

Міністерство освіти і науки України
Львівський національний університет імені Івана Франка
Механіко-математичний факультет

Кафедра математичної економіки,
економетрії, фінансової та страхової
математики

Магістерська робота
Дослідження операційних систем за допомогою теорії ігор

Виконала: студентка групи МТЕМ-21с
спеціальності 111 – математика ,
спеціалізації *математична економіка та
економетрика*

Михаленич Маріанна Степанівна

Науковий керівник:
доц. Козицький В.А.

*Роботу рекомендовано до захисту
на засіданні кафедри математичної
економіки, економетрії, фінансової та
страхової математики
протокол від 04 грудня 2020 року №4
В. о. завідувача кафедрою
проф. Оліскевич М. О.*

Львів - 2020

Зміст

1	Вступ	3
2	Загальні поняття в теорії ігор	4
3	Ігрова модель	6
3.1	Припущення моделі	7
4	Змішана рівновага Неша стратегії гри для безпеки з три-рівневими стратегіями:	10
5	Доведення основних лем	14
6	Формулювання задач і розв'язання	16
6.1	Задача вартості стратегії	16
6.2	Задача: два рівня інтенсивності	17
6.3	Задача: Припущення моделі	18
6.4	Гра: Нападник з декількома стратегіями	20
6.5	Задача 1	21
7	Висновок	25
8	Використана література	26

1 Вступ

Концепція теорії ігор останнім часом знайшла широке застосування в галузі безпеки, яку зазвичай називають іграми безпеки. Гра може мати нормальну, або обширну форму і використовується для моделювання поведінки гравців у простому, або складному змаганні за ресурси в рамках даного сценарію. У цій роботі розглядається застосування теорії ігор у кібербезпеці.

Таким чином, окрім пошуку конкретного алгоритму захисту, однаково, або навіть важливіше розробити динамічну захисну систему, яка може коригувати свої стратегії для досягнення найкращих захисних показників від розумних нападників та в різних ситуаціях атаки.

У цій роботі представляється новий підхід до механізму захисту від декількох типів атак/загроз у мережах - механізму гіперзахисту, який враховує обмеження ресурсів, а також цінність безпеки активу мережі. Модель забезпечує відповіді захисника, враховуючи різну інтенсивність атак та відносну вартість їх запуску. Ми моделюємо взаємодію між нападниками та захисниками як гру в кібервійну, оскільки вона виявилася високоефективним математичним методом для аналізу та моделювання сценаріїв із суперечливими цілями. Крім того, для управління майбутніми загрозами в системах безпеки теорія ігор корисна при пропонуванні різних ймовірних дій та прогнозуванні пов'язаних з ними результатів. Представимо гру нападника-захисника з нульовою сумою, що не співпрацює.

Крім того, ми досягаємо оптимальних стратегій для захисника та нападника, враховуючи, що вони можуть динамічно вибирати свої стратегії, щоб максимізувати власну виплату на основі мінімізації витрат.

2 Загальні поняття в теорії ігор

Означення 2.1. Гра в стратегічній або нормальній формі визначається системою $G = (N, (A_i), (u_i))$:

- $N = \{1, \dots, n\}$ –множина гравців;
- A_i –множина стратегій i -го гравця;
- $u_i : A = \otimes A_i \rightarrow R$ –функція виграшу i -того гравця.

Сукупність стратегій $a = (a_1, \dots, a_n)$ –називається **ситуацією гри** або **профілем гри**. Нехай $a \in A$ –профіль гри, тоді $u_i(a)$ –виграш гравця при реалізації ситуації a .

Означення 2.2. Профіль гри $a^* = (a_1^*, \dots, a_n^*) \in A$ –називається **рівновагою Неша** гри G , якщо

$$\forall i \in N, u_i(a^*) \geq u_i(a_i, a_{-i}^*), \forall a_i \in A_i,$$

$$\text{де } a_{-i}^* = (a_1^*, \dots, a_{i-1}^*, a_{i+1}^*, \dots, a_n^*) \in \otimes_{j \neq i} A_j.$$

Рівновагою Неша гри є головною концепцією гри. Для відшукання рівноваги Неша, або точки Неша гри визначаються нульові реакції i -го гравця на вибір партнерів гри:

$$\begin{aligned} BR_i(a_{-i}) &= \{a_i \in A_i : u_i(a_i, a_{-i}) = \max_{a'_i \in A_i} u_i(a'_i, a_{-i})\}. \\ &= \arg \max_{a'_i \in A_i} u_i(a'_i, a_{-i}). \end{aligned}$$

Отже, профіль $a^* \in A$ –точка Неша гри G тоді і тільки тоді, коли

$$\forall i \in N, a_i^* \in BR_i(a_{-i}).$$

Розглянемо, як гра безпеки зловмисника-захисника сформульована як гра з нульовою сумою, що не співпрацює. Також, опишемо стратегії нападника та захисника та знайдемо їх розв'язок. Будучи раціональними гравцями у грі, зловмисник змагається за найкращу дію, а його мета -

максимізувати власну корисність. Отже, в нашій грі гравці не зобов'язані співпрацювати один з одним.

Зловмисник вибирає таку стратегію, щоб максимізувати свої шанси на успіх та витратити ресурси системи. На відміну від цього, захисник також вибирає відповідну стратегію, щоб максимізувати свої шанси на захист від суперників без надмірної витрати енергії або розрахунків на ефективність. Більшість моделюють нападників та захисників на основі таких стратегій: відсутність атаки/захисту або атаки/захисту. Для того, щоб забезпечити більш широке моделювання нападників / захисників, де вони можуть коригувати свої стратегії атаки / оборони з різною інтенсивністю, ми моделюємо кожного гравця з трьома рівнями стратегій: відсутність атаки / захисту, низький рівень інтенсивності та високий рівень інтенсивності.

