КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.168178
УДК 004.94:519.83

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
кандидат фізико-математичних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук, доцент
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Бойко Софія Валеріївна
магістр Факультету інформаційних технологій та математики
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-8586-5964
svboiko.fitm22@kubg.edu.ua

ТЕОРЕТИКО-ІГРОВИЙ ПІДХІД ДО МОДЕЛЮВАННЯ КОНФЛІКТІВ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Зростання кількості та складності кіберзагроз примушує вивчати не лише технічні аспекти кібербезпеки, але й соціальні та взаємодії між учасниками цифрового простору. Теоретико-ігровий підхід відкриває можливості для більш глибокого розуміння виникаючих конфліктів та розробки ефективних стратегій управління для забезпечення кібербезпеки. У цьому контексті, важливо досліджувати, як теорія ігор може бути застосована до аналізу конфліктів у кіберпросторі та які практичні висновки можна зробити для вдосконалення систем кібербезпеки в цілому, що й визначило актуальність і важливість даної роботи.

Спираючись на наукову літературу, було здійснено огляд різних підходів до застосування теорії ігор в системах інформаційної та кібернетичної безпеки. Виділені основні поняття концепції теорії ігор, такі як гравець, стратегія, виграш та втрата, що дозволяє структурувати та розуміти взаємодії в системах безпеки. Охарактеризовані найбільш поширені види ігор з точки зору управляння інформаційною безпекою: максимінна рівновага, рівновага Неша, Парето-оптимальні ситуації, рівновага Штакельберга. Розроблено формальний опис моделі гри в умовах конфлікту та механізм застосування теорії ігор до моделювання рішень у конфліктних ситуаціях в системах безпеки. Представлено предметну область гри конфліктної ситуації для кожного з рівнів «суб'єкт-суб'єкт»: рівень особистості (зловмисник – користувач); рівень бізнесу (внутрішній та/або зовнішній порушник — керівник компанії); рівень держави (порушники/хакери — державні установи, державні діячі); рівень міжнародних відносин (держави, група суб'єктів/хакерів — установи та/або політичні лідери іншої держави). Запропоновано конкретні сценарії управління конфліктними ситуаціями у системах безпеки за допомогою теоретико-ігрового підходу.

Результати дослідження можуть бути використані у практиці вирішення конфліктних ситуацій в організаціях, слугувати для розробки програмного забезпечення з цієї проблеми, а також в якості навчального матеріалу для студентів спеціальності 125 Кібербезпека та захист інформації.

Ключові слова: інформаційна безпека; інформаційні конфлікти; теоретико-ігровий підхід; гравець; максимінна рівновага; рівновага Штакельберга; сценарій управління конфліктною ситуацією.

ВСТУП

Постановка проблеми. Зважаючи на те, що загрози кібербезпеки стають все більш виразними та складними в сучасному цифровому середовищі, виникає необхідність розглядати питання управління конфліктами в рамках систем кібербезпеки. Теоретико-ігровий підхід є корисним інструментом для аналізу та моделювання таких ситуацій, що дозволяє контролювати та моделювати конфліктні взаємодії між різними сторонами в цифровому просторі.

Зростання кількості та складності кіберзагроз примушує вивчати не лише технічні аспекти кібербезпеки, але й соціальні та взаємодії між учасниками цифрового простору, що робить цю область дослідження важливою. Теоретико-ігровий підхід дозволяє краще зрозуміти виникнення конфліктів і створити ефективні стратегії управління для забезпечення кібербезпеки. У цьому контексті надзвичайно важливо дослідити, як теорія ігор може бути використана для аналізу конфліктів у кіберпросторі, а також які конкретні висновки можна зробити, щоб досягти більш ефективних систем управління в кібербезпеці в цілому.

