УДК 004.415.056.5(075) **І.М. Павлов, С.В. Толюпа**

АНАЛІЗ ПІДХОДІВ МОДЕЛЮВАННЯ ПРОЦЕСІВ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПРОЕКТУВАННІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇМ.

Пропонується класифікація теорії ігор по класам в напрямку захисту інформації. Надані авторами підходи моделювання процесів прийняття рішень, під час проектування систем захисту інформації, у подальшому надають можливість розкрити ознаки класу ефективності математичних моделей прийняття рішень. Надано класифікацію математичних моделей теорії прийняття рішень при проектування систем захисту інформації, яку можливо застосовувати як під час проектування систем захисту інформації, так і процесів, які моделюються для оцінки ефективності систем захисту інформації у різних життєвих циклах роботи.

Ключові слова: загрози, гравці, коаліції, механізми захисту, моделі, теорія ігор, системи захисту інформації, стратегії.

Постановка проблеми

У багатьох ситуаціях проектування систем захисту інформації виникає необхідність розробки та прийняття рішень в умовах невизначеності. Невизначеність може мати різний характер. 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 по застосуванню системи захисту, здатна встановлювати не тільки усі можливі результати рішень, але й вірогідність можливих умов їх появи. Умови проектування впливають на прийняття рішень підсвідомо, незалежно від дій суб'єкта, що приймає рішення. Коли відомі всі наслідки можливих рішень, але невідома їх вірогідність, очевидно, що рішення приймають в умовах повної невизначеності. Основною перспективною теорією аналізу процесів прийняття рішень на етапі проектування систем захисту інформації є теорія ігор. Застосування теорії ігор в області моделювання процесів прийняття рішень має різні підходи, які в наступний час не систематизовані а інколи і вступають в протиріччя між собою.

У зв’язку з цим, аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації та обґрунтування класифікації таких підходів, є актуальними науковими завданнями.

Аналіз останніх досліджень і публікацій дає змогу дійти висновку, що сучасні методичні підходи розрізнені, неповні, а у деяких випадках суперечливі.

Так, використання математичного аналізу [1] дає змогу обґрунтувати лише часткові данні класифікації моделей теорії ігор такі як, кількість зацікавлених сторін та кількість коаліцій дій гравців. Математичні моделі аналізу [2] розкривають тільки моделі за результатами гри, за характером та об’ємом інформації, в залежності від кількості можливих стратегій. Джерело [3] розкриває моделі за кількістю коаліцій дій гравців, за виграшем гри, за характером отримання інформації, за кількістю стратегій. Автори [4] розкривають тільки класичні кооперативні ігри, не вдаючись до їх місця у загальній теорії ігор. Автори [5] у загалі надають приклади безкінцевих антагоністичних ігор не розкриваючи класифікації математичних підходів теорії ігор. Автор [6] розкриваючи моделі статистичних та динамічних ігор і будуючи математичні перетворення в інтересах моделювання нападів на інформацію, зовсім не визначив місце і роль математичних моделей теорії ігор в аналізі систем захисту інформації. Надаючи обґрунтування доцільності застосування теорії ігор для моделювання процесів нападу на інформацію автор [6] пропонує такі перетворення тільки для 2-х гравців, що є частковим прикладом коаліційної гри, а не питання розгляду роботи системи захисту інформації у цілому. Особливо це важливо при розгляді питань аналізу систем захисту інформації під час проектування.

Для проведення аналізу процесів прийняття рішення розробнику необхідно мати чітку уяву місця своїх досліджень в предметній області. Пропонуючи основні результати досліджень в області захисту інформації необхідно відштовхуватися від зрозумілих посилань

на місце аналітичних моделей прийняття рішень в процесі моделювання роботи систем захисту інформації.

Таким чином, *метою статті є* надання системного аналізу підходам моделювання процесів прийняття рішень при проектуванні систем захисту інформації.

Основна частина

Усі математичні моделі теорії ігор, які застосовуються для прийняття рішень при проектування систем захисту інформації, умовно можна поділити на 2 класи: клас моделювання процесів прийняття рішень та клас оцінки ефективності математичних моделей прийняття рішень (рис. 1.).