Зловмисники та захисники відчують різну цінність, щоб досягнути свого успіху в атаці чи обороні. Тому в нашій грі кожен зловмисник і захисник має різні рівні стратегій. Кожен з гравців має відповідні свої стратегії: приймає нульовий рівень інтенсивності, низький рівень інтенсивності або високий рівень інтенсивності.

3 Ігрова модель

Ми розглядаємо двокористувацьку гру з безпекою з нульовою сумою, представлену $G = \langle (N); (S); (U) \rangle$; де $N = \{A, D\}$ представляє двох гравців:

Гравець I: A - нападник, а інший гравець II: D - захисник.

$S = \{a_i, d_i | i \in \{0, 1, 2\}\}$ - це простір стратегій, що являє собою набір дій, доступних для кожного гравця, а їх виграші задаються U , де $U = (u_i)$.

Як ми вже згадували вище, під час гри зловмисник і захисник можуть використовувати один із трьох рівнів доступних стратегій.

- 1) $a_0 = \text{Немає атаки}$, для зловмисника нульовий рівень означає, що він вирішив не атакувати;
- 2) рівень перший - низька інтенсивність атаки, позначається $a_1 = \text{Атака-1}$;
- 3) $a_2 = \text{Атака-2}$, другий рівень - висока інтенсивність атаки.

Взагалі кажучи, з точки зору зловмисника, у порівнянні зі стратегією a_2 , стратегія a_2 є більш ефективною у створенні успішної атаки, але вимагає більше ресурсів або створення стратегії для здійснення зловмисником. Буде правильна така нерівність: $a_2 > a_1 > a_0$.

Стратегії для захисника:

- рівень нуль для захисника означає, що він вирішив не застосовувати жодний захист, позначається $d_0 = \text{Немає захисту}$;
- $d_1 = \text{Захист-1}$, перший рівень - це низька інтенсивність захисту;
- $d_2 = \text{Захист-2}$, другий рівень - висока інтенсивність захисту.

Отже, у зловмисника A є три стратегії: $a_0 = \text{Немає атаки}$, $a_1 = \text{Напад-1}$ і $a_2 = \text{Напад-2}$. У захисника D , тобто у другого гравця також є три стратегії: $d_0 = \text{Немає захисту}$, $d_1 = \text{Захист-1}$ і $d_2 = \text{Захист-2}$. Обидва гравці обирають свої стратегії одночасно без будь-якої співпраці, припускаючи загальні знання про гру G і яким буде виграш, тобто U .

	Захист		
	d_0	d_1	d_2
a_0	0,0	$c_{d1}, -c_{d1}$	$c_{d2}, -c_{d2}$
a_1	$u - c_{a1}, c_{a1} - u$	$c_{d1} - c_{a1}, c_{a1} - c_{d1}$	$c_{d2} - c_{a1}, c_{a1} - c_{d2}$
a_2	$u - c_{a2}, c_{a2} - u$	$u + c_{d1} - c_{a2}, c_{a2} - c_{d1} - u$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

Табл. 1: Стратегічна форма для гри Атака і Захист.

Ми вважаємо, що функція виграшу захисника D і A дорівнює u_n . В нас виграш єдиний для двох гравців.

Розглядаючи таку концепсію, зловмиснику або захиснику також потрібно докласти певних зусиль (тобто заплатити певні витрати) для реалізації своїх стратегій атаки або оборони. Для зловмисника ми позначаємо вартість атаки як c_{an} , де $n \in \{1, 2\}$:

- c_{a1} - вартість розгортання стратегії Атака-1,
- c_{a2} - вартість розгортання стратегії Атака-2.

Так само для захисника ми позначаємо вартість захисту як c_{dn} , де $n \in \{1, 2\}$:

- c_{d1} - вартість розгортання стратегії Захист-1,
- c_{d2} - вартість розгортання стратегії Захист-2.

3.1 Припущення моделі

Розглянемо тепер модель, де гравці мають різну функцію виграшу. При такій побудові гри ми відповідно будемо мати різні виграші. Ми вважаємо, що функція виграшу захисника D дорівнює u_n , де $u_n > 0$ і $n \in \{1, 2\}$; u_1 - функція виграшу, при використанні стратегії Атака-1, успішно розгорнутою зловмисником; u_2 - функція виграшу, при використанні стратегії Атака-2, успішно розгорнутою зловмисником. Відповідно до гри з нульовою сумою, ми вважаємо, що виграш одного гравця дорівнює тотальній втраті другого гравця, тобто суперника.

Отже, u_n - виграш зловмисника, якщо його стратегія Атака- n є успішною, а $-u_n$ означає втрату або шкоду захисником. Значення цієї втрати

захисником стосується ступеня або суми збитків, таких як втрата енергії, кількість порушених або відключених вузлів, втрата цілісності даних тощо.

Для запропонованої нами трирівневої моделі стратегії нападу / оборони ми робимо наступні припущення:

- Функція загального виграшу завжди перевищує вартість захищати або нападати на них, оскільки в іншому випадку захисник або нападник не має жодних стимулів для захисту або нападу, відповідно; тобто, $u_n > c_{an}, c_{dn}, n \in \{1, 2\}$.
- Вартість стратегії атаки $a_1 = \text{Атака-1}$ менша, ніж вартість стратегії атаки $a_2 = \text{Атака-2}$ для зловмисника. Оскільки a_2 є більш агресивною та ефективною стратегією атаки, ніж a_1 . a_2 вимагає більше атакуючих зусиль або витрат на розгортання. (тобто $c_{a1} < c_{a2}$)
- Вартість стратегії захисту $d_1 = \text{Захист-1}$ менша, ніж вартість стратегії $d_2 = \text{Захист-2}$ для захисника. Знову ж таки, це тому, що d_2 є більш ефективною стратегією захисту, ніж d_1 . (тобто $c_{d1} < c_{d2}$).
- Загалом кажучи, більш агресивна / ефективна атака завдасть більшої шкоди цілі, якщо атака буде успішною. Таким чином, виходячи з визначення u_n у попередньому підрозділі, можна впевнено припустити, що $(u_2 \geq u_1)$.

