ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА

УДК 004.415.056.5
DOI https://doi.org/10.17721/ISTS.2020.4.38-47

С. В. Толюпа, orcid.org/0000-0002-1919-9174, **tolupa@i.ua**
Н. В. Лукова-Чуйко, orcid.org/0000-0003-3224-4061, **lukova@ukr.net**
В. С. Наконечний, orcid.org/0000-0002-0247-5400, **nvc2006@i.ua**
В. Г. Сайко, orcid.org/0000-0002-3059-6787, **vgsaiko@gmail.com**
Київський національний університет імені Тараса Шевченка, Київ, Україна
О. Кулінич, orcid.org/0000-0002-0643-6898,
oleh_nicol@gmail.com
Національний технічний університет України імені Ігоря Сікорського

ФОРМУВАННЯ СТРАТЕГІЇ УПРАВЛІННЯ РЕЖИМАМИ РОБОТИ СИСТЕМ ЗАХИСТУ НА ОСНОВІ МОДЕЛІ ІГРОВОГО УПРАВЛІННЯ

Основними сферами застосування теорії ігор є економіка, політологія, тактичні й воєнно-стратегічні задачі, еволюційна біологія і, останнім часом, інформаційні технології, безпека та штучний інтелект. Теорія ігор вивчає задачі прийняття рішень декількох осіб (гравців). Вона стосується поведінки гравців, рішення яких впливають один на одного. Теорія ігор призначена для вирішення ситуацій, в яких результат рішення гравців залежить не лише від того, як вони їх вибирають, а й від вибору рішень інших гравців, з якими вони взаємодіють. Якщо розглядати сферу інформаційної безпеки, то особливістю інформаційного конфлікту системи оперативного управління захистом інформації та порушника, який намагається здійснити несанкціонований доступ, є те, що протидіючі сторони, які мають декілька способів дій, можуть застосовувати їх багаторазово, вибираючи найкращий спосіб з урахуванням інформації про дії протилежної сторони. Причому кожен крок розв'язання конфлікту характеризується не фінальним станом, а деякою платіжною функцією. У багатьох ситуаціях під час проєктування систем захисту інформації виникає необхідність розроблення та прийняття рішень в умовах невизначеності. Невизначеність може мати різний характер. Невизначеними є сплановані дії хакерів, які скеровані на зменшення ефективності систем захисту. Невизначеність може стосуватися ситуації ризику, в якій система управління інформаційної мережі, що приймає рішення щодо застосування системи захисту, здатна встановлювати не тільки всі можливі результати рішень, але й вірогідність можливих умов їхньої появи. Умови проєктування впливають на прийняття рішень підсвідомо, незалежно від дій суб'єкта, що приймає рішення. Коли відомі всі наслідки можливих рішень, але невідома їхня вірогідність, очевидно, що рішення приймають в умовах повної невизначеності. Основною перспективною теорією аналізу процесів прийняття рішень на етапі проєктування систем захисту інформації є теорія ігор. Застосування теорії ігор в області моделювання процесів прийняття рішень у сфері інформаційної безпеки має різні підходи, які нині не систематизовані, а інколи і вступають у протиріччя між собою. Тому виникає необхідність розроблення методів оперативного (адаптивного) управління захистом інформації залежно від наявності апріорної інформації про можливість атак порушника й реалізовані ним стратегії створення несанкціонованого доступу до інформаційного ресурсу. Теорія ігор дозволяє запропонувати рекомендації із формування стратегії управління режимами роботи систем захисту.

Ключові слова: *захист інформації; система безпеки; теорія ігор; оптимальна стратегія; система порушника; прийняття рішення.*

1. ВСТУП

У дослідженнях конфліктів існує значна кількість наукових проблем, для розв'язання яких теорія ігор може бути екстремально корисною. Наприклад, важливим, але недостатньо дослідженим напрямком є аналіз дій супротивників у кількох періодах, стратегічної поведінки учасників в умовах неповної інформації. Іншою сферою, яка практично не береться до уваги як у класичних, так і в сучасних дослідженнях та іграх – це моральні норми, цінності суспільства, моральна сторона кожної стратегії.

У багатьох ситуаціях проєктування систем захисту інформації виникає необхідність розроблення та прийняття рішень в умовах невизначеності. Невизначеність може мати різний характер. Останнім часом досить гостро постало питання протидії атакам в інформаційні системи [1, 2]. Так, невизначеними є сплановані дії хакерів, які скеровані на зменшення ефективності систем захисту. Невизначеність може стосуватися ситуації ризику, в якій система управління інформаційної мережі, що приймає рішення із застосування системи захисту, здатна встановлювати не тільки всі можливі результати рішень, але й вірогідність можливих умов їхньої появи. Умови проєктування впливають на прийняття рішень підсвідомо, незалежно від дій суб'єкта, що приймає рішення. Коли відомі всі наслідки можливих рішень, але невідома їхня вірогідність, очевидно, що рішення приймають в умовах повної невизначеності. Основною перспективною теорією аналізу процесів прийняття рішень на етапі проєктування систем захисту інформації є теорія ігор [3–6]. Застосування теорії ігор в області моделювання процесів прийняття рішень має різні підходи, які нині не систематизовані, а інколи і вступають у протиріччя між собою. Тому дослідження вказаної тематики є актуальними науковими завданнями.

2. ПОСТАНОВКА ПРОБЛЕМИ

Теорія ігор призначена для врегулювання ситуацій, в яких результат рішення гравців залежить не тільки від того, як вони їх вибирають, а й від вибору рішень інших гравців, з якими вони взаємодіють. Ігри залежать від кількості гравців; до них належать ігри з нульовою сумою (антагоністичні) і з ненульовою сумою. Множини стратегій можуть бути скінченними або нескінченними (матричні ігри й ігри на компактах відповідно). Також гравці можуть діяти незалежно один від одного або утворювати коаліції. Відповідними моделями є некооперативні та кооперативні ігри. Існують також ігри з повною або частковою інформацією [7, 8].