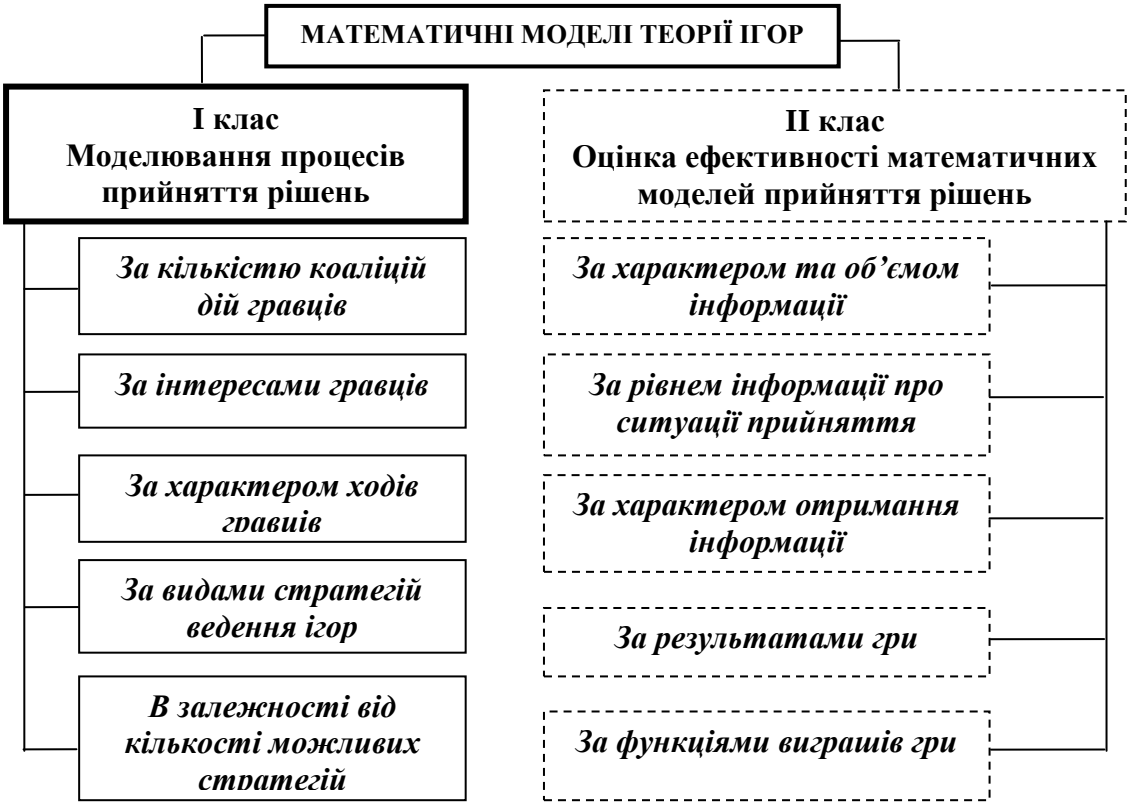

Рис. 1. Загальна класифікація математичних моделей теорії ігор при проектування систем захисту інформації

Першою ознакою класу моделювання процесів прийняття рішень є ***кількість коаліцій гравців*** (рис. 2). Перш за все відомо, що розгляд ігор з пустою множиною коаліцій дій немає сенсу: множина ситуацій складається не більш чим з одного елемента і питання про відношення переваги не виникає. Якщо в грі (у нашому випадку гра розуміється як процес протиборства загроз – з одної сторони і механізмів захисту – з іншої сторони) мається хоча б одна (і тільки одна) коаліція дій K, (наприклад, коаліція механізмів захисту), то дослідження гри становиться змістовним. У цьому випадку мається єдина множина стратегій S_k, а множина усіх ситуацій є її підмножиною: $S \subset S_k$. Тому розгляд моделі гри можна починати з цієї множини ситуацій, рахуючи їх стратегіями однієї коаліції дії. Оскільки для таких моделей гри стратегії співпадають з ситуаціями, термін "стратегія" можна до них не застосовувати. У зв'язку з тим такого роду моделі мають назву ***нестратегічних***. До числа нестратегічних моделей ігор відносяться ***кооперативні ігри*.**

