УДК 004.056, 004.75

І.Р. Опірський

Національний університет «Львівська політехніка», Львів

ВИЗНАЧЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ КОНФЛІКТУ ЗАГРОЗ З КОМПЛЕКСНОЮ СИСТЕМОЮ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ

У статті проведено аналітичний аналіз захищеності системи захисту інформації з повним перекриттям загроз. На основі теорії ігор визначаються результати гри, в якій використовується принцип оптимальності розподілу виграшу між гравцями, який в задачі теорії кооперативних ігор має назву вектору Шеплі. Використовуючи теорії ігор приводиться опис біометричної гри, що описується двома матрицями, які зводяться до задачі лінійного програмування і вирішуються за допомогою симплекс методу та на основі цього представляється характеристична функція. Представлено кооперативну гру КСЗІ в ІМД та загроз у вигляді сукупності біоматричних ігор та на основі цього визначено матрицю моделі конфлікту загроз комплексної системи захисту інформації в інформаційних мережах держави.

Ключові слова: *комплексні системи захисту, інформаційна мережав держави, загроза, теорія ігр, біометрична гра, математична модель, коаліція гри.*

Вступ

Відомо, що до підсистеми захисту інформації інформаційної системи приділяється ряд вимог: функціональних, економічних, технічних та організаційних. Одною з головних вимог є економічна. Побудова комплексної системи захисту інформації проводиться з максимальною економічною ефективністю. В літературі оптимальні, по економічним показникам, системи розглядаються з двох різних позицій: при заданих ресурсах встановлюється максимальний рівень безпеки інформації або при заданому рівні безпеки визначаються мінімальні витрати на ресурси, які виділяються для забезпечення безпеки інформаційних технологій.

При таких підходах в процесі розробки комплексних систем захисту інформації (КСЗІ) виникає задача визначення оптимального об'єму ресурсів для реалізації підсистеми і вибору оптимального рівня захисту інформації. В ряді підходів пропонується визначати вимоги до забезпечення безпеки інформації на основі експертних оцінок по сукупності таких факторів, як характер і об'єм інформаційного і програмного забезпечення, тривалості перебування інформації на об'єкті обробки інформації, структурі самого об'єкта тощо.

В інших підходах оцінка об'єму ресурсів, які необхідно виділяти для систем захисту інформації, проводиться виходячи з того, що вартість засобів забезпечення безпеки повинна бути менше розміру можливої шкоди.

В деяких підходах розглядається достатній рівень безпеки. Забезпечення такого рівня безпеки, коли вартість його подолання становить більше вартості інформації, яку необхідно отримати (ефект, який необхідно досягти), або коли за час отримання інформації вона настільки стане застарілою, що отримувати її стане неважливим. Тому у цьому пункті тільки ставиться задача визначення оптимального рівня безпеки: важливо правильно вибрати той або інший достатній рівень захисту, при якому витрати, риск та розмір можливої шкоди були б неруйнівними (задача аналізу ризиків).

Метою роботи є проведення аналізу захищеності системи захисту інформації з повним перекриттям загроз та на основі цього визначити математичну модель конфлікту загроз з КСЗІ в інформаційних мережах держави.

Основна частина

Аналізу ризиків, під час розробки системи захисту інформації, для побудови стратегії захисту, приділяється велика увага. Аналіз ризиків використовується для вибору найбільш реальних загроз інформаційному і програмному забезпеченню КСЗІ та цілеспрямованим способам захисту інформаційного середовища.

Однак, етап аналізу ризиків має на увазі тільки оцінку реальних витрат та виграшу від застосування заходів захисту, які повинні бути обов'язково. І на основі величини виграшу пропонується приймати рішення про вибір стратегії безпеки. Величина виграшу може мати як позитивне так і негативне значення. В першому випадку це означає, що використання КСЗІ принесе виграш, а в другому –принесе додаткові витрати на забезпечення особистої безпеки. Очевидно, такі підходи не враховують економічну ефективність КСЗІ в Інформаційних мережав держави (ІМД), під якою розуміється співвідношення можливих втрат до впровадження і після впровадження систем захисту інформації з врахуванням вартості самої КСЗІ.