Якщо розглядати сферу інформаційної безпеки (ІБ), то особливістю інформаційного конфлікту системи оперативного управління захистом інформації та порушника, який намагається здійснити несанкціонований доступ (НСД) є те, що протидіючі сторони, які мають декілька способів дій, можуть застосовувати їх багаторазово, вибираючи найкращий спосіб з урахуванням інформації про дії протилежної сторони. Причому кожний крок вирішення конфлікту характеризується не фінальним станом, а деякою платіжною функцією. Традиційний ігровий підхід до аналізу дій порушника не дозволяє врахувати багатокроковість конфлікту й не відображує залежність способів дій сторін від інформації про протилежну сторону, а відомий конфліктний підхід на основі розрахунку фінальних імовірностей перебування систем у стані виграшу до заданого моменту часу не відображує багатоваріантність дій сторін і неповну завершеність конфлікту на кожному кроці [9, 10].

Якщо розглядати конфліктність між системою оперативного управління захистом інформації (ЗІ) та порушником, то можна розглядати різні стратегії ведення ігор.

Так модель чистої стратегії ведення ігор – це пара стратегій (одна – для загрози, а друга – для механізму захисту), які перехрещуються в сідловій точці, яка в цьому випадку і визначає ціну гри.

Нехай загроза A обрала стратегію A_i, тоді у найгіршому разі вона отримає виграш, що дорівнює $\min a_{ij}$, тобто навіть тоді, якщо механізм захисту B знав би стратегію загрози A. Передбачаючи таку можливість, загроза A має вибрати таку стратегію, щоб максимізувати свій мінімальний виграш, тобто $\alpha = \max\limits_i \min\limits_j a_{ij}$.

Така стратегія загрози A позначається A_{i_0} і має назву максимінної, а величина гарантованого виграшу цього гравця називається нижньою ціною гри.

Механізм захисту B, який програє суми у розмірі елементів платіжної матриці, навпаки має вибрати стратегію, що мінімізує його максимально можливий програш за всіма варіантами дій загрози A. Стратегія механізму захисту B позначається через B_{j_0} і називається мінімаксною, а величина його програшу – верхньою ціною гри, тобто $\beta = \min\limits_j \max\limits_i a_{ij}$.

Оптимальний розв'язок цієї задачі досягається тоді, коли жодній стороні невигідно змінювати вибрану стратегію, оскільки її противник може у відповідь вибрати іншу стратегію, яка забезпечить йому кращий результат.

Якщо $\max\limits_i \min\limits_j a_{ij} = \min\limits_j \max\limits_i a_{ij} = \upsilon$, тобто, якщо $\alpha = \beta = \upsilon$, то гра називається цілком визначеною. У такому разі виграш загрози A (програш механізму захисту B) називається значенням гри і дорівнює елементу матриці $a_{i_0 j_0}$.

Цілком визначені ігри називають іграми із сідловою точкою, а елемент платіжної матриці, значення якого дорівнює виграшу загрози A (програшу механізму захисту B) і є сідловою точкою. У цій ситуації оптимальним рішенням гри для обох сторін є вибір лише однієї з можливих, так званих чистих стратегій – максимінної

для загрози *A* та мінімаксної для механізму захисту *B*, тобто якщо один із гравців притримується оптимальної стратегії, то для другого відхилення від його оптимальної стратегії не може бути вигідним. Такий приклад можемо розглядати як частковий випадок аналізу захищеності системи захисту інформації.

Також широке застосування отримала модель змішаної стратегії ведення гри – модель стратегії ведення гри, яка полягає у тому, що гравець застосовує одну із своїх чистих стратегій, обрану в кожній грі за випадковим законом.

Змішану стратегію можна ототожнити з імовірнісною мірою на множині можливих для гравця дій, тобто його чистих стратегій.

Уведенням змішаної стратегії розширюють клас допустимих дій гравця для того, щоб домогтися існування розв'язків гри, що вимагається принципом здійснення мети [11, 12].

Імовірності (або частоти) вибору кожної стратегії задають відповідними векторами: для загрози *A* – вектор $X=(x_1, x_2,..., x_m)$, де $\sum_{i=1}^{m} x_i = 1$; для механізму захисту *B* – вектор $Y=(y_1, y_2,..., y_n)$, де $\sum_{j=1}^{n} y_j = 1$. Очевидно, що $x_i \geq 0 \left(i=\overline{1,m}\right)$; $y_j \geq 0 \left(j=\overline{1,n}\right)$.

Виявляється, що коли використовуються змішані стратегії, то для кожної скінченної гри можна знайти пару стійких оптимальних стратегій. Існування такого розв'язку визначає основна теорема теорії ігор.

Теорема (основна теорема теорії ігор). Кожна скінченна гра має, принаймні, один розв'язок, можливий в області змішаних стратегій.

Нехай маємо скінченну матричну гру з платіжною матрицею:

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Оптимальні змішані стратегії гравців *A* і *B* за теоремою визначають вектори $X^*=(x_1^*, x_2^*,..., x_m^*)$ і $Y^*=(y_1^*, y_2^*,..., y_n^*)$, що дають змогу отримати виграш: $\alpha \leq \upsilon \leq \beta$.