Аналіз останніх досліджень і публікацій. Інтерес до ігрових підходів у процесі вирішення конфліктних ситуацій у кібернетичних системах на сучасному етапі зростає, зокрема, під впливом методологій забезпечення інформаційної безпеки як особистості, бізнесу, так і на державному рівні. З іншого боку, аналіз конфліктних сторін є можливим через привнесення в кібербезпеку наукових теорій математичних наук. Зростання кількості кіберзагроз та загальна складність кіберпростору зумовлюють потребу в ефективних засобах протистояння, а теорія ігор в цьому контексті визначається як потужний інструмент для моделювання, аналізу та управління кібербезпековими стратегіями [1, с. 657]. В оглядовій статті [2] з даної проблеми було проаналізовано 48 статей з 2017 по 2022 рік і визначено, що підходи теорії ігор оптимізовано для оборонної ефективності заходів безпеки та реалізовано для передбачення та підготовки до контрзаходів. Зрозуміло, що підступи порушників і їхня діяльність постійно розвиваються та змінюються. З цієї причини аналіз взаємодії зацікавлених сторін у інформаційному конфлікті за допомогою теоретико-ігрових підходів є важливим і актуальним. Саме це визначило мету цього дослідження.

Мета статті. Метою статті є висвітлення питань, що розширюють можливості в управлінні конфліктними ситуаціями в системах безпеки на основі теоретико-ігрового підходу.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Надто докладно зупинятися на математичних основах теорії ігор у даній статті не ставимо як задачу. Проте основні поняття цієї теорії варто розглянути для наступних питань дослідження. Основні концепції теорії ігор, такі як гравець, стратегія, виграш та втрата, надають можливість структурувати та розуміти взаємодії в системах безпеки.

Гра — опис стратегічної взаємодії між конфліктуючими або співпрацюючими сторонами, де враховуються обмеження та наслідки за різні дії.

Гравець — у системах безпеки це може бути країна, організація або навіть окрема особа.

ISSN 2663 - 4023

Стратегія — план дій гравця в умовах конфлікту.

Виграш та втрата — визначення того, що гравець отримує чи втрачає в результаті своїх стратегічних дій.

У результаті аналізу наукових досліджень [3] – [13] було встановлено кілька типів ігор, як показано на рис. 1, і найпоширеніші з них будуть розглянуті з метою впровадження їх у системи безпеки.

Рис. 1. Типи ігор

Максимінна рівновага (maximin equilibrium). Гравець вважає, що в грі реалізується найгірша для нього обстановка, і вибором своєї стратегії $y_i \in A_i$ він максимізує гарантоване значення цільової функції $U_i(y_i)$:

$$y_i = arg \max_{y_i \in A_i} \min_{y_{-i} \in A_{-i}} U_i(y_i, y_{-i}).$$

Інтерпретація: «Всі довкола мої вороги і всі вони прагнуть зробити мені якнайгірше (при цьому навіть не аналізуючи свої власні виграші), а я вибираю найкращий варіант».

В рамках предметної області «управління інформаційною безпекою» описує песимістичний сценарій [4].

Рівновага Неша (Nash equilibrium). Вектор y^N називається рівновагою Неша (точкою Неша) для даної гри, якщо виконана така нерівність:

$$\forall i \in I, \forall y_i: U_i(y_i^N, y_{-i}^N) \geq U_i(y_i^N, y_{-i}^N).$$

Іншими словами, жоден з гравців не має мотивації змінювати стратегію Неша, за умови, що інші гравці також віддаватимуть перевагу стратегії Неша.

В рамках предметної області «управління інформаційною безпекою» описує ситуацію, яку можна назвати оптимально прогнозованою: всі гравці самостійно і без примусу слідкують за тим, щоб виконувати відому діяльність [4].

Рівновага в домінантних стратегіях (dominant strategies equilibrium). Ситуація гри $y^d = \{y_1^d, \dots, y_n^d\}$ називається рівновагою в домінантних стратегія якщо:

$$\forall i \in I, \forall y_{-1} \in \forall y_{-1} \in A_1 \qquad f_1\left(y_1^d, y_{-1}\right) \geq f_1(y_1, y_{-1}).$$

Кожен елемент має домінантну стратегію, яка є абсолютно оптимальною, оскільки вона не залежить від стратегій, які обирають інші гравці.

Парето-оптимальні ситуації (Pareto optimal situations). Вектор усіх гравців y^n називається Парето-оптимальним, якшо не існує іншої ситуації гри, за якої всі гравці виграють не менше і хоча б один гравець виграє більше:

$$\forall y \in A \ \exists i \in I: \ U_i(y) < U_i(y^p).$$

Парето-оптимум розраховано на альтруїстичних гравців: ніхто з них не дозволить собі вибрати стратегію $y_i \neq y_i^p$ та виграти більше, якщо хоч один із інших гравців при цьому отримає менше.

В рамках предметної області «управління інформаційною безпекою» описує оптимістичний сценарій [4].