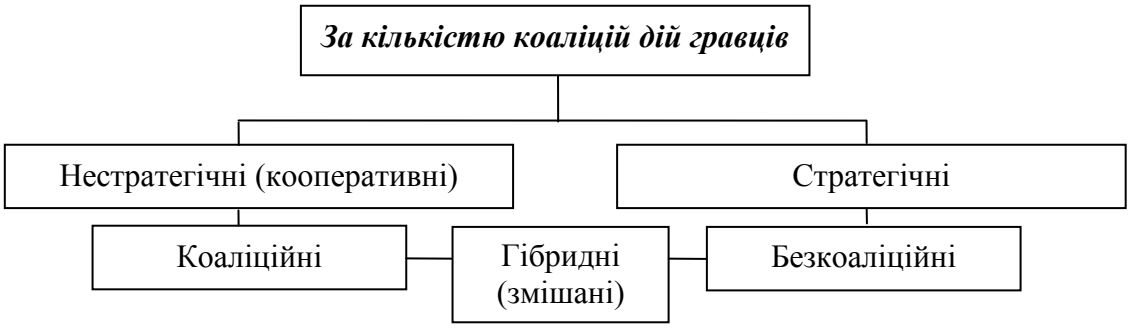

Рис. 2. Класифікація математичних моделей теорії ігор за кількістю коаліцій дій гравців класу моделювання процесів прийняття рішень при проектуванні систем захисту інформації

Прикладом нестратегічної (кооперативної) моделі гри може служити проста модель гри, яка складається з наступного. У неї множиною ситуацій є все можливі розподіли між гравцями деякої кількості однозначної корисності. Кожний розподіл описується теми сумами переваг, які при цьому отримують окремі гравці (механізми захисту). Коаліція інтересів є виграшною, якщо вона може (навіть в умовах протидії усіх інших гравців) присвоїти та розподілити між своїми членами (кооперативом) усю корисність, яка є. Усі коаліції (*коаліційні моделі*), які не є виграшими, зовсім не можуть присвоїти яку-небудь долю корисності. Такі коаліції є програшними. Зазвичай рахується, що виграшна коаліція припускає один розподіл іншому, якщо доля кожного з її членів в умовах першого розподілу більше, чим в умовах другого. Програвши коаліції не можуть порівнювати розподіли за перевагою (ця умова також зрозуміла: коаліція інтересів, яка сама не в стані добитися нічого, змушена погоджуватися на будь-який розподіл і не має можливості вибору між розподілами).

Якщо в моделі грі мається більш однієї коаліції дій, то така модель гри стає ***стратегічною***. Важливий клас моделей стратегічних ігор складають ***безкоаліційні моделі ігри***, в яких коаліції дій співпадають з коаліціями інтересів (гравців), а переваги для гравців описуються їх функціями виграшів: гравець віддає перевагу іншої ситуації, якщо в першій ситуації він отримує більший виграш, чим в другій.

Одним з простих прикладів моделі безкоаліційної гри може служити наступна модель гри: три загрози одночасно впливають на 1 або 2 механізма захисту кожен. Якщо усі три загрози впливають на один і той-же механізм захисту, то виграш кожної загрози дорівнює нулю (по відношенню до загроз). У протилежному випадку один з механізмів захисту показує $a = 1$, або $a = 2$, а інші показують $b \neq a$, то перший механізм захисту має виграш, а інші не отримують нічого. У безкоаліційних моделях ігор гравці домагаються до ситуацій рівноваги, тобто до таких ситуацій, відхилення від яких окремого гравця (при цьому інші гравці не змінюють своїх стратегій) може привести до його програшу.

Частіше рахують, що моделі кооперативних ігор відрізняються можливістю спілкування гравців друг з другом. У загальному випадку це невірно. Існують моделі ігор, де комунікація дозволена, але гравці переслідують особисті цілі та інше, що важливо для досліджень систем захисту інформації. З двох типів моделей ігор ***некооперативні*** описують ситуації у дрібних деталях і видають більш точніші результати. Моделі кооперативних ігор розглядають процес гри у цілому.

Гібридні (змішані) моделі ігор включають до себе елементи кооперативних і некооперативних ігор. Наприклад, загрози або механізми захисту можуть утворювати групи, але гра буде вестися в некооперативному стилі. Це визначає наступне, що гравець буде

слідкувати інтересам своєї групи, але стараючись досягти особистої користі, це важливо для дослідження роботи механізмів захисту у складі системи захисту інформації.

За інтересами гравців моделі ігор можна представити як антагоністичні та неантагоністичні (рис. 3).