Прийняття оптимальних рішень в умовах ризиків і невизначеності потребує великого об'єму обчи-

слень. Це обумовлено обмеженістю, по об'єму і номенклатурі, масивів статистичних даних, які характеризують роботу реальних систем захисту інформації у складі КСЗІ в ІМД. Такий недолік інформації збільшує множину варіантів розвитку вихідних ситуацій, і кожен з них повинен бути проаналізований, що стає можливим при застосуванні теорії ігор.

При існуванні відомої функціональної залежності критерію оптимізації від вхідних управляючих параметрів, задача оптимізації зводиться до знаходження таких параметрів, при яких цільова функція доходять до екстремуму. Коли на об'єкт впливають загрози, то залежність має не функціональну а регресивну залежність, яка утворює поверхню відклику. Для знаходження екстремуму існує два принципово різних підходів:

1. Коли мається можливість знайти n-факторну математичну модель в той частині простору дослідження, де розташований екстремум, то задача вирішується аналітичними або чисельними методами – формалізованим способом.

2. Коли математичний опис не отримується, то виконується експериментальний пошук області екстремуму.

Побудова моделі взаємовідносин загроз і систем захисту інформації може бути виконана на основі умовної гри двох або більше гравців, яка ефективно вирішується з використанням потужних технологій. В цієї моделі першим гравцем буде система захисту інформації. Стратегії КСЗІ в ІМД являють собою набір методів і засобів, які забезпечують захист інформації за допомогою адміністративних, технічних і програмно-апаратних складових.

Іншими $(n-1)$ гравцями (n – це загальне число гравців під час моделювання) є загрози. Стратегії загроз – це реалізації впливів на КСЗІ шляхом атак, аварій систем захисту та відмов, в результаті яких буде порушені конфіденційність, цілісність, доступність та спостережливість інформації.

З теорії ігор відомо, що ігри мають продовження в тому випадку, коли в грі n гравцям дозволяється утворювати визначенні коаліції (в цієї моделі утворювання коаліції загроз та системи захисту неможливо і не дозволяється).

Позначимо через N множину усіх гравців, при $N=\overline{1,n}$; а через К – будь-яку підмножину цієї множини. Нехай гравці (загрози) з К домовляються між собою про узгоджені дії і, таким чином, утворюють коаліцію. Утворив коаліцію, множина К гравців діє як один гравець проти інших гравців, і виграш цієї коаліції залежить від застосування стратегій кожним з n гравців. Для опису гри необхідно визначити характеристичну функцію v, яка ставить, у відповідності кожній коаліції К найбільший, вірно отриманий виграш V(K). Потужність множини коаліцій, на якій визначена характеристична функція, дорівнює 2^n, причому коаліція з номером 0, є пустою коаліцією і її виграш, згідно умови, завжди дорівнює нулю.

Для рішення гри слід побудувати оптимальний розділ, який розподіляє перемоги $X=\overline{x_1,x_n}$, гравців з врахуванням таких умов:

1. $x_i \geq v(N), i \in N$ – принцип індивідуальної раціональності.

2. $\sum_{i\in N} x_i = v(N)$ – принцип колективної раціональності.

В безкоаліційних іграх закінчення гри формується в результаті дій гравців, які в цій ситуації отримали свій виграш. Для визначення порядку проведення, кооперативна гра задається у вигляді $n\times(n-1)$ матриць розміру $k\times g$, де n – кількість гравців, k– кількість стратегій у гравців, наприклад, матриця виграшів гравця А:

$$A_{xy}=\begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{g1} & \dots & a_{gk} \end{bmatrix}, \qquad (1)$$

де $a_{ij}(i=\overline{1,k}, j=\overline{1,g})$ – виграш гравця x в грі з гравцем y. Стратегії коаліції визначаються вибором гравців – учасників коаліції (загроз або бар'єрів механізмів захисту системи захисту інформації). Таким чином, коаліція з m гравців буде мати k^m чистих стратегій, де k– кількість виборів гравця.

