DOI 10.15276/imms.v13.no3-4.236
УДК 004.056:351.861

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 236-242

МЕТОДИКА РІШЕННЯ ЗАДАЧ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ

В.В. Білозерський, О.Ю. Лебедєва, Н.П. Волкова, В.О. Назаров

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
e-mails: o.y.lebedieva@op.edu.ua, volkova.n.p@op.edu.ua tasknavigator@gmail.com

Розроблено методику розв'язання задач із захисту інформації. Кібербезпека є однією з найважливіших проблем сучасного світу. Зростаюче використання цифрових технологій у всіх сферах життя робить кіберпростір все більш привабливим для кіберзлочинців. Захист інформаційних систем – одне з найважливіших завдань будь-якої служби безпеки будь-якої організації та будь-якого підприємства. Щоб протистояти цій загрозі, необхідно розробляти ефективні методи захисту інформації. В роботі розглянуті такі інструменти як відкритий стандарт для оцінки серйозності вразливостей безпеки комп'ютерної системи CVSS та база даних загальновідомих вразливостей інформаційної безпеки CVE. Є доцільним використання цих інструментів для створення списку ефективних сучасних атак. Крім цього ще необхідно визначитися з наявними інструментами захисту комп'ютерних систем організації. Кібербезпека спирається на різні математичні апарати, одним із таких є теорія ігор. Теорія ігор є одним із інструментів, які можуть бути використані для підвищення рівня кібербезпеки. В роботі використовуються матричні ігри двох гравців. В якості гравців виступають зловмисник, який атакує комп'ютерну систему якоїсь організації та представник організації, що відповідає за забезпечення захисту інформації. Теорія ігор дозволяє представити завдання захисту комп'ютерної системи в математичному вигляді, що дозволяє скористатися встановленими критеріями знаходження оптимальних стратегій захисту, дотримуючись яких адміністратор здатний усунути, або принаймні звести до мінімуму збитки інформації, що завдається зловмисником. Знаходження оптимальних чистих стратегій пов'язано з пошуком сідлової точки. Не кожна матрична гра має оптимальну чисту стратегію. Якщо матрична гра має сідлову точку, то гра має рішення в чистих стратегіях і дослідження гри закінчується знаходженням цієї точки та відповідної пари чистих стратегій гравців. В протилежному випадку застосовують змішані стратегії. Для пошуку змішаних стратегій пропонується використовувати метод Брауна-Робінсон.

Ключові слова: захист інформаційних систем, теорія ігор, матрична гра, метод Брауна-Робінсон.

Вступ. Комп'ютерні системи в наш час стають найпоширенішим ресурсом, на якому зберігається найрізноманітніша інформація. Підключення цих систем до мережі Інтернет призводить до того, що інформація, що зберігається, стає об'єктом нападу найрізноманітніших зловмисників, від окремих хакерів, що горять бажанням «пробити» захист ресурсу, до організованих злочинних спільнот, а також розвідувальних і військових служб різних держав.

Актуальність теми дослідження обумовлена постійним зростанням загроз кібербезпеці. Комп'ютерні системи багатьох підприємств часто стають об'єктами, куди спрямовані помисли зловмисників. Через несанкціонований доступ зловмисник може викрасти інформацію, а за допомогою комп'ютерної атаки або знищити її, або тимчасово обмежити доступ до неї. У будь-якому разі підприємства зазнають як фінансових втрат, так і моральних, як, наприклад, падіння рівня довіри до банків, якщо вони стали жертвами атаки хакерів.

Захист інформаційних систем – одне з найважливіших завдань будь-якої служби безпеки будь-якої організації та будь-якого підприємства.

Кіберзлочинці розробляють все більш складні методи атак, а кіберзахисники повинні постійно вдосконалювати свої методи захисту. Теорія ігор може стати цінним інструментом для вирішення цієї проблеми.

Мета та задачі роботи. Метою роботи є розробка методики рішення задач із захисту інформації шляхом використання теорії ігор.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- аналіз існуючих атак зловмисників та засобів захисту;
- розробка методики рішення задач із захисту інформації;
- розробка програмного додатку що реалізує розроблену методику.

