УДК 004.056.5 DOI: 10.31673/2412-4338.2022.011524

Казімко В.В. *Національний авіаційний університет, Київ*

ЗАСТОСУВАННЯ ТЕОРІЇ ІГОР ДЛЯ МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ ПРОБЛЕМ БЕЗПЕКИ

Анотація. *Відбувається безперервний розвиток інформаційних технологій з точки зору різноманітності та рівня їх складності, що супроводжується збільшенням вимог щодо захисту інформації. З розвитком наукового прогресу, зловмисники також вдосконалюють свої вміння і знання завдаючи більшої шкоди. Постійний зв'язок та збільшення доступності обчислювальних ресурсів для зловмисників допомагають їм виконувати складні та розподілені атаки у будь-який момент часу. Від початку існування мережі Інтернет дослідники вивчають проблему кібербезпеки. Проте проблема ще далеко не повністю вирішена. Останнім часом концепції теорії ігор були застосовані до всіх рівнів безпеки, включаючи кіберпростір, які часто називають іграми безпеки. Ігри передбачають дії двох або більше раціональних гравців, які мають певну стратегію і змагаються за певну винагороду. Теорія ігор забезпечує безпеку умовного депонування за допомогою кількісних заходів безпеки, а не якісних заходів, передбачених криптографічною безпекою. Крім того, теоретико-ігрові підходи можна поширити на розробку механізмів, які дозволяють розробникам систем змінювати баланс, а також передбачати результати на користь захисників, використовуючи складні ігрові конструкції.*

Були описані якісні способи перевершення традиційних підходів до кібербезпеки та конфіденційності методами теорії ігор. Крім того, у зв'язку з кібер-конфіденційністю, теорія ігор також знаходить застосування в обміні інформацією, анонімності, конфіденційності та криптографії.

У цій статті розглядаються дослідження теорії ігор та теорії диференційних ігор у мережевій безпеці на прикладному рівні. Було помічено, що більшість дослідницьких робіт із застосуванням концепцій теорії ігор не є специфічними для мережі через складність кіберпростору. Також ми представляємо найкращі методи дослідження, які можна використовувати для досягнення кращих результатів у захисті кіберпростору з використанням теорії ігор.

Ключові слова: *теорія ігри, проблеми інформаційної безпеки, ігри безпеки.*

Kazimko V.V. *National Aviation University, Kyiv*

APPLICATION OF GAME THEORY FOR MODELING INFORMATION SECURITY PROBLEMS

Abstract. *There is a continuous development of information technologies in terms of diversity and level of their complexity, which is accompanied by an increase in requirements for information protection. With the development of scientific progress, attackers also improve their skills and knowledge causing more damage. Constant communication and increased availability of computing resources for attackers help them to carry out complex and distributed attacks at any moment of time. Since the beginning of the Internet, researchers have been studying the problem of cyber security. However, the problem is far from completely solved. Recently, game theory concepts have been applied to all levels of security, including cyberspace, often referred to as security games. Games involve the actions of two or more rational players who have a certain strategy and compete for a certain reward. Game theory secures escrow using quantitative security measures rather than the qualitative measures provided by cryptographic security. In addition, game-theoretic approaches can be extended to design mechanisms that allow system designers to shift balances and predict outcomes in favor of defenders using complex play designs.*

Qualitative ways of overcoming traditional approaches to cyber security and privacy with game theory methods were described. In addition, in relation to cyber privacy, game theory has applications in information sharing, anonymity, privacy, and cryptography.

This article examines research on game theory and differential game theory in network security at the applied level. It has been observed that most research works applying game theory concepts are not network specific due to the complexity of cyberspace. So, we present the best research methods that can be used to achieve better results in the defense of cyberspace using game theory.

Keywords: *game theory, information security problems, security games.*

1. Вступ. Відбувається безперервний розвиток інформаційних технологій з точки зору різноманітності та рівня їх складності, що супроводжується збільшенням вимог щодо захисту інформації. З розвитком наукового прогресу, зловмисники також вдосконалюють свої вміння і знання завдаючи більшої шкоди. Невід'ємною частиною нашого повсякденного життя стало цілодобове підключення до мережі, тож захист конфіденційної інформації та активів є як ніколи важливим. Постійний зв'язок та збільшення доступності обчислювальних ресурсів для зловмисників допомагають їм виконувати складні та розподілені атаки у будь-який момент часу. Від початку існування мережі Інтернет дослідники вивчають проблему кібербезпеки. Проте проблема ще далеко не повністю вирішена.

Стандартна концепція безпеки піддавалась багатьом змінам перед тим, як визначились основні принципи, які ще називають тріадою КЦД — конфіденційність, цілісність, доступність. Криптографія є однією з міцних теоретичних основ безпеки, що залежить від секретності криптографічного ключа. Але при атаках соціальної інженерії чи розвиненій сталій загрозі, коли зловмисники викрадають повні криптографічні ключі, концепція конфіденційності ключів порушується, що призводить до проникнення у системи [1]. Потрібна нова теоретична основа та інноваційна перспектива, щоб охопити сценарії, за яких зловмисник може повністю скомпрометувати систему, а захисник може захистити її без основного припущення про секретність ключа. Взаємодію між захисними технологіями та атаками можна представити як гру між адміністратором системи та зловмисником. Щоб передбачити розвиток подій та наслідки того чи іншого результату таких ігор використовують математичні ігрові моделі.

Теорія ігор покликана допомогти нам зрозуміти ситуації, коли особи, які приймають рішення, впливають один на одного. Гра в повсякденному розумінні – це змагальна діяльність, в якій гравці прагнуть певного рівня переваги один над одним відповідно до набору правил або заздалегідь визначених дій [2]. Теорія ігор описує сценарії прийняття рішень кількома особами як ігри, де кожен гравець обирає дії, які призводять до найкращої винагороди для себе, передбачаючи раціональні дії інших гравців. Оскільки теорія ігор вирішує проблему конкуренції кількох гравців із протилежними цілями, вона може забезпечити математичну основу для моделювання та аналізу проблем безпеки.

2. Аналіз останніх досліджень та публікацій. Теорія ігор може надати кількісний показник якості безпеки, наданої концепцією рівноваги Неша, коли захисники, як і зловмисники, шукають оптимальну стратегію, і ніхто не має стимулу в односторонньому порядку відхилятися від своєї рівноважної стратегії, незалежно від їх цілі. Ця концепція рівноваги також кількісно визначає результати сценаріїв, охоплених ігровою моделлю. Таким чином, теорія ігор забезпечує безпеку умовного депонування за допомогою кількісних заходів безпеки, а не якісних заходів, передбачених криптографічною безпекою. Крім того, теоретико-ігрові підходи можна поширити на розробку механізмів, які дозволяють розробникам систем змінювати баланс, а також передбачати результати на користь захисників, використовуючи складні ігрові конструкції. Протягом більше десяти років інтерес до галузі теорії ігор і прийняття рішень зріс, і вона стала добре перевіреною, систематичною та міцною теоретичною основою для сучасних досліджень безпеки [1].