Крім того, ігрова модель вимагає від нас визначити результат, коли зловмисник застосовує одну конкретну стратегію атаки, а захисник реалізує одну конкретну стратегію оборони. Ми робимо наступні припущення щодо результатів гри:

- Атака успішна за таких сценаріїв: a_1 проти d_0 ; a_2 проти d_1 або d_0 .
- Захист успішний за таких сценаріїв: d_1 проти a_1 або a_0 ; d_2 проти a_2 або a_1 або a_0 .
- Нульовий виграш або втрата, коли немає атаки та не розгорнуто оборону, тобто a_0 проти d_0 .

	Захист		
	d_0	d_1	d_2
a_0	0,0	$c_{d1}, -c_{d1}$	$c_{d2}, -c_{d2}$
a_1	$u_1 - c_{a1}, c_{a1} - u_1$	$c_{d1} - c_{a1}, c_{a1} - c_{d1}$	$c_{d2} - c_{a1}, c_{a1} - c_{d2}$
a_2	$u_2 - c_{a2}, c_{a2} - u_2$	$u_2 + c_{d1} - c_{a2}, c_{a2} - c_{d1} - u_2$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

Табл. 2: Стратегічна форма для гри Атака і Захист.

Вищезазначені припущення означають, що більш агресивна оборонна стратегія, *Захист-2*, захищена від усіх атак. Однак стратегія захисту низького рівня, *Захист-1*, добре захищає атаку низького рівня *Атаки-1*, але все ще вразлива для боротьби з агресивною атакою *Атаки-2*. Таблиця (2) ілюструє матрицю виплат гри у стратегічній формі.

4 Змішана рівновага Неша стратегії гри для безпеки з трирівневими стратегіями:

Означення 4.1. *Змішана рівновага Неша стратегії гри - це розподіл ймовірності P по набору чистих стратегій S для будь-якого гравця, такий що:*

$$P = (p_1, p_2, p_3, \dots, p_r) \in \mathbb{R}^R \geq 0, i \sum_{t=1}^R p_t = 1 \quad (1)$$

Нехай p_{a_0} - це ймовірність відтворення стратегії a_0 , p_{a_1} - ймовірність відтворення стратегії a_1 , і $p_{a_2} = 1 - p_{a_0} - p_{a_1}$ буде ймовірністю для стратегії a_2 для нападника. Аналогічно проведемо міркування для захисника, другого гравця, нехай p_{d_0} є ймовірністю відтворення стратегії d_0 , p_{d_1} - ймовірністю для стратегії d_1 , а $p_{d_2} = 1 - p_{d_0} - p_{d_1}$ для стратегії d_2 .

Згідно з визначенням **змішаної рівноваги Неша стратегії гри**, опоненти ставляться байдуже до вибору своїх стратегій, зрівнюючи очікувані виграші. Отже, у запропонованій нами грі змішана стратегія робить кожного гравця байдужим серед усіх трьох своїх стратегій, коли очікувані утиліти від ігрових стратегій a_0 , a_1 та a_2 рівні для зловмисника, а очікувані утиліти від стратегій d_0 , d_1 , і d_2 рівні для захисника.

$$EU(p_{a_0}) = EU(p_{a_1}) = EU(p_{a_2}) \quad (2)$$

$$EU(p_{d_0}) = EU(p_{d_1}) = EU(p_{d_2}) \quad (3)$$

Потім, з таблиці I, ми знаходимо очікувану корисність зловмисника для відтворення стратегій a_0 , a_1 і a_2 як функції змішаної стратегії, які задаються:

$$EU(p_{a_0}) = (p_{d_0})(0) + p_{d_1}(-c_{d_1}) + p_{d_2}(-c_{d_2}) \quad (4)$$

$$EU(p_{a_1}) = (p_{d_0})(0)(u_1 - c_{a_1}) + p_{d_1}(c_{d_1} - c_{a_1}) + p_{d_2}(-c_{d_2}) \quad (5)$$

$$EU(p_{a_2}) = (p_{d_0})(0)(u_2 - c_{a_2}) + p_{d_1}(u_2 + c_{d_2} - c_{a_2}) + p_{d_2}(c_{d_2} - c_{a_2}) \quad (6)$$

Підставивши (4), (5) та (6) у (2), ми маємо ймовірність розподіл p_{a_0} , p_{a_1} , і p_{a_2} для зловмисника, наприклад:

$$p_{a_0} = \frac{c_{a_1}}{u_1}, p_{a_1} = \frac{c_{a_2}}{u_2} - \frac{c_{a_1}}{u_1}, p_{a_2} = 1 - \frac{c_{a_2}}{u_2} \quad (7)$$

Подібним чином очікувана корисність захисника для відтворення стратегій d_0 , d_1 , і d_2 є функцією змішаної стратегії, яка визначається:

$$EU(p_{d_0}) = (p_{d_0})(0) + p_{d_1}(c_{a_1} - u_1) + p_{d_2}(c_{a_2} - u_2) \quad (8)$$

$$EU(p_{d_1}) = (p_{d_0})(c_{d_1}) + p_{d_1}(c_{a_1} - c_{d_1}) + p_{d_2}(c_{a_2} - u_2 c_{d_1}) \quad (9)$$

$$EU(p_{d_2}) = (p_{d_0})(u_2 - c_{a_2}) + p_{d_1}(c_{a_1} - c_{d_2}) + p_{d_2}(c_{a_2} - c_{d_2}) \quad (10)$$