Основна частина. Виявлення CVSS (Common Vulnerability Scoring System) – це відкритий стандарт для оцінки серйозності вразливостей безпеки комп'ютерної системи. Він був розроблений спільно групою експертів у галузі безпеки та впроваджений у 2005 році [1]. CVSS використовується для оцінки вразливостей за двома основними критеріями:

- вплив – виявлення потенційного впливу, який може мати вразливість на систему;
- експлуатація – оцінка того, наскільки легко може бути експлуатована вразливість.

CVSS оцінює вразливості за шкалою від 0 до 10, де 10 – найсерйозніша вразливість. Оцінки CVSS використовуються для розміщення пріоритетів на відповіді на вразливості та визначення того, які вразливості є найнебезпечнішими.

CVSS використовується багатьма організаціями, в тому числі уряди, підприємства та некомерційні організації. Він також використовується багатьма продуктами та послугами безпеки для оцінки вразливостей. CVSS постійно оновлюється, щоб враховувати нові загрози та можливості. Остання версія, CVSS 3.1, була опублікована в 2020 році.

CVE (Common Vulnerabilities and Exposures) – це база даних загальновідомих вразливостей інформаційної безпеки [2]. Кожній уразливості присвоюється унікальний ідентифікатор, який складається з року виявлення вразливості та послідовного номеру. CVE-номери присвоюються Центром з оцінки та розробки безпеки (CERT) при Національному інституті стандартів і технологій (NIST). Наприклад, уразливість, виявлена в 2023 році, буде мати ідентифікатор CVE-2023-0001.

CVE-номери використовуються для ідентифікації вразливостей безпеки в різних продуктах і системах, в тому числі програмне забезпечення, апаратне забезпечення та мережі. Вони використовуються розробниками програмного забезпечення, виробниками обладнання та організаціями з безпеки для спілкування про вразливості та розробки методів усунення. CVE-номери є важливим інструментом для забезпечення безпеки інформаційних систем. Вони допомагають організувати вразливості, зробити їх зрозумілими та сприяти їх усунення.

National Vulnerability Database (NVD) надає оцінки CVSS для всіх опублікованих записів у CVE.

Наприклад, якщо в якості комп'ютерної системи взяти операційну систему Windows 11, то згідно з CVE можна на даний час визначити такі категорії вразливостей:

- виконання довільного коду (Execute code);
- ескалація привілеїв (Privilege Escalation, Gain Privilege);
- відмова в обслуговуванні (Denial of Service);
- витік інформації (Information Leak).

Кожна категорія має певну кількість вразливостей.

Наприклад, вразливість CVE-2023-21554 **(**Windows Message Queuing Remote Code Execution Vulnerability, або віддалене виконання коду через чергу повідомлень Windows) виникає через помилку в обробці запитів на створення черг. Вразливість класифікується як критична, CVSS оцінюється в 9,8 балів. Вона може бути скомпрометована віддалено, тобто зловмиснику не потрібно мати фізичний доступ до комп'ютера.

Наприклад, вразливість CVE-2023-36028 (Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability або уразливість віддаленого виконання коду в захищеному розширюваному протоколі автентифікації від Microsoft) – це критична вразливість віддаленого виконання коду, яка існує в PEAP. Вразливість виникає через помилку в обробці запитів на аутентифікацію. Вразливість класифікується як критична, тобто CVSS оцінюється в 9,8. Може бути скомпрометована віддалено.

Наприклад, вразливість CVE-2023-21823 (Microsoft Graphics Component Denial of Service Vulnerability або відмова в обслуговуванні в графічному компоненті Microsoft) виникає через помилку в обробці повідомлень про помилки. Вразливість класифікується як критична, CVSS оцінюється також в 9.8. Вона може бути також скомпрометована віддалено, зловмиснику не потрібно мати фізичний доступ до комп'ютера.

В якості атак, ми пропонуємо розглянути всі вразливості з вказаних категорій, які мають високу оцінку CVSS. Аналіз показав що вони є найбільш поширеними та є максимально застосовуваними. Деякі з них є модифікаціями вразливостей попередніх років. Також є велика ймовірність того що деякі нові вразливості будуть модифіковані у майбутньому, так як нові вразливості є дуже гарною базою для цього.