В останні роки теорія ігор використовувалася для вирішення багатьох проблем мереж зв'язку [3-6]. Її використовували для пропонування нових стратегій ціноутворення на Інтернет-послуги [7]. Багато інших питань, що стосуються бездротових мереж, були змодельовані та проаналізовані з використанням теорії ігор, наприклад, розподіл ресурсів [8], маршрутизація мережі [9], кешування мережі [10], безпека [1, 3, 6, 11 - 17] тощо. У сфері кібербезпеки нещодавні застосування теорії ігор до різноманітних тем, що розвиваються, включають безпеку критичної інфраструктури, управління кіберризиками, захист рухомих цілей, внутрішні загрози, міжрівневу кібербезпеку, конкурентне машинне навчання та кіберобман. Теоретико-ігровий метод може бути ефективно використаний для аналізу безпеки комп'ютерних мереж [17]. Взаємодія між зловмисником і адміністратором як стохастична гра двох гравців і побудова моделі для гри була запропонована Лаєм і його співавтором у своїй роботі під назвою «Стратегії гри в мережі» [17].

3. Мета роботи. Щоб показати, як теорію ігор можна використовувати для кібербезпеки та конфіденційності, ми вирішили вивчити три основні напрямки: кіберфізичну безпеку, безпеку зв'язку та конфіденційність. Ми представляємо ігрові моделі, особливості та рішення для окремих робіт, а також описуємо їх сильні сторони.

4. Основна частина.

4.1. Теорія ігор. Як ми згадували раніше, теорія ігор — це розділ прикладної математики, який допомагає гравцям аналізувати рішення в конфліктних ситуаціях. Це відбувається, коли в системі є два або більше гравців, які мають різні цілі або використовують однакові ресурси. У грі можуть бути як два гравці, так і кілька гравців. У конкретній грі теорія ігор забезпечує математичний процес для гравця, щоб вибрати найкращу відповідь проти свого опонента, який також має свою власну стратегію.

Гравець — це основна складова гри, що приймає рішення, а потім виконує дії.

Гра — це точний опис стратегічної взаємодії, що включає обмеження та виплати за дії, які гравці можуть зробити, але нічого не говорить про те, які дії вони насправді роблять.

Концепція — це систематичний опис того, як відбуватиметься гра з використанням найкращих можливих стратегій і якими можуть бути результати.

Стратегія гравця — це повний план дій для всіх можливих ситуацій під час гри. Стратегія називається чистою стратегією, якщо вона визначає виконання унікальних дій у ситуації. Якщо план визначає розподіл ймовірностей усіх можливих дій у ситуації, то стратегія називається змішаною [3].

Гра представлена в стратегічній формі, що описує дії гравців. Відповідно до [16] стратегічна форма гри оформлюється наступним чином:

$$Game = (P, (S_j)_{i\epsilon P}, (U_j)_{i\epsilon P}). \quad (1)$$

В грі беруть участь P гравців. Гравець обирає стратегію з S_j і отримує виграш з можливих u_j. Комбінація обраних стратегій гравця є концепцією стратегії, а змішана концепція формується з набору можливих стратегій. Функція виплати U_j – це відношення між простором усіх можливих концепції $S = \{S_j, j \epsilon P\}$ та вихідним простором дійсних чисел $\mathbb{R}$.

Дуже важливою концепцією в теорії ігор є рівновага Неша. У концепції рівноважної стратегії Неша немає гравця, що міг би збільшити свій прибуток за допомогою односторонньої зміни власної стратегії, коли дії інших гравців сталі. Розглянемо профіль гри для N гравців:

$$a_1, a_2 \dots a_N^*, \quad (2)$$

де a_N^* відповідає рівновазі Неша, при чому кожен i гравець отримує U_i виплату, тоді

$$U_i(a_i^*, a_{-i}^*) \geq U_i(a_i, a_{-i}^*) \quad (3)$$

має виконуватись для кожного i гравця та де a_i^* – це профіль дій гравця, а a_{-i}^* – рівновага дій інших гравців.

Проте рівновага Неша не завжди така ефективна, як може бути оптимум Паретто. Стратегія може досягти оптимальності Паретто, якщо в профілі будь-який гравець не може збільшити свою виплату, не зменшуючи виплату іншого гравця. Математичне визначення профілю стратегії Паретто є таким:

$$\begin{aligned} &\forall i \;\; U_i(\gamma) \geq U_i(\gamma^p), \\ &\exists i \;\; U_i(\gamma) > U_i(\gamma^p). \end{aligned} \quad (4)$$

Для кожної гри є дві важливі концепції. Це раціональність та обізнаність. Раціональність – це просто здатність послідовно приймати рішення не зважаючи на особисте ставлення до

гравців. Обізнаність складається зі знань про першочерговий результат та знань кожного гравця про результати[2].

Тактичний аналіз може використовувати теорію ігор для вивчення атак з кількох вузлів або з одного вузла. Тому теорія ігор важлива для вивчення сценаріїв стратегічних рішень захисників та аналізу мотивації нападників.

Розрізняють п’ять основних типів ігор [11]:

1) *Ідеальна інформаційна гра.* Гра, в якій кожен гравець знає про дії, які відбулися для всіх інших гравців. Прикладами ідеальних інформаційних ігор є: шахи, хрестики-нулики та го. Ігри, в яких хоча б один гравець не знає про дії хоча б одного гравця, що відбулися, називаються іграми з неповною інформацією.

2) *Байєсівська гра*. Гра отримала свою назву через використання байєсівського аналізу для прогнозування результатів. В таких іграх інформація про стратегії та виплати інших гравців неповна, і на початку гри гравці призначають "типи" іншим гравцям.

3) *Статичні/Стратегічні ігри.* Одноразова гра, де кожен гравець обирає свій план дій, а всі гравці приймають рішення одночасно. Це означає, що при виборі плану дій кожен гравець не інформується про план дій, обраний іншими гравцями.

4) *Динамічні/розширені ігри.* Ігри з кількома етапами, де гравці можуть розглядати свої дії на кожному етапі. Його можна розглядати як послідовну структуру проблем прийняття рішень, з якими стикаються гравці в статичній грі. Ігрові послідовності можуть бути як скінченними, так і нескінченними.

5) *Стохастична гра.* Гра, що включає ймовірність переходів через кілька станів системи. Гра розвивається як послідовність станів. Гра починається з початкового стану; гравець вибирає дію та отримує виплату, яка залежить від поточного стану гри, потім гра переходить у новий стан з ймовірністю, що залежить від дій гравців та поточного стану.

Методи теорії ігор перевершують традиційні підходи до кібербезпеки та конфіденційності кількома способами, як описано нижче [16]:

1) Своєчасні дії: через відсутність стимулів для учасників традиційні рішення щодо безпеки приймаються досить повільно. Однак методи теорії ігор підтримують прихильників, використовуючи фундаментальні стимули для виділення обмежених ресурсів для збалансування усвідомленого ризику.