Використання оптимальної змішаної стратегії загрозою *A* має забезпечувати виграш на рівні, не меншому, ніж ціна гри за умови вибору механізмом захисту *B* будь-яких стратегій. Математично ця умова записується так:

$$\sum_{i=1}^{m} a_{ij} x_i^* \geq \upsilon \left(j=\overline{1,n}\right).$$

З другого боку, використання оптимальної змішаної стратегії механізмом захисту *B* має забезпечувати за будь-яких стратегій загрози *A* програш, що не перевищує ціну гри υ, тобто

$$\sum_{j=1}^{n} a_{ij} y_j^* \geq \upsilon \left(i=\overline{1,m}\right).$$

Ці співвідношення використовують для знаходження розв'язку гри [13, 14].

Зауважимо, що в цьому разі розраховані оптимальні стратегії завжди є стійкими, тобто якщо один із гравців притримується своєї оптимальної змішаної стратегії, то його виграш залишається незмінним і дорівнює ціні гри υ незалежно від того, яку з можливих змішаних стратегій вибрав інший гравець.

Оптимальне рішення гри є його виграшем. Тому існують моделі оптимальних змішаних стратегій гри, основою яких є змішані моделі стратегій. Оптимальна модель стратегії гри у змішаних моделях стратегій має такі властивості: кожен гравець не зацікавлений у відході від своєї оптимальної змішаної стратегії, якщо його противник застосовує оптимальну змішану стратегію так, як йому не вигідно. Чисті стратегії гравців у їхніх оптимальних змішаних стратегіях мають назву активних.

Застосування оптимальної змішаної стратегії забезпечує гравцю максимальний середній виграш (або мінімальний середній програш), який дорівнює ціні гри, незалежно від того, які дії застосовує інший гравець, якщо тільки він не виходить за межі своїх активних стратегій. Такі оптимальні рішення більш імовірні для часткових прикладів під час аналізу проєктів окремих складових системи ЗІ.

Тому виникає необхідність розроблення методів оперативного (адаптивного) управління захистом інформації залежно від наявності апріорної інформації про можливість атак порушника й реалізовані ним стратегії створення НСД [15, 16].

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для характеристики поточного стану конфлікту будемо використовувати показник захищеності системи $a_{ij} = P_{зах}$ при реалізації в ній *i*-ї, $i \in I = \{1, 2, ... n\}$, стратегії (способу) захисту й застосуванні *j*-ї, $j \in J = \{1, 2, ... m\}$, стратегії (способу) створення контуру безпеки, *m* і *n* – кількість стратегій захисту і створення контурів безпеки, реалізованих у системі безпеки (СБ) і в системі порушника відповідно.

Стороною *A* назвемо підсистему оперативного управління ЗІ, стороною *B* – систему протидії цьому захисту, а величину a_{ij} – виграшем сторо-

ни A (програшем сторони B) у ситуації (i, j). За традиційного ігрового підходу до аналізу систем безпеки передбачається, що сторонам відома матриця гри і скінченна множина стратегій порушника, але невідомо, яка стратегія реалізується в конкретній ситуації. У цьому випадку в матричній грі формалізується ситуація вибору стратегій захисту в умовах невизначеності. Однак такий підхід не відображує динаміку конфлікту, а також можливість цілеспрямованого вибору стратегій захисту на кожному кроці залежно від інформації про дії системи порушника. Тому пропонується для опису розглянутого конфлікту використати модель крокової матричної гри із запізнюванням і помилками в інформованості сторін про дії порушника (матрично-ігрового процесу). Позначимо: $T_{СЗ}(T_{СП})$ – час однократної реалізації стороною A (B) своєї чистої стратегії; $t_{СЗ}(t_{СП})$ – час реакції сторони A (B), який дорівнює інтервалу часу від моменту початку реалізації стратегії стороною B (A) до моменту початку реалізації відповідної стратегії стороною A (B).

Будемо вважати, що сторонам відома: матриця гри $\mathbf{A} = (a_{ij})_m^n$, множини активних стратегій I, J і оцінки величин $T_{СЗ}(T_{СП})$ і $t_{СЗ}(t_{СП})$; матриця гри A є невиродженою і має рішення у вигляді ціни гри v і векторів оптимальних змішаних стратегій сторони $A - P^* = (P_1^*, P_2^*, ..., P_3^*, ..., P_n^*)$ і сторони $B - Q^* = (Q_1^*, Q_2^*, ..., Q_j^*, ..., Q_m^*)$; протягом часу гри T відсутня післядія, а множини I і J є незмінними.

Методика призначена для адаптивної зміни параметрів і режимів роботи СБ за ігровим алгоритмом залежно від наявності апріорної інформації про параметри системи порушника і стратегії створення нею атак на ІС.

Сутність ігрового алгоритму управління полягає в порівнянні великої кількості можливих у цих умовах якісно різних рішень, визначенні оптимального або найкращого з урахуванням всіх обмежень рішення та формування відповідної команди.

Для підвищення ефективності у разі вирішення динамічних ігор використовують метод прогнозування.

Одним із можливих рішень ігор у змішаних стратегіях є, як зазначалося вище, збільшення швидкості реакції (зниження часу адаптації) однієї зі сторін, що дозволяє підвищити результативність використання стратегій.

Розповсюджений спосіб рішення матричної гри у змішаних стратегіях, наприклад, методами лінійного програмування, істотно ускладнюється для матриць великої розмірності.

Застосування декомпозиційних методів не завжди можливе, а ітеративні методи рішення, такі, наприклад, як метод Брауна – Робінсона, мають найчастіше недостатньо високу швидкість збіжності. Як альтернативний може бути застосований метод динамічного програмування, що використовує результати короткочасного та довгострокового прогнозування [9].

Розглянемо алгоритм рішення матричних ігор, що використовує метод динамічного програмування. Стосовно до розглянутих випадків довгострокове прогнозування дозволяє з досить великим ступенем надійності обмежити кількість імовірних стратегій системи порушника й редукувати ігрову матрицю.

