ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 004.056:004.052

А.Б. КАЧИНСЬКИЙ, В.М. ТКАЧ, А.А. ПОДЕНКО

ІЄРАРХІЯ ФАКТОРІВ ТИПОВИХ СЦЕНАРІЇВ РЕАЛІЗАЦІЇ DDOS-АТАК

(частина ІІ)

Анотація. *Запропоновано перелік рекомендацій щодо запобігання реалізації DDoS-атак залежно від об'єкта захисту на основі аналізу сценаріїв реалізації методами аналізу ієрархій та аналізу мереж.*
Ключові слова: *DDoS-атака, особа, суспільство, держава, когнітивні карти, ієрархія факторів, метод аналізу ієрархій.*

Вступ

У попередній статті [1] було розглянуто сутність DDoS-атак [2], наведено перелік їх основних причинних факторів, а також запропоновано методологію застосування ієрархічної структуризації когнітивних карт. Це дозволяє усувати причинні фактори реалізації DDoS-атак для різних сценаріїв, а саме: безпека особи, суспільства та держави.

У розвиток вищенаведеного, пропонується проведення аналізу сценаріїв та відповідних їм ієрархічних структур, кінцевою метою якого є формування рекомендацій щодо запобігання реалізації DDoS-атак.

1. Обґрунтування вибору інструментів аналізу

В даній статті за допомогою методу аналізу ієрархій (MAI) та методу аналізу мереж (MAM) [3] було здійснено аналіз сценаріїв реалізації DDoS-атак, що були розглянуті в попередній роботі, зокрема, для основних об'єктів захисту національної безпеки: особи, суспільства та держави. Вибір таких математичних методів спричинений тим, що за допомогою цих методів можна дати відповідь на питання, наскільки сильно окремі чинники певних рівнів впливають на інші рівні. В даному випадку – визначити пріоритетність рівнів. Для визначення таких показників, як пріоритети елементів (оцінка впливу зацікавлених сторін на вибір фактора), пріоритети критеріїв відносно елементів (ступені важливості критеріїв для зацікавлених сторін) та пріоритети альтернатив відносно критеріїв використовувалися алгоритми пошуку в глибину та ширину отриманих раніше ієрархій. Також для кожного сценарію були наведені відповідні таблиці порівнянь.

© А.Б. Качинський, В.М. Ткач, А.А. Поденко, 2018

Таким чином, було здійснено 2-й крок MAI – обчислення локальних пріоритетів та здійснена оцінка узгодженості суджень. Далі у статті наводиться процес синтезу пріоритетів альтернатив та оцінюється загальна узгодженість ієрархій.

2. Аналіз сценаріїв реалізації DDoS-атаки

Визначення пріоритетів здійснимо методом пошуку в глибину з урахуванням ієрархічного рівня фактора. Для цього застосуємо MAI, що дає змогу оцінити величину впливу факторів, які знаходяться на вищих ієрархічних рівнях, на фактори нижніх рівнів для всіх сценаріїв реалізації DDoS-атак.

Процес отримання оцінки величини впливу факторів наведено для рівня особи, як демонстрація методики розрахунку. Для інших рівнів – суспільства, держави – наведено лише результати.

Дослідимо вплив фактора x_1, що знаходиться на 1-му рівні ієрархії, на фактори нижчих рівнів. Для цього побудуємо граф пріоритетів, який ілюструє вплив фактора x_1 на решту факторів (рис. 1) для ієрархічно структурованого графу відповідного сценарію (див. [1], рис. 4).

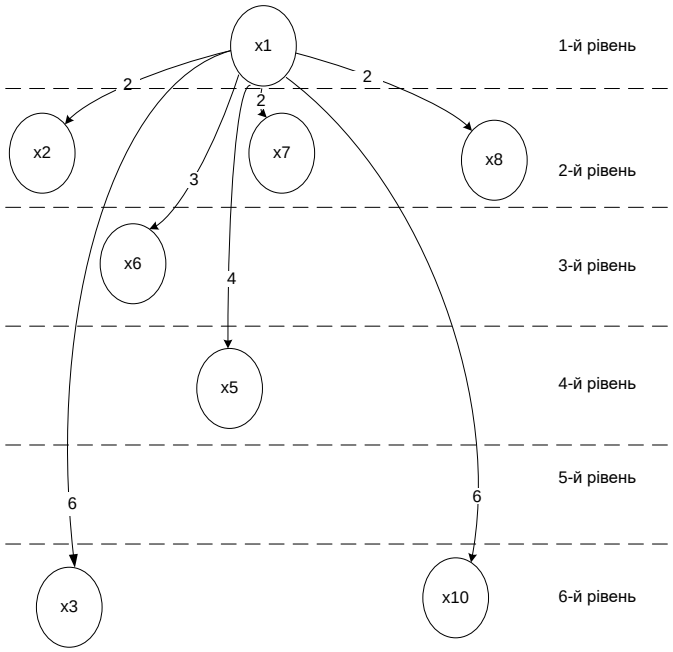

Рисунок 1 – Граф пріоритетів факторів відносно фактора x_1

Проведемо оцінку величини переваги одних факторів над іншими відносно фактора x_1. Для визначення переваги факторів один над одним застосуємо один з найбільш математично обґрунтованих методів – метод власного вектору. Отримані величини запишемо в таблицю порівнянь (табл. 1).