2) Перевірена математика: більшість традиційних методів безпеки, реалізованих у реактивних пристроях, таких як антивірусні програми або профілактичні інструменти, такі як брандмауери, покладаються лише на евристики. Однак методи теорії ігор використовують перевірену математику для методичного аналізу рішень щодо безпеки.

3) Розподілене прийняття рішень. Прийняття рішень у звичайному прийнятті рішень щодо безпеки є централізованим, а не розподіленим (або індивідуалізованим) за своєю природою. Через відсутність координаторів в автономних системах централізований процес прийняття рішень майже неможливий в іграх з кібербезпекою. Тому рішення безпеки можуть бути реалізовані розподіленим способом, використовуючи теорію ігор.

4) Надійний захист: дослідники можуть сформулювати стратегії захисту для надійних і надійних систем безпеки мережі від атак (або егоїстичної поведінки) на основі результатів аналізу, наданих теорією ігор.

Таким чином, теорія ігор відіграє невід’ємну роль у набутті рівноважної стратегії для виживання від непередбачуваних перерв і атак через взаємодію між користувачами в кіберкомунікації.

Крім того, у зв’язку з кібер-конфіденційністю, теорія ігор також знаходить застосування в обміні інформацією, анонімності, конфіденційності та криптографії.

4.2. Теорія диференціальних ігор. Теорія диференціальних ігор вивчає конфліктні проблеми в системах управління, керованих кількома контролерами. Типовою диференціальною грою є так звана гра в переслідування-уникнення, в якій один гравець (переслідувач) намагається якомога швидше зловити свого супротивника (ухильника). Оскільки контролери часто мають різні цілі, це частина теорії ігор. Зокрема, вона стикається з тими ж проблемами: як

формалізувати те, що гравці грають одночасно і спостерігають один за одним, що таке «хороше» поняття рішення (цінність, баланс) тощо. Однак, оскільки система безперервно керується диференціальними рівняннями, вона також має багато спільного з теорією управління: зокрема, вона використовує ті ж математичні засоби, що й принципи динамічного програмування, рівняння Гамільтона-Якобі або системи явним обчисленням характеристик. Теорія диференціальних ігор виникла на початку 1960-х років за участю Айзекса, з одного боку, і Понтрягіна з іншого, які проаналізували перші приклади таких ігор безперервного часу [18].

Перші результати щодо диференціальних ігор з неповною інформацією сходять до [19] та [20], що стосуються стохастичних та детермінованих диференціальних ігор відповідно.

Диференціальні ігри з ідеальною інформацією

Почнемо з опису стандартного методу аналізу стохастичних диференціальних ігор з досконалою інформацією та спостереженням. Наступна техніка та результат сходяться до фундаментальної роботи Флемінга та Суганідіса [21]. Ми вивчаємо гру, в якій:

– кінцевий час $T > 0$ і початковий час $t_0 \in [0, T]$;
– початкове положення $x_0 \in \mathbb{R}^N$ та стохастична керована система

$$\begin{cases} dX_s = b(s, X_s, u_s, v_s)ds + \sigma(s, X_s, u_s, v_s)dB_s\,, \ s \in [t, T], \\ X_{t_0} = x_0\,, \end{cases} \tag{5}$$

де B – це d-вимірний стандартний Броунівського руху у заданому ймовірнісному просторі $(\Omega, \mathcal{F}, P)$, $b : [0,T] \times \mathbb{R}^N \times U \times V \to \mathbb{R}^N$ і $\sigma : [0, T] \times \mathbb{R}^N \times U \times V \to \mathbb{R}^N \times d$ є однорідними, обмеженими похідними, відображення U і V є компактними підмножинами деякого скінченного простору;

–пробіг і кінцевий виграш $\ell : [0, T] \times \mathbb{R}^N \to R$ і $g : \mathbb{R}^N \to \mathbb{R}$, також вважаються однорідними, обмеженим похідними.

Гравці керують системою за допомогою відповідних елементів керування (u_s) і (v_s), які є покроковими вимірюваними процесами зі значеннями U і V відповідно. Для подальшого використання завжди будемо позначати єдиний розв'язок (5) $X^{t_0,x_0;\,u,v}$. Виходячи з наведених вище припущень, він завжди існує.

На відміну від того, що відбувається в теорії контролю, тепер ми повинні описати, як гравець спостерігає за ситуацією та поведінкою суперника. Деякі люди використовують стратегії для опису цього спостереження. Однак, загального визначення стратегії, прийнятного для всіх, не існує: насправді кожна книга з теорії диференціальних ігор має власну концепцію стратегії, яка відповідає її конкретним проблемам. Причина в тому, що це важко формалізувати в безперервному часі та безперервному просторі спостереження, на яке можна негайно відреагувати.

Для цього нам потрібно ввести деякі символи. Нехай Ω — множина неперервних відображень від $[0, T]$ до $\mathbb{R}^d$, наділених $\mathcal{F}$, σ-алгеброю, породженою процесом координат, і P — мірою Вінера. Позначимо через B сталий процес $B_t(\omega) = \omega(t)$. Для фіксованого $t \in [0, T]$ введемо фільтрацію $\mathcal{F} = (\mathcal{F}_t, s = \sigma\{B_r - B_t, r \in [t, s]\}$, доповнену всіма нульовими множинами P і позначимо через Ω_t множину $\omega \in \Omega$ з $\omega(t) = 0$. Нехай U_t (відповідно V_t) позначає множину кадлаг-карт від [t, T] до U (відповідно V), тобто карт, які неперервні праворуч і мають ліву множини U_t, V_t і Ω_t нормовані, і через це мають борелівське σ-поле. Нам також знадобляться множини U(t) (відповідно V(t)) адаптованих кадлаг процеси зі значеннями в U (відповідно V) [18].

Фіксуємо початковий час $t_0 \in [0, T]$. Чистою стратегією для гравця I в момент часу t_0 є визначена по Борелю карта $\alpha : \Omega_{t_0} \times V_{t_0} \to U_{t_0}$, яка є непередбачуваною із затримкою, тобто існує розділ $t_0 < t_1 < \cdots < t_K = T$, такий, що для P будь-які $(\omega_1, \omega_2) \in \Omega_2$ і всі $(v_1, v_2) \in V_{t_0}^2$, якщо $(\omega_1, v_1) = (\omega_2, v_2)$ на $[t_0, t_i]$ для деякого $i \in \{0, \ldots, k-1\}$, то $\alpha(\omega_1, v_1) = \alpha(\omega_2, v_2)$ на $[t_0, t_{i+1}]$.

Чисті стратегії для гравця II визначаються аналогічним чином. Набір чистих стратегій для гравця I (відповідно гравця II) позначається $A(t_0)$ (відповідно $B(t_0)$).

