DOI 10.31891/2307-5732-2020-289-5-307-309
УДК 004.832.2

В.Ю. ТІТОВА, О.С. АНДРОЩУК, В.С. ОРЛЕНКО, І.М. ШЕВЧУК, В.С. ДАЦЕНКО
Хмельницький національний університет

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ РІШЕНЬ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

В даній статті розглянуто відомі методи оцінювання ефективності рішень. Проаналізовано можливість їх використання для оцінювання ефективності рішень, що приймаються системами захисту інформації стосовно класифікації та визначення загроз. На основі визначених переваг та недоліків існуючих методів запропоновано власний метод оцінювання ефективності рішень, який дозволяє підвищити відсоток прийнятих правильних рішень та оптимізувати ефективність системи захисту інформації в цілому.

Ключові слова: системи захисту інформації, багатокритеріальна оптимізація, метод аналізу ієрархій, метод Парето.

V. TITOVA, O. ANDROSHCHUK, V. ORLENKO, I. SHEVCHUK, V. DATSENKO
Khmelnytskyi National University

EVALUATION OF DECISIONS EFFICIENCY IN INFORMATION SECURITY SYSTEMS

The functioning of most information security systems is reduced to the recognition of many active processes, their classification in order to identify malicious and dangerous processes and make decisions to respond to them. The decision-making process is based on taking into account a large number of conflicting requirements and evaluating decision options according to many criteria. The inconsistency of the characteristics of the processes, the ambiguity of the evaluation of the process, the incompleteness of the information obtained greatly complicate the final decision and significantly affect its quality.

To increase the efficiency of the final decision, it is necessary to develop a method of multi-objective optimization of decisions, which is why this work was devoted. To evaluate the efficiency of decisions in information security systems, the method was proposed that includes the advantages of the analytic hierarchy process and the Pareto efficiency. It is based on three matrices. Two of these matrices contain normalized values of threat characteristics, one - a set of decisions that need to be optimized, ranked on the analytic hierarchy process scale of preferences. Criteria for optimization are also calculated using pairwise comparisons of analytic hierarchy process preference scale values.

The proposed method provides increasing the percentage of identified correct decisions and has the following advantages: the result is always a single and effective decision; the possibility of compensation of values of partial criteria is eliminated. The method was implemented and tested in the subsystem for evaluating the decision efficiency of intrusion detection system based on in-depth learning networks and was used as the tools of multi-objective optimization of decisions for computer systems protection system.

Keywords: information security system, multi-objective optimization, analytic hierarchy process, Pareto efficiency.

Вступ. Забезпечення захисту інформації в комп'ютерних системах є однією з ключових проблем сьогодення. При цьому треба враховувати, що функціонування більшості систем захисту інформації, по факту, зводиться до розпізнавання множини активних в комп'ютері процесів, їх класифікації з метою визначення шкідливих та небезпечних процесів та прийняття рішень щодо їх блокування або ігнорування. Причому процес прийняття рішень ґрунтується на врахуванні великої кількості суперечливих вимог і оцінюванні варіантів рішень за багатьма критеріями. Суперечливість характеристик процесів, неоднозначність оцінювання процесу, неповнота отриманої інформації значною мірою ускладнюють прийняття остаточного рішення і суттєво впливають на його якість. Для підвищення ефективності остаточного рішення необхідно ввести в структуру систем захисту інформації модуль, який забезпечить можливість вибору кращої альтернативи за допомогою методу оцінювання ефективності рішень, тобто буде реалізовувати багатокритеріальну оптимізацію рішень. Розроблення методу зазначеної багатокритеріальної оптимізації рішень і є метою даної роботи.

Характеристика предметної області. На сьогоднішній день методи вирішення задач багатокритеріальної оптимізації розділяють на два класи [1], [2]: методи, що дозволяють виділити деяку множину прийнятних варіантів, та методи пошуку єдиного ефективного рішення.

До методів першого класу, наприклад, належить метод Парето. Але подібні методи не можуть бути використані в системах захисту інформації, оскільки головною метою захисту пошук єдиного ефективного рішення, яке б дозволило максимізувати захищеність та мінімізувати загрози інформації.

До методів другого класу, наприклад, відносяться методи з використанням узагальнюючого критерію (адитивний, мультиплікативний, максимінний) [1] та аналітична ієрархічна процедура (Analytic Hierarchy Process) Сааті або метод попарних порівнянь [2].

Перевагою перших методів є те, що завжди вдається визначити єдиний оптимальний варіант рішення. До недоліків відносять суб'єктивізм у визначенні вагових коефіцієнтів критеріїв та компенсацію значень часткових критеріїв [1], [3]. Останній недолік може призвести до того, що рішення, обране за найкращим сумарним результатом, має не найкращі результати за критеріями з найбільшими ваговими коефіцієнтами, які компенсуються найкращими результатами за критеріями з меншими ваговими коефіцієнтами. Як результат, обране рішення буде не самим ефективним, а це, в свою чергу, може призвести до ігнорування небезпечного або шкідливого процесу, реалізації сценарію його загрозу та, як наслідок, порушення конфіденційності, цілісності або доступності інформації.