Таблиця 1 – Таблиця порівнянь для фактора x_1

x_1	x_2	x_3	x_5	x_6	x_7	x_8	x_{10}
x_2	1	0,333	0,5	0,667	1	1	0,333
x_3	3	1	1,5	2	3	3	1
x_5	2	0,667	1	1,333	2	2	0,667
x_6	1,5	0,5	0,75	1	1,5	1,5	0,5
x_7	1	0,333	0,5	0,667	1	1	0,333
x_8	1	0,333	0,5	0,667	1	1	0,333
x_{10}	3	1	1,5	2	3	3	1

Таблиця 1 відповідає матриці порівнянь для даного фактора x_1. Знайдемо тепер власний вектор та власне значення λ для одержаної матриці D_1.

$$D_1 = \begin{pmatrix} 1 & 0,333 & 0,5 & 0,667 & 1 & 1 & 0,333 \\ 3 & 1 & 1,5 & 2 & 3 & 3 & 1 \\ 2 & 0,667 & 1 & 1,333 & 2 & 2 & 0,667 \\ 1,5 & 0,5 & 0,75 & 1 & 1,5 & 1,5 & 0,5 \\ 1 & 0,333 & 0,5 & 0,667 & 1 & 1 & 0,333 \\ 1 & 0,333 & 0,5 & 0,667 & 1 & 1 & 0,333 \\ 3 & 1 & 1,5 & 2 & 3 & 3 & 1 \end{pmatrix}$$

Додаємо елементи рядків і запишемо результат у вигляді вектору-стовпчика $\overrightarrow{b_1}$, отримаємо:

$$\overrightarrow{b_1} = \begin{pmatrix} 4,833 \\ 14,5 \\ 9,667 \\ 7,25 \\ 4,833 \\ 4,833 \\ 14,5 \end{pmatrix}$$

Далі підсумовуємо всі елементи вектору-стовпчика $\overrightarrow{b_1}$, отримуємо $\sum b_i = 60,417$.

Розділимо на одержану суму всі елементи вектору-стовпчика $\overrightarrow{b_1}$ та отримаємо вектор пріоритетів (корисності) $\overrightarrow{W_1}$:

$$\overrightarrow{W_1} = \begin{pmatrix} 0,08 \\ 0,24 \\ 0,16 \\ 0,12 \\ 0,08 \\ 0,08 \\ 0,24 \end{pmatrix}$$

Отже, фактор x_1 може впливати в такому співвідношенні на фактори нижчих рівнів (табл. 2):

Таблиця 2 – Пріоритети впливу фактора на фактори нижчих рівнів

Позначення фактора	Пріоритет фактора (%)	Зміст фактора
x_1 – недосконаліть законодавчої бази (правовий аспект)		
x_2	8%	відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект)
x_3	24%	провокація зловмисника до реалізації DDoS-атаки
x_5	16%	безкарність за проведення атак
x_6	12%	низький рівень виявлення атак
x_7	8%	доступність інформації про можливість реалізації DDoS-атаки
x_8	8%	недостатня обізнаність звичайних користувачів
x_{10}	24%	нарощування ресурсів зловмисниками

Тепер дослідимо вплив факторів, що знаходяться на 2-му рівні ієрархії, на фактори нижчих рівнів. Для цього побудуємо графи пріоритетів, які відповідно ілюструють вплив факторів x_2, x_7 (даний фактор не має залежних від нього факторів) та x_8 на фактори нижчих рівнів (рис. 2) для ієрархічно структурованого графу відповідного сценарію (див. [1], рис. 4).

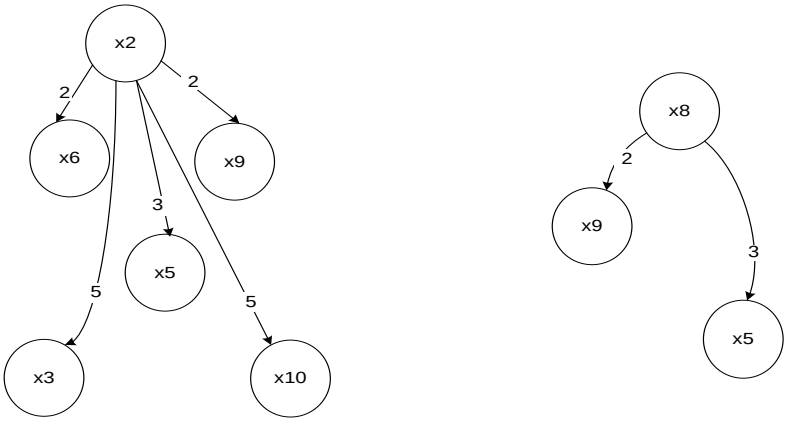

Рисунок 2 – Графи пріоритетів факторів відносно x_2 та x_8

Для даних факторів проведемо оцінку ступеня переваги одних факторів над іншими, як і для попереднього рівня. Отримані величини запишемо в таблицю порівнянь (табл. 3).

