & -P_c \\ -P_c + A_c - Esc * w_b & -P_c + A_c + Cap * w_c & -P_c \\ A_c - Esc * w_b & A_c - Esc * w_c & 0 \end{bmatrix}.$$

Матриця винагороди нападника: $R_2 = -R_1$. Нагорода, $R_1(1,1)$ і $R_1(2,2)$, представляє спійманого зловмисника, оскільки захисник розмістив приманку на атакований вузол. Таким чином, захисник сплачує вартість розміщення P_c і отримує винагороду за захоплення, зважену на вартість захищеного вузла. Зловмисник несе витрати на атаку, A_c, що представляє винагороду для захисника в грі з нульовою сумою. З іншого боку, $R_1(1,2)$ і $R_1(2,1)$ представляють успішну атаку, коли приманка розміщена на іншому вузлі. Таким чином, є втрата Esc, зважена за значенням зламаного вузла. У $R_1(3,1)$ і $R_1(1,3)$ захисник вирішує не розміщувати жодної приманки, щоб зберегти вартість розміщення P_c. Так само в $R_1(3,1), R_1(2,3), R_1(3,3)$ - зловмисник відступає, щоб уникнути витрат на захоплення або втрати A_c.

Функцію винагороди для довільної кількості ребер можна узагальнити:

$$R_1(a_1, a_2) = \begin{cases} -P_c + A_c + Cap * w_v;\ a_1 = e_{a,v}, a_2 = v\ \forall v \in \mathcal{V} \\ -P_c + A_c - Esc * w_u;\ a_1 = e_{a,v}, a_2 = u\ \forall u \neq v \in \mathcal{V} \\ -P_c;\ a_1 = e_{a,v}, a_2 = 0\ \forall v \in \mathcal{V} \\ 0;\ a_1 = 0, a_2 = 0 \end{cases},$$

де $a_1 = 0$ означає, що захисник не виділяє жодної нової приманки. Подібним чином $a_2 = 0$ означає, що зловмисник вирішив відступити.

Визначено дії, доступні для кожного гравця в грі, тобто $\mathcal{A}_1, \mathcal{A}_2$. Чиста стратегія - це стратегія, яка вибирає одну з цих дій. Крім того, гравець може вибрати використання змішаної стратегії, визначеної за допомогою розподілу ймовірностей цих дій. Дано набір дій першого гравця, $\mathcal{A}_1$, нехай $\Pi(\mathcal{A}_1)$ позначає множину всіх розподілів ймовірностей над $\mathcal{A}_1$. Тоді множиною змішаних стратегій для гравця 1 є $\Pi(\mathcal{A}_1)$, що позначається як $\mathcal{X}_1$. Отже, у змішаній стратегії $X \in \mathcal{X}_1$ дія a_1^i виконується з ймовірністю x_i такою, що $X = [x_1, x_2, \dots, x_n]^T$, де $n = |\mathcal{A}_1|$. Для нападника аналогічно робимо: він має стратегію $Y = [y_1, y_2, \dots, y_m]^T$, де $m = |\mathcal{A}_2|$.

Тоді, винагорода захисника, яку позначимо через U_1, має вигляд:

$$U_1 = X^T R_1 Y. \tag{2.1}$$

Кожен гравець прагне максимізувати власну винагороду. У грі з нульовою сумою це передбачає мінімізацію винагороди іншого гравця. Очікувана корисність для гравця 1 у рівновазі становить $U_1 = -U_2$. Теорема про мінімакс передбачає, що U_1 є постійним у всіх станах рівноваги та є тим самим значенням, якого досягає гравець 1 за мінімаксної стратегії гравця 2. Використовуючи цей результат, ми можемо побудувати задачу оптимізації гравця 1 як задачу лінійного програмування (ЗЛП) наступним чином:

Знайти $\max_X U_1$, якщо

$\sum_{a_1 \in \mathcal{A}_1} r_1(a_1, a_2) x_{a_1} \geq U_1$, $\forall a_2 \in \mathcal{A}_2$, $\mathrm{X} = (x_1, \dots, x_n)$, $\sum_{i=1}^m x_i = 1$, $x_i \geq 0$, $i = 1, \dots, n$.