Рис. 3. Класифікація математичних моделей теорії ігор
за інтересами гравців класу моделювання процесів прийняття рішень при проектуванні систем захисту інформації

Антагоністична модель гри (гра з нульовою сумою англ. *zero-cum*) – це модель кооперативної гри, у якій приймають участь два гравця, виграші яких протилежні. Така модель є частковим випадком аналізу гри загрози і механізму захисту.

Формально модель антагоністичної гри може бути представлена трійкою $\langle x, y, f \rangle$, де *x*, *y* – множини стратегій першого і другого гравців, відповідно; f – функція виграшу першого гравця, яка ставить у відповідність кожній парі стратегій (ситуацій) $x \in X, y \in Y$ дійсне число, яке відповідає корисності першого гравця при реалізації цієї ситуації. Історично антагоністичні ігри є першим класом математичних моделей теорії ігор, за допомогою яких описуються азартні ігри. У наступний час антагоністичні ігри розглядаються як частина більш широкого класу некооперативних ігор.

Найпростішим прикладом антагоністичної гри є гра “Орлянка”. перший гравець скриває монету орлом або решкою вгору, а другий вгадує де вона схована. Якщо він не вгадає – він сплачує одну грошову одиницю, якщо вгадає – перший сплачує йому одну грошову одиницю. У цій грі кожен гравець має дві стратегії “орел” та “решка”. Множина ситуацій у грі складається з 4-х елементів. У строках таблиці вказані стратегії першого гравця – *x*, у стовбцях – стратегії другого гравця – *y*. Для кожної ситуації вказуються виграші першого і другого гравців (таблиця 1).

Таблиця 1

Виграші гравців

X/*Y*	**Орел**	**Решка**
Орел	-1, 1	1, -1
Решка	1, -1	-1, 1

У аналітичному вигляді функція виграшу першого гравця має наступну форму:

$$F_1(x, y) = \begin{cases} 1, & при \quad x \neq y \\ -1, & при \quad x = y \end{cases}, \tag{1}$$

де $x \in X, y \in Y$ – стратегії першого і другого гравців, відповідно. Так як виграш першого гравця дорівнює програшу другого, то $F_2(x, y) = -F_1(x, y)$. Якщо результат повністю визначається гравцем, який здійснив останній крок (якщо правила кроків ідентичні для гравців), стратегія може бути знайдена за допомогою функції Гранді:

$$G(x) = \min\{n \geq 0 : n \neq G(y), y \in F(x)\}, \quad (2)$$

де n – будь-яке позитивне число; y – одна з позицій, у яку можна перейти безпосередньо з позиції x за один крок; $G(y)$ – значення Шпрага-Гранді, у які можна перейти безпосередньо з позиції x за один крок; $F(x)$ – список позицій, у які можна перейти безпосередньо з позиції x за один крок. Таким чином, $G(x)$ – найменше негативне ціле число, яке не знайдене серед значень Шпрага-Гранді для визначених x.

У неантагоністичних моделях ігор гравці переслідують різні, але не прямо протилежні цілі (такі моделі частіше використовують при аналізу економічних ситуацій) (рис. 4).

За характером ходів гравців моделі гри можна поділити на особисті та випадкові. Розвиток гри в часі представляється з ряду послідовних етапів або рухів. ***Особистою моделлю ходу*** називають свідомий вибір одним з гравців одного з можливих в цієї ситуації ходів і його виконання. Прикладом особистого ходу є будь-який з ходів у грі в шахи.

Рис. 4. Класифікація математичних моделей теорії ігор за характером ходів гравців класу моделювання процесів прийняття рішень при проектуванні систем захисту інформації

Виконуючи черговий хід, гравець робить свідомий вибір одного з варіантів, можливих при розташуванні фігур на дошці. Набір можливих варіантів при кожному особистому ході регламентований правилами гри і залежить від усієї сукупності попередніх ходів обох сторін. Така модель не притаманна аналізу систем захисту інформації, але її можливо розглядати для аналізу роботи технічних засобів захисту інформації, інформація про роботу яких відома.