Підставивши (8), (9) і (10) у (3), ми маємо ймовірність розподіл p_{d_0} , p_{d_1} і p_{d_2} для захисника, наприклад:

$$p_{d_0} = 1 - \left(\frac{c_{d_2} - c_{d_1}}{u_2} + \frac{c_{d_1}}{u_1} \right), p_{d_1} = \frac{c_{d_1}}{u_1}, p_{d_2} = \frac{c_{d_2} - c_{d_1}}{u_2} \quad (11)$$

Змішана стратегія Рівноваги Неша для гри безпеки без співпраці задається розподілом $\{p_{a_0}, p_{a_1}, p_{a_2}\}$ та $\{p_{d_0}, p_{d_1}, p_{d_2}\}$ рівнянь (7) та (11), що означає, що кожен гравець рандомізує свою відповідність вибору із розподілом ймовірностей. Отже, отримаємо те, що суперники в грі будуть байдужими щодо результатів гри.

2) Змішана стратегія Рівноваги Неша для гри в безпеку з дворівневими стратегіями: у випадку $c_{a_2} \ll u_2$, ми могли б мати $p_{a_1} < 0$ відповідно до рівняння (7), що означає, що зловмисникові потрібно було б надати негативну вагу стратегії a_1 , щоб зробити іншого гравця байдужим між своїми трьома стратегіями, а це неможливо.

З іншого боку, ця негативна ймовірність означає, що зловмисник взагалі не має стимулу розгортати стратегію a_1 і має сильний стимул завжди грати в стратегію a_2 (рівень 2 атаки) замість стратегії a_1 (рівень 1 атаки), коли він намагається атакувати систему з метою максимізації його виграшу.

a_0	$0,0$	$c_{d2}, -c_{d2}$
a_2	$u_2 - c_{a2}, c_{a2} - u_2$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

Табл. 3: Стратегічна форма для гри Атака і Захист з двома стратегіями

На відміну від цього, захисник не має жодних стимулів грати в стратегію d_1 (рівень 1 захисту), яка мінімізує його виграш і коштує йому дорожче через збільшення цінності безпеки.

Таким чином, дві стратегії a_1 та d_1 можуть бути повністю виключені із простору стратегій. Як результат, гра зменшиться до 2-х стратегій для кожного гравця з новою змішаною стратегією Рівноваги Неша.

Якщо система перебуває під агресивною атакою з дуже малими витратами на атаку, некоординаційна гра безпеки з нульовою сумою буде переформульована за допомогою нового простору стратегій $A = \{a_r, d_r | r \in \{0, 2\}\}$. У зловмисника є дві чисті стратегії $a_0 =$ Немає атаки, і $a_2 =$ Атака-2. Крім того, захисник має дві чисті стратегії: $d_0 =$ Немає захисту і $d_2 =$ Захист -2. Таблиця (3) ілюструє матрицю виграшів гри з двома стратегіями.

Розподіл $\{p_{a0}, p_{a2} = 1 - p_{a0}\}$ для I-го гравця та $\{p_{d0}, p_{d2} = 1 - p_{d0}\}$ для II-го гравця є змішаною стратегією рівноваги Неша для гри безпеки, що не співпрацює. У цьому випадку кожен гравець рандомізує свій вибір двох стратегій на відповідність розподілу ймовірностей, і йому також буде байдуже щодо результатів гри.

Для обчислення цих ймовірностей для зловмисника ми розраховуємо очікувану корисність як функцію змішаної стратегії, що задається за допомогою:

$$EU(p_{d_0}) = (p_{a_0})(0) + p_{a_2}(c_{a_2} - u_2) \quad (12)$$

$$EU(p_{d_2}) = (p_{a_0})(-c_{d_2}) + p_{a_2}(c_{a_2} - u_2) \quad (13)$$

Очікувана корисність захисника для ігрових стратегій d_0 і d_2 є функцією змішаної стратегії, яка визначається:

$$EU(p_{a_0}) = (p_{d_0})(0) + p_{d_2}(c_{d_2}) \quad (14)$$

$$EU(p_{a_2}) = (p_{d_0})(u_2 - c_{a_2}) + p_{d_2}(c_{d_2} - c_{a_2}) \quad (15)$$

Як вже було згадано вище, очікувані корисні можливості гри за двома стратегіями кожного гравця рівні, і жоден гравець не має стимулу змінити свою стратегію. Таким чином,

$$EU(p_{d_0}) = EU(p_{d_2}) \quad (16)$$

$$EU(p_{a_0}) = EU(p_{a_2}) \quad (17)$$

На основі цього, підставивши (12), (13) в (16), (14) і (15) в (17) і розв'язавши вираз, щоб знайти ймовірності, що відповідають рівновазі, отримуємо:

$$p_{a_0} = \frac{u_2 - c_{a_1}}{u_2}, p_{a_2} = 1 - \frac{u_2 - c_{a_1}}{u_2} \quad (18)$$

$$p_{d_0} = \frac{c_{d_2}}{u_2}, p_{d_2} = 1 - \frac{c_{d_2}}{u_2} \quad (19)$$

5 Доведення основних лем

Для більш чіткого розуміння основних стратегій наведемо основні леми.