Для нападника задача виглядає так:

Знайти $\min_Y U_2$, якщо

$\sum_{a_2 \in \mathcal{A}_2} r_1(a_1, a_2) y_{a_2} \leq U_1$, $\forall a_1 \in \mathcal{A}_1$, $\mathrm{Y} = (y_1, \dots, y_m)$, $\sum_{j=1}^m y_j = 1$, $y_j \geq 0$, $j = 1, \dots, m$.

Перше обмеження випливає з визначення рівноваги Неша. Отже, очікувана винагорода більша, ніж вартість гри. Оскільки цінність гри залежить від змішаної стратегії гравця 2 (зловмисника), адміністратор повинен обмежити свою відповідь найкращим набором відповідей, який гарантує вищу винагороду. Решта два обмеження гарантують, що X є дійсним розподілом ймовірностей. Зловмисник вирішує відповідну ЗЛП, який можна охарактеризувати за тими самими лініями, щоб переконатися, що оптимальна змішана стратегія Y є найкращою відповіддю на кожну можливу дію, яку виконує захисник. Отримані змішані стратегії формують рівновагу Неша для двох гравців.

Щоб краще зрозуміти вплив і роль кожного з параметрів, описаних раніше, проаналізуємо детальніше їх теоретично. Розглянемо іграшковий граф. Припустимо, що два вузли, u, v, з'єднані через одне ребро. Зараз зловмисник входить у мережу через вузол u. Він повинен вирішити, чи атакувати наступний вузол v, чи відступити. З іншого боку, захисник вирішує розмістити приманку в наявному ребрі або заощадити витрати на розміщення приманки. Щоб отримати рівновагу в змішаних стратегіях, нехай нападник атакує вузол v з імовірністю y, а захисник розміщує приманку з імовірністю x. Матрицю винагороди можна отримати з (2.1), видаливши другий рядок і другий стовпець і замінивши w_b на w_v. Отже, очікувану винагороду захисника можна виразити так:

$$u_d(x,y) = (-P_c - A_c + Cap * w_v)xy - P_c(1-y)x + (A_c - Esc * w_v)y(1-x).$$

Для кожної стратегії атаки y нападника, винагорода захисника має вигляд:

$$u_d(x) = (-2A_c y + (Cap + Esc)w_v y - P_c)x + (A_c - Esc * w_v)y(1-x), y \in [0,1].$$

Як показано в попередній формулі, очікувана винагорода захисника утворює лінійне рівняння, тобто $u_d(x) = mx + b$. Якщо нахил цієї лінії є від'ємним, найкраща відповідь захисника для стратегії нападника у полягає в тому, щоб грати $x^* = 0$. З іншого боку, якщо m > 0, найкраща відповідь

захисника є $x^* = 1$, тобто захисник розміщує приманку на ребрі $e_{u,v}$. Якщо нахил m = 0, це робить дії захисника байдужими до застосованої стратегії y. Отже, він задовольняє точку рівноваги гри. Тому, в [1] формулюються леми 1,2 та теорема.

Лема 1. Для сформульованої гри захисник обов'язково розміщує приманку, якщо вартість розміщення A_c задовольняє таку умову[1]:

$$A_c < \frac{(Cap + Esc)w_v y - P_c}{2y};\ \forall y \in [0;1].$$

Лема 2. Подібним чином зловмисник вирішує відступити, якщо вартість захопленого Cap задовольняє таку умову[1]:

$$Cap > \frac{Esc(1-x) - A_c(1-2x)}{w_v};\ \forall x \in [0;1].$$

Теорема. Сформульована гра має рівновагу Неша в змішаних стратегіях при $x^* = \frac{Escw_v - A_c}{(Cap+Esc)w_v - 2A_c}$, $y^* = \frac{P_c}{(Cap+Esc)w_v - 2A_c}$. Крім того, гра допускає рівновагу Неша у чистих стратегіях, де захисник виділяє приманку, а атакуючий відступає, якщо виконується лема 1 та $Cap > \frac{A_c}{w_v}$ [1].