Традиційний захисний механізм включає брандмауери, систему виявлення вторгнення (IDS) та антивірусні програми. Деякі з цих стратегій захисту розроблені лише для певних загроз.

В результаті, придбання та встановлення різноманітних засобів захисту інформаційного комп'ютерного ресурсу, може призвести до матеріальних витрат, потребує наявності інструкцій щодо ефективного їх використання. Необхідно розробити для системного адміністратора, служби безпеки комп'ютерної мережі оптимальну стратегію забезпечення захисту інформації, що зберігається.

Для вибору засобу ефективного захисту від різноманітних комп'ютерних атак можна використовувати методи теорії ігор. Метою теорії ігор є вироблення природних уявлень про оптимальність ситуацій і стратегій гравців, передбачення їх існування у грі та зазначення способу їх знаходження та перерахування [3].

Одним з важливих класів антагоністичних ігор є матричні ігри, які можуть бути використані для моделювання та аналізу конфліктних ситуацій [3]. Матриця гри – це інструмент, який представляє вибір гравців та їхні можливі варіанти дій (стратегії). Кожен гравець має свої власні стратегії, і результат гри залежить від комбінацій вибору кожного з учасників. Така концепція дозволяє аналізувати різноманітні сценарії та прогнозувати оптимальні стратегії для кожного гравця.

Основними елементами матричних ігор є правила гри, гравці, стратегії, виграші та втрати. Гравці приймають рішення, обираючи свої стратегії, і отримують виграш або втрату в залежності від вибору інших учасників. Задача теорії ігор – розробити моделі та аналізувати ситуації, де раціональні гравці вибирають стратегії для максимізації свого виграшу.

Зацікавлені сторони в грі називаються гравцями. Гравцем прийнято вважати одного учасника або групу учасників гри, які мають одні спільні для них інтереси, що не збігаються з інтересами інших груп.

В роботі використовувались матричні ігри двох гравців. В якості гравців ми використовували зловмисника, який атакує комп'ютерну систему якоїсь організації та представника організації, що відповідає за забезпечення захисту інформації (адміністратор безпеки).

Правила чи умови гри визначають можливі поведінки, вибір та ходи гравців на будь-якому етапі розвитку гри. Зробити вибір гравцеві, це означає зупинитися на одній із його можливостей поведінки. Потім гравець здійснює цей вибір за допомогою ходів.

Кожен гравець на певному етапі гри робить хід згідно зробленого вибору. Інший гравець, знаючи чи не знаючи про вибір першого гравця, також робить хід. Кожен із гравців намагається врахувати інформацію про минулий розвиток гри, якщо така можливість дозволяється правилами гри.

Будь-яка можлива для гравця дія (в рамках заданих правил гри) називається його стратегією. У разі конфлікту кожен гравець вибирає свою стратегію, у результаті складається набір стратегій, званий ситуацією. Стратегія в теорії ігор означає певний закінчений план дій гравця, що показує, як треба діяти йому у всіх можливих випадках розвитку гри. В якості стратегій зловмисника, або гравця А, використовуємо атаки на комп'ютерну систему організації, в якості стратегій сторони захисту, або гравця В, існуючі засоби захисту в організації.

Зацікавленість гравців у ситуації відображається в тому, що кожному гравцю в кожній ситуації приписується число, що виражає ступінь задоволення його інтересів у цій ситуації та називається його виграшем у ній. Як стратегії зловмисника будемо розуміти рядки матриці гри, а як стратегії адміністратора безпеки – її стовпці. На перетині рядка і стовпця в матриці ставиться виграш зловмисника (гравця А).

Вважатимемо, що зловмисник захоплений бажанням завдати якомога більшої шкоди комп'ютерній системі, що атакується. При такому припущенні виграш зловмисника дорівнюватиме програшу адміністратора безпеки і в цій ситуації використовується матриця гри для гри двох осіб з нульовою сумою.

Виграш зловмисника можна оцінити заподіяною матеріальною шкодою та ймовірністю реалізації атак зловмисника за обраної стратегії. Імовірність реалізації атак може бути визначена за результатами статистичних досліджень. Якщо ймовірності атак невідомі, можна припустити, що вони рівноймовірні.