В подальшому необхідно знайти матриці виграшів усіх коаліцій в грі з іншими гравцями (кожна загроза перекривається бар'єром у складі механізмів захисту системи захисту інформації). Кожна матриця розміру $k^m \times g^{n-m}$ (де m– кількість гравців в коаліції, яка приймає участь в грі) має вигляд:

$$\overline{A_{\overline{xy}}}=\begin{bmatrix} \overline{a}_{11} & \dots & \overline{a}_{1k^{n-m}} \\ \dots & \dots & \dots \\ \overline{a}_{g^m 1} & \dots & \overline{a}_{g^m k^{n-m}} \end{bmatrix}, \qquad (2)$$

при $0<m\leq n$, де $\overline{a}_{ij}$ – виграш коаліції $\overline{X}$ в грі з коаліцією $\overline{Y}$, і та j – комбіновані стратегії коаліції.

Кожна біоматрична гра описується двома матрицями, які зводяться до задачі лінійного програмування і вирішуються за допомогою симплекс методу. В результаті отримаємо характеристичну функцію.тДля находження результатів гри використовується принцип оптимальності розподілу виграшу між гравцями, який в задачі теорії кооперативних ігор має назву вектору Шеплі. Представимо кооперативну гру КСЗІ в ІМД та загроз у вигляді сукупності біоматричних ігор такого вигляду:

$$B_{xy_{kg}}=\begin{bmatrix} -b_{11} & \dots & -b_{1k} \\ \dots & \dots & \dots \\ -b_{g1} & \dots & -b_{gk} \end{bmatrix}, \qquad (3)$$

де X – це КСЗІ, Y_{kg} – k-та загроза (зловмисник, атака, відмова), або їх коаліція, $-b_{ij}(i=\overline{1,k}, j=\overline{1,g})$ включає витрати на КСЗІ, яка реалізує і-ту стратегію та втрати від дій загроз j-ої стратегії:

$$\overline{B}_{XY_{kg}} = \begin{bmatrix} \overline{b}_{11} & \cdots & \overline{b}_{1k^{n-m}} \\ \cdots & \cdots & \cdots \\ \overline{b}_{g^{m}1} & \cdots & \overline{b}_{g^{m}k^{n-m}} \end{bmatrix}, \qquad (4)$$

де $\overline{b}_{ij}$ – користь від подолання КСЗІ, яка реалізує і-ту стратегію, за винятком витрат на реалізацію загрози, і – номер стратегії КСЗІ, j – номер загрози.

Таким чином матриці загроз визначаються, як:

$$\widetilde{A}_Y = \begin{bmatrix} \tilde{a}_{11} & \cdots & \tilde{a}_{1k} \\ \cdots & \cdots & \cdots \\ \tilde{a}_{g1} & \cdots & \tilde{a}_{gk} \end{bmatrix}, \ \tilde{B}_Y = \begin{bmatrix} \tilde{b}_{11} & \cdots & \tilde{b}_{1k^{n-m}} \\ \cdots & \cdots & \cdots \\ \tilde{b}_{g^{m}1} & \cdots & \tilde{b}_{g^{m}k^{n-m}} \end{bmatrix}, \qquad (5)$$

де $\tilde{a}_{ij}$ – аналіз усіх загроз, які впливають, $\tilde{b}_{ij}$ – користь, яку отримують загрози, від подолання КСЗІ, а матриці роботи КСЗІ в ІМД будуть мати вигляд:

$$C_Y = \begin{bmatrix} c_{11} & \cdots & c_{1k} \\ \cdots & \cdots & \cdots \\ c_{g1} & \cdots & c_{gk} \end{bmatrix}, \ D_Y = \begin{bmatrix} d_{11} & \cdots & d_{1k^{n-m}} \\ \cdots & \cdots & \cdots \\ d_{g^{m}1} & \cdots & d_{g^{m}k^{n-m}} \end{bmatrix}, \qquad (6)$$

де c_{ij} – кількість механізмів захисту у складі КСЗІ, d_{ij} – аналіз процесу відмови або пошкодження механізмів захисту КСЗІ (або навпаки, аналіз процесу блокування механізмами захисту) загроз, які впливають на КСЗІ в ІМД.