Вищезазначені недоліки фактично ліквідовані аналітичною ієрархічною процедурою Сааті, але ця процедура має ряд недоліків, а саме: недосконалість шкали переваг та отримання результатів типу «критерій К1 важливіший за критерій К2» [2], не завжди враховуючи наскільки саме важливіший. Сааті пропонує таку шкалу переваг:

1 – рівноцінність;
3 – помірна перевага;
5 – велика перевага;
7 – дуже велика перевага;
9 – найвища перевага.

Розглянемо ситуацію, коли критерій К1 має дуже велику перевагу над критерієм К2, критерій К2 має дуже велику перевагу над критерієм К3. Що можна сказати про перевагу критерію К1 над критерієм К3?

Логічно зробити висновки, що критерій К1 має перевагу над К3 в 49 разів (7 помножити на 7), але цей висновок не входить у рамки даної шкали. Єдиним рішенням залишається зробити висновок, що критерій К1 має найвищу перевагу над критерієм К3, і в подальшому використовувати градацію шкали «9». Проте, при оцінювання ефективності рішень в системах захисту інформації через велику кількість прямих і зворотних зв'язків між характеристиками загроз, розглянути у [4] перевага кожного критерію над іншими має дуже велике значення, тому цей метод не може бути використаний.

Тому, для оцінювання ефективності рішень в системах захисту інформації використаємо переваги двох вищезазначених методів.

Метод оцінювання ефективності рішень в системах захисту інформації. Як вже зазначалося вище, в ході свого функціонування система захисту інформації здійснює вибір рішення зі скінченої множини можливих рішень $R = \{r_j\}, j = \overline{1,q}$. Ці рішення є реакціями на діяльність одного з активних процесів p з множини усіх процесів $P = \{p_t\}, t = \overline{1,w}$. Щоб прийняти рішення rj для процесу p, система має проаналізувати характеристики кожного процесу $A = \{a_{jm}\}, j = \overline{1,q}, m = \overline{1,n}$ для кожного критерію, обраного з відповідної множини $\{k_m\}, m = \overline{1,n}$, де n – максимальна можлива кількість критеріїв, та визначити для кожного рішення rj його ефективність.

Причому треба враховувати, що в один момент часу можуть мати місце як один, так і кілька класів загроз, а характеристики можуть змінюватися в процесі прийняття рішення. І з їх зміною один клас загрози може перейти в інший або корелювати з ним [4]. Отже, формальний опис моделі задачі оцінювання ефективності рішень має такий вигляд:

$$E_{r_j} = M(A_p, k_p), \tag{1}$$

де E_{r_j} – ефективність рішення rj, M – це метод, за яким ведеться пошук ефективного рішення; Ap – характеристики процесу p; kp – множина критеріїв для оцінювання характеристик процесу p, згідно з якими оцінюється ефективність можливих рішень.

На основі наведених множин сформуємо три матриці. В першу (A) заносяться дані відношень критеріїв, в другу (B) і третю (C) значення, які відображають характеристики для кожного процесу за кожним з критеріїв.

Значення критеріїв обчислюються за допомогою методу попарних порівнянь з використанням шкали переваг Сааті. Попарно порівнюється лише один окремий критерій з усіма іншими. У результаті визначається перевага критерію ki. Після цього дані заносяться у перший рядок матриці A (2). Всі подальші переваги обчислюються за математичними розрахунками. Таким чином, можна уникнути обмежень, що накладаються градацією шкали переваг.

$$A = \begin{bmatrix} 1 & kx_1/kx_2 & \dots & kx_1/kx_n \\ kx_2/kx_1 & 1 & \dots & kx_2/kx_n \\ \dots & \dots & \dots & \dots \\ kx_n/kx_1 & kx_n/kx_2 & \dots & 1 \end{bmatrix}, \tag{2}$$

де $kx_1 \dots kx_n$– відповідні критерії, n – максимальна кількість критеріїв, за якими виконується оцінювання.

Далі значення критеріїв нормуються таким чином, щоб їх сума дорівнювала одиниці, тобто визначається ваговий коефіцієнт кожного критерію. Для цього вони обчислюються за такими формулами:

$$kx_j^{\sim} = \sum_{i=1}^{n} kx_{ij}, j = \overline{1,m}$$

$$v_i = kx_i^{\sim} / \sum_{j=1}^{n} kx_j^{\sim}, i = \overline{1,m}$$

де $v_1 \dots v_n$– вагові коефіцієнти відповідних критеріїв.

В матрицю B (3) заносяться характеристики процесів за кожним обраним критерієм.

$$B = \begin{bmatrix} ax_{11} & ax_{12} & \dots & ax_{1n} \\ ax_{21} & ax_{22} & \dots & ax_{2_n} \\ \dots & \dots & \dots & \dots \\ ax_{f_1} & ax_{f2} & \dots & ax_{f_n} \end{bmatrix}, \quad (3)$$

де $ax_{11} \dots ax_{fn}$– значення відповідних характеристик процесів за відповідними критеріями, f – максимальна кількість рішень, для яких виконується оцінювання.