У теорії ігор сідлова точка гри – це ситуація, в якій гравець не може поліпшити свій результат, змінивши свою стратегію, якщо інший гравець також дотримується своєї стратегії. Іншими словами, сідлова точка гри – це ситуація, в якій кожен гравець досягає найкращого можливого результату, беручи до уваги стратегію іншого гравця.

Сідлові точки мають важливе значення в теорії ігор, оскільки вони можуть допомогти гравцям знайти оптимальні стратегії.

Оптимальною називається стратегія, яка при багаторазово повторюваній грі гарантує гравцеві максимально можливий середній виграш (або еквівалентно мінімально можливий середній програш). Вибір оптимальної стратегії базується на принципі, який передбачає, що обидва гравці розумні в однаковому ступені та поведінка кожного з них спрямована на протидію противнику в досягненні його мети.

Теорія ігор дозволяє представити завдання захисту комп'ютерної системи в математичному вигляді, що дозволяє скористатися розробленими критеріями знаходження оптимальних стратегій захисту, дотримуючись яких адміністратор здатний усунути, або принаймні звести до мінімуму збитки інформації, що завдається зловмисникам.

Дослідження матричної гри починається з знаходження її сідлової точки у чистих стратегіях. Потенційно знаходження сідлової точки може бути корисно для кібербезпеки з кількох причин.

- можуть вказувати на потенційні вразливості в системі безпеки. Наприклад, якщо сідлова точка знаходиться в точці, де атакуючий може отримати доступ до конфіденційних даних, це може вказувати на те, що система безпеки невідповідно захищена.
- можуть бути використані для розробки нових стратегій безпеки. Наприклад, якщо сідлова точка знаходиться в точці, де атакуючий може отримати доступ до системи, але не може її повністю контролювати, це може вказувати на те, що атака може бути відбита, якщо будуть використані правильні заходи.
- можуть бути використані для оцінки ефективності існуючих стратегій безпеки. Наприклад, якщо сідлова точка знаходиться в точці, де атакуючий може легко отримати доступ до системи, це може вказувати на те, що існуючі заходи безпеки недостатньо ефективні.

Не кожна матрична гра має оптимальну чисту стратегію. Якщо матрична гра має рішення в чистих стратегіях, тобто для даної гри існує сідлова точка, то дослідження гри закінчується знаходженням даної сідлової точки та відповідних чистих стратегій гравців. Якщо ж гра повторюється багато разів, то кожен з гравців, з одного боку, отримує інформацію про попередні ходи супротивника, а з іншого боку, хоче приховати від супротивника свої наміри в майбутніх ходах. Кожен гравець може змінювати ймовірність застосування своїх чистих стратегій таким чином, щоб максимально збільшити свій середній виграш і на цьому шляху отримувати оптимальні стратегії. Така ідея призвела до поняття змішаної стратегії.

Змішаною стратегією гравця називається повний набір ймовірностей застосування його чистих стратегій. Для пошуку змішаних стратегій пропонується використовувати метод Брауна-Робінсон.

Алгоритм методу Брауна-Робінсон для гри з двома гравцями виглядає наступним чином:

- гравці обирають довільні змішані стратегії;
- гравці грають одну гру з обраними стратегіями;
- кожен гравець розраховує свій очікуваний виграш у цій грі;
- кожен гравець коригує свою стратегію таким чином, щоб збільшити свій очікуваний виграш.
- повторюються другий та останній кроки до досягнення бажаної точності.

В роботі запропонована методика для вирішення задач із захисту інформації, яка складається з наступних кроків:

Крок 1. Визначення стратегій зловмисника, а саме аналіз поширених вразливостей та ризиків.

Крок 2. Визначення засобів захисту. Цей крок являє собою відповідь на проаналізовані загрози, які можуть спричинити збитки.

Крок 3. Створення таблиці кореляції стратегій. Для кожного такого аналізу повинна бути створена таблиця, що показує кореляцію між стратегіями захисту та атаки.

Крок 4. Пошук величини збитків. Цей крок відповідає за розрахунок відповідних збитків, який повинен проводити адміністратор.