Випадковою моделлю ходу гравця є вибір з ряду можливостей, який виконується не рішенням гравця, а яким-небудь механізмом випадкового вибору (киданням монети, грального кості, тасування та здачі карт і т.п.). Наприклад, здача першої карти одному з гравців в преферанс є випадковий хід з 32 рівноможливими варіантами. Щоб гра була математично визначеною, правила гри повинні для кожного випадкового ходу вказувати розподіл вірогідностей можливих результатів. Деякі моделі ігри можуть складатися з випадкових ходів (притаманно аналізу роботи систем захисту інформації) або тільки з особистих ходів (шахи, шашки). Більшість карточних ігор належить до ігор змішаного типу, або ***змішаних моделей гри***, тобто складаються як з випадкових, так і особистих моделей гри. Також змішанні моделі необхідно розглядати для проектування систем захисту інформації, коли використовуються відомі особисті моделі технічних засобів захисту та випадкові моделі роботи самої системи захисту інформації.

За видами стратегій ведення ігор моделі можуть бути чистими, змішаними, оптимальними (рис. 5).

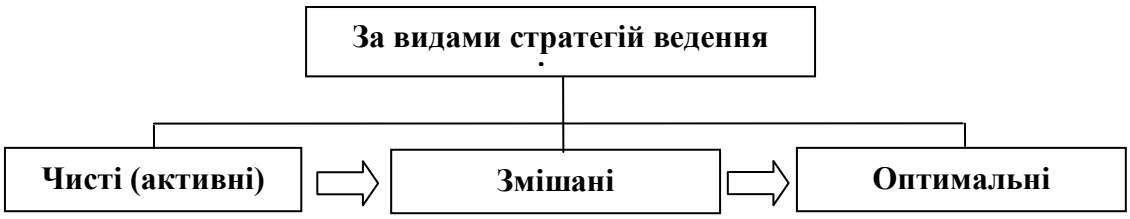

Рис. 5. Класифікація математичних моделей теорії ігор
за видами стратегій ведення ігор класу моделювання процесів прийняття
рішень при проектуванні систем захисту інформації

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

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

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

Механізм захисту В, який програє суми у розмірі елементів платіжної матриці, навпаки має вибрати стратегію, що мінімізує його максимально можливий програш за всіма варіантами дій загрози А. Стратегія механізму захисту В 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 $\max \min a_{ii} = \min \max a_{ii} = \upsilon$, тобто, якщо $\alpha = \beta = \upsilon$, то гра називається *цілком визначеною*. В такому разі виграш загрози А (програш механізму захисту В) називається *значенням гри* і дорівнює елементу матриці $a_{i_0 i_0}$.

Цілком визначені ігри називаються *іграми з сідловою точкою,* а елемент платіжної матриці, значення якого дорівнює виграшу загрози А (програшу механізму захисту В) і є сідловою точкою. В цій ситуації оптимальним рішенням гри для обох сторін є вибір лише однієї з можливих, так званих чистих стратегій — максимінної для загрози А та мінімаксної для механізму захисту В, 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.

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

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

Введенням змішаної стратегії розширюють клас допустимих дій гравця для того, щоб домогтися існування розв'язків гри, яке вимагається принципом здійснення мети.

Ймовірності (або частоти) вибору кожної стратегії задаються відповідними векторами:

для загрози А – вектор $X=(x_1,x_2,...,x_m)$, де $\sum_{i=1}^{m}x_i=1$;

для механізму захисту В – 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:

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}. \qquad (3)$$

Оптимальні змішані стратегії гравців А і В 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 А має забезпечувати виграш на рівні, не меншому, ніж ціна гри за умови вибору механізмом захисту В будь-яких стратегій. Математично ця умова записується так:

$$\sum_{i=1}^{m}a_{ij}x_i^*\geq\upsilon\ \left(j=\overline{1,n}\right). \qquad (4)$$

З другого боку, використання оптимальної змішаної стратегії механізмом захисту В має забезпечувати за будь-яких стратегій загрози А 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 використовуються для знаходження розв'язку гри.

Зауважимо, що в даному разі розраховані оптимальні стратегії завжди є стійкими, тобто якщо один з гравців притримується своєї оптимальної змішаної стратегії, то його виграш залишається незмінним і дорівнює ціні гри υ незалежно від того, яку із 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 наступні властивості: кожен гравець не зацікавлений в відході від своєї оптимальної змішаної стратегії, якщо його противник застосовує оптимальну змішану стратегію, так як йому не вигідно. Чисті стратегії гравців у їх 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 відходить за межи своїх активних стратегій. Такі оптимальні рішення більш ймовірні для часткових прикладів під час аналізу проектів окремих складових системи захисту інформації.