Нехай $t_0 \in [0, T]$ — фіксований початковий час і $(\alpha, \beta) \in A(t_0) \times B(t_0)$ — пара стратегій.

Тоді існує єдина пара $(u, v) \in U(t_0) \times V(t_0)$ таких, що

$$\alpha(v) = u \text{ і } \beta(u) = v \quad \text{на } [t_0, T]. \tag{6}$$

Встановимо $X^{t_0,x_0,\alpha,\beta} := X^{t_0,x_0,u,v}$ і $(\alpha_s, \beta_s) := (u_s, v_s)$, де (u, v) визначається (6), і визначимо верхнє і нижнє значення функцій V^+ і V^- гри:

$$V^+(t,x) = \inf_{\alpha\in A(t)} \sup_{\beta\in B(t)} E\left[\int_t^T \ell\left(s, X_s^{t,x,\alpha,\beta}, \alpha_s, \beta_s\right)ds + g\left(X_T^{t,x,\alpha,\beta}\right)\right], \tag{7}$$

$$V^-(t,x) = \sup_{\beta\in B(t)} \inf_{\alpha\in A(t)} E\left[\int_t^T \ell\left(s, X_s^{t,x,\alpha,\beta}, \alpha_s, \beta_s\right)ds + g\left(X_T^{t,x,\alpha,\beta}\right)\right].$$

Очевидно, маємо, що $V^-(t, x) \le V^+(t, x)$. Основне завдання теорії диференціальних ігор полягає в тому, щоб довести, що насправді обидві функції збігаються (одна з них свідчить, що в грі функція має значення) і охарактеризувати цю функцію. Інший момент полягає в описі оптимальних стратегій. Щоб отримати значення функції, потрібно припустити умову на структуру гри: це так звана умова Айзекса: : для всіх $(t, x) \in [0, T] \times \mathbb{R}^N$, $\xi \in \mathbb{R}^N$ і всіх $A \in S_N$ (де S_N — множина симетричних $n \times n$ матриць), ми припустимо, що

$$H(t,x,\xi,A) := inf_u\, sup_v \{ \langle b(t,x,u,v), \xi\rangle + \tfrac{1}{2} Tr(A\sigma(t,x,u,v)\sigma^*(t,x,u,v)) + \ell(t,x,u,v)\} = sup_v\, inf_u \{ \langle b(t,x,u,v), \xi\rangle + \tfrac{1}{2} Tr(A\sigma(t,x,u,v)\sigma^*(t,x,u,v)) + \ell(t,x,u,v)\} \tag{8}$$

Ця умова зазвичай виконується у випадку, який часто зустрічається на практиці – окремої динаміки. Теорема (Флемінг-Суганідіс)[21].

За умовою Айзекса: гра має значення: $V^+ = V^-$ у $[0, T] \times \mathbb{R}^N$. Крім того, $V := V^+ = V^-$ є єдиним розв'язком рівняння Гамільтона-Якобі:

$$\begin{cases} V_t + H(t,x,DV,D^2V) = 0 & \text{на } (0,T) \times \mathbb{R}^N \\ V(T,\cdot) = g \text{ in } \mathbb{R}^N \end{cases} \tag{9}$$

Рівняння Гамільтона-Якобі є нелінійним параболічним рівнянням: гарною основою для його аналізу є поняття розв'язків в'язкості, яке вперше було введено Крендаллом і Лайонсом у рівняннях першого порядку та розширене на рівняння другого порядку кількома авторами. (див., наприклад, знамените опитування Крендалла, Ішіі та Лайонса [22]). Перше застосування розв'язків в'язкості в диференціальних іграх сходить до роботи Еванса і Суганідіса [23]. З тих пір з'явилася дуже велика література з цього питання, і дана теорема була поширена на багато різних динамічностей і виплат. Зазначимо, що в більшості робіт ключовим припущенням завжди є те, що гравці чудово спостерігають один за одним і мають повне знання про структуру гри.

Щоб зрозуміти, де це припущення відіграє роль, було коротко описано доказ теореми [18]: його ключовим компонентом є наступний принцип динамічного програмування (ПДР): для будь-якого $0 \le t_0 \le t_1 \le T$ і будь-якого $x_0 \in \mathbb{R}^N$,

$$V^+(t_0,x_0) = \inf_{\alpha\in A(t)} \sup_{\beta\in B(t)} E\left[\int_{t_0}^{t_1} \ell\left(s, X_s^{t_0,x_0,\alpha,\beta}, \alpha_s, \beta_s\right)ds + V^+\left(t_1, X_{t_1}^{t_0,x_0,\alpha,\beta}\right)\right]$$

Коли:

$$V^-(t_0,x_0) = \sup_{\beta\in B(t)} \inf_{\alpha\in A(t)} E\left[\int_{t_0}^{t_1} \ell\left(s, X_s^{t_0,x_0,\alpha,\beta}, \alpha_s, \beta_s\right)ds + V^-\left(t_1, X_{t_1}^{t_0,x_0,\alpha,\beta}\right)\right] \tag{10}$$

З цього можна зробити висновок, що V^+ і V^- задовольняють рівнянню Гамільтона-Якобі (9), яке є лише нескінченно малою версією наведеного вище ПДР. Оскільки рівняння (9) має унікальний розв'язок щодо в'язкості, необхідно мати $V^+ = V^-$, і тоді буде наступний результат. У цьому контексті роль умови Айзекса полягає в тому, щоб гарантувати, що, незважаючи на те, що V^+ і V^- задовольняють різному ПДР, отримане рівняння Гамільтона-Якобі буде однаковим.

Отже, найбільша частина труднощів зосереджена, з одного боку, на ПДР, а з іншого боку – на єдиності розв'язку (9). Для пояснення коректності (9) ми знову звернемося до [22]. Приблизно стверджується, що в момент t_1 гравці можуть забути все минуле і грати в гру так, ніби вона розпочалася в цей момент для позиції X_{t_1}. Дійсно, оскільки гравці спостерігають за станом і простором, вони нічого не дізнаються в інтервалі часу $[t_0, t_1]$, тому вони можуть забути минулу траєкторію в момент t_1 і грати так, ніби гра в цей момент розпочалася щойно.

Коли хтось має справу з іграми з неповною інформацією або спостереженнями, виявляється, що це вже не так, і треба бути дуже обережним з динамічним програмуванням [18].

Диференціальні ігри з неповною інформацією – це диференційна гра, в якій хоча б один гравець має певні приватні знання про структуру гри: наприклад, він може точно знати реалізацію випадкового виграшу або реалізацію випадкової вихідної позиції, тоді як інші гравці знають лише правило платежу або початкову позицію. Оскільки ми використовуємо гру для двох гравців, ми припускаємо, що це перший гравець з корисною приватною інформацією. Ми також припускаємо, що гравці чудово контролюють один одного. Справа в тому, що таким чином неінформований гравець може спробувати вгадати інформацію, яку йому бракує, спостерігаючи за поведінкою поінформованого гравця. Більшість роботи в намаганні зрозуміти, як необізнаний гравець може кількісно оцінити кількість інформацію, яку він досліджує, а для поінформованого гравця — скільки інформації він розкрив протягом гри.