Для розкриття роботи КСЗІ в ІМД можна визначити матриці роботи бар'єрів у складі h – кількості механізмів захисту, які в свою чергу також розкриваються згідно (6).

Висновки

Отже для рішення кооперативних ігор застосовується об'єднання коаліційних ігор в стратегічні ігри і рішення кожної симплекс-методом, для подальшого находження тих або інших результатів.

В статті представлено алгоритм побудови кооперативної гри КСЗІ в ІМД та загроз у вигляді сукупності біоматричних ігор, що дозволило визначити матрицю моделі конфлікту загроз комплексної системи захисту інформації в інформаційних мережах держави.

Список літератури

1. Тихонов В.И. Статистический анализ и синтез радиотехнических устройств и систем / В.И. Тихонов, В.Н. Харисов. – М.: Радио и связь, 1991. – 608 с.

2. Управління інформаційною безпекою. В 2-х т. / Л.Ф. Єжова, А.О. Корченко, І.О. Мачалін, Я.В. Невойт, В.О. Хорошко. – Т. 1. – К.: НАУ, 2012. – 373 с .

3. Згуровський М.З. Основи системного аналізу/ М.З. Згуровський, Н.Д. Панкратова. – К.: ВНУ, 2007. –544 с.

4. Борисенков, Е.П. Алгоритми и программи статичтической обработки информации на ЭВМ / Е.П. Борисенков, Н.А. Романов. – Л-д : ГМИ, 1989. – 454 с.

5. Щеглов А.Ю. Защита компьютерной безопасности от несанкционированного доступа / А.Ю. Щеглов. – С.Пб., 2004. – 384 с.

6. Тартаковский А.Г. Последовательные методы в теории информационных систем / А.Г. Тартаковский. – М.: Радио и связь, 1991. – 280 с.

Надійшла до редколегії 29.02.2016

Рецензент: д-р техн. наук, проф. Л.Т. Пархуць, Національний університет «Львівська політехніка», Львів.

ОПРЕДЕЛЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ КОНФЛИКТА УГРОЗ С КОМПЛЕКСНОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ ГОСУДАРСТВА

И.Р. Опирский

В статье проведен аналитический анализ защищенности системы защиты информации с полным перекрытием угроз. На основе теории игр определяются результаты игры, в которой используется принцип оптимальности распределения выигрыша между игроками, который в задачи теории кооперативных игр называется вектора Шепли. Используя теории игр приводится описание биометрической игры, описывается двумя матрицами, которые сводятся к задаче линейного программирования и решаются с помощью симплекс метода и на основе этого представляется характеристическая функция. Представлены кооперативную игру КСЗИ в ИМД и угроз в виде совокупности биоматричных игр и на основе этого определена матрица модели конфликта угроз комплексной системы защиты информации в информационных сетях государства.

Ключевые слова: *комплексные системы защиты, информационная сеть государства, угроза, теория игр, биометрическая игра, математическая модель, коалиция игры.*

THE DEFINITION OF A MATHEMATICAL MODEL OF CONFLICT THREATS WITH THE COMPLEX SYSTEM OF INFORMATION PROTECTION IN THE INFORMATION NETWORKS OF THE STATE

I.R. Opirsky

In the article the analytical analysis of security information protection system with full overlapping threats. On the basis of the theory of games are the results of the game, which uses the principle of optimum distribution between the players win, which is the task of the theory of cooperative games is called the Shapley value. Using game theory describes biometric games, is described by two matrices, which are reduced to a linear programming problem and solved using the simplex method and on the basis of this, it is the characteristic function. Presented cooperative game ISS in SIS and threats in the form of a set biomatrix games and on the basis of defined matrix model of conflict threats complex system of information protection in the information networks of the state.

Keywords: *complete protection, state information system, game theory, biometric game, mathematical model, a coalition of the game.*