Крок 5. Визначення сідлової точки, та при її наявності оптимальних стратегій. Шляхом знаходження сідлової точки, при наявних результатах можливих атак, можна визначити оптимальні стратегії, які вплинуть на вибір захищаючої сторони.

Крок 6. Якщо сідлова точка не знайдена, визначення змішаних стратегій. Визначення змішаних стратегій виконується за допомогою методу Брауна-Робінсон.

Було розроблено програмний продукт, який реалізує запропоновану методику для вирішення задач із захисту інформації (рис. 1).

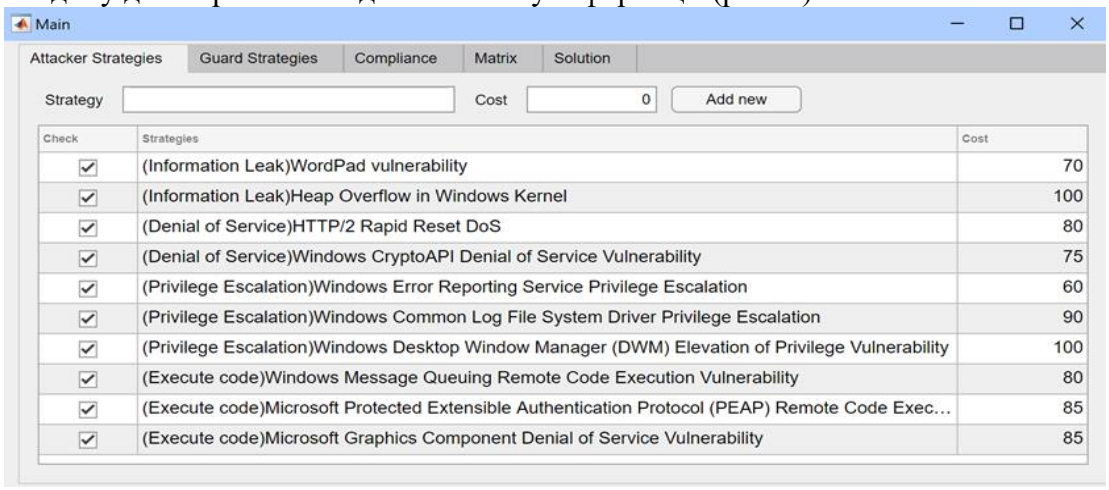

Рис. 1. Загальний вигляд головного вікна програмного застосунку

В окремих excel-файлах знаходяться списки стратегій зловмисника та адміністратора безпеки. При загрузці програми ці списки додаються у програму у відповідні таблиці на вкладках «Attacker Strategies» та «Guard Strategies». Вкладка «Compliance» відображає відповідність між стратегіями атакуючої та захищаючої сторони. Нулі в цій таблиці означають що відповідність стратегії атакуючої сторони та захищаючої не дає ніякого ефекту останнім. І навпаки, якщо в таблиці є одиниця значить даній стратегії атакуючого є протидіюча стратегія захищаючого.

Вкладка Matrix демонструє побудовану матрицю гри, згідно якої йде розрахунок гри. На вкладці «Solution» знаходиться рішення в заданій грі, а саме оптимальні чисті стратегії, якщо вони є та змішані стратегії, якщо вони потрібні (рис. 2).