ISSN 2663 - 4023

Рівновага Штакельберга описується ситуацією (x_1, x_2), якщо

$$u_i(x_1, x_2) = \sup_{(y_1,y_2)\in R_j} u_i(y_1, y_2); \quad i, j = 1,2, \ i \neq j$$

В рамках предметної області «управління інформаційною безпекою» описує сценарій, коли один із гравців є лідер і починає гру першим, тому пропонуємо його для прогнозування у сфері безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Формальний опис моделі гри в умовах конфлікту

Для нашого дослідження теорія ігор — це теорія математичних моделей для оптимального прийняття рішень у інформаційних конфліктах, особливо на рівні «суб'єкт-суб'єкт» — згідно з результатами дослідження [3], [4], [7].

Модель конфлікту «суб'єкт-суб'єкт» — гра, у якій гравці є сторонами конфлікту. Хід гравця — це один крок з передбачених правил дій, зокрема, які можуть бути особистими чи випадковими. Кожен гравець має власну стратегію гри, яка складається з набору правил, на основі яких він приймає рішення на кожному кроці гри. Таким чином, для кожної моделі конфліктної ситуації мають бути такі елементи, як гравці, стратегія, яку використовують гравці, і їхні інтереси.

Позначимо множину гравців $G = \{g_1, g_2, \dots, g_k\}$. Кожний гравець з множини G має набір стратегій, які позначимо як $S = \{S_1, S_2, \dots, S_k\}$. Цей набір також називається набором профілів дій гравців. У процесі гри кожен гравець зі свого профілю дій обирає якійсь один: $s_1 \in S_1$, $s_2 \in S_2$, …, $s_k \in S_k$. В результаті будемо мати ігрову ситуацію виду $(s_1, s_2, \dots, s_k)$, яку назвемо результатом гри і яка є елементом декартового добутку $F = S_1 \times S_2 \times \dots \times S_k$ множин $S_1, S_2, \dots, S_k$. Є очевидним, що будь-який гравець є зацікавленим у виграші в кожній конфліктній ситуації. Введемо числову функцію $U(S): F \to R$, яка буде представляти виграш у кожній конкретній ігровій ситуації s. Тоді для кожного гравця маємо набір виграшу в ситуації s: $U^1(s), U^2(s), \dots, U^k(s)$. Таким чином, конфліктну ситуацію у теоретико-ігровому підході можна задати у вигляді кортежу

$$K = \langle G, \{S_1, S_2, \dots, S_k\}, \{U^1, U^2, \dots, U^k\}\rangle \quad (1)$$

Вираз (1) називається нормальною формою гри.

Процес моделювання сценаріїв для конфліктних ситуацій

У дослідженні розглянемо теорію конфліктології в контексті інформаційної безпеки з точки зору «суб'єкт-суб'єкт» [14], [15].

1. Рівень особистості (зловмисник — користувач);
2. Рівень бізнесу (внутрішній та/або зовнішній порушник — керівник компанії);
3. Рівень держави (порушники/хакери — державні установи, державні діячі);
4. Рівень міжнародних відносин (держави, група суб'єктів/хакерів — установи та/або політичні лідери іншої держави).

Процес моделювання сценаріїв для конфліктних ситуацій рівня «суб'єкт-суб'єкт» на основі теоретико-ігрового підходу поділяється на основні етапи:

1 етап. Визначення предметної області конфлікту. Для цього необхідно визначити тип системи, гравців, інформативність, функцію корисності для кожного гравця та правила гри.

2 етап. Побудова алгоритму взаємодії гравців у конфліктній ситуації на основі стратегії, вибраної на першому етапі.

3 етап. Розгляд всіх рішень, отриманих в результаті гри, і визначення, як їх можна використовувати в системах інформаційної та кібернетичної безпеки.

Рис. 2 показує, як теорія ігор може бути використана для моделювання рішень у конфліктних ситуаціях у системах безпеки.