4.3. Застосування диференційних ігор в кібербезпеці. За умовою диференційної ігрової постановки задачі під моделлю процесу інформаційної атаки слід розуміти ігрову траєкторію, що визначається. Нехай модель інформаційного конфлікту в ІТС описується системою диференціальних рівнянь загального вигляду:

$$\begin{cases} x = f(t, u, v) \\ x(t_0) = x_0 \end{cases}, \tag{11}$$

де $x = (x_1, x_2, K, x_n)$ – точка n -вимірного фазового простору R_n, що визначає стан процесу, оj моделюється і належить області $X \in R_n$;

$u = (u_1, u_2, K, u_n)$ і $v = (v_1, v_2, K, v_n)$ – параметри керування першого та другого гравців відповідно, такі, що $u \in E_u$ і $v \in E_v$ в евклідових просторах R_l і R_m;

$f = (f_1, f_2, K, f_n)$ – дійсна векторна функція визначена на $X \times E_u \times E_v$ множин;

$x(t_0) = x_0$ – початкові умови в момент початку гри $t_0 > 0$, в точці x_0, $t \in [t_0, T]$.

Рішенням x(t) системи диференціальних рівнянь (11) при обраних гравцями стратегіях u(t) і v(t) з початковими умовами $x(t_0) = x_0$ є абсолютна неперервна функція. що є траєкторією/партією:

$$x(t) = x_0 + \int_{t_0}^{T} f(\tau, x(\tau), u(\tau))d\tau. \tag{12}$$

Для широкого класу диференціальних ігор плата може бути задана у формі функціонала:

$$I\big(t, x(t), u(t), v(t)\big) = \int_{t_0}^{T} G\big(t, x(t), u(t), v(t)\big)dt + S[x(T)]\,, \tag{13}$$

де G – обмежена, вимірювана за Борелем функція, визначена на декартовому добутку $X \times E_u \times E_v$;

$S[x(T)]$ – функція кінцевого стану визначена на термінальному багатовиді M , непере-

рвна за сукупністю аргументів, крім того, визначена на X × G . Виконання даних умов забезпечує існування функціонала (13). Залежно від випадків, при яких S[x(T)]= 0 або G = 0 , плата називається інтегральною чи термінальною, відповідно [14].

Оскільки гравці ставлять на маті протилежні цілі, то їх стратегії формуються за принципом мінімаксу, мінімізуючи плати один одного:

$$\min_{u(t)\in E_u} \max_{v(t)\in E_v} = I\left(t, x(t), u(t), v(t)\right),$$
$$\min_{v(t)\in E_v} \max_{u(t)\in E_u} = I\left(t, x(t), u(t), v(t)\right). \quad (14)$$

При виконанні співвідношення

$$\min_{u(t)\in E_u} \max_{v(t)\in E_v} I\left(t, x(t), u(t), v(t)\right) =$$
$$\min_{v(t)\in E_v} \max_{u(t)\in E_u} I\left(t, x(t), u(t), v(t)\right) = I\left(t, x^{opt}(t), u^{opt}(t), v^{opt}(t)\right) = I^* \quad (15)$$

стратегії $u^{opt}(t)$ і $v^{opt}(t)$ називаються оптимальними при оптимальній траєкторії $x^{opt}(t)$, а плата $I\left(t, x^{opt}(t), u^{opt}(t), v^{opt}(t)\right) = I^*$ – ціна гри.

У визначенні оптимальних стратегій, траєкторії та ціни гри і полягає основна задача диференціальних ігор.

Застосування теорії диференціальних ігор для моделювання процесу атаки інформації як загальної моделі для задач динамічної оптимізації вимагає використання складних сучасних методів та інструментів моделювання. В якості таких пристроїв в монографії [14] запропоновано використовувати математичні методи теорії диференціальних перетворень. На відміну від відомих інтегральних перетворень Лапласа і Фур'є, метод диференціальних перетворень заснований на перетворенні вихідних даних в області зображення диференціюванням.

Диференційовані перетворення розширюють сферу роботи на дослідження станів фізичних об'єктів і процесів, що описані нелінійними диференціальними рівняннями, що показано в монографії [14].

Крім того в монографії [14] було вперше розроблено диференціально-ігрову графову модель процесу нападу на інформацію, яка на відміну від відомих моделей дискретизована на графах, що дає можливість моделювати процеси нападу на інформацію як задачу про найкоротший шлях.

4.4. Диференціально-ігрова нетейлорівська модель. Теорія диференціальних перетворень нетейлорівського типу є досить новим напрямом в теорії Р-перетворень, але вже зараз її застосування надає змогу точно описувати процеси нападу на інформацію.

Нетейлорівськими диференціальними перетвореннями є функціональні перетворення вигляду:

$$X(k) = \underline{x}(k) = \frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \overline{\bullet}\ x(t) = \varphi(t, C_0, C_1, \dots, C_n)\ , \quad (16)$$

де x(t) – оригінальна, безперервна функція дійсного аргументу t, диференційовна на всьому проміжку і обмежена зі своїми похідними;

X(k) і $\underline{x}(k)$ – еквівалентні позначення диференціального зображення оригінальної функції, що становлять дискретну функцію аргументу $k \in \mathbb{Z}$, k =: 0, 1, 2, ….;

H – масштабна стала, що має розмірність t і загалом обирається на відрізку, шо розглядається функція x(t), як $0 \le t \le H$;

$\overline{\bullet}$ – символ відповідності диференціального зображення до його оригіналу.

Диференціальні зображення X (k) називаються диференціальними Т-спектрами, а значення Т-функції X (k) при конкретних значеннях аргументу k – дискретами.

Нетейлерівські диференціальні перетвореннями відрізняються від диференціальних пе-

ретворень більшою складністю на моменті відновлення оригіналу за диференційним спектром, у всіх інших діях та перетвореннях вони збігаються.

У монографії [14], використавши початкову спектральну модель

$$P_0(k+1) = \frac{T}{k+1}\left(\mu ъ(k) - (\lambda+\mu)P_0(k)\right), \quad (17)$$

за початкових умов $P_0(t_0) = 1$, де T = H – тривалість моделювання;

λ, μ – інтенсивності потоку захисних дій та атак на інформацію відповідно;

ъ(k) – теда.

Визначили вигляд траєкторії диференціальної гри зі спектральної моделі (17) – знайшовши перші чотири дискрети шляхом послідовного присвоєння цілочислових значень аргументу k =: 0,1,2.