Далі дані нормуються таким чином, щоб сума значень у кожному стовпчику дорівнювала одиниці, і матриця В перетворюється в матрицю В~.

$$B^{\sim} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2_n} \\ \dots & \dots & \dots & \dots \\ a_{f_1} & a_{f2} & \dots & a_{f_n} \end{bmatrix}, \quad (4)$$

де $a_{11} \dots a_{fn}$– нормовані характеристики процесів.

В матрицю С (5) також заносяться характеристики процесів за кожним обраним критерієм.

$$C = \begin{bmatrix} ax_{11} & ax_{12} & \dots & ax_{1n} \\ ax_{21} & ax_{22} & \dots & ax_{2_n} \\ \dots & \dots & \dots & \dots \\ ax_{f_1} & ax_{f2} & \dots & ax_{f_n} \end{bmatrix}, \quad (5)$$

Перетворення над нею виконуються наступним чином. Якщо найкращим результатом для j-го критерію є максимальне значення наслідку рішення, то $n_{ij}^o = n_{ij}/n_{max\,j}$, де n_{ij}^o – нормоване значення відповідного наслідку, $n_{\max j}$ – максимальне значення наслідку в j-му стовпці. Якщо для j-го критерію найкращим результатом є мінімальне значення наслідку рішення, то $n_{ij}^o = n_{ij}/n_{min\,j}$, де $n_{\min j}$ – мінімальне значення наслідку в j-му стовпці. Матриця С~ буде мати вигляд:

$$C^{\sim} = \begin{bmatrix} a_{11}^o & a_{12}^o & \dots & a_{1n}^o \\ a_{21}^o & a_{22}^o & \dots & a_{2_n}^o \\ \dots & \dots & \dots & \dots \\ a_{f_1}^o & a_{f2}^o & \dots & a_{f_n}^o \end{bmatrix}, \quad (6)$$

де $a_{11}^o \dots a_{fn}^o$– нормовані значення відповідних наслідків.

Після формування усіх матриць для кожного рішення обчислюється його ефективність за формулою:

$$E_{r_j} = \sum_{i=1}^{n} k_i * n_{i_j} * n_{ij}^o \quad (7)$$

Висновки. У статті було розглянуто задачу оцінювання ефективності рішень систем захисту інформації. Аналіз зазначеної задачі показав, що вона є задачею багатокритеріальної оптимізації і потребує для свого вирішення задіювання відповідних методів. Виявлено, що існуючі методи оцінювання ефективності рішень не задовольняють вирішенню даної задачі, а тому не можуть бути використані. Було запропоновано удосконалений метод, який базується на використанні матриці відношення критеріїв та врахуванні наслідків рішень. Запропонований метод оцінювання ефективності рішень дозволяє підвищити відсоток визначених правильних рішень та має наступні переваги:

- результатом завжди є єдине та ефективне рішення;
- усунена можливість компенсації значень часткових критеріїв.

Зазначений метод був реалізований та апробований у підсистемі оцінювання ефективності рішень системи виявлення вторгнень на базі мереж глибинного навчання та як засіб багатокритеріальної оптимізації рішень для системи захисту комп'ютерних систем.

Література

1. Штойер Р. Многокритериальная оптимизация. Теория вычислений и приложения/ Р. Штойер. – М.: Наука, 1992. – 204 с.

2. Саати Т. Принятие решений. Метод анализа иерархий/ Т. Саати. – М.: Радио и Связь, 1993. – 320 с.

3. Кини Р.Л. Принятие решений при многих критериях: предпочтения и замещения/ Р.Л. Кини, Х. Райфа. – М.: Радио и связь, 1981. – 560 с.

4. Тітова В.Ю. Класифікація моделей загроз в комп'ютерних системах/ В.Ю. Тітова, Ю.П. Кльоц, С.О. Савчук. – Вісник Хмельницького національного університету. – №2, 2020 (283). – С. 201-204.

References

1. Shtoyer R. Mnogokriterialnaya optimizatsiya. Teoriya vyichisleniy i prilozheniya/ R. Shtoyer. – M.: Nauka, 1992. – 204 s.

2. Saati T. Prinyatie resheniy. Metod analiza ierarhiy/ T. Saati. – M.: Radio i Svyaz, 1993. – 320 s.

3. Kini R.L. Prinyatie resheniy pri mnogih kriteriyah: predpochteniya i zamescheniya/ R.L. Kini, H. Rayfa. – M.: Radio i svyaz, 1981. – 560 c.

4. Titova V.Iu. Klasyfikatsiia modelei zahroz v kompiuternykh systemakh/ V.Iu. Titova, Yu.P. Klots, S.O. Savchuk. – Visnyk Khmelnytskoho natsionalnoho universytetu. – №2, 2020 (283). – S. 201-204.

Надійшла / Paper received : 23.09.2020 р. Надрукована/Printed : 27.11.2020 р.