Рішенням матричної гри з урахуванням принципу прогнозування на основі марковського підходу є оптимізація умовної стратегії СБ на N циклів уперед по прогнозованій стратегії системи порушника. Очевидно, що зі зростанням N точність прогнозування знижується. У зв'язку із цим розглянемо випадок, коли $N = 1$. Можна виокремити три етапи алгоритму формування оптимальної стратегії СБ.

Методика управління системою безпеки на базі методів теорії ігор, блок-схема алгоритму реалізації, складається з таких етапів (рис. 1).

Уведення вихідних даних. Уводяться параметри засобів безпеки і каналу прийняття рішення $\Psi = \{\psi_i\}$, а також значення допустимої величини ймовірності помилкового приймання рішення .

Отримання інформації про дії системи порушника. За допомогою одного з методів контролю стану системи безпеки визначає стратегію або розпізнає факт дії на неї системи порушника.

Визначення оптимальної стратегії СБ. Задача оптимізації алгоритмів функціонування СБ полягає у визначенні такої оптимальної стратегії $à^* \in À^*$, при якій забезпечується максимальна ефективність функціонування СБ протягом необхідного часу функціонування. Для підвищення ефективності під час вирішення динамічних ігор використовується метод прогнозування.

Одним із можливих рішень ігор у змішаних стратегіях є, як зазначено вище, збільшення швидкості реакції (зниження часу адаптації) однієї зі сторін, що дозволяє підвищити результативність використання стратегій.

Коефіцієнт адаптації СБ залежить від співвідношення $T_{СБ}/T_{СП}$, а значення $T_{СБ}, T_{СП}$ – від тривалостей часу регулювання і зміни режимів роботи засобів захисту, які залежать від їхнього стану в попередньому циклі. Тривалість переходу СБ зі стану H_n у стан H_m на етапах регулювання (H_n і H_m – вектори станів засобів захисту) задається заздалегідь відомою квадратною матрицею часу переходу з будь-якого можливого (узятого з області визначення) стану в будь-який можливий.

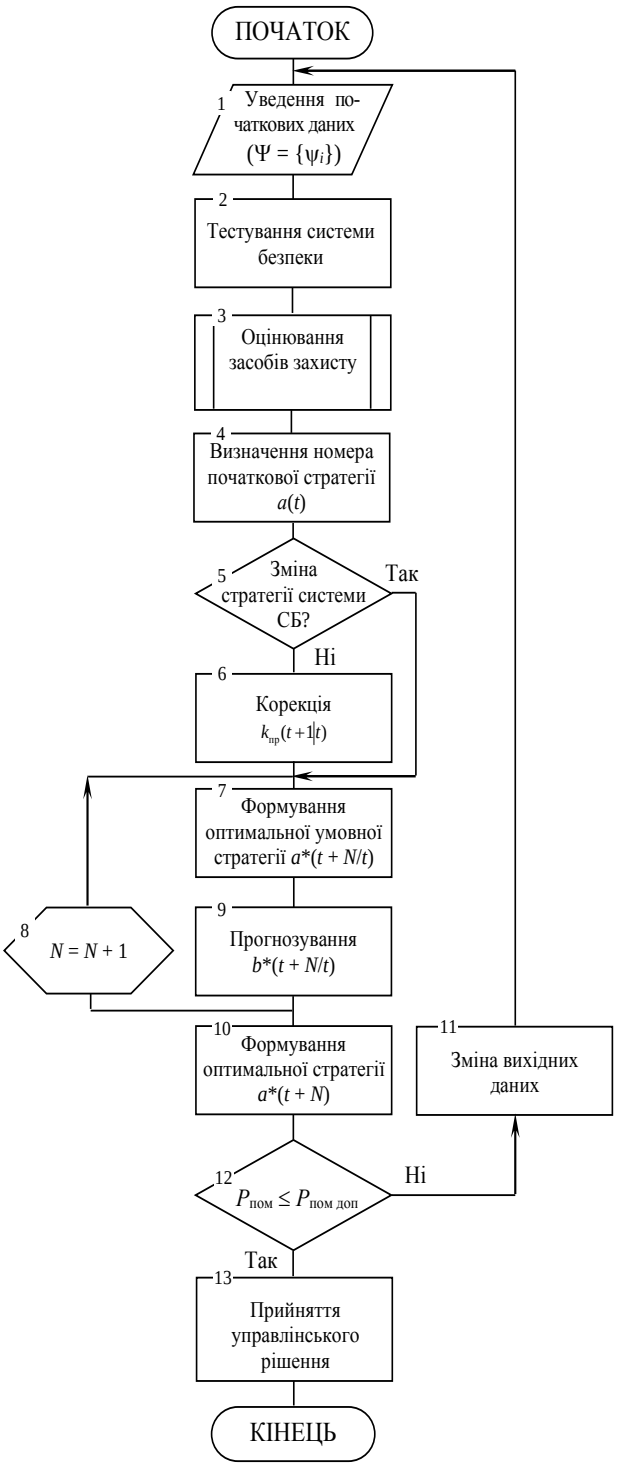

Рис. 1. Блок-схема алгоритму реалізації методики управління системою безпеки на основі моделі ігрового управління

Рис. 1. Блок-схема алгоритму реалізації методики управління системою безпеки на основі моделі ігрового управління

Елементами матриці будуть $T_{\text{СБ}nm}^{\text{рег}}$, що входять до складу $T_{\text{СБ}}^{H}$ на етапі регулювання параметрів і зміни режимів роботи системи. Тоді процес переходу з H_n в H_m з урахуванням можливих проміжних станів може бути описаний апаратом однорідних марковських ланцюгів із дискретними станами в дискретному часі. Порядок переходу від $H_n(t)$ до $H_m(t+1)$ задається відповідною стратегією $a_i \in S_{\text{СБ}}$. Аналогічний стан системи порушника при переході визначається як $H_{\text{СП}n}(t)$ і $H_{\text{СП}m}(t+1)$.