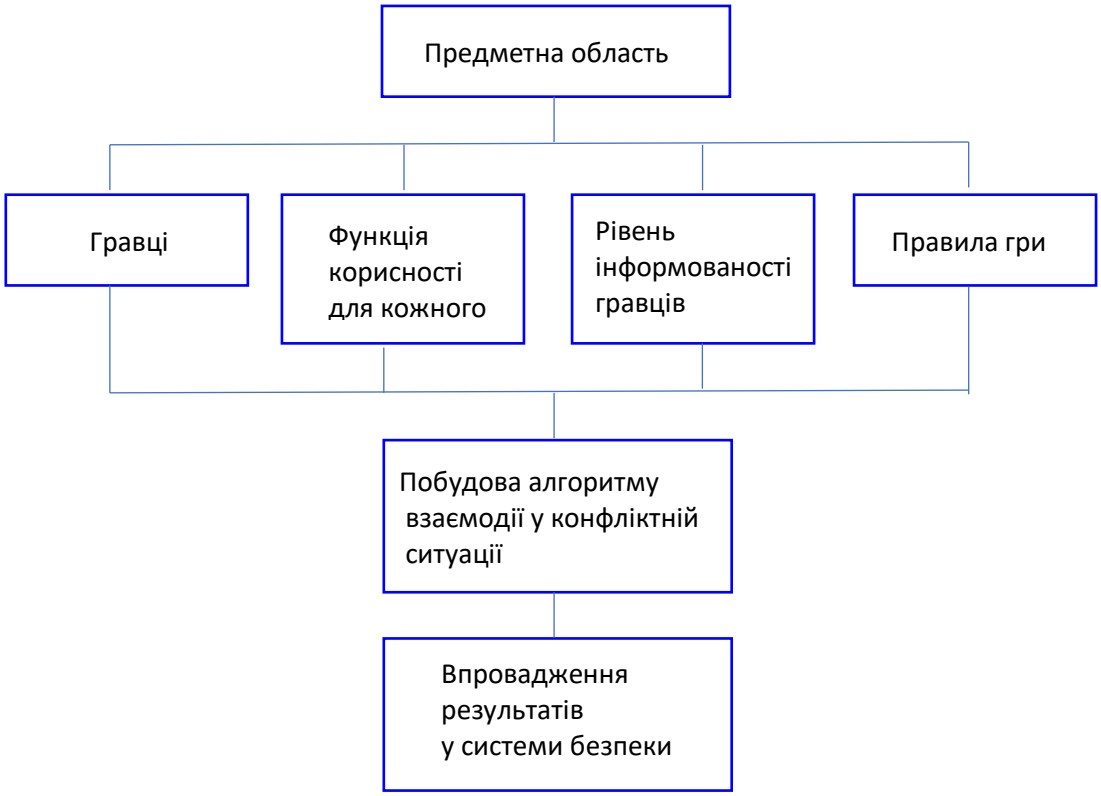

Рис. 2. Механізм застосування теорії ігор до моделювання рішень у конфліктних ситуаціях в системах безпеки

Надалі представимо характеристику конфліктної ситуації для кожного з рівнів «суб'єкт-суб'єкт» та предметну область гри на даних рівнях (таблиця 1).

Таблиця 1

Предметна область гри на рівнях «суб'єкт-суб'єкт»

	Рівні	**Гравець А**	**Гравець В**	**Інформативність**	**Вид гри**
1	Рівень особистості	Зловмисник — хакер	Користувач	Повна: користувач виявив вторгнення та будує свою стратегію захисту	Неколективна гра; матрична гра двох учасників: рівновага Штакельберга
2	Рівень бізнесу	Внутрішній порушник (інсайдер)	Керівник компанії або адміністратор	Повна: керівник компанії здійснює інвестиції у впровадження елементів «нульової довіри», внутрішній порушник виявляє уразливості інформаційної системи для своїх цілей	Неколективна гра; матрична гра двох учасників з нульовою сумою: рівновага максиміна

3	Рівень держави	Зловмисник — хакер (група хакерів)	Державні установи	Неповна	Неколективна гра (вважатимемо одну особу, організацію чи державу одним гравцем); стохастична гра з нульовою або ненульовою сумою; динамічна гра з неповною та досконалою інформацією
4	Міжнародний рівень	Група хакерів однієї держави	Установи іншої держави		

Після аналізу перейдемо до моделювання ситуацій конфлікту, що були описані вище.