Було розроблено точну модель процесу нападу на інформацію

$$P_0^{NT}(t) = \frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu}. \quad (18)$$

Відрізок ряду Тейлора побудований за тими ж вихідними даними, що і модель, має вигляд

$$P_0(t) = 1 - \lambda t + \frac{1}{2}\lambda(\lambda+\mu)t^2 - \frac{1}{6}\lambda(\lambda+\mu)^2 t^3. \quad (19)$$

Про точність моделей (18) і (19) можна стверджувати, обчисливши значення функцій $P_0^{NT}(t)$ та $P_0(t)$, наприклад у точці t =1 при $\lambda = \mu$ = 1: $P_0^{NT}(t)$ = 0.5685, $P_0(t)$ = 0.3333. Тобто точність моделювання процесів нападу на інформацію нетейлорівськими диференціальними перетвореннями з використанням 4-х дискрет диференціального спектра в 1,7 разів більше порівняно з основними перетвореннями [14].

4.5. Неперервна дискретна диференціально-ігрова модель процесу нападу на інформацію. Неперервна безперервна дискретно-диференційна ігрова модель процесу інформаційної атаки розробляється на основі умов конкретного інформаційного конфлікту, що виникає в СЗІ окремої КС або мережі.

На відміну від нетейлорівських та гібридних моделей процесів нападу на інформацію підвищення точності в неперервній дискретній диференціально-ігровій моделі досягається за рахунок методу числово-аналітичного моделювання на базі зміщених диференціальних перетворень [14].

Розглянуто деяку СЗІ, що піддається впливу методів НСД та МЗІ. Припустимо, що в деякий момент часу t , що належить інтервалу часу, на якому здійснюється моделювання процесу нападу на інформацію в СЗІ (t ∈ [0,T]), система може перебувати в одному із станів $P_z(t)$, $z = \overline{0,c}$. Усі стани системи задані зліченною множиною станів системи $\{P_z(t)\}$, у яких вона може перебувати під впливом методів НСД або МЗІ [14].

Для моделювання процесу нападу на інформацію на значному часовому інтервалі, було застосовано числово-аналітичний метод. Динаміку процесу нападу на інформацію, було подано як систему локальних диференціальних рівнянь вигляду [14]:

$$\begin{cases} \frac{dP_0^{opt}{}_i(t)}{dt} = \varphi_i\left(t, P_0^{opt}{}_i(t)\right) \\ P_0^{opt}(0) = 1, \qquad t \in [0,T] \end{cases}, \quad (20)$$

де $i = \overline{0,n}$, n – кількість рівних частин, на які розбивається інтервал $t \in [0,T]$.

У монографії [14] був змодельований процес нападу на інформацію застосувавши метод зміщених диференціальних перетворень у точках t = t_i та t = t_{i+1}. Систему (20) було зведено та отримано рекурентний вираз для знаходження прямих диференціальних спектрів у числовому вигляді в кожний момент часу, що у подальшому дозволять відновити оригінал – функцію

$P_0^{opt}{}_i(t)$. Застосувавши прямі диференціальні перетворення у другій точці до системи локальних векторних рівнянь (20), отримано її зображення у вигляді системи спектральних рівнянь, за якими знаходиться аналітичний вигляд оберненого диференціального спектра. Спряження функцій $P_0^{opt}{}_i(t)$та $P_0^{opt}{}_{i+1}(t)$ здійснюється у спільній точці t_i + h, звідки невідома величина $P_0^{opt}{}_{i+1}(t)$ визначається з точного рівняння загального вигляду

$$\sum_{k=0}^{k=\infty} P_0^{opt}{}_i(k) = \sum_{k=0}^{k=\infty}(-1)^k P_0^{opt}{}_{i+1}(k). \quad (21)$$

Після чого, обмежившись деякою кількістю дискрет q, що було враховано при моделюванні диференціальних спектрів, розрахунок невідомих дискрет здійснюється за наближеним виразом

$$\sum_{k=0}^{k=q} P_0^{opt}{}_i(k) \approx \sum_{k=0}^{k=q}(-1)^k P_0^{opt}{}_{i+1}(k). \quad (22)$$

Значення q обирається, виходячи із заданої точності заміни нескінченного ряду (21) скінченним (22), шляхом розв'язання задачі Коші.

Дана числово-аналітична процедура повторюється до того часу, як неперервна дискретна диференціально-ігрова модель процесу нападу на інформацію P_0^{opt}(t) не досягне певної заданої точності моделювання на визначному часовому інтервалі [0,T] [14].

4.6. Марківська модель поширення шкідливого програмного забезпечення мережевою архітектурою довільної конфігурації. Марківський процес - це випадковий процес, ймовірність певного значення якого в будь-який момент часу t_0, якщо врахувати відомі раніше значення в попередні моменти, залежить тільки від значення в останній момент, що відбувся t - 1. Інакше кажучи, розвиток процесу залежить лише від останнього відомих станів, і не враховує попередні.

Постановка задачі. Для критичної мережевої архітектури довільної конфігурації, що складається з N об'єктів, M об'єктів з яких є об'єктами з критичною кібернетичною інфраструктурою. Представимо мережу у вигляді графа, об'єкти зображені у вигляді вузлів, а канали – дугами між ними (рис.1). Кожен з вузлів може знаходитись у двох станах – незараженому S та зараженому I.

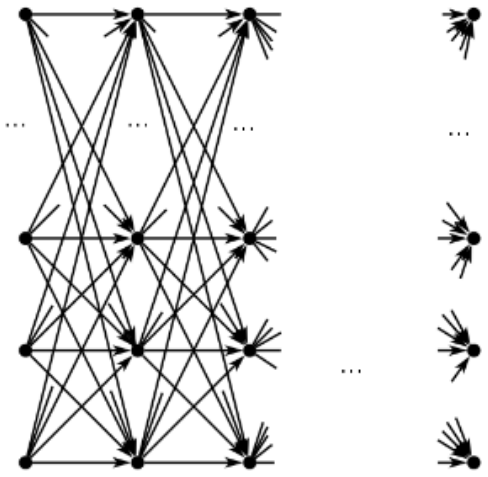

Рис.1 Загальний вигляд марковської моделі графа
поширення шкідливого програмного забезпечення

Станом критичної мережевої архітектури у деякий момент часу t є сукупність усіх вузлів мережі. Припустимо, що вага w_{ij} означає ймовірність переходу шкідливого програмного забезпечення від i - го об'єкта мережі – до j - го за деякий час t. Тоді процес розповсюдження

шкідливого програмного забезпечення у критичній мережевій архітектурі довільної конфігурації набуває вигляду ланцюга Маркова, для якого перехідні ймовірності в загальному вигляді можуть бути визначені як [13]:

$$P_{il} = P[f^t = s^j | f^{t-1} = s^i]\ . \tag{23}$$

Тоді можна зробити висновок, що мережа змінить стан від s^i до стану s^j, якщо всі вузли мережі перейдуть в новий стан ${s_c}^j$ з старого ${s_c}^i$, де с – номер вузла. Ймовірність даного переходу може бути описана так:

$$P_{il} = \prod_{c=0}^{N} P[{f_c}^t = {s_c}^j | {f_c}^{t-1} = {s_c}^i]. \tag{24}$$