Тому задача умовної оптимізації часу адаптації на етапі регулювання полягає у виборі такої стратегії a^* на циклі $(t+1)$, при якій

$$\begin{cases} T_{\text{СБ}}((t+1),a^*) = \min\limits_{a_i \in S_{\text{СБ}}} T_{\text{СБ}}(H_n(t),H_m(t+1),a_i); \\ T_{\text{СП}}((t+2),a^*) = \max\limits_{a_i \in S_{\text{СП}}} T_{\text{СП}}(H_{\text{СП}n}(t+1),H_{\text{СП}m}(t+2),a_i) \end{cases} \quad (1)$$

за умови $T_{\text{СБ}} < T_{\text{СП}}$, що й відбувається у процесі рішення гри за рахунок уведення k_a під час розрахунку елементів матриці.

Чисельно точність передбачуваного значення функції виграшу задається деяким коефіцієнтом помилки прогнозування:

$$\left|R_{(\text{рег})nm}\right| N \times M,\ n = \overline{1,N},\ m = \overline{1,M}.$$

$$k_{\text{пр}}(t+1|t) = \frac{\Phi(t+1)}{\Phi_{RL}(t+1)},$$

де $\Phi_{RL}(t+1)$ обчислено в разі досягнення $(t+1)$ у результаті моніторингу. Так, у випадку незмінної протягом ряду циклів стратегії системи СП при $\Phi(t)$, відбувається корекція $\Phi(t+1)$ за рахунок $k_{\text{пр}}(t+1|t)$, що входить до складу коефіцієнта $\beta_m(t+1)$. Це усуває систематичну помилку в розрахунках значень $\Phi(t)$ і деякою мірою впливає на вибір $a^*(t+1)$ у ході рішення матричної гри.

Оскільки коефіцієнт помилки прогнозування перебуває у зворотній залежності від коефіцієнта інформованості k_{inf}^{a}, функція $f(k_{\text{inf}}^{a}) = \left|k_{\text{пр}}(t+1|t) - 1\right|$. У цьому випадку має місце постановка наступної задачі умовної оптимізації:

$$k_{\text{inf}}^{\hat{a}} \to \max,$$

де $\max k_{\text{inf}}^{\hat{a}} = k_{\text{inf}}^{S}$ при обмеженні

$$\left|k_{\text{пр}}(t+1|t) - 1\right| \le \delta_{\text{пом}},$$

де $\delta_{\text{пом}}$ – деяка центрована випадкова величина з нульовим математичним очікуванням і дисперсією δ^2, яка визначає деяке граничне значення помилки.

4. РЕЗУЛЬТАТИ

Розглянемо алгоритм рішення матричних ігор, що використовує метод динамічного програмування. Стосовно до розглянутих випадків довгострокове прогнозування дозволяє з досить великим ступенем надійності обмежити кількість імовірних стратегій системи порушника в наступних циклах управління до 2...4 і редукувати ігрову матрицю. Рішенням матричної гри з урахуванням принципу прогнозування на основі марковського підходу є оптимізація умовної стратегії СБ на N циклів уперед по прогнозованій

стратегії системи порушника. Очевидно, що зі зростанням N точність прогнозування знижується. У зв'язку із цим розглянемо випадок, коли $N = 1$. Можна виокремити три етапи алгоритму формування оптимальної стратегії СБ.

На першому етапі на підставі інформації про поточний стан засобів захисту, передбачуваного значення перехідних ймовірностей СБ, яка застосовує на циклі управління t стратегії системи порушника $b(t)$, а також з урахуванням попередніх стратегій СП формується оптимальна умовна стратегія $\grave{a}^*(t+1)t$:

$$a^*(t+1)t = \arg\left[\max_{a\in S_{СБ}} P(a(t), b(t), H(t))\right]. \quad (2)$$

На другому етапі розв'язується завдання прогнозування стратегії, яка використовується на циклі управління $t+1$ системою порушника і яка забезпечить мінімізацію функціонала

$$b^*(t+1)t = \arg\left[\min_{b\in S_{РЕП}} P(a^*(t+1), b(t+1))\right]. \quad (3)$$

На третьому етапі формується оптимальна стратегія управління СБ з урахуванням прогнозованої стратегії системи порушника і поточного стану засобів захисту:

$$a^*(t+1|t) = \arg\begin{bmatrix} \max\limits_{a\in S_{SS}} P(a(t+1), \\ b^*(t+1|t), \\ H(t+1), \\ \beta_m(t+1), \\ k_a(H(t+1)|H(t))) \end{bmatrix}. \quad (4)$$

Для підвищення надійності результату алгоритм може повторюватися обмежену кількість разів за наявності певної дисперсії розподілу ймовірностей застосування стратегії $a_1^*(t+1|t)\ldots a_n^*(t+1|t)$ з їх наступним оцінюванням на основі критеріїв переваги, що вводяться. У випадку неможливості визначення такої стратегії $a^*(t+1)$, за якої втрати не перевищують припустимого значення, розв'язується завдання розширення множини допустимих стратегій СБ, після чого знову визначається $a^*(t+1)$. Аналогічно формують стратегії СБ шляхом оптимізації умовної стратегії управління СБ по прогнозованій на N кроків стратегії системи порушника. Третій етап алгоритму в цьому випадку матиме вигляд

$$a^{*(N)}(t+N) = \arg[\max_{a\in S_{SS}} P(a(t+N), b^*(t+N|t+N-1), H(t+N), \beta_m(t+N), k_a(H(t+N)|H(t+N-1))], \quad N = 2, 3\ldots \quad (5)$$

Апарат марковських кіл використовується на другому і третьому етапах, що дозволяє розраховувати ймовірності застосування тієї або іншої стратегії на черговому циклі управління і вибору оптимальної стратегії.