Розробка сценаріїв

Конфліктна ситуація «суб'єкт-суб'єкт» на рівні особистості: зловмисник — користувач

У системах безпеки найчастіше виділяється ситуація, коли один гравець, у цьому випадку зловмисник, має домінантну позицію. Це означає, що він виступає першим (а не одночасно, як у теорії ігор). Після вибору першого гравця звичайний користувач вибере свою стратегію. У цьому випадку можна використовувати рівновагу Штакельберга, де зловмисник буде виконувати функцію «лідера» або першого гравця. Правило гри таке:

1) зловмисник знає усі виграші, тому вибирає той, що є максимальним для користувача;
2) користувач лише після цього вибирає теж для себе найбільш вигідний виграш, але із залишених після зловмисника;
3) надалі зловмисник дії циклічно, вибираючи ту ж стратегію, що описана у 1);
4) створюється множина виграшів для зловмисника, вибирається з них найвигідніший, що й буде рішенням за Штакельбергом.

Приклад. Позначимо зловмисника як гравця A, а звичайного користувача як гравця B. Зловмисник A знає уразливості інформаційної системи користувача B і починає гру. Нехай числові результати представлені у таблиці 2.

Таблиця 2

Результат гри

	b_1	b_2	b_3
a_1	(2,3)	(–1,–3)	(3,2)
a_2	(–4,–1)	(0,–2)	(–2,–1)
a_3	(4,–4)	(1,–4)	(–3,1)

Зловмисник A починає першим і вибирає першу стратегію (a_1, b_1), що є максимальним виграшом для користувача B. Аналогічно, друга стратегія гравця A – це (a_2, b_1) або (a_2, b_3), третя – (a_3, b_3). Тобто множиною виграшів є {(2,3), (–4,–1), (–2,–1), (–3,1)}. Найбільший з них є (2,3), тому зловмисник A вибере стратегію (a_1, b_1) і матиме виграш (2,3).

ISSN 2663 - 4023

Конфліктна ситуація «суб'єкт-суб'єкт» на рівні особистості: внутрішній порушник — керівник компанії

Змоделюємо сценарій антагоністичної гри $G = \{A, B\}$, яка є актуальною для інформаційних систем, де кожний з гравців вибором своєї стратегії прагне зробити найбільшим свій виграш. Для гравця A виграш буде $U(a, b)$, а для гравця B — $(-U(a, b))$, оскільки вони мають протилежні цілі, як в конфліктній ситуації *«внутрішній порушник — керівник компанії».* Виграш кожного гравця визначений на ситуаціях $(a, b) \in A \times B$ і залежить не тільки від особистого вибору, але й від стратегії супротивника. Розберемо цей випадок, який у спеціальній літературі має назву «гра полковника Блотто» [16] на прикладі.

Приклад. Нехай керівник компанії має m способів захисту двох уразливостей, а внутрішній порушник — n можливостей використати ці уразливості, і нехай $m > n$. У керівника компанії є наступні стратегії:

$a_0 = (m, 0)$ — захистити лише першу уразливість усіма m способами;

$a_1 = (m-1, 1)$ — захистити першу уразливість $m-1$ способом, а другу — одним способом;

……

$a_m = (0, m)$ — захистити лише другу уразливість усіма m способами.

У внутрішнього порушника є наступні стратегії:

$b_0 = (n, 0)$ — використати лише першу уразливість усіма n способами;

$b_1 = (n-1, 1)$ — використати першу уразливість $n-1$ способом, а другу — одним способом;

……

$b_n = (0, n)$ — використати лише другу уразливість усіма n способами.

Виграші $U_{ij}, i = 1, \ldots, m,\ j = 1, \ldots, n$ обчислюються наступним чином:

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

При $m = 4, n = 3$ будемо мати:

$$U = \begin{array}{c} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{array} \begin{array}{c} \begin{array}{cccc} b_0 & b_1 & b_2 & b_3 \end{array} \\ \left(\begin{array}{cccc} 4 & 2 & 1 & 0 \\ 1 & 3 & 0 & -1 \\ -2 & 2 & 2 & -2 \\ -1 & 0 & 3 & 1 \\ 0 & 1 & 2 & 4 \end{array} \right) \end{array} \left| \begin{array}{c} \min\limits_j U_{ij} \\ 0 \\ -1 \\ -2 \\ -1 \\ 0 \end{array} \right.$$

У цьому випадку можливо застосувати максимінний критерій:

$$\max_i \left(\min_j U_{ij} \right) = 0,$$

отже, оптимальна стратегія керівника компанії визначається ситуаціями (a_0, b_3), (a_4, b_0), тобто вибором стратегії захистити одну з уразливостей усіма доступними способами.