РОЗДІЛ 3 РОЗВ'ЯЗАННЯ ГРИ «НАПАДНИК-ЗАХИСНИК»

3.1 Взаємодія нападника і захисника та алгоритм визначення матричних коефіцієнтів гри

У [7] проводилися експерименти, які досліджують взаємодію між двома гравцями: «нападником» і «захисником». Зловмисник відноситься до будь-якого гравця, який отримує вигоду від успішного вторгнення, наприклад, терористична група, кібер-хакер або злочинне угруповання. У кожному періоді часу обидва агенти приймають такі рішення: зловмисник повинен вибрати, чекати чи атакувати, що тягне за собою додаткові витрати F_A. Захисник повинен вибрати, чи залишатися в стані низької готовності, чи взяти на себе плату F_D за позицію високої готовності, яка б блокувала атаку. Зловмисник і захисник мають різні виграші, які залежать як від того, чи розпочато атаку, так і від того, чи була атака успішною, як показано в таблиці 3.1. Витрати захисника віднімаються у верхньому рядку (висока тривога), а витрати нападника віднімаються в правій (атака) колонці. Найвищий виграш K_A для нападника отримується, якщо атака здійснюється, коли захисник перебуває в стані низької готовності (нижнє праворуч поле в таблиці). Але заблокована атака, яка відбувається, якщо захисник перебуває у стані підвищеної готовності, призведе до зменшення виграшу нападника N_A. З іншого боку, рішення не атакувати призводить до зменшення виграшу G_A нападника незалежно від рівня тривоги захисника, як показано виграшами атакуючого в стовпці «Чекати» таблиці 2.1. Це зменшення представляє вартість бездіяльності для групи, яка має намір завдати шкоди захиснику. Передбачається, що захисник дбає в першу чергу про те, щоб уникнути успішної атаки нападника, незалежно від того, чи є це результатом нападника, який утримався від спроби, чи невдалої атаки через вибір високої готовності. Таким чином, виграш захисника збільшується на додатну величину

G_D за відсутності успішної атаки та зменшується на N_D у разі успішної атаки нападника[7].

Таблиця 3.1

		Нападник	
		Чекати	Атакувати
Захисник	Висока готовність	$G_D - F_D, -G_A$	$G_D - F_D, -N_A - F_A$
	Низька готовність	$G_D, -G_A$	$-N_D, K_A - F_A$

Судячи з таблиці 3.1, можна зробити висновок, що в цій грі немає чистих стратегій в рівновазі Неша, якщо виконуються умови 3.1, 3.2:

$$G_D - F_D > -N_D \tag{3.1}$$

(краще бути в стані підвищеної готовності, якщо очікується атака).

$$K_A - F_A > -G_A > -N_A - F_A. \tag{3.2}$$

(краще атакувати тільки коли очікується атака).

Існує рівновага у змішаних стратегіях, коли захисник буде у стані підвищеної готовності з ймовірністю p_H, а нападник атакує з ймовірністю p_A. Ці рівноважні ймовірності можна знайти, прирівнявши очікувані виграші для кожного вибору. Зокрема, очікувані виграші захисника від високої готовності ($E\pi^H$) і низької готовності ($E\pi^L$) залежать від імовірності того, що зловмисник вирішить атакувати, як детально описано у рівняннях 3.3, 3.4:

$$E\pi^H = G_D - F_D, \tag{3.3}$$

$$E\pi^L = (1 - p_A)G_D + p_A(-N_D). \quad (3.4)$$

Захисник має бути байдужим до випадковості, тому прирівнюємо ці два рівняння, щоб знайти рівноважні ймовірності в змішаних стратегіях:

$$G_D - F_D = (1 - p_A)G_D + p_A(-N_D).$$

Тоді, отримаємо рівняння 3.5:

$$p_A^* = \frac{F_D}{G_D + N_D}. \quad (3.5)$$

Аналогічно знаходяться очікувані виграші нападника від очікування та атаки(3.6 і 3.7):

$$E\pi^W = -G_A, \quad (3.6)$$

$$E\pi^A = p_H(-N_A) + (1 - p_H)(-K_A) - F_A. \quad (3.7)$$

Маємо: $-G_A = p_H(-N_A) + (1 - p_H)(-K_A) - F_A$, отримуємо формулу 3.8:

$$p_H^* = \frac{K_A - F_A + G_A}{K_A + N_A}. \quad (3.8)$$

Кожен гравець має свою «безпечну» стратегію з конкретним виграшем, очікування для нападника і стан підвищеної готовності для захисника, тому природньо враховувати ефекти уникнення ризику. Нехай EU^H і EU^L (3.9, 3.10)– очікувані корисності, отримані шляхом заміни виграшів захисників для кожного результату в рівняннях 3.3 і 3.4 відповідними корисностями, позначеними U(·), які, як припускається, є зростаючими та диференційованими.

$$EU^H = U(G_D - F_D), \tag{3.9}$$

$$EU^L = (1 - p_A)U(G_D) + p_A U(-N_D). \tag{3.10}$$

Нехай EV^W і EV^A (3.11,3.12) представляють очікувані корисності зловмисника, отримані шляхом заміни виграшів зловмисника для кожного результату в рівнянні (5) відповідними корисностями, позначеними як V(·), які вважаються зростаючими та диференційовними.

$$EV^W = V(-G_A), \tag{3.11}$$

$$EV^A = p_H V(-N_A - F_A) + (1 - p_H)V(-K_A - F_A). \tag{3.12}$$

Рівновага Неша за наявності ухилення від ризику прирівняє очікувані корисності двох дій кожного гравця, і отриману систему рівнянь можна розв'язати для наступних прогнозів Неша зі змішаною стратегією.

$$U(G_D - F_D) = (1 - p_A)U(G_D) + p_A U(-N_D),$$

$$V(-G_A) = p_H V(-N_A - F_A) + (1 - p_H)V(-K_A - F_A).$$

Тоді маємо формули 3.13, 3.14

$$p_A^* = \frac{U(G_D) - U(G_D - F_D)}{U(G_D) - U(-N_D)}, \tag{3.13}$$

$$p_H^* = \frac{V(K_A - F_A) - V(-G_A)}{V(K_A - F_A) - V(-N_A - C_A)}. \tag{3.14}$$

Імовірності атаки (3.5) і (3.13) залежать лише від параметрів виграшу захисника, і, отже, на них не впливають зміни вартості атаки. Цей результат не вимагає, щоб атакуючий і захисник були нейтральними до ризику або навіть мали однакову функцію корисності фон Неймана-Моргенштерна.

Хоча проста інтуїція може припустити, що менші витрати на атаку призведуть до вищої ймовірності атаки, рівноважна ймовірність атаки за Нешем у рівнянні (3.13) залишається незмінною. Оскільки нижчі витрати на атаку атаки призводить до вищих виграшів від атаки, захисник збільшує ймовірність високого рівня готовності (3.14), щоб компенсувати ці вищі виграші та тримати зловмисника байдужим, а отже, бажаючим рандомізувати.