Таблиця 3 –Таблиця порівнянь для факторів x_2 та x_8

x_2	x_3	x_5	x_6	x_9	x_{10}	x_8	x_5	x_9
x_3	1	1,667	2,5	2,5	1	x_5	1	1,5
x_5	0,6	1	1,5	1,5	0,6	x_9	0,667	1
x_6	0,4	0,667	1	1	0,4			
x_9	0,4	0,667	1	1	0,4			
x_{10}	1	1,667	2,5	2,5	1			

Таблиця 3 відповідає двом матрицям порівнянь для даних факторів x_2 та x_8, знайдемо тепер власний вектор та власне значення λ для одержаних матриць D_2 та D_8 :

$$D_2 = \begin{pmatrix} 1 & 1{,}667 & 2{,}5 & 2{,}5 & 1 \\ 0{,}6 & 1 & 1{,}5 & 1{,}5 & 0{,}6 \\ 0{,}4 & 0{,}667 & 1 & 1 & 0{,}4 \\ 0{,}4 & 0{,}667 & 1 & 1 & 0{,}4 \\ 1 & 1{,}667 & 2{,}5 & 2{,}5 & 1 \end{pmatrix}, D_8 = \begin{pmatrix} 1 & 1{,}5 \\ 0{,}667 & 1 \end{pmatrix}$$

Додаємо елементи рядків і запишемо результат у вигляді вектору-стовпчика $\overrightarrow{b_2}$ та $\overrightarrow{b_8}$, отримаємо:

$$\overrightarrow{b_2} = \begin{pmatrix} 8{,}667 \\ 4 \\ 3{,}467 \\ 3{,}467 \\ 8{,}667 \end{pmatrix}, \overrightarrow{b_8} = \begin{pmatrix} 2{,}5 \\ 1{,}667 \end{pmatrix}$$

Далі підсумовуємо всі елементи вектору-стовпчика $\overrightarrow{b_2}$, отримуємо $\sum b_i = 29{,}467$ і відповідно для $\overrightarrow{b_8} - \sum b_i = 4{,}167$.

Розділимо на одержану суму всі елементи векторів-стовпчиків $\overrightarrow{b_2}$ та $\overrightarrow{b_8}$, отримаємо вектори пріоритетів (корисності) $\overrightarrow{W_2}$ та $\overrightarrow{W_8}$:

$$\overrightarrow{W_2} = \begin{pmatrix} 0{,}2941 \\ 0{,}1765 \\ 0{,}1176 \\ 0{,}1176 \\ 0{,}2941 \end{pmatrix}, \overrightarrow{W_8} = \begin{pmatrix} 0{,}6 \\ 0{,}4 \end{pmatrix}$$

Отже, фактори x_2 та x_8 можуть таким чином впливати на фактор нижчих рівнів (табл. 4):

Таблиця 4 – Пріоритети впливу фактора на фактори нижчих рівнів

Позначення фактора	Пріоритет фактора (%)	Зміст фактора
x_2 – відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект)		
x_3	29,41%	провокація зловмисника до реалізації DDoS-атаки
x_5	17,65%	безкарність за проведення атак
x_2 – відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект)		
x_6	11,76%	низький рівень виявлення атак
x_9	11,76%	невідповідна захищеність користувацьких ресурсів
x_{10}	29,41%	нарощування ресурсів зловмисниками
x_8 – недостатня обізнаність звичайних користувачів		
x_5	60%	безкарність за проведення атак
x_9	40%	невідповідна захищеність користувацьких ресурсів

Тепер дослідимо вплив факторів, що знаходяться на 3-му рівні ієрархії, на фактори нижчих рівнів. Для цього побудуємо графи пріоритетів, які відповідно ілюструють вплив факторів x_6 та x_9 (оскільки має лише один залежний фактор x_3, **тому використання маі є недоцільним**) на фактори нижчих рівнів (рис. 3) для ієрархічно структурованого графу відповідного сценарію (див. [1], рис. 4).

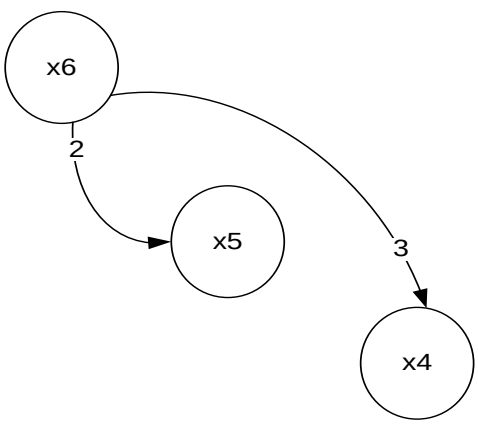

Рисунок 3 – Граф пріоритетів факторів відносно x_6

Для даного фактора проведемо оцінку ступеня переваги одних факторів над іншими, як і для попереднього рівня. Отримані величини запишемо в таблицю порівнянь (табл. 5).

Таблиця 5 – Таблиця порівнянь для фактора x_6

x_6	x_4	x_5
x_4	1	1,5
x_5	0,667	1

Таблиця 5 відповідає матриці порівнянь для фактора x_6, знайдемо тепер власний вектор та власне значення λ для матриці D_6:

$$D_6 = \begin{pmatrix} 1 & 1{,}5 \\ 0{,}667 & 1 \end{pmatrix}$$

Додаємо елементи рядків і запишемо результат у вигляді вектору-стовпчика $\overrightarrow{b_6}$, отримаємо:

$$\overrightarrow{b_6} = \begin{pmatrix} 2{,}5 \\ 1{,}667 \end{pmatrix}$$

Далі підсумовуємо всі елементи вектору-стовпчика $\overrightarrow{b_6}$, отримуємо $\sum b_i = 4{,}167$.