Огляд можливих сценаріїв на рівнях «група хакерів — державні установи» і «група хакерів однієї держави — установи іншої держави»

Для зручності будемо вважати, що організація чи група осіб є одним гравцем. Тому моделюємо неколективну гру, яка найчастіше є динамічною, проте її переріз (здійснення одного ходу) є статичною моделлю. Можливо введення поняття ймовірності при виборі стратегії кожним гравцем і тоді модель буде стохастичною грою. Як правило, це гра з неповною інформацією.

У нашому дослідженні будемо використовувати результати наукових робіт [6], [17], [18] на основі диференціальних ігор. Припустимо, що в мережі N користувачів, кожен з яких передає дані зі швидкістю $x(t)$. Здійснимо переріз даного процесу та обчислимо навантаження на сервісний елемент $\sum_{i=1}^{N} x\,(t)$.

Позначимо $M = \{1,2,\dots,m\}$ — індекси вузлів мережі;

$u_i(t)$ — швидкість обслуговування;

$A = \{a_{ij}\}$ — матриця з елементами

$$a_{ij} = \begin{cases} 1, & \text{якщо } j \text{ надсилає запит на вхід сервера;} \\ 0, & \text{у протилежному випадку.} \end{cases}$$

$R = \{r_{ij}\}$ — матриця маршрутизації з елементами

$$r_{ij} = \begin{cases} 1, & \text{якщо вихід } i-\text{го сервісного елемента є входом } j\,; \\ 0, & \text{у протилежному випадку.} \end{cases}$$

$B = M - R^T$.

Тоді процес взаємодії користувачів у мережі можна описати системою диференціальних рівнянь

$$y'(t) = A\bar{x} - B\bar{u}.$$

Тип рівноваги залежить від параметрів, що характеризують протоколи та поведінку користувача.

Деякі автори [19], [20] пропонують візуально представляти динаміку таких ігор за допомогою дерева рішень або когнітивних карт, використовуючи теоретико-ймовірнісний підхід.

Дослідження сценаріїв розв’язання конфліктної ситуації «суб’єкт-суб’єкт» у системах безпеки за допомогою теорії ігор виявилося важливим кроком у напрямку розуміння та управління конфліктами у цьому контексті.

За останні роки наукова спільнота у сфері захисту інформації приділяє достатню увагу щодо застосування теоретико-ігрового підходу до проблем інформаційної та кібернетичної безпеки. Моделі та ідеї даної теорії надають нові можливості в управлінні інформаційною безпекою, проте внаслідок складності цих методів реалізація на практиці дещо уповільнюється.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Протягом останніх років вчені, що спеціалізуються в галузі інформаційного захисту, активно вивчають можливості теоретико-ігрового підходу для вирішення проблем інформаційної та кібернетичної безпеки. Моделі та ідеї даної теорії надають нові можливості в управлінні інформаційною безпекою, проте внаслідок складності цих методів реалізація на практиці дещо уповільнюється. У межах подальших досліджень планується порівняти різні математичні методи для вирішення конфліктних ситуацій у системах безпеки та визначити їх ефективність