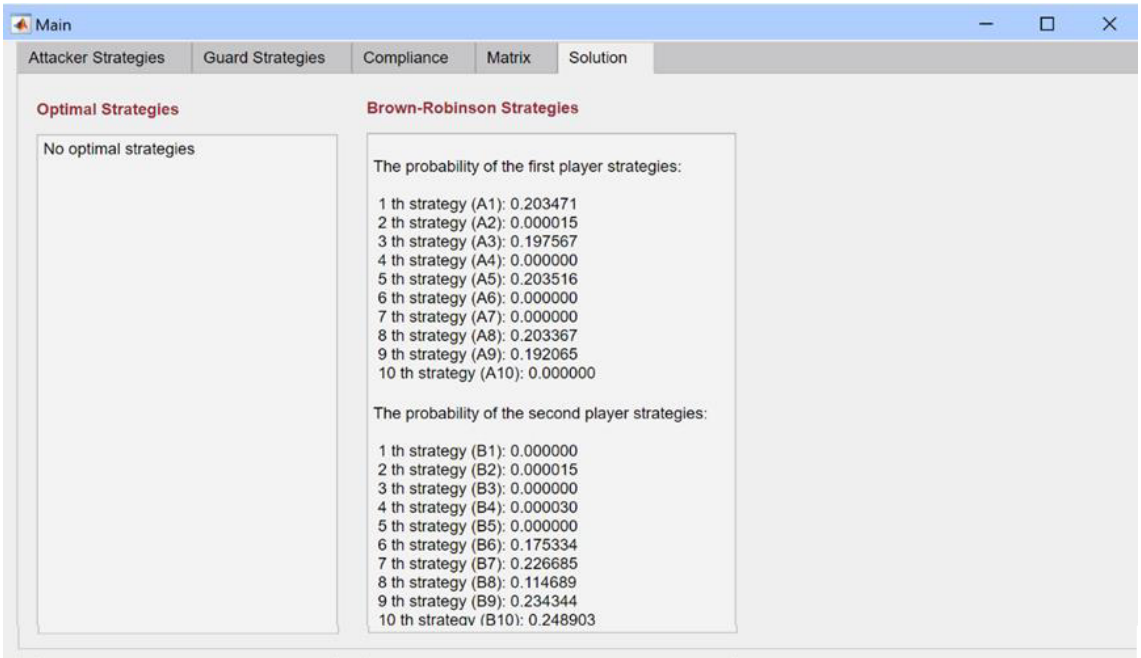

Рис. 2. Приклад рішення

Таким чином, в роботі запропонована методика рішення задач із захисту інформації. Методика використовує теорію ігор, а саме матричну гру двох гравців з нульовою сумою. Для пошуку оптимальних чистих стратегій використовується пошук сідлової точки. Для визначення змішаних стратегій використовується метод Брауна-Робінсона.

Список літератури

1. First. Загальна система оцінки вразливостей CVSS. URL: https://www.first.org/cvss/
2. Cvedetails. Поширені вразливості та ризики CVE. Вільний статистичний матеріал вразливостей стандарту CVE. URL: https://www.cvedetails.com/
3. Бартіш М. Я., Роман Л. Л. Теорія ігор. Львів: Видавничий центр ЛНУ, 2005. 120 с.

METHODS OF SOLVING PROBLEMS OF INFORMATION PROTECTION

V. Bilozerskyi, O. Lebedieva, N. Volkova, V. Nazarov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine;
e-mails: o.y.lebedieva@op.edu.ua, volkova.n.p@op.edu.ua, tasknavigator@gmail.com

The work developed a methodology for solving information protection problems. Cyber security is one of the most important problems of the modern world. The growing use of digital technologies in all areas of life makes cyberspace increasingly attractive to cybercriminals. Protection of information systems is one of the most important tasks of any security service of any organization and any enterprise. To counter this threat, it is necessary to develop effective information protection methods. The work considers such tools as an open standard for assessing the severity of computer system security vulnerabilities CVSS and a database of well-known information security vulnerabilities CVE. It makes sense to use these tools to create a list of effective modern attacks. In addition, it is still necessary to decide on the available tools for protecting the organization's computer systems. Cybersecurity relies on various mathematical tools, one of which is game theory. Game theory is one of the tools that can be used to improve cyber security. The work uses two-player matrix games. The players are an attacker who attacks the computer system of some organization and a representative of the organization responsible for ensuring information protection. Game theory allows you to present the task of computer system protection in a mathematical form, which allows you to use the established criteria for finding optimal protection strategies, following which the administrator is able to eliminate, or at least minimize, information damage caused by an attacker. Finding optimal pure strategies involves finding a saddle point. Not every matrix game has an optimal pure strategy. If the matrix game has a saddle point, then the game has a solution in pure strategies and the study of the game ends by finding this point and the corresponding pair of pure strategies of the players. Otherwise, mixed strategies are used. To search for mixed strategies, it is suggested to use the Brown-Robinson method.

Key words: protection of information systems, game theory, matrix game, Brown-Robinson method.