Розділимо на одержану суму всі елементи вектору-стовпчика $\overrightarrow{b_6}$, отримаємо вектор пріоритетів (корисності) $\overrightarrow{W_6}$:

$$\overrightarrow{W_6} = \begin{pmatrix} 0{,}6 \\ 0{,}4 \end{pmatrix}$$

Отже, фактор x_6 може таким чином впливати на фактор нижчих рівнів (табл. 6):

Таблиця 6 – Пріоритети впливу фактора на фактори нижчих рівнів

Позначення фактора	Пріоритет фактора (%)	Зміст фактора
x_6 – низький рівень виявлення атак		
x_4	60%	грошовий інтерес зловмисників
x_5	40%	безкарність за проведення атак

Виконаємо аналогічні дії для дослідження впливу факторів x_5 та x_4, що знаходяться відповідно на 4-му та 5-му рівнях ієрархії, на фактори нижчих рівнів. Побудуємо граф пріоритетів, для факторів x_5 та x_4 (рис. 4).

Для даних факторів проведемо оцінку ступеня переваги одних факторів над іншими, як і для попереднього рівня. Отримані величини запишемо в таблицю порівнянь (табл. 7).

Таблиця 7 – Таблиця порівнянь для фактора x_5 та x_4

x_5	x_3	x_4	x_4	x_3	x_{10}
x_3	1	1,5	x_3	1	1
x_4	0,667	1	x_{10}	1	1

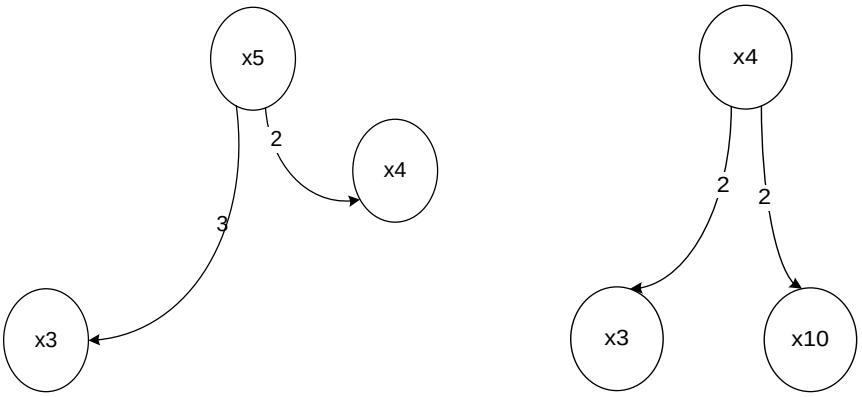

Рисунок 4 – Граф пріоритетів факторів відносно x_5 та x_4

Таблиця 7 відповідає матриці порівнянь для фактора x_5 та x_4, знайдемо тепер власний вектор та власне значення λ для матриці D_5 та D_4:

$$D_5 = \begin{pmatrix} 1 & 1{,}5 \\ 0{,}667 & 1 \end{pmatrix}, D_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Додаємо елементи рядків і запишемо результат у вигляді вектору-стовпчика $\overrightarrow{b_5}$ та $\overrightarrow{b_4}$, отримаємо:

$$\overrightarrow{b_5} = \begin{pmatrix} 2{,}5 \\ 1{,}667 \end{pmatrix}, \overrightarrow{b_4} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

Далі підсумовуємо всі елементи вектору-стовпчика $\overrightarrow{b_5}$, отримуємо $\sum b_i = 4{,}167$, для $\overrightarrow{b_4} - \sum b_i = 4$.

Розділимо на одержану суму всі елементи вектору-стовпчика $\overrightarrow{b_5}$ та $\overrightarrow{b_4}$, отримаємо вектор пріоритетів (корисності) $\overrightarrow{W_5}$ та $\overrightarrow{W_4}$:

$$\overrightarrow{W_5} = \begin{pmatrix} 0{,}6 \\ 0{,}4 \end{pmatrix}, \overrightarrow{W_4} = \begin{pmatrix} 0{,}5 \\ 0{,}5 \end{pmatrix}$$

Отже, фактори x_5 та x_4 можуть таким чином впливати на фактори нижчих рівнів (табл. 8):

Таблиця 8 – Пріоритети впливу фактора на фактори нижчих рівнів

Позначення фактора	Пріоритет фактора (%)	Зміст фактора
x_5 – безкарність за проведення атак		
x_3	60%	провокація зловмисника до реалізації DDoS-атаки
x_4	40%	грошовий інтерес зловмисників
x_4 – грошовий інтерес зловмисників		
x_3	50%	провокація зловмисника до реалізації DDoS-атаки
x_{10}	50%	нарощування ресурсів зловмисниками

Оскільки решта факторів даного сценарію мають не більше одного залежного фактора, тому використання методу аналізу ієрархій для їх дослідження є недоцільним.