Лема 1: Стратегія зловмисника A^* - найкраща відповідь на стратегію захисника D у G , якщо $\hat{A}^* = \mu(A^*)$ - найкраща відповідь зловмисника на D у \hat{G}

Доведення: Щоб довести цю лему, ми повинні довести що:

$$U_A^G(D, A^*) - U_A^G(D, A') \geq 0 \Leftrightarrow U_{\hat{A}}^{\hat{G}}(D, \hat{A}^*) - U_{\hat{A}}^{\hat{G}}(D, \hat{A}') \geq 0, \forall A'$$

Ми маємо, що $a_i = \frac{1}{\lambda} \hat{a}_i \frac{\Delta U_A(t_i)}{\Delta U_D(t_i)}$. І як ми знаємо, що $U_A(t_i), U_D(t_i), \lambda \geq 0$ має місце наступне:

$$\begin{aligned} U_A^G(D, A^*) - U_A^G(D, A') &\geq 0 \Leftrightarrow \sum_{i=1}^n a_i^* (c_i U_A^{bp}(t_i) + (1 - c_i) U_A^{bl}(t_i)) - \\ &\sum_{i=1}^n a_i' (c_i U_A^{bp}(t_i) + (1 - c_i) U_A^{bl}(t_i)) \geq 0 \\ &\Leftrightarrow \sum_{i=1}^n (a_i^* - a_i') (c_i U_A^{bp}(t_i) + (1 - c_i) U_A^{bl}(t_i)) \\ &\Leftrightarrow \sum_{i=1}^n \frac{1}{\lambda} \frac{\Delta U_A(t_i)}{\Delta U_D(t_i)} (a_i^* - a_i') (c_i U_A^{bp}(t_i) + (1 - c_i) U_A^{bl}(t_i)) \geq 0 \\ &\Leftrightarrow \sum_{i=1}^n (a_i^* - a_i') (c_i U_A^{bp}(t_i) + (1 - c_i) U_A^{bl}(t_i)) \geq 0 \\ &\Leftrightarrow U_{\hat{A}}^{\hat{G}}(D, \hat{A}^*) - U_{\hat{A}}^{\hat{G}}(D, \hat{A}') \geq 0 \end{aligned}$$

△

Лема 2: Стратегія захисника D є найкращою відповіддю на стратегію зловмисника A у грі G , якщо D також є найкращою відповіддю на стратегію зловмисника $\mathcal{A} = \mu(A)$ у грі \mathcal{G} .

Доведення: Щоб довести цю лему, ми повинні довести що:

$$U_D^G(D^*, A) - U_D^G(D', A) \geq 0 \Leftrightarrow U_{\hat{D}}^{\hat{G}}(D^*, \hat{A}) - U_{\hat{D}}^{\hat{G}}(D', \hat{A}) \geq 0, \forall D'$$

Ми доведемо цю нерівність має місце наступне:

$$\begin{aligned} U_D^G(D^*, A) - U_D^G(D', A) &\geq 0 \Leftrightarrow \sum_{i=1}^n a_i (c_i^* U_D^{bp}(t_i) + (1 - c_i^*) U_D^{bl}(t_i)) - \\ &\sum_{i=1}^n a_i (c_i' U_D^{bp}(t_i) + (1 - c_i') U_D^{bl}(t_i)) \geq 0 \\ &\Leftrightarrow \sum_{i=1}^n a_i (c_i^* \Delta U_D(t_i) + U_D^{bl}(t_i)) - \sum_{i=1}^n a_i (c_i' \Delta U_D(t_i) + U_D^{bl}(t_i)) \geq 0 \\ &\Leftrightarrow \sum_{i=1}^n a_i (c_i^* - c_i') \Delta U_D(t_i) \geq 0 \\ &\Leftrightarrow \sum_{i=1}^n \frac{1}{\lambda} \frac{\Delta U_A(t_i)}{\Delta U_D(t_i)} \hat{a}_i (c_i^* - c_i') \Delta U_D(t_i) \geq 0 \\ &\Leftrightarrow \sum_{i=1}^n \hat{a}_i (c_i^* - c_i') \Delta U_A(t_i) \geq 0 \Leftrightarrow \sum_{i=1}^n \hat{a}_i (c_i^* - c_i') \geq 0 \\ &\Leftrightarrow \Delta \hat{U}_D(t_i) \geq 0 \sum_{i=1}^n \hat{a}_i (c_i^* - c_i') \Delta \hat{U}_D(t_i) \geq 0 \\ &\Leftrightarrow U_{\hat{D}}^{\hat{G}}(D^*, \hat{A}) - U_{\hat{D}}^{\hat{G}}(D', \hat{A}) \geq 0 \end{aligned}$$

△

Теорема 1: Контрольна підгрупа з кібербезпекою з нульовою сумою $G_{j\lambda}$ допускає рівновагу Неша у змішаних стратегіях $(Q_{j\lambda}^*, H_{j\lambda}^*)$, з властивістю, що

$$Q_{j\lambda}^* = \arg \max_{Q_{j\lambda}} \min_{H_{j\lambda}} U_D(Q_{j\lambda}, H_{j\lambda})$$

і також $H_{j\lambda}^* = \arg \max_{H_{j\lambda}} \min_{Q_{j\lambda}} U_A(Q_{j\lambda}, H_{j\lambda})$

Теорема мінімаксу стверджує, що для ігор з нульовою сумою рівноваги Неша та $\min \max$ рішення розбігаються. Тому план кібербезпеки $G_{j\lambda}$ Неша мінімізує виграш учасника. Якщо якийсь $G_{j\lambda}$ приймає кілька планів кібербезпеки Неша, то вони мають упорядковану властивість взаємозамінності, що означає, що гравці досягають того самого рівня оборони, незалежного від стратегії, тобто

$$Q_{j\lambda}^* = \arg \max_{Q_{j\lambda}} \min_{H_{j\lambda}} U_A(Q_{j\lambda}, H_{j\lambda})$$

6 Формулювання задач і розв'язання

Маємо сценарій, де зловмисник не знає як захисник збирається захищатися. Відповідно і навпаки: захисник не знає, куди буде атакувати зловмисник. Ми маємо гру, де гравці не мають достатньо інформації один про одного.