Припустимо, що в циклі управління t використовується стратегія системи порушника: b_2. Нехай, за критерієм $\max_{\grave{a}_1} P_{i,2}(t) = P_{3,2}$ вибирається стратегія a_3 (табл. 1).

***Таблиця* 1**

Алгоритм прогнозованого переходу станів СБ

t	**Процес прогнозування**					$t+1$
1-й етап	**2-й етап**			**3-й етап**		
Рішення на циклі	Імовірність переходу $P_{3j} = 1 - k_N \Phi_{3j}$	$\min\limits_{b_j}(1 - P_{3_j}(t+1))$		Імовірність переходу $P_{i4} = k_N \Phi_{i4}$	$\max\limits_{a_1} P_{i2}(t+1)$	
a_3	P_{31} ⇒	b_1	b_4	P_{14} ⇒	a_1	a_{12}
	P_{32} ⇒	b_2		P_{24} ⇒	a_2	
	P_{33} ⇒	b_3		P_{34} ⇒	a_3	
	P_{34} ⇒	b_4		P_{44} ⇒	a_4	
	…	…		…	…	
	P_{3j} ⇒	a_j		P_{i4} ⇒	a_{i4}	
a_3; b_2						a_2; b_4

Одночасно із цим реалізується алгоритм прогнозування. У табл. 1 представлено спрощений приклад прогнозованого переходу системи зі стану в циклі t у стан $(t+1)$ на основі неоднорідних марковських кіл. Відповідно до принципу оптимальності, у разі пошуку оптимального рішення в багатокроковому завданні оптимізації вибір стратегії управління $a(t)$ на кожному кроці незалежно від початкового стану має бути спрямований на оптимізацію не тільки даного, але й усіх наступних

кроків. З урахуванням прогнозування на (t + N) кроків уперед (у цьому випадку, не більше трьох кроків) механізм вибору оптимальної стратегії $a^*(t)$ у циклі t буде також визначатися обчисленням зворотної функції Беллмана останніх прогнозованих $N - t + 1$ циклів управління. Так, для $t = N$:

$$B_N(H(N-1)) = \max_{a(N)\in\Lambda_N^I(H(N-1))} P_N(H(N-1),a(N)),$$

де $H(N–1)$ – стан СБ на (N–1)-му циклі управління; a(N) – стратегія управління на циклі N; $\Lambda_N(\acute{I}\ (N-1))$ – скінченна множина допустимих стратегій на циклі (N – 1).

Метод Беллмана використовують для підвищення точності прогнозу, обґрунтованості вибору поточних стратегій і підтримки прийняття рішень пристроєм управління системи безпеки.

Основні проблеми за використання теорії ігор виникають під час визначення функції виграшу для конкретної ситуації. Для завдань, які розв'язує СБ-функція виграшу, у першу чергу, повинна відображати зміну якості системи безпеки.

Розглянемо приклад, що відображає реальну ситуацію, що описана матрицею виграшу 2×2. Розмірність указує на кількість чистих стратегій у гравців. Як гравці виступають СБ і СП. Вибір цих прикладів обумовлений такими міркуваннями. Гра 2×2 дозволяє яскраво продемонструвати можливості й обмеження теорії ігор.

СБ і СП можуть вибрати різні змішані стратегії: для СБ маємо $S^*_{\text{СБ}} = (P_1,\ 1–P_1)$, для СП – $S^*_{\text{СП}} = (P_2,\ 1–P_2)$. У результаті рішення гри мають бути отримані оптимальні стратегії гравців і значення гри, тобто трійка $(S'_{\text{СБ}}, S'_{\text{СП}}, V')$. У нашому випадку потрібно визначати P'_1 і P'_2. Значенням гри буде математичне очікування ймовірності правильного прийняття рішення, обчислене з урахуванням усіх можливих ситуацій.

У табл. 2 і на рис. 2 наведено результати вирішення гри.

Оптимальними стратегіями з позиції теорії ігор є: $P'_1 = 0{,}466$ і $P'_2 = 0{,}534$. Отже, СБ повинна вибирати перший режим роботи з імовірністю 0,466, а другий з імовірністю 1 – 0,466 = 0,534. Система СП має вибирати свої режими з імовірностями 0,534 і 0,466. Видно, що, вибравши оптимальну стратегію, СБ гарантовано забезпечить собі математичне очікування виграшу 0,466 незалежно від того, як діятиме супротивник.

Виграш невеликий, але зрозуміло, що математичне очікування величини не може бути більше 0,5, якщо в половині випадків вона набуває нульових значень. Причому, якщо СП дотримується оптимальної стратегії, то підвищити математичне очікування ймовірності правильного прийняття рішення при забезпеченні контуру безпеки не вдасться.

Якщо вказана ситуація не влаштовує СБ, то слід вживати заходів щодо підвищення виграшу за певних поєднань методів і засобів безпеки. Проте видно, що якщо СП відхиляється від своєї оптимальної стратегії, то СБ має можливість підвищити свій виграш, також відхилившись від оптимальної стратегії.