Побудуємо структурований граф ієрархії для даного сценарію, з відображенням визначених пріоритетів факторів (рис. 5).

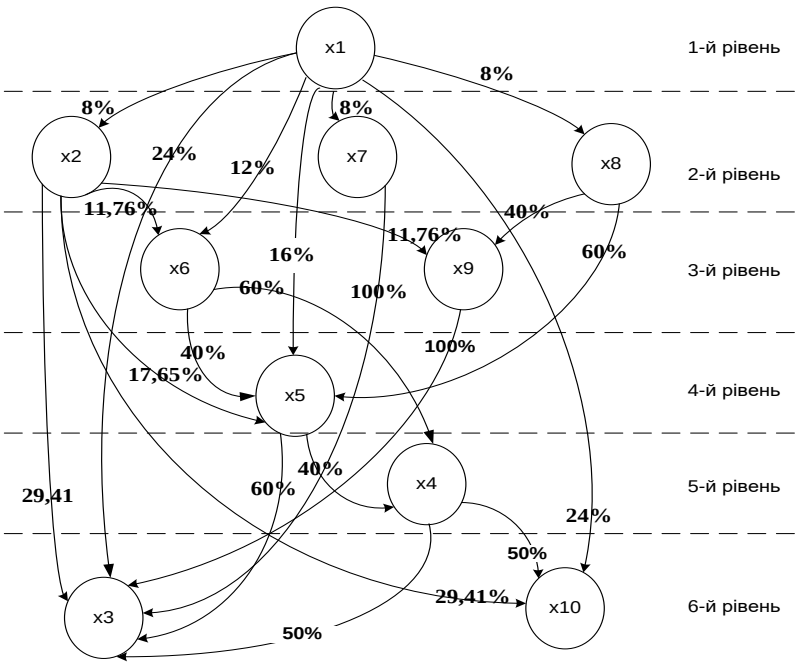

Рисунок 5 – Розподіл пріоритетів в ієрархії для сценарію реалізації DDoS-атаки як загрози безпеці особи

Аналогічні обчислення для сценаріїв реалізації DDoS-атаки як загрози безпеці суспільства та держави (див. [1], рис. 6, рис. 8 відповідно) представлено на рис. 6, рис. 7.

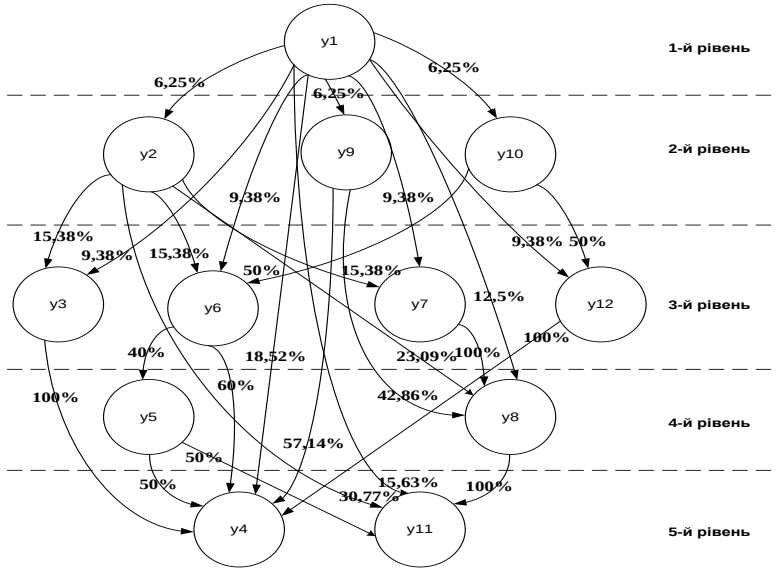

Рисунок 6 – Розподіл пріоритетів в ієрархії для сценарію реалізації DDoS-атаки як загрози безпеці суспільства

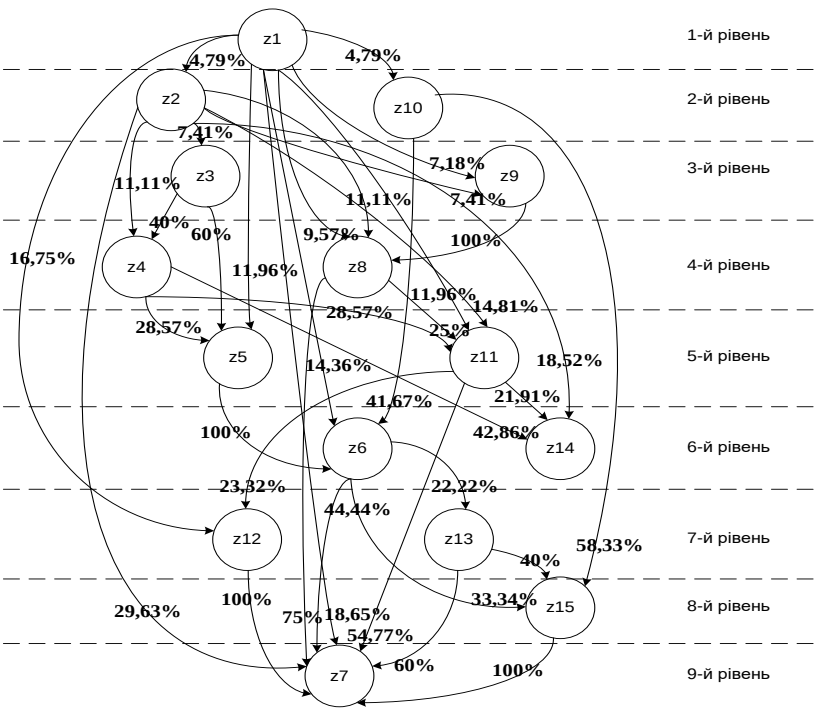

Рисунок 7 – Розподіл пріоритетів в ієрархії для сценарію реалізації DDoS-атаки як загрози безпеці держави