6.1 Задача вартості стратегії

Задача 1. Маємо гру G . Зображення стратегії гравців у таблиці. Припустимо вони мають однакову вартість розгортання стратегії.

	c_{di}
d_0	0
d_1	100
d_2	200

Зображення для гравця, який захищає.

	c_{ai}
a_0	0
a_1	100
a_2	200

Зображення для гравця, який атакує.

	d_0	d_1	d_2
a_0	0,0	$c_{d1}, -c_{d1}$	$c_{d2}, -c_{d2}$
a_1	$c_{a1}, -c_{a1}$	$c_{d1} - c_{a1}, c_{a1} - c_{d1}$	$c_{d2} - c_{a1}, c_{a1} - c_{d2}$
a_2	$c_{a2}, -c_{a2}$	$c_{d1} - c_{a2}, c_{a2} - c_{d1}$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

Таблиця 1. Стратегічна форма для гри Атаки і Захисту.

На основі таблиці 1, маємо розв'язок:

	d_0	d_1	d_2
a_0	0,0	100, -100	200, -200
a_1	100, -100	0, 0	100, -100
a_2	200, -200	-100, 100	0, 0

Таблиця 2. Стратегічна форма для гри Атаки і Захисту.

Отже, рівновага Неша буде така: (a_2, d_1) .

Задача 2. Для гри G . Маємо зображення форми у таблиці. Припустимо вони мають однакову вартість розгортання стратегії. Тепер розглядаючи припущення моделі u -функція виграшу загальна для всіх. $u = 10000$

	c_{di}		c_{ai}
d_0	0	a_0	0
d_1	4000	a_1	4500
d_2	6000	a_2	5500

Стратегії двох гравців.

На основі таблиці 1, Стратегічна форма для гри Атака і Захист. маємо:

	d_0	d_1	d_2
a_0	0,0	$c_{d1}, -c_{d1}$	$c_{d2}, -c_{d2}$
a_1	$u - c_{a1}, c_{a1} - u$	$c_{d1} - c_{a1}, c_{a1} - c_{d1}$	$c_{d2} - c_{a1}, c_{a1} - c_{d2}$
a_2	$u - c_{a2}, c_{a2} - u$	$u + c_{d1} - c_{a2}, c_{a2} - c_{d1} - u$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

Наш розв'язок:

	d_0	d_1	d_2
a_0	0,0	4000, -4000	6000, -6000
a_1	5500, -5500	-500, 500	1500, -1500
a_2	4500, -4500	8500, -8500	500, -500

Розглянувши тепер функцію виграшу, будемо мати інший вигляд розв'язку.

Рівновага Неша буде: (a_2, d_2) .

6.2 Задача: два рівня інтенсивності

Гра G . Припустимо вони мають однакову вартість розгортання стратегії. Тепер розглядаючи припущення моделі u -функція виграшу для кожного гравця. $u = 10000$

	c_{di}		c_{ai}
d_0	0	a_0	0
d_2	6000	a_2	5500

Стратегія гравців

В основі задачі маємо те, що інший гравець або взагалі ніяк не реагує - $c_{a_0} = 0$ або реагує на високому рівні, тобто повна ліквідація учасника - $c_{a_i} = \max_i c_i$.

Гра в якій, гравці $n = \{1, 2\}$, захисник або зловмисник, отримують весь виграш або втрачають повністю все. Тобто нічого неможливо відновити.

Відповідно наша стратегія зміниться:

	d_0	d_2
a_0	0,0	$c_{d2}, -c_{d2}$
a_2	$u - c_{a2}, c_{a2} - u$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

Функція виграшу.

Провівши додаткові обчислення і врахувавши наведену вище формулу, маємо:

	d_0	d_2
a_0	0,0	6000, -6000
a_2	4500, -4500	500, -500

В даній задачі, ми не розглядаємо стратегії з низьким рівнем інтенсивності. Відповідно, це впливає на хід розв'язку і функція виграшу гравців буде залежати тільки від того як буде діяти супротивник. Ми маємо загальну функцію виграшу і від того віднімаємо вартість кожної стратегії. Відповідно, маємо те, що дійсно отримає гравець.

6.3 Задача: Припущення моделі

Маємо зображення форми у таблиці. Припустимо вони мають однакову вартість розгортання стратегії. Тепер розглядаючи припущення моделі, де u - функція виграшу для кожного гравця різна. $u_1 = 10000$, $u_2 = 20000$. Кожен гравець має різний виграш, якщо правильно обере стратегію, не знаючи при тому як діє інший гравець.

Стратегії ті ж самі, що у попередній задачі:

	c_{di}		c_{ai}
d_0	0	a_0	0
d_1	4000	a_1	4500
d_2	6000	a_2	5500

Стратегії двох гравців.