У формалізованому вигляді описані варіанти для різних станів об'єкта на попередньому і поточному кроках відповідно до монографії [13] описані виразом вигляду:

$$P\left[{f_c}^t = {s_c}^j \middle| {f_c}^{t-1} = {s_c}^i\right] = \begin{cases} P_{\text{зар}}(c, s^i), & \text{якщо } {s_c}^i = S,\ {s_c}^j = I \\ \left[1 - P_{\text{зар}}(c, s^i)\right], & \text{якщо } {s_c}^i = S,\ {s_c}^j = S \\ 0, & \text{якщо } {s_c}^i = I,\ {s_c}^j = S \\ 1, & \text{якщо } {s_c}^i = I,\ {s_c}^j = I \end{cases}. \tag{25}$$

Крім того була описана також ймовірність розповсюдження шкідливого програмного забезпечення від вузла *c* до вузла *m*:

$$P_{\text{розп}}(m, c, s_m^i) = \begin{cases} w_{mc}, & \text{якщо } {s_m}^i = I, \\ 0, & \text{якщо } {s_m}^i = S. \end{cases} \tag{26}$$

Вузол *c* перейде за одиницю часу в заражений стан, якщо хоча б від одного сусіднього вузла передасться шкідливе програмне забезпечення. Зараження незараженого *c*-го вузла не залежить від різних джерел і ймовірність його зараження може бути визначена як [13]:

$$P_{\text{зар}}(c, s^i) = 1 - \prod_{m=1}^{N} \left(1 - P_{\text{розп}}(m, c, s_m^i)\right). \tag{27}$$

Крім того у монографії [13] було виведено аналіз матриці ймовірності переходів шкідливого програмного забезпечення між вузлами мережі, де ймовірність зараження певного окремого *c*-го вузла визначається, як:

$$\mathrm{P}_{\text{зар}}(\mathrm{c}) = 1 - \prod_{m=1}^{N} (1 - P_{\text{розп}}(m, c)) \tag{28}$$

Тоді ймовірність передачі шкідливого програмного забезпечення від вузла *m* до вузла *c* дорівнюватиме добутку ймовірності зараження вузла *m* на попередньому кроці на ймовірність переходу по зв'язку $m - c$, тобто

$$P_{\text{розп}}(m, c) = P_m^{t-1}(I) w_{mc}\ . \tag{29}$$

Врахувавши формули (28) та (29) було виведено модель ймовірності зараження [13], з аналізу якої можна стверджувати, що ланцюг маркова для кожного вузла однорідний:

$$P = \begin{bmatrix} \prod_{m=1}^{N} (1 - {P_m}^{t-1}(I) w_{mc}) & 1 - \prod_{m=1}^{N} (1 - {P_m}^{t-1}(I) w_{mc}) \\ 0 & 1 \end{bmatrix}. \tag{30}$$

Практичне застосування даних моделей поширення шкідливого програмного забезпечення мережевою архітектурою довільної конфігурації на рівні мережі та на рівні окремих вузлів можливе лише у разі відомих початкових розподілів ймовірностей знаходження мережі або вузлів у початковий момент часу. Якщо задати вектор ймовірностей знаходження мережі на початок моніторингу то можна визначити математичне очікування кількості заражених вузлів.

Оскільки заражений стан передається між сусідніми вузлами, а всі вузли в системі пов'язані через декілька спільних «сусідів», то через певний проміжок часу вся архітектура буде заражена шкідливим програмним забезпеченням. Дана модель не враховує можливість лікування системи, то ж ймовірність виліковування комп'ютера дорівнює нулю.

Висновок. Теорія ігор є важливою концепцією в різних ситуаціях безпеки і широко використовується в мережевій безпеці. Останні дослідження показали, що теорія ігор застосовна до маршрутизації мережі, кешування мережі, кібербезпеки тощо. Використовуючи ігри можна розробляти та аналізувати оптимальні дії гравців та знаходити можливі математичні рішення безпекових задач. З точки зору безпеки, поєднання кіберпростору та фізичного простору призводить до кібер-фізичної безпеки, або поєднання елементів безпеки та економіки створює кіберстрахування. Для вирішення проблем безпеки та конфіденційності в нових сферах найбільш підходящими інструментами є теоретичні ігрові методи, оскільки вони надають різноманітні перевірені математичні методи для створення багатокористувацьких стратегій з використанням різних способів для охоплення аспектів конфіденційності та безпеки взаємодії гравців. Представлені теорії показують ефективність та доцільність використання теорії ігор та теорії диференціальних ігор у сфері захисту інформації. На сьогодні, ще багато проблем інтеграції теорії ігор та диференціальних ігор є не вирішеним. Про застосування теорії диференціальних ігор у якості вирішення проблем захисту інформації існує дуже мало відомостей, що робить цю сферу пріоритетною для майбутніх досліджень.

Список використаної літератури

1. Q. Zhu and S. Rass, "Game Theory Meets Network Security: A Tutorial", in CCS '18: 2018 ACM SIGSAC Conference on Computer & Communications Security, October 15-19, 2018, Toronto, ON, Canada, J. B. Sartor, T. D'Hondt, and W. De Meuter (Eds.), ACM, New York, NY, USA, Article 4, p. 4, 2018.

2. M. J. Osborne, "An Introduction to Game Theory by Please send comments to Department of Economics This version," 2000.

3. S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in Proceedings of the 2010 43Rd Hawaii International Conference on System Sciences, pp. 1–10, IEEE, Honolulu, HI, USA, 5 January 2010.

4. M. Outanoute, H. Garmani, M. Baslam, R. Ayachi, and B. Bouikhalene, "A non-cooperative game analysis of competition between content providers in the internet market," International Journal of Business Data Communications and Networking, vol. 15, no. 1, pp. 88–104, 2019.

5. B. Gu, X. Yang, Z. Lin, W. Hu, M. Alazab, and R. Kharel, "Multiagent actor-critic network-based incentive mechanism for mobile crowdsensing in industrial systems," IEEE Transactions on Industrial Informatics, vol. 17, p. 1, 2020.

6. S. Handouf and E. Sabir, "Strategic availability and cost-effective UAV-based flying access networks: S-modular game analysis," Mobile Information Systems, vol. 2019, pp. 1–11,2019

7. D. Ait Omar, H. Garmani, M. El Amrani, M. Baslam, and M. Fakir, "A customer confusion environment in telecom-munication networks: analysis and policy impact," International Journal of Cooperative Information Systems, vol. 28, no. 02, Article ID 1930002, 2019.

8. Z. Zhou, B. Wang, B. Gu et al., "Time-dependent pricing for bandwidth slicing under information asymmetry and price discrimination," IEEE Transactions on Communications, p. 1,2020.