3. Аналіз сценаріїв реалізації DDoS-атак із застосуванням МАМ

Застосуємо метод аналізу мереж для визначення величини впливу факторів, що знаходяться на вищих рівнях, на фактори нижніх рівнів мережі для даного

сценарію реалізації DDoS-у. Для визначення пріоритетів застосуємо метод пошуку в глибину з урахуванням ієрархічного рівня фактора (рис. 8).

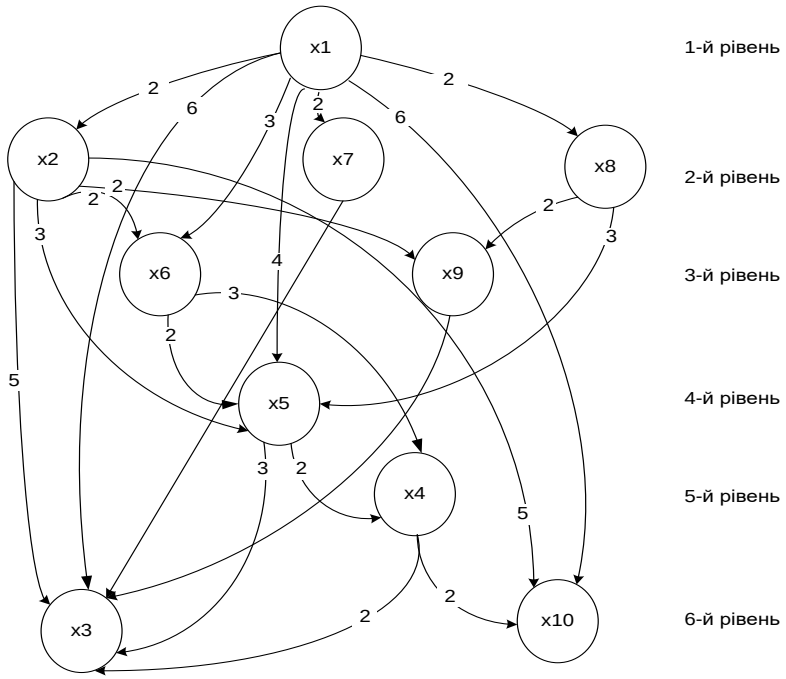

Рисунок 8 – Мережа взаємовпливів для сценарію реалізації DDoS-атаки як загрози безпеці особи

Скористаємось результатами методу парних порівнянь та побудуємо суперматрицю взаємних впливів компонентів мережі (табл. 9).

Таблиця 9 – Суперматриця для сценарію реалізації DDoS-атаки як загрози безпеці особи

№	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	0	0	0	0	0
2	0,08	0	0	0	0	0	0	0	0	0
3	0,24	0,29411765	0	0,5	0,6	0	1	0	1	0
4	0	0	0	0	0,4	0,6	0	0	0	0
5	0,16	0,17647059	0	0	0	0,4	0	0,6	0	0
6	0,12	0,11764706	0	0	0	0	0	0	0	0
7	0,08	0	0	0	0	0	0	0	0	0
8	0,08	0	0	0	0	0	0	0	0	0
9	0	0,11764706	0	0	0	0	0	0,4	0	0
10	0,24	0,29411765	0	0,5	0	0	0	0	0	0

Таблиця 9 відповідає суперматриці для даного сценарію W:

$$W = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0{,}08 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0{,}24 & 0{,}294118 & 0 & 0{,}5 & 0{,}6 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0{,}4 & 0{,}6 & 0 & 0 & 0 & 0 \\ 0{,}16 & 0{,}176471 & 0 & 0 & 0 & 0{,}4 & 0 & 0{,}6 & 0 & 0 \\ 0{,}12 & 0{,}117647 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0{,}08 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0{,}08 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0{,}176471 & 0 & 0 & 0 & 0 & 0 & 0{,}4 & 0 & 0 \\ 0{,}24 & 0{,}294118 & 0 & 0{,}5 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Знайдемо тепер граничну суперматрицю, послідовно підносячи суперматрицю в степені, поки значення елементів практично не перестануть змінюватись.

Таблиця 10 – Гранична суперматриця (W^2)

№	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0.19952941176	0.2235294118	0	0	0.2	0.54	0	0.76	0	0
4	0.136	0.1411764706	0	0	0	0.16	0	0.24	0	0
5	0.11011764704	0.0470588236	0	0	0	0	0	0	0	0
6	0.00941176472	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0.04141176472	0	0	0	0	0	0	0	0	0
10	0.02352941176	0	0	0	0.2	0.3	0	0	0	0

Як результат проведеного аналізу мережі отримуємо такі головні фактори для даного сценарію DDoS-у: x_1, x_2, x_5, x_6, x_8 , розподіл пріоритетів впливу яких показаний в табл. 11.