На основі таблиці 1, Стратегічна форма для двох гравців, маємо:

	d_0	d_1	d_2
a_0	0,0	$c_{d1}, -c_{d1}$	$c_{d2}, -c_{d2}$
a_1	$u_1 - c_{a1}, c_{a1} - u_1$	$c_{d1} - c_{a1}, c_{a1} - c_{d1}$	$c_{d2} - c_{a1}, c_{a1} - c_{d2}$
a_2	$u_2 - c_{a2}, c_{a2} - u_2$	$u_2 + c_{d1} - c_{a2}, c_{a2} - c_{d1} - u_2$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

На основі даних, отримаємо розв'язок:

	d_0	d_1	d_2
a_0	0,0	4000, -4000	6000, -6000
a_1	5500, -5500	-500, 500	1500, -1500
a_2	4500, -4500	18500, -18500	500, -500

6.4 Гра: Нападник з декількома стратегіями

Розглянемо іншу модель задачі. Тепер у нашій грі нападник має множину різних методів нападати на систему і інший гравець - захист "0", тобто відсутня відповідь на дії іншого гравця.

	0	1	2	3	4	5	6
0	0	10	10	10	20	20	20
1	10	0	20	20	20	10	20
2	10	20	0	20	10	20	20
3	10	20	20	0	20	20	10
4	20	20	10	20	0	10	10
5	20	10	20	20	10	0	10
6	20	20	20	10	10	10	0

Оптимальний хід такий: 0,3,4,6,6,1,3,0 із загальними витратами $c(N) = 80$. Якщо різні методи нападника утворюють коаліції S розміру $|S| = 4$ (де нападник має різні варіанти відвідування), то для коаліції $S \cup \{0\} = \{0, 1, 2, 4, 5\}$ оптимальний метод 0,2,4,5,1,0 з завданною шкодою $x_1 + x_2 + x_4 + x_5 \leq 50$, для іншої коаліції оптимальний метод - 0,2,4,6,3,0 з завданною шкодою $x_2 + x_4 + x_6 + x_3 \leq 50$ і метод - 0,3,6,5,1,0 з завданною шкодою $x_3 + x_6 + x_5 + x_1 \leq 50$.

Лінійна комбінація цих трьох нерівностей є:

$$x_1 + x_2 + x_4 + x_5 \leq 50 +$$

$$x_2 + x_4 + x_6 + x_3 \leq 50 +$$

$$x_3 + x_6 + x_5 + x_1 \leq 50 =$$

$$2x_1 + 2x_2 + 2x_3 + 2x_4 + 2x_5 + 2x_6 \leq 150.$$

Звідки матимемо $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \leq 75$, але відомо, що $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \geq 80$. Звідки випливає, що ядро такої гри порожня множина. Отже, на основі такого розподілу витрат $c(N) = 80$, легко бачити, що гравець отримає найбільший виграш.

6.5 Задача 1

Розглянемо тепер очікувані виграші гравців. u - функція виграшу і маємо $u_1 = 10000$, $u_2 = 20000$.

Стратегії тіж самі, що у попередній задачі:

	c_{di}		c_{ai}
d_0	0	a_0	0
d_1	4000	a_1	4500
d_2	6000	a_2	5500

Стратегії двох гравців.

На основі таблиці 1, Стратегічна форма для двох гравців, маємо:

	d_0	d_1	d_2
a_0	0,0	$c_{d1}, -c_{d1}$	$c_{d2}, -c_{d2}$
a_1	$u_1 - c_{a1}, c_{a1} - u_1$	$c_{d1} - c_{a1}, c_{a1} - c_{d1}$	$c_{d2} - c_{a1}, c_{a1} - c_{d2}$
a_2	$u_2 - c_{a2}, c_{a2} - u_2$	$u_2 + c_{d1} - c_{a2}, c_{a2} - c_{d1} - u_2$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

На основі даних, отримаємо розв'язок:

	d_0	d_1	d_2
a_0	0,0	4000, -4000	6000, -6000
a_1	5500, -5500	-500, 500	1500, -1500
a_2	4500, -4500	18500, -18500	500, -500

Отже, на основі визначенням **змішаної рівноваги Неша стратегії гри**, ми маємо, що опоненти ставляться байдуже до вибору своїх стратегій. Гравці лише зрівнюють очікувані виграші. У даній грі змішана стратегія робить кожного гравця байдужим серед усіх трьох своїх стратегій, коли очікувані утиліти від ігрових стратегій a_0 , a_1 та a_2 рівні для зловмисника, а очікувані утиліти від стратегій d_0 , d_1 , і d_2 рівні для захисника.

$$EU(p_{a_0}) = (p_{d_0})(0) + p_{d_1}(-c_{d_1}) + p_{d_2}(-c_{d_2}) \quad (20)$$

$$EU(p_{a_1}) = (p_{d_0})(0)(u_1 - c_{a_1}) + p_{d_1}(c_{d_1} - c_{a_1}) + p_{d_2}(-c_{d_2}) \quad (21)$$

$$EU(p_{a_2}) = (p_{d_0})(0)(u_2 - c_{a_2}) + p_{d_1}(u_2 + c_{d_2} - c_{a_2}) + p_{d_2}(c_{d_2} - c_{a_2}) \quad (22)$$

$$p_{a_0} = \frac{c_{a_1}}{u_1}, p_{a_1} = \frac{c_{a_2}}{u_2} - \frac{c_{a_1}}{u_1}, p_{a_2} = 1 - \frac{c_{a_2}}{u_2} \quad (23)$$

На основі наших даних отримаємо:

$$p_{a_0} = \frac{9}{20}, p_{a_1} = \frac{21}{40} - \frac{9}{20}, p_{a_2} = 1 - \frac{21}{40} = \frac{19}{40}$$

Подібним чином очікувана корисність захисника для відтворення стратегій d_0 , d_1 , і d_2 є функцією змішаної стратегії, ми маємо ймовірність розподіл p_{d_0} , p_{d_1} і p_{d_2} для захисника, наприклад:

$$p_{d_0} = 1 - \left(\frac{c_{d_2} - c_{d_1}}{u_2} + \frac{c_{d_1}}{u_1} \right), p_{d_1} = \frac{c_{d_1}}{u_1}, p_{d_2} = \frac{c_{d_2} - c_{d_1}}{u_2} \quad (24)$$

Отримаємо:

$$p_{d_0} = \frac{1}{2}, p_{d_1} = \frac{2}{5}, p_{d_2} = \frac{1}{10}$$

Отримали ймовірнісний розподіл для двох гравців.