Можна ввести «середню» готовність, тобто,маємо гру 3×2, у захисника 3 стратегії. «Середню» готовність визначимо як середнє арифметичне між значеннями у високій і низькій готовності (табл.3.2)

Таблиця 3.2

		Нападник	
		Чекати	Атакувати
Захисник	Висока готовність	$G_D - F_D, -G_A$	$G_D - F_D, -N_A - F_A$
	Середня готовність	$\frac{1}{2}(2G_D - F_D);\ -G_A$	$\frac{1}{2}(G_D - F_D - N_D); \frac{1}{2}\ (-N_A - 2F_A - K_A)$
	Низька готовність	$G_D, -G_A$	$-N_D, K_A\ - F_A$

3.2 Чисельні приклади розв’язання гри «нападник-захисник»

Нехай є три процедури, описані в [7], вони змінювали витрати нападника від 1 до 3 до 5 євро, при цьому витрати на режим високої готовності захисника - 3 євро. Мета процедури полягала в оцінці реакцій поведінки на зміни витрат нападника, які, за прогнозами, не змінять ймовірність атаки в результаті підвищеної тенденції для захисників вибирати варіант високої готовності, коли вартість атаки є низькою. Виграші зроблено такими, щоб успішна атака була дуже дорогою для захисника (N_D = 5 євро), а, отже, дуже цінною для нападника (K_A = 5 євро). На невдалі атаки зазвичай не звертають увагу, і, отже, ефект

виграшу від них був встановлений меншим, N_A = 1 євро. Аналогічно є витрати за відсутність атаки (або невдалу атаку для захисників), вони також були підібрані невеликими: G_D = 1 євро і G_A = 1 євро.

Під час перегляду матриці виграшів, рішення, який виграш вказати, приймалися незалежно. Виплати для кожного елемента матриці були пояснені з точки зору вартості атаки, захисту та бездіяльності, а також витрат і прибутків від успішних і невдалих атак. Тому, стандартне представлення матриці виграшів було доповнено «гарячою» термінологією, пов'язаною з атакою(неочікуванням), очікуванням, високою та низькою готовністю. Додатково, разом з виграшами, залежних від результату, кожен гравець отримував зовнішній дохід кожного раунду, тобто фіксовану оплату, яка не залежала від результату гри. Однак цей фіксований платіж відображався окремо від матриці виграшів, і гравці не знали фіксований дохід для іншої особи, що має бажаний ефект у вигляді зменшення міркувань справедливості, які не є властивістю більшості налаштувань нападника та захисника. Фіксовані виграші, 3 євро для захисників і 2 євро для нападників, були встановлені для вирівнювання очікуваних виграшів у рівновазі у змішаних стратегіях. Навіть незважаючи на те, що суб'єкти не знали про фіксовану оплату іншого і їм не було показано фіксованих виграшів у матриці виграшів, було б повчально подивитися на матрицю виграшів, яка включає ці виграші.

Матриці виграшу наведено в таблиці 3.3. Наприклад, у другій матриці (2 процедура), вартість атаки - 3 євро, виграш захисника в 1 євро для результату високої тривоги/очікування розраховується як 3 – 3 + 1 (фіксований дохід у розмірі 3 євро мінус вартість захисту від високої тривоги у розмірі 3 євро плюс виграш захисника у розмірі 1 євро, коли немає атаки). Однак на сторінках рішень гравців цей запис матиме значення −2, оскільки фіксований платіж у три не вставлено в поле, і справді, цей фіксований платіж відомий лише захиснику. З матриці виграшів очевидно, що кожен гравець має безпечну стратегію: висока готовність для захисника та очікування для нападника. Кожна з цих стратегій дає

впевнений виграш у розмірі 1 євро (якщо включено фіксований дохід), і, отже, очікуваний прибуток становить 1 євро для кожного гравця в нейтральній до ризику рівновазі Неша. Для обох гравців така ймовірність вибору, що дорівнює 0,5, дає очікувані виграші в 1 за кожне рішення в процедурі з середніми витратами на атаку. Звичайно, кожен гравець знає, що інший також має безпечну стратегію, але не знає, скільки інший гравець заробляє на цій стратегії.