Таблиця 11 – Розподіл пріоритетів факторів

Позначення фактора	Пріоритет фактора (%)	Зміст фактора
1	2	3
x_1 – недосконаліть законодавчої бази (правовий аспект)		
x_3	19,95%	провокація зловмисника до реалізації DDoS-атаки
x_4	13,6%	грошовий інтерес зловмисників
x_5	11,01%	безкарність за проведення атак
x_6	0,94%	низький рівень виявлення атак
x_9	4,14%	невідповідна захищеність користувацьких ресурсів
x_{10}	2,35%	нарощування ресурсів зловмисниками

Продовження таблиці 11

1	2	3
x_2 – відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект)		
x_3	22,35%	провокація зловмисника до реалізації DDoS-атаки
x_4	14,12%	грошовий інтерес зловмисників
x_5	4,71%	безкарність за проведення атак
x_6 – низький рівень виявлення атак		
x_3	54%	провокація зловмисника до реалізації DDoS-атаки
x_4	16%	грошовий інтерес зловмисників
x_{10}	30%	нарощування ресурсів зловмисниками
x_5 – безкарність за проведення атак		
x_3	20%	провокація зловмисника до реалізації DDoS-атаки
x_{10}	20%	нарощування ресурсів зловмисниками
x_8 – недостатня обізнаність звичайних користувачів		
x_3	76%	провокація зловмисника до реалізації DDoS-атаки
x_4	24%	грошовий інтерес зловмисників

Отримані результати, подані в табл. 11, дозволяють дещо спростити побудовану в [1] когнітивну карту даного сценарію. Також, як бачимо, фактор «доступність інформації про можливість реалізації DDoS-атаки» суттєво не впливає на решту факторів та ним можна знехтувати, а фактори «правовий аспект», «організаційний аспект», «недостатня обізнаність звичайних користувачів» є такими, мінімізація впливу яких – першочергове завдання при організації процесу запобігання причинам реалізації DDoS-атак для даного сценарію.

Аналогічно для двох інших сценаріїв реалізації DDoS-атак отримаємо такі таблиці (табл. 12, табл. 13).

Таблиця 12 – Розподіл пріоритетів факторів

Позначення фактора	Пріоритет фактора (%)	Зміст фактора
1	2	3
y_1 – недосконаліть законодавчої бази (правовий аспект)		
y_3	0,96%	сприятливе для реалізації DDoS-су конкурентне середовище
y_4	27,96%	провокація зловмисників до реалізації DDoS-атак
y_5	3,75%	грошовий інтерес зловмисника

Продовження таблиці 12

1	2	3
y_6	4,09%	безкарність за проведення атак
y_7	0,96%	низький рівень виявлення атак
y_8	13,5%	самоорганізація зловмисників у злочинні угруповання
y_{11}	1,92%	нарощування ресурсів зловмисників
y_{12}	3,12%	застарілість використовуваного програмного та апаратного забезпечення
y_2 – організаційний аспект (відсутність налагоджених процедур виявлення кіберзлочинців)		
y_4	24,62%	сприятливе для реалізації DDoS-су конкурентне середовище
y_5	6,15%	грошовий інтерес зловмисника
y_8	15,38%	самоорганізація зловмисників у злочинні угруповання
y_6– безкарність за проведення атак		
y_4	20%	провокація зловмисників до реалізації DDoS-атак
y_{11}	20%	нарощування ресурсів зловмисників
y_{10} – недостатня обізнаність працівників компаній		
y_4	80%	сприятливе для реалізації DDoS-су конкурентне середовище
y_5	20%	грошовий інтерес зловмисника

Таблиця 13 – Розподіл пріоритетів факторів

Позначення фактора	Пріоритет фактора (%)	Зміст фактора
1	2	3
z_1 – недосконаліть законодавчої бази		
z_3	0,35%	внутрішня політична боротьба
z_4	0,53%	агресія держав
z_6	13,96%	відсутність достатнього фінансування державних структур, що займаються проблемами інформаційної безпеки
z_7	38,28%	сприятливі умови для реалізації DDoS-атак
z_8	7,71%	безкарність за проведення атак
z_9	0,35%	низький рівень виявлення атак
z_{11}	3,1%	самоорганізація зловмисників у злочинні угруповання
z_{12}	2,79%	доступність інформації про можливість реалізації DDoS-атаки