Задача 2

Гра G . Припустимо вони мають однакову вартість розгортання стратегії. Тепер розглядаючи припущення моделі, де u - функція виграшу для кожного гравця різна. $u_1 = 10000$, $u_2 = 20000$.

	c_{di}		c_{ai}
d_0	0	a_0	0
d_2	6000	a_2	5500

Стратегія гравців

В основі задачі маємо те, що інший гравець або взагалі ніяк не реагує - $c_{a_0} = 0$ або реагує на високому рівні, тобто повна ліквідація учасника - $c_{a_i} = \max_i c_i$.

Гра в якій, гравці $n = \{1, 2\}$, захисник або зловмисник, отримують весь виграш або втрачають повністю все. Тобто нічого неможливо відновити.

Відповідно наша стратегія зміниться:

	d_0	d_2
a_0	0,0	$c_{d2}, -c_{d2}$
a_2	$u - c_{a2}, c_{a2} - u$	$c_{d2} - c_{a2}, c_{a2} - c_{d2}$

Функція виграшу.

Провівши додаткові обчислення і врахувавши наведену вище формулу, маємо:

	d_0	d_2
a_0	0,0	6000, -6000
a_2	4500, -4500	500, -500

В даній задачі, ми не розглядаємо стратегії з низьким рівнем інтенсивності. Відповідно, це впливає на хід розв'язку і функція виграшу гравців буде залежати тільки від того як буде діяти супротивник.

Тепер розглянемо випадок, коли дві стратегії a_1 та d_1 повністю виключені із простору стратегій. У цьому випадку кожен гравець рандомізує свій вибір двох стратегій на відповідність розподілу ймовірностей, і йому також буде байдуже щодо результатів гри.

$$p_{a_0} = \frac{29}{40}, p_{a_2} = \frac{11}{40} \quad (25)$$

$$p_{d_0} = \frac{3}{10}, p_{d_2} = \frac{7}{10} \quad (26)$$

На основі нашої задачі отримаємо іншу ймовірність двох гравців, врахувавши їх інтенсивність, ніж у попередній задачі.

7 Висновок

У цій роботі ми запропонували гру для захисту від нападу та оборони, яка не співпрацює, щоб моделювати безперервні та постійно розвиваються взаємодії та кібервійни між зловмисниками та захисниками. З ігрової моделі ми вивели змішану стратегію рівноваги Неша. Нарешті, ми продемонстрували ефективність запропонованої моделі у порівнянні з двома різними системами постійного захисту, як це було продемонстровано в наших експериментах.

Розглянули різні рівні інтенсивності та які при цьому можуть бути стратегії у гравців.

Отже, визначаючи різні стратегії гри ми можемо описати хід гри. В кожній грі ми можемо максимізувати наш виграш і при цьому мінізувати витрати.

8 Використана література

Література

- [1] Gaurdiola L. (2008) Production inventory games and PMS - games: characterizations of the Owen point/ L. Guardiola, A. Meca, J. Puerto// Mathematical social sciences. -Vol. 56.
- [2] Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, ShaoleiRen, Niki Pissinou, and Sundaraja Sitharama Iyengar. 2017. Game theory for cyber security and privacy. ACM Comput. Surv. 50, 2, Article 30 (May 2017), 37 pages
- [3] Козицький В.А. Математична теорія кооперативних ігор.-Львів: ЛНУ імені Івана Франка,2016.-490с.
- [4] Дослідження операцій. Частина 3. Ухвалення рішень і теорія ігор / М.Я. Бартіш, І.М. Дудзяний. - Львів : Видавничий центр ЛНУ імені Івана Франка, 2009. - 278с.
- [5] Опуклі структури, методи оптимізацій та їхнє застосування в економічному аналізі / В.А. Козицький. - Львів : Видавничий центр ЛНУ імені Івана Франка, 2008. - 450с.
- [6] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," Syst. Sci. (HICSS), 2010 43rd Hawaii Int. Conf., pp. 1–10, 2010.
- [7] А.А. Шиян. Теорія ігор: основи та застосування в економіці та менеджменті. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 164 с.
- [8] М.П. Моклячук, Р.Є. Ямненко. Теорія вибору та прийняття рішень. –Київ,2007. - 258с.
- [9] Теория игр и экономическое поведение. Дж. фон Нейман, О.Моргенштерн. Перев. с англ. под ред. и с доб. Н.Н. Воробьева. Главная редакция физико-математической литературы, изд-ва «Наука»,1970

- [10] Theory of Games and Economic Behavior / By John Von Neumann, and Oscar Morgenstern. - Princeton university press,1953.
- [11] Помаренко О.І., Перестюк М.О., Бурдим В.М. Основи математичної економіки. За редакцією О.І.Пономаренка. - К.:Інформтехніка,1995. - 320с.
- [12] C. F. Camerer, T. Ho, and J. K. Chong, “Behavioural Game Theory: Thinking, Learning and Teaching.”
- [13] Amadi Emmanuel Chukwudi, Eze Udoka, Ikerionwu Charles. Game Theory Basics and Its Application in Cyber Security. Advances in Wireless Communications and Networks. Vol. 3, No. 4, 2017, pp. 45-49.
- [14] Course “Game Theory” - coursera.org
- [15] K. Lye and J. Wing, “Game Strategies in Network Security,” Copenhagen, Denmark, 2002.