Таблиця 3.3

			Нападник	
			Чекати	Атакувати
1 процедура	Захисник	Висока готовність	1,1	1,0
		Низька готовність	4,1	-2,6
			Нападник	
			Чекати	Атакувати
2 процедура	Захисник	Висока готовність	1,1	1,-2
		Низька готовність	4,1	-2,4
			Нападник	
			Чекати	Атакувати
3 процедура		Висока готовність	1,1	1,-4
		Низька готовність	4,1	-2,2

Нехай матриця виграшів для захисника має вигляд(табл 3.4):

Таблиця 3.4

		Нападник	
		Чекати	Атакувати
Захисник	Висока готовність	1	1
	Низька готовність	4	-2

Знайдемо оптимальні розв’язки, звівши цю задачу до ЗЛП.

ЗЛП для захисника має вигляд:

$$\begin{cases} F = v \to max, \\ x_1 + 4x_2 \geq v, \\ x_1 - 2x_2 \geq v, \\ x_1 + x_2 = 1, \\ x_1, x_2 \geq 0, \\ v \in R. \end{cases}$$

Для атакуючого

$$\begin{cases} F = v \to min, \\ y_1 + y_2 \leq v, \\ 4y_1 - 2y_2 \leq v, \\ y_1 + y_2 = 1, \\ y_1, y_2 \geq 0, \\ v \in R. \end{cases}$$

Нехай $v \geq 0, a_i = \frac{p_i}{v}, b_j = \frac{q_j}{v}, i = 1;2, j = 1;2$, p_i, q_j – значення ймовірностей. Тоді для нападника маємо (а для захисника є двоїстою задачею):

$$\begin{cases} b_1 + b_2 \to max, \\ b_1 + b_2 \leq 1, \\ 4b_1 - 2b_2 \leq 1, \\ b_1, b_2 \geq 0. \end{cases}$$

Зведемо цю задачу до канонічного вигляду, ввівши додаткові змінні (в даному випадку - b_3, b_4) та розв'яжемо симплекс-методом.

$$\begin{cases} b_1 + b_2 + 0b_3 + 0b_4 \to max, \\ b_1 + b_2 + b_3 = 1, \\ 4b_1 - 2b_2 + b_4 = 1, \\ b_1, b_2, b_3, b_4 \geq 0. \end{cases}$$

Початкова таблиця(табл.3.5)

Таблиця 3.5

	b_1	b_2	b_3	b_4	p
b_1	**1**	**1**	**1**	**0**	**1**
b_2	4	**-2**	0	1	1
	1	**1**	0	0	0

1 ітерація(табл 3.6)

Таблиця 3.6

	b_1	b_2	b_3	b_4	p
b_2	1	1	1	0	1
b_4	6	0	2	1	3
	0	0	-1	0	-1

Отже, $b_1 = 0, b_2 = 1, b_3 = 0, b_4 = 3$, max=1.

Але коефіцієнт при змінній b_1 дорівнює 0, і якщо ми будемо її змінювати, то останній рядок таблиці 3.6 не зміниться, і тому, ми отримаємо другий розв'язок. Тоді, маємо(табл.3.7)

Таблиця 3.7

	b_1	b_2	b_3	b_4	p
b_2	**1**	1	1	0	1
b_4	**6**	**0**	**2**	**1**	**3**
	0	0	-1	0	-1

Продовжуємо далі (табл.3.8)

Таблиця 3.8

	b_1	b_2	b_3	b_4	p
b_2	0	1	$\frac{2}{3}$	$\frac{-1}{6}$	$\frac{1}{2}$
b_4	1	0	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{2}$
	0	0	-1	0	-1

Маємо: $b_1 = \frac{1}{2}, b_2 = \frac{1}{2}, b_3 = 0, b_4 = 0, v = 1.$

Тоді оптимальний план першої задачі(для захисника): (1,0,0,0), ціна гри $v = 1.$

Оптимальний розв'язок першої задачі(p_1, p_2) $(1 \times 1; 0 \times 1) = (1; 0).$

Тепер, крім високої та низької готовності, додамо середню готовність, яка визначена в таблиці 2.2 (Табл 3.9).

Таблиця 3.9

		Нападник	
		Чекати	Атакувати
Захисник	Висока готовність	1	1
	Середня готовність	2,5	-0,5
	Низька готовність	4	-2

За мінімаксним критерієм знайдемо оптимальні розв’язки, звівши цю задачу до ЗЛП.

ЗЛП для захисника має вигляд:

$$\begin{cases} F = v \to max, \\ x_1 + 2{,}5x_2 + 4x_3 \geq v, \\ x_1 - 0{,}5x_2 - 2x_3 \geq v, \\ x_1 + x_2 + x_3 = 1, \\ x_1, x_2, x_3 \geq 0, \\ v \in R. \end{cases}$$

Для атакуючого

$$\begin{cases} F = v \to min, \\ y_1 + y_2 \leq v, \\ 2{,}5y_1 - 0{,}5y_2 \leq v, \\ 4y_1 - 2y_2 \leq v, \\ y_1 + y_2 = 1, \\ y_1, y_2 \geq 0, \\ v \in R. \end{cases}$$

Нехай $a_i = \frac{p_i}{v}, b_j = \frac{q_j}{v}, i = 1; 2; 3, j = 1; 2,$ p_i, q_j – значення ймовірностей. Тоді для нападника маємо (а для захисника є двоїстою задачею):

$$\begin{cases} b_1 + b_2 \to max, \\ b_1 + b_2 \leq 1, \\ 2{,}5b_1 - 0{,}5b_2 \leq 1, \\ 4b_1 - 2b_2 \leq 1, \\ b_1, b_2 \geq 0. \end{cases}$$

Зведемо цю задачу до канонічного вигляду, ввівши додаткові змінні (в даному випадку - b_3, b_4, b_5) та розв’яжемо симплекс-методом.

$$\begin{cases} b_1 + b_2 + 0b_3 + 0b_4 \to max, \\ b_1 + b_2 + b_3 = 1, \\ 2{,}5b_1 - 0{,}5b_2 + b_4 = 1, \\ 4b_1 - 2b_2 + b_5 = 1, \\ b_1, b_2, b_3, b_4, b_5 \geq 0. \end{cases}$$

Початкова таблиця(табл.3.10)

Таблиця 3.10

	b_1	b_2	b_3	b_4	b_5	p
b_1	**1**	**1**	**1**	**0**	**0**	**1**
b_2	$\frac{5}{2}$	$\frac{\mathbf{-1}}{\mathbf{2}}$	0	1	0	1
b_3	4	**-2**	0	0	1	1
	1	**1**	0	0	0	0

1 ітерація(табл 3.11)

Таблиця 3.11

	b_1	b_2	b_3	b_4	b_5	p
b_2	1	1	1	0	0	1
b_4	3	0	$\frac{1}{2}$	1	0	$\frac{3}{2}$
b_5	6	0	2	0	1	3
	0	0	-1	0	0	-1

Отже, $b_1 = 0, b_2 = 1, b_3 = 0, b_4 = \frac{3}{2}, b_5 = 3$, max=1

Але коефіцієнт при змінній b_1 дорівнює 0, і якщо ми будемо її змінювати, то останній рядок таблиці 3.11 не зміниться, і тому, ми отримаємо другий розв'язок. Тоді, маємо(табл.3.12)

Таблиця 3.12

	b_1	b_2	b_3	b_4	b_5	p
b_2	**1**	1	1	0	0	1
b_4	**3**	0	$\frac{1}{2}$	1	0	$\frac{3}{2}$
b_5	**6**	**0**	**2**	**0**	**1**	**3**
	0	0	-1	0	0	-1

Продовжуємо далі (табл.3.13)