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cavusoglu, H., & Zhang, J. (2008). Security Patch Management: Share the Burden or Share the Damage? *Management Science, 54(4),* 657–670.
2. Khalid, M., Al-Kadhimi, A., Singh, M. (2023). Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): *A Systematic Review Mathematics, 11, 1353*. https://doi.org/10.3390/math11061353
3. Шиян, А. (2009) Теоретико-ігровий аналіз раціональної поведінки людини та прийняття рішень в управлінні соціально-економічними системами. *УНІВЕРСУМ-Вінниця*.
4. Бурячок, В., & Шиян, А. (2014). Класифікація технологій для здійснення інформаційно-психологічного впливу на процес раціональної діяльності людини. *Сучасний захист інформації*, *1*, 64–70.
5. Коломієць, Г. (2020). Застосування теорії ігор в оподаткуванні як сфері узгодження суспільних і приватних інтересів. *Вісник Хмельницького національного університету*, 4(3), 202–205.
6. Ігнатенко, О. (2017). Теоретико-ігровий підхід до проблеми безпеки мереж. *Проблеми програмування, 3*, 149–160.
7. Roy, S., et al. (2010). A Survey of Game Theory as Applied to Network Security, *Proc. 43rd Hawaii International Conf. on Systems Sciences*, 880–889.
8. Anwar, F., et al (2020). A Comprehensive Insight into Game Theory in relevance to Cyber Security. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI*), 8, 189-203. https://doi.org/10.11591/ijeei.v8i1.1810
9. Ho E., et al. (2022). Game Theory in Defence Applications: A Review. *Sensors, 22(3):1032*. https://doi.org/10.3390/s22031032
10. Yevseiev, S., et al. (2020). Development and analysis of game-theoretical models of security systems agents interaction. *Eastern-European Journal of Enterprise Technologies, 2,* 15-29. https://doi.org/10.15587/1729-4061.2020.201418
11. D. Bauso. (2014). Game Theory: Models, Numerical Methods and Applications. *Foundations and Trends in Systems and Control, 1(4),* 379–522.
12. Казімко, В. (2022). Застосування теорії ігор для моделювання інформаційних проблем безпеки. *Телекомунікаційні та інформаційні технології, 1(74).* https://doi.org/10.31673/2412-4338.2022.011524
13. Akinwumi D., et al. (2017). A review of game theory approach to cyber security risk management. *Nigerian Journal of Technology, 36(4).* https://doi.org/10.4314/njt.v36i4.38
14. Шевченко, С., Складанний, П., Негоденко, О., & Негоденко, В. (2022). Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка*, *2(18)*, 150–162, https://doi.org/10.28925/2663-4023.2022.18.150162
15. Shevchenko S., et al. (2023). Conflict Analysis in the Information Security System: Subjct – Subject. *CEUR Workshop Proceedings.*, 3421, 56-66. https://ceur-ws.org/Vol-3421/paper6.pdf
16. Borel, E. (1921). La théorie du jeu les équations intégrales á noyau symétrique. *Comptes Rendus de l'Académie, 173,* 1304–1308.
17. Mi, Y., et al. (2021). Optimal Network Defense Strategy Selection Method: A Stochastic Differential Game Model. *Security and Communication Networks*, 2021, 1–16. https://doi.org/10.1155/2021/5594697
18. Huang, S., et al. (2018). Markov differential game for network defense decision-making method. *IEEE Access*, *6*, 39621–39634. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8387766
19. Kumar, R. et al. (2018). Effective Analysis of Attack Trees: A Model-Driven Approach. *Fundamental Approaches to Software Engineering. Lecture Notes in Computer Science, 10802.* https://doi.org/10.1007/978-3-319-89363-1_4
20. Nguyen T., et al. (2018). Multistage Attack Graph Security Games: Heuristic Strategies, with Empirical Game-Theoretic Analysis. *Security and Communication Networks, 2018*. https://doi.org/10.1155/2018/2864873

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Svitlana Shevchenko
PhD, associate professor
associate professor of the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Yuliia Zhdanova
PhD, associate professor
associate professor of the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Pavlo Skladannyi
PhD
Head of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Sofia Boiko
Master of the Faculty of Information Technology and Management
Borys Grinchenko Kyiv University, Kyiv, Ukraine
svboiko.fitm22@kubg.edu.ua

GAME THEORETICAL APPROACH TO THE MODELING OF CONFLICTS IN INFORMATION SECURITY SYSTEMS

Abstract. The increase in the number and complexity of cyber threats forces us to study not only the technical aspects of cyber security, but also the social and interaction between participants in the digital space. The game-theoretic approach opens up opportunities for a deeper understanding of emerging conflicts and the development of effective management strategies to ensure cyber security. In this context, it is important to investigate how game theory can be applied to the analysis of conflicts in cyberspace and what practical conclusions can be drawn for the improvement of cyber security systems as a whole, which determined the relevance and importance of this work.
Based on the scientific literature, a review of various approaches to the application of game theory in information and cyber security systems was carried out. The main concepts of the concept of game theory are highlighted, such as player, strategy, winning and losing, which allows to structure and understand interactions in security systems. The most common types of games from the point of view of information security management are characterized: maximin equilibrium, Nash equilibrium, Pareto-optimal situations, Stackelberg equilibrium. A formal description of the game model in conflict conditions and a mechanism for applying game theory to modeling decisions in conflict situations in security systems have been developed. The subject area of the game of the conflict situation is presented for each of the "subject-subject" levels: the level of the individual (criminal — user); business level (internal and/or external violator — company manager); state level (violators/hackers — state institutions, state officials); the level of international relations (states, a group of subjects/hackers — institutions and/or political leaders of another state). Specific scenarios for managing conflict situations in security systems using a game-theoretic approach are proposed.
The results of the research can be used in the practice of solving conflict situations in organizations, serve for the development of software on this problem, and also as educational material for students of the specialty 125 Cybersecurity and information protection.