Продовження таблиці 13

1	2	3
z_{13}	3,19%	низький рівень кваліфікації співробітників
z_{14}	3,51%	нарощування ресурсів зловмисників
z_{15}	7,58%	застарілість використовуваного програмного та апаратного забезпечення
z_2 – відсутність налагоджених процедур виявлення кіберзлочинців		
z_4	2,96%	агресія держав
z_5	7,62%	незадовільна робота влади
z_7	16,45%	сприятливі умови для реалізації DDoS-атак
z_8	7,40%	безкарність за проведення атак
z_{11}	5,95%	самоорганізація зловмисників у злочинні угруповання
z_{12}	3,46%	доступність інформації про можливість реалізації DDoS-атаки
z_{14}	8,01%	нарощування ресурсів зловмисників
z_3 – внутрішня політична боротьба		
z_5	11,43%	незадовільна робота влади
z_6	60%	відсутність достатнього фінансування державних структур, що займаються проблемами інформаційної безпеки
z_{11}	11,42%	самоорганізація зловмисників у злочинні угруповання
z_{14}	17,14%	нарощування ресурсів зловмисників
z_4 – агресія держав		
z_6	28,57%	відсутність достатнього фінансування державних структур, що займаються проблемами інформаційної безпеки
z_7	15,65%	сприятливі умови для реалізації DDoS-атак
z_{12}	6,66%	доступність інформації про можливість реалізації DDoS- атаки
z_{14}	6,29%	нарощування ресурсів зловмисників
z_5– незадовільна робота влади		
z_7	44,44%	сприятливі умови для реалізації DDoS-атак
z_{13}	22,22%	низький рівень кваліфікації співробітників
z_{15}	33,33%	застарілість використовуваного програмного та апаратного забезпечення

Продовження таблиці 13

1	2	3
z_6 – відсутність достатнього фінансування державних структур, що займаються проблемами інформаційної безпеки		
z_7	46,66%	сприятливі умови для реалізації DDoS-атак
z_{15}	8,89%	застарілість використовуваного програмного та апаратного забезпечення
z_8– безкарність за проведення атак		
z_7	13,69%	сприятливі умови для реалізації DDoS-атак
z_{12}	5,83%	доступність інформації про можливість реалізації DDoS- атаки
z_{14}	5,48%	нарощування ресурсів зловмисників
z_9– низький рівень виявлення атак		
z_7	75%	сприятливі умови для реалізації DDoS-атак
z_{11}	25%	самоорганізація зловмисників у злочинні угруповання
z_{10} – легковажне ставлення до інформаційної безпеки		
z_7	76,85%	сприятливі умови для реалізації DDoS-атак
z_{13}	9,26%	низький рівень кваліфікації співробітників
z_{15}	13,89%	застарілість використовуваного програмного та апаратного забезпечення
z_{11} – самоорганізація зловмисників у злочинні угруповання		
z_7	23,32%	сприятливі умови для реалізації DDoS-атак
z_{13} – низький рівень кваліфікації співробітників		
z_7	40%	сприятливі умови для реалізації DDoS-атак

Слід відмітити, що для сценарію реалізації DDoS-атаки як загрози безпеці суспільства фактор «доступність інформації про можливість реалізації DDoS-атаки» суттєво не впливає на решту факторів та ним можна знехтувати, а фактори «правовий аспект», «організаційний аспект», «недостатня обізнаність працівників компанії» є такими, мінімізація впливу яких – першочергове завдання при запобіганні реалізації DDoS-атак для даного сценарію.

Також, як бачимо, для сценарію реалізації DDoS-атаки як загрози безпеці держави фактори «правовий аспект», «організаційний аспект», «легковажне ставлення до інформаційної безпеки» та «застарілість використовуваного програмного та апаратного забезпечення» є такими, мінімізація впливу яких – першочергове завдання при організації процесу запобігання причинам реалізації DDoS-атак для даного сценарію.

4. Рекомендації щодо запобігання реалізації DDoS-атаки

Завершальним етапом проведеного дослідження природи DDoS-атак, виконаного із застосуванням когнітивного підходу, що включає сценарне прогнозування та ієрархічну структуризацію отриманих когнітивних карт із подальшим їх аналізом, є формування рекомендацій.

Першим кроком організації запобігання DDoS-су є визначення специфіки об'єкта захисту та вибір відповідного сценарію: DDoS-атаки як загрози безпеці особи; як загрози безпеці суспільства; як загрози безпеці держави.

Далі для обраного сценарію визначаємо множину факторів впливу й відповідно усуваємо чи мінімізуємо величину їх впливів. Кожний з отриманих факторів має певний пріоритет його усунення, тому необхідно дотримуватись такої послідовності нейтралізації їх впливів:

Сценарій реалізації DDoS-атаки як загрози безпеці особи

1-й пріоритет:

– недосконалість законодавчої бази (правовий аспект);
– відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект);
– доступність інформації про можливість реалізації DDoS-атаки;

2-й пріоритет:

– безкарність за проведення атак;
– низький рівень виявлення атак;
– недостатня обізнаність звичайних користувачів;

3-й пріоритет:

– провокація зловмисника до реалізації DDoS-атаки;
– грошовий інтерес зловмисників;
– невідповідна захищеність користувацьких ресурсів;
– нарощування ресурсів зловмисниками.

Сценарій реалізації DDoS-атаки як загрози безпеці суспільства

1-й пріоритет:

– правовий аспект (недосконалість законодавчої бази);
– організаційний аспект (відсутність налагоджених процедур виявлення кіберзлочинців);
– недостатня обізнаність працівників компаній;

2-й пріоритет:

– безкарність за проведення атак;

3-й пріоритет:

– сприятливе для реалізації DDoS-су конкурентне середовище;
– провокація зловмисників до реалізації DDoS-атак;
– грошовий інтерес зловмисника;