Таблиця 3.13

	b_1	b_2	b_3	b_4	b_5	p
b_2	0	1	$\frac{2}{3}$	0	$\frac{-1}{6}$	$\frac{1}{2}$
b_4	0	0	$\frac{-1}{2}$	1	$\frac{-1}{2}$	0
b_1	1	0	$\frac{1}{3}$	0	$\frac{1}{6}$	$\frac{1}{2}$
	0	0	-1	0	0	-1

Маємо: $b_1 = \frac{1}{2}, b_2 = \frac{1}{2}, b_3 = 0, b_4 = 0, b_5 = 0, v = 1.$

Тоді оптимальний план першої задачі(для захисника): (1,0,0,0,0), ціна гри $v = 1$.

Оптимальний розв'язок першої задачі (p_1, p_2, p_3) $(1 \times 1; 0 \times 1; 0 \times 1) = (1; 0; 0)$.

ВИСНОВКИ

У процесі дослідження взаємодії агентів нападник – захисник у системах захисту відмічається актуальність теми роботи через значне приділення уваги багатьма дослідниками, що підтверджується наявними розглянутими опублікованими науковими статтями за останні роки та сучасною літературою.

Запропонований спосіб отримання коефіцієнтів платіжних матриць гри нападник-захисник може покращити якість роботи протекційних систем за допомогою налаштування відповідних її параметрів. Подальше розв‘язання гри за допомогою методів лінійного програмування є відомою задачею.

Подальші дослідження як самої гри нападник-захисник, так і способів знаходження коефіцієнтів платіжних матриць має важливе значення, особливо у випадках групи нападників та ієрархічної захисної структури протекційної системи, а також у багатьох інших випадках.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Jyn Atli Benediktsson, Xiaoou Li, Jeffrey Reed and others. Game Theory and Machine Learning for Cyber Security, IEEE Press, Wiley - New Jersey 2021. 547 p
2. Теорія ігор: курс лекцій [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалаври, за освітніми програмами «Системний аналіз і управління», «Системи і методи штучного інтелекту» спеціальностей 124 «Системний аналіз», 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; уклад. Л. В. Барановська. – Електронні текстові дані (1 файл: 21,06 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 245 с. – Назва з екрана.
3. Оуэн Г. Теория игр; пер. с англ. Врублевской И. Н., Дюбина Г. Н., Ляпунова А. Н. Москва: Мир, 1971. 230 с.
4. Дж. Мак-Кинси. Введение в теорию игр; пер. с англ. И. В. Соловьева. Москва: Физматгиз, 1960. 422 с.
5. Партхасаратхи, Рагхаван Т. Некоторые вопросы теории игр двух лиц. – М.: Мир, 1974. 297 с.
6. Attacker-Defender Games: An Introduction - Режим доступу:https://imowensims.wordpress.com/2015/12/29/attacker-defender-games-an-introduction (дата звернення 10.05.2023)
7. Charles A. Holt, Ricky Sahu, Angela M. Smith An experimental analysis of risk effects in attacker-defender games Southern Economic Journal Volume 89, Issue 1 p. 185-215.
8. E.O., Ibidunmoye, Alese B.K., and Ogundele O.S.. "Modeling Attacker-Defender Interaction as a Zero-Sum Stochastic Game." Journal of Computer Sciences and Applications 1.2 (2013): 27-32.DOI: 10.12691/jcsa-1-2-3
9. Мулен Э. Теория игр с примерами из математической экономики; пер. с франц. Меньшиковой О. Р., Меньшикова И. С. – М.: Мир, 1985. 200 с.
10. Писарук Н. Н. Введение в теорию игр. Минск: БГУ, 2019. 283 с.

11. Петросян Л. А., Зенкевич Н. А., Семина Е. А. Теория игр: Учебное пособие для университетов. Высш. шк., Книжный дом «Университет», 1998. 304 с.
12. Воробьев Н. Н. Основы теории игр. Бескоалиционные игры. Москва: Наука, 1984. 495 с.