Keywords: informational security; information conflicts; game-theoretic approach; player; maximin balance; Stackelberg balance; conflict management scenario.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Cavusoglu, H., & Zhang, J. (2008). Security Patch Management: Share the Burden or Share the Damage? *Management Science, 54(4),* 657–670.
2. Khalid, M., Al-Kadhimi, A., Singh, M. (2023). Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): *A Systematic Review Mathematics, 11, 1353*. https://doi.org/10.3390/math11061353
3. Shiyan, A. (2009) Game-theoretic analysis of rational human behavior and decision-making in the management of socio-economic systems. *UNIVERSUM-Vinnytsia.*
4. Buryachok, V., & Shiyan, A. (2014). Classification of technologies for informational and psychological influence on the process of rational human activity. *Modern information protection, 1*, 64–70.
5. Kolomiets, G. (2020). Application of game theory in taxation as a sphere of reconciliation of public and private interests. *Bulletin of the Khmelnytskyi National University*, 4(3), 202–205.
6. Ignatenko, O. (2017). Game-theoretic approach to the problem of network security. *Programming problems, 3*, 149–160.
7. Roy, S., et al. (2010). A Survey of Game Theory as Applied to Network Security, *Proc. 43rd Hawaii International Conf. on Systems Sciences*, 880–889.
8. Anwar, F., et al (2020). A Comprehensive Insight into Game Theory in relevance to Cyber Security. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI*), 8, 189-203. https://doi.org/10.11591/ijeei.v8i1.1810
9. Ho E., et al. (2022). Game Theory in Defence Applications: A Review. *Sensors, 22(3):1032.* https://doi.org/10.3390/s22031032
10. Yevseiev, S., et al. (2020). Development and analysis of game-theoretical models of security systems agents interaction. *Eastern-European Journal of Enterprise Technologies, 2,* 15-29. https://doi.org/10.15587/1729-4061.2020.201418
11. D. Bauso. (2014). Game Theory: Models, Numerical Methods and Applications. *Foundations and Trends in Systems and Control, 1(4),* 379–522.
12. Kazimko, V. (2022). Application of game theory for modeling information security problems. *Telecommunications and information technologies, 1(74).* https://doi.org/10.31673/2412-4338.2022.011524
13. Akinwumi D., et al. (2017). A review of game theory approach to cyber security risk management. *Nigerian Journal of Technology, 36(4).* https://doi.org/10.4314/njt.v36i4.38
14. Shevchenko, S., Skladanniy, P., Negodenko, O., & Negodenko, V. (2022). Study of applied aspects of conflict theory in security systems. *Cybersecurity: education, science, technology*, *2(18),* 150–162, https://doi.org/10.28925/2663-4023.2022.18.150162
15. Shevchenko S., et al. (2023). Conflict Analysis in the Information Security System: Subjct – Subject. *CEUR Workshop Proceedings.*, 3421, 56-66. https://ceur-ws.org/Vol-3421/paper6.pdf
16. Borel, E. (1921). La théorie du jeu les équations intégrales á noyau symétrique. *Comptes Rendus de l'Académie, 173*, 1304–1308.
17. Mi, Y., et al. (2021). Optimal Network Defense Strategy Selection Method: A Stochastic Differential Game Model. *Security and Communication Networks*, 2021, 1–16. https://doi.org/10.1155/2021/5594697
18. Huang, S., et al. (2018). Markov differential game for network defense decision-making method. *IEEE Access, 6*, 39621–39634. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8387766
19. Kumar, R. et al. (2018). Effective Analysis of Attack Trees: A Model-Driven Approach. *Fundamental Approaches to Software Engineering. Lecture Notes in Computer Science, 10802.* https://doi.org/10.1007/978-3-319-89363-1_4
20. Nguyen T., et al. (2018). Multistage Attack Graph Security Games: Heuristic Strategies, with Empirical Game-Theoretic Analysis. *Security and Communication Networks, 2018*. https://doi.org/10.1155/2018/2864873