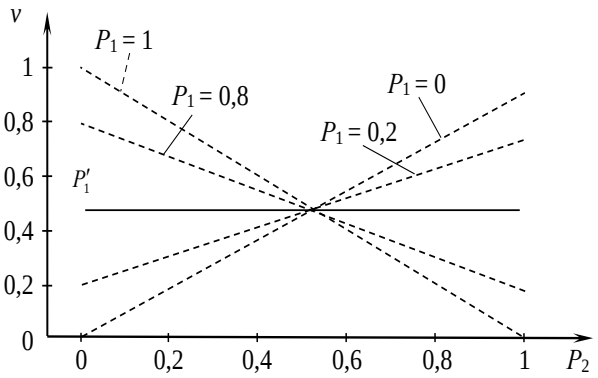

Рис. 2. Залежності виграшу від вибору стратегій СБ і СП

Рис. 2. Залежності виграшу від вибору стратегій СБ і СП

***Таблиця* 2**

Виграш у разі різних стратегій СБ і систем порушника

P_1 \ P_2	0	0,2	0,4	0,6	0,8	1	P'_2 =0,534
0	0	0,175	0,349	0,524	0,699	0,874	0,466
0,2	0,200	0,300	0,399	0,499	0,599	0,699	0,466
0,4	0,400	0,425	0,450	0,474	0,499	0,524	0,466
0,6	0,600	0,550	0,500	0,450	0,399	0,349	0,466
0,8	0,800	0,675	0,550	0,425	0,300	0,175	0,466
1	0,999	0,800	0,600	0,400	0,200	0	0,466
P'_1 = 0,466	0,466	0,466	0,466	0,466	0,466	0,466	0,466

5. ВИСНОВКИ

Таким чином, у процесі умовної оптимізації з урахуванням поточної ігрової матриці будуть формуватися умовно оптимальні стратегії, що визначають фазову траєкторію СБ, починаючи із заключного циклу прогнозування $t = N$ до поточного значення t.

Основні проблеми під час використання теорії ігор виникають при визначенні функції виграшу для конкретної ситуації. Для завдань, які розв'язує система безпеки, функція виграшу, у першу чергу, має відображати зміну якості системи безпеки.

У разі, якщо вказана ситуація не влаштовує СБ, слід вживати заходів щодо підвищення виграшу за певних поєднань методів і засобів захисту.

Якщо зловмисник відхиляється від своєї оптимальної стратегії, то СБ має можливість підвищити свій виграш, також відхилившись від оптимальної стратегії.

Результати імітаційного моделювання процесу функціонування СБ за запропонованим ігровим алгоритмом показав, що додаткове застосування прогнозування стратегії на *N* циклів уперед дозволяє підвищити ефективність функціонування системи на 5–8 %.

Отже, теорія ігор дозволяє запропонувати рекомендації з формування стратегії управління режимами роботи систем захисту. Причому, принаймні, для певних типів конфліктів і матриць виграшів ці рекомендації дозволяють СБ отримати виграш і досягнути поліпшення своїх технічних характеристик.

Аналіз виграшу, який отримує СБ в різних ситуаціях, показав, що теорія ігор не тільки дозволяє сформувати оптимальну стратегію, що забезпечує гарантії певного виграшу, але й дає змогу видати рекомендації з її зміни з метою збільшення виграшу, якщо система порушника відступає від своєї оптимальної стратегії. Коли система порушника слідує своїй оптимальній стратегії, теорія ігор дозволяє оцінити цю ситуацію. Якщо результати оцінювання не влаштовують, то необхідно вживати заходів зі зміни ситуації.

Подальші напрямки досліджень на основі теорії ігор. Застосування ігрового підходу до розв'язання проблем безпеки (що включає моделювання, постановку проблеми і її розв'язання) усе ще сильно залежить від вибраної схеми ігрової взаємодії користувачів, яка, як правило, є спрощенням реального світу. Наприклад, якщо розглядаються ігри між одним нападником і системою захисту, то використовують ігри двох учасників. Якщо ситуація розгортається у часі, використовують динамічну постановку. Важливим є також припущення про інформованість учасників, залежно від чого використовуються ігри з досконалою або недосконалою та повною або неповною інформованістю.

Найбільш перспективні можливі напрямки досліджень, у яких буде розвиватись теоретико-ігровий підхід у області кібербезпеки, – це хмарні технології. Сучасна хмарна система існує в середовищі постійних змін. Змінюються технології, протоколи та програмне забезпечення. Змінюються користувачі, їхні пріоритети, задачі й поведінка. Усі ці зміни є непередбачуваними. Тому теорія ігор, яка вже має історію успішного застосування до розв'язання задач маршрутизації, планування, керування потоками даних і перевантаженнями, є головним напрямком аналітичного моделювання хмарних систем. Застосування теорії ігор використовують у технологіях інтернет-речей, що об'єднує в одну мережу всі розумні прилади, що вже в недалекому майбутньому забезпечуватимуть людське життя. Проникнення розумних речей у наше життя стає тотальним, а тому і загрози, які при цьому виникають, також є тотальними. Слід виокремити технологію блокчейн, на основі якої будуються криптовалюти і деякі нові сервіси. Однією з ключових проблем є забезпечення ефективного та безпечного "майнингу" (тобто обчислення підтвердження нових операцій або одиниць валюти). Теорія ігор моделює процес майнингу як взаємодію автономних агентів, що конкурують за ресурси. Враховуючи сучасну вартість криптовалюти біткоїн, атака на механізми обчислення може бути надзвичайно прибутковою. Таким чином можна сказати, що застосування теоретико-ігрового підходу до проблем безпеки, хоч і продовжується два десятиліття, усе ще є новим підходом із багатьма нерозв'язаними проблемами. Складність ігор із багатьма учасниками за умов конфлікту і невизначеності стимулює дослідників до створення нових моделей і методів, які допоможуть створити новий безпечний і ефективний кіберпростір.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Fei He, Jun Zhuang, and United States. Game-theoretic analysis of attack and defense in cyber-physical network infrastructures. In Proceedings of the Industrial and Systems Engineering Research Conference. 2012.

[2] Johnson, Benjamin, et al. "Game-theoretic analysis of DDoS attacks against Bitcoin mining pools." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014.