У залежності від кількості можливих стратегій моделі ігор можуть біти ***кінцевими*** або ***безінцевими*** (рис. 6).

Кінцевою називають таку модель гри, при якій у кожного гравця мається тільки кінцева кількість стратегій. Кінцева модель гри, у якій гравець A має m стратегій, а гравець B – n стратегій називають моделлю гри $m \times n$. Для пояснення розглянемо модель гри $m \times n$ двох гравців А і В (загроза і механізм захисту – частковий випадок). Будемо позначати стратегії загрози $\overline{A_1, A_m}$; стратегії механізму захисту $\overline{B_1, B_n}$.

Рис. 6. Класифікація математичних моделей теорії ігор
у залежності від кількості можливих стратегій класу моделювання процесів
прийняття рішень при проектуванні систем захисту інформації

Пускай кожна сторона обрала визначену стратегію: для загрози – A_i, для механізму захисту – B_j. Якщо модель гри складається тільки з особистих ходів, то вибір стратегій A_i, B_j однозначно визначає результат гри – тобто виграш загрози. Позначимо його як a_{ij}.

Якщо модель гри має, крім особистих, випадкові ходи, то виграш при парі стратегій A_i, B_j є величиною випадковою, яка залежить від результатів усіх випадкових ходів. У цьому випадку оцінкою очікування виграшу є середнє значення (математичне очікування). Це можна позначити тим же знаком a_{ij}, як сам виграш (у грі без випадкових ходів), так і його середнє значення (у грі з випадковими ходами). Пускай нам відомі значення a_{ij} виграшу (або середнього виграшу) при кожній парі стратегій. Тоді значення a_{ij} можна записати у вигляді таблиці, де строки відповідають стратегіям загрози (A_i), а стовбці – стратегіям механізму захисту (B_j), що представлено у таблиці 2.

Таблиця 2

Таблиця виграшів

A\B	B_1	B_2	…	B_n
A_1	a_{11}	a_{12}	…	a_{1n}
A_2	a_{21}	a_{22}	…	a_{2n}
…	…	…	…	…
A_m	a_{m1}	a_{m2}	…	a_{mn}

У моделях ігор ***з безкінцевим*** числом можливих стратегій, виграш та переможець не будуть визначені до кінця усіх ходів. Задача полягає не у пошуку оптимального рішення, а у пошуку хоча-б однієї виграшної стратегії. Використовуючи аксіому вибору (2) можна

доказати, що іноді для ігор з повною інформацією і двома виходами – "програв" або "виграв" – ні один з гравців не має такої стратегії.

Аксіома вибору: Для будь-якого сімейства X непустих множин існує функція f, яка кожній множині сімейства співставляє один з елементів цієї множини, де функція f є функцією вибору для заданого сімейства:

$$\forall X\left[\otimes \notin X \Rightarrow \exists f : X \to \cup X \quad \forall A \in X\left(f\left(A\right) \in A\right)\right]. \tag{5}$$

Висновки

Надані авторами підходи моделювання процесів прийняття рішень, під час проектування систем захисту інформації, у подальшому надають можливість розкрити ознаки класу ефективності математичних моделей прийняття рішень (які запропоновані авторами у наступній статті).

У цілому автори пропонують стрункy класифікацію математичних моделей теорії прийняття рішень при проектування систем захисту інформації, яку можливо застосовувати як під час проектування самих систем захисту інформації, так і процесів, які моделюються для оцінки ефективності систем захисту інформації у різних життєвих циклах роботи.

Література

1. Оуен. Г. Теория игр / Г. Оуен. – М.: 1971. – Мир. – 230. с.
2. Вентцель Е.С. Элементы теории игр / Е.С. Вентцель. – М.: 1961. – Физматгиз. – Вип. 32. – 72 с.
3. Петросян Л.А. Теория игр / Л.А. Петросян, Н.А. Зенкевич, Е.А. Семина. – М.: 1998. – Вища школа. – 304 с.
4. Дюбин Г.Н. Введение в прикладную теорию игр / Г.Н. Дюбин, В.Г. Суздаль. – М.: 1981. – Наука. – 336 с.
5. Воробьев Н.Н. Бесконечные антагонистические игры / под ред. Н.Н. Воробьева. – М.: 1993. – Вища школа. – 505 с.
6. 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.

Надійшла 10.06.2014 р. Рецензент: д.т.н., проф. Барабаш О.В.