9. T. Roughgarden, Selfish Routing and the price of Anarchy, Vol. 174, MIT press, Cambridge, UK, 2005.

10. H. Garmani, M. Baslam, and M. Jourhmane, "Caching games between ISP in information

centric network", vol. 11, no. 4, pp. 125–142.

11. S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security", in Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, pp. 1–10, IEEE, Honolulu, HI, USA, 5 January 2010.

12. І. Грабар, "Безпекова синергетика: кібернетичний та інформаційний аспекти": монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир: ЖНАЕУ, 2019. – 280 с.

13. Р. Грищук "Основи кіберенетичної безпеки": Монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

14. Р. Грищук "Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень": Монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.

15. R. Sankardas, E. Charles, S. Sajjan, D. Dipankar, S. Vivek and W. Qishi, "A Survey of Game Theory as Applied to Network Security," in Hawaii International Conference on System Sciences, 2010.

16. C.T. Do, N.H. Tran, C. Hong, C.A. Kamhoua, K.A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S.S. Iyengar, "Game Theory for Cyber Security and Privacy", ACM Computing Surveys (CSUR), vol. 50, no. 2, pp. 30, 2017.

17. K. Lye and J. Wing, "Game Strategies in Network Security," Copenhagen, Denmark, 2002.

18. P. Cardaliaguet " Information issues in differential game theory" EDP Sciences, SMAI 2012, Vol. 35, p. 1-13

19. P. Cardaliaguet, C. Rainer, "Stochastic differential games with asymmetric information." Appl. Math. Optim. 59: 1-36,2009.

20. P. Cardaliaguet, "Differential games with asymmetric information.", SIAM J. Control Optim. 46, no. 3, 816–838, 2007.

21. W. Fleming, P. Souganidis, "On the existence of value functions of two-player, zero-sum stochastic differential games." Indiana Univ. Math. J. 38, No.2, 293-314, 1989

22. M. Crandall, H. Ishii, P. Lions "User's guide to viscosity solutions of second order Partial Differential Equations." Bull. Amer. Soc., 27, pp. 1-67, 1992.

23. L. Evans, P. Souganidis, "Differential games and representation formulas for solutions of Hamilton-Jacobi Equations." Indiana Univ. Math. J., 282, pp. 487-502, 1984.

References

1. Q. Zhu and S. Rass, "Game Theory Meets Network Security: A Tutorial", in CCS '18: 2018 ACM SIGSAC Conference on Computer & Communications Security, October 15-19, 2018, Toronto, ON, Canada, J. B. Sartor, T. D'Hondt, and W. De Meuter (Eds.), ACM, New York, NY, USA, Article 4, p. 4, 2018.

2. M. J. Osborne, "An Introduction to Game Theory by Please send comments to Department of Economics This version," 2000.

3. S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in Proceedings of the 2010 43Rd Hawaii International Conference on System Sciences, pp. 1–10, IEEE, Honolulu, HI, USA, 5 January 2010.

4. M. Outanoute, H. Garmani, M. Baslam, R. Ayachi, and B. Bouikhalene, "A non-cooperative game analysis of competition between content providers in the internet market," International Journal of Business Data Communications and Networking, vol. 15, no. 1, pp. 88–104, 2019.

5. B. Gu, X. Yang, Z. Lin, W. Hu, M. Alazab, and R. Kharel, "Multiagent actor-critic network-based incentive mechanism for mobile crowdsensing in industrial systems," IEEE Transactions on Industrial Informatics, vol. 17, p. 1, 2020.

6. S. Handouf and E. Sabir, "Strategic availability and cost-effective UAV-based flying access networks: S-modular game analysis," Mobile Information Systems, vol. 2019, pp. 1–11,2019

7. D. Ait Omar, H. Garmani, M. El Amrani, M. Baslam, and M. Fakir, "A customer confusion environment in telecom-munication networks: analysis and policy impact," International Journal of

Cooperative Information Systems, vol. 28, no. 02, Article ID 1930002, 2019.

8. Z. Zhou, B. Wang, B. Gu et al., “Time-dependent pricing for bandwidth slicing under information asymmetry and price discrimination,” IEEE Transactions on Communications, p. 1,2020.

9. T. Roughgarden, Selfish Routing and the price of Anarchy, Vol. 174, MIT press, Cambridge, UK, 2005.

10. H. Garmani, M. Baslam, and M. Jourhmane, “Caching games between ISP in information centric network”, vol. 11, no. 4, pp. 125–142.

11. S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, “A survey of game theory as applied to network security”, in Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, pp. 1–10, IEEE, Honolulu, HI, USA, 5 January 2010.

12. I. Grabar, "Security synergy: cybernetic and informational aspects": monograph / I. G. Grabar, R. V. Hryshchuk, K. V. Molodetska; in general ed. Ph.D., prof. R. V. Hryshchuk. - Zhytomyr: ZhNAEU, 2019. - 280 p.

13. R. Hryshchuk "Basics of cybernetic security": Monograph / R. V. Hryshchuk, Yu. G. Danyk; in general ed. Prof. Y. G. Danyka. - Zhytomyr: ZhNAEU, 2016. - 636 p.

14. R. Hryshchuk "Theoretical foundations of modeling of information attack processes using the methods of the theories of differential games and differential transformations": Monograph / R. V. Hryshchuk. - Zhytomyr: Ruta, 2010. - 280 p.

15. R. Sankardas, E. Charles, S. Sajjan, D. Dipankar, S. Vivek and W. Qishi, "A Survey of Game Theory as Applied to Network Security," in Hawaii International Conference on System Sciences, 2010.

16. C.T. Do, N.H. Tran, C. Hong, C.A. Kamhoua, K.A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S.S. Iyengar, “Game Theory for Cyber Security and Privacy”, ACM Computing Surveys (CSUR), vol. 50, no. 2, pp. 30, 2017.

17. K. Lye and J. Wing, “Game Strategies in Network Security,” Copenhagen, Denmark, 2002.

18. P. Cardaliaguet “ Information issues in differential game theory” EDP Sciences, SMAI 2012, Vol. 35, p. 1-13

19. P. Cardaliaguet, C. Rainer, “Stochastic differential games with asymmetric information.” Appl. Math. Optim. 59: 1-36,2009.

20. P. Cardaliaguet, “Differential games with asymmetric information.”, SIAM J. Control Optim. 46, no. 3, 816–838, 2007.

21. W. Fleming, P. Souganidis, “On the existence of value functions of two-player, zero-sum stochastic differential games.” Indiana Univ. Math. J. 38, No.2, 293-314, 1989

22. M. Crandall, H. Ishii, P. Lions “User’s guide to viscosity solutions of second order Partial Differential Equations.” Bull. Amer. Soc., 27, pp. 1-67, 1992.

23. L. Evans, P. Souganidis, “Differential games and representation formulas for solutions of Hamilton-Jacobi Equations.” Indiana Univ. Math. J., 282, pp. 487-502, 1984.