[3] Бурячок В. Теорія ігор, як метод управління інформаційною безпекою / Володимир Бурячок, Анатолій Шиян // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2013. – Вип. 2(26). – С. 21–28.

[4] Петросян Л.А. Теория игр / Л.А. Петросян, Н.А. Зенкевич, Е.А. Семина. – М.: 1998. – Вища школа. – 304 с.

[5] Дюбин Г.Н. Введение в прикладную теорию игр / Г.Н. Дюбин, В.Г. Суздаль. – М.: 1981. – Наука. – 336 с.

[6] Воробьев Н.Н. Бесконечные антагонистические игры / под ред. Н.Н. Воробьева. – М.: 1993. – Вища школа. – 505 с.

[7] Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор та диференціальних перетворень / Р.В. Грищук. – Монографія. – Житомир. – 2010. – 280 с.

[8] Дослідження операцій. Ч. 3. Ухвалення рішень і теорія ігор / М. Я. Бартіш, І. М. Дудзяний. – Львів: Видавничий центр Львівського національного університету ім. І. Франка, 2009 . – 277 с. : іл. – Бібліогр.: с.271–272 (36 назв) . – ISBN 966-613-496-9

[9] Baranovska L. V. Mixed strategy Nash equilibrium in one game and rationality / L. V. Baranovska, O. M. Bukovskiy // International Scientific and Practical Conference "WORLD SCIENCE". Proceedings of the III International Scientific and Practical Conference "Scientific Issues of the Modernity" (April 27, 2017, Dubai, UAE). – 2017. – No 5(21), Vol. 1, May. – Pp. 4–8.

[10] Alpcan T., Başar T. Network security: A decision and game-theoretic approach. Cambridge University Press, 2010.

[11] Толюпа С.В., Павлов І.М. Аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації. // Науково-технічний журнал "Сучасний захист інформації". – 2014. – №2. – С. 96–104.

[12] Толюпа С.В., Павлов І.М. Аналіз підходів оцінки ефективності математичних моделей при проектуванні систем захисту інформації. // Науково-технічний журнал "Сучасний захист інформації". – 2014. – №3. – С. 36–44.

[13] Alpcan T., Başar T. A game theoretic approach to decision and analysis in network intrusion detection. Decision and Control, 2003. Proceedings. 42nd IEEE Conference on. Vol.

[14] Roy, Sankardas, et al. A survey of game theory as applied to network security. System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, 2010.

[15] Liang, Xiannuan, and Yang Xiao. Game theory for network security. IEEE Communications Surveys & Tutorials 15.1. 2013. P. 472–486.

[16] Do, Cuong T., et al. Game Theory for Cyber Security and Privacy. ACM Computing Surveys (CSUR) 50.2. 2017. 30 p.

Стаття надійшла до редколегії **14.10.2020**

Formation of a strategy for managing the modes of operation of protection systems based on the game management model

The main areas of application of game theory are economics, political science, tactical and military-strategic tasks, evolutionary biology and, more recently, information technology, security and artificial intelligence. Game theory studies the problems of decision-making of several people (players). It concerns the behavior of players whose decisions affect each other. The application of game theory in the field of modeling decision-making processes has different approaches, which are not systematized in the future, and sometimes contradict each other. Game theory is designed to solve situations in which the outcome of players' decisions depends not only on how they choose them, but also on the choices of other players with whom they interact. If we consider the field of information security, the peculiarity of the information conflict between the operational management system of information protection and the infringer who tries to gain unauthorized access is that opposing parties who have several ways of action can apply them repeatedly, choosing the best way based on information about the opposite parties. In this case, each step of resolving the conflict is characterized not by the final state, but by some payment function. In many situations, when designing information security systems, there is a need to develop and make decisions in conditions of uncertainty. Uncertainty can be of different nature. The planned actions of hackers, which are aimed at reducing the effectiveness of security systems, are uncertain. Uncertainty may relate to a risk situation in which the management system of the information network that decides on the application of the protection system is able to establish not only all possible results of decisions, but also the probability of possible conditions for their occurrence. Design conditions affect decision-making subconsciously, regardless of the actions of the decision-maker. When all the consequences of possible decisions are known, but their probability is unknown, it is obvious that decisions are made in conditions of complete uncertainty. The main promising theory of analysis of decision-making processes at the stage of designing information security systems is game theory. Therefore, there is a need to develop methods of operational (adaptive) management of information protection, depending on the availability of a priori information about the possibility of attacks by the infringer and his strategy to create unauthorized access to information resources. Game theory allows us to offer recommendations for the formation of management strategies for protection systems.

Keywords: *information protection; security system; game theory; optimal strategy; system of the violator; making a decision.*

Сергій Толюпа,
доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Serhii Toliupa,
Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.

Наталія Лукова-Чуйко,
доктор технічних наук, професор завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Natalia Lukova-Chuiko,
Doctor of Technical Sciences, Professor, Head of the Department of Cybersecurity and Information Protection of the Kyiv National Taras Shevchenko University of Kyiv.

Володимир Наконечний,
доктор технічних наук, старший науковий співробітник, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Volodymyr Nakonechnyi,
Doctor of Technical Sciences, Senior Research Fellow, Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.

Володимир Сайко,
доктор технічних наук, професор, професор кафедри прикладних інформаційних систем Київського національного університету імені Тараса Шевченка.

Volodymyr Saiko,
Doctor of Technical Sciences, Professor, Professor of the Department of Applied Information Systems, Taras Shevchenko National University of Kyiv.

Олег Куліныч,
кандидат технічних наук, доцент, доцент спеціальної кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Oleg Kulinich,
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Special Department of the Institute of Special Communications and Information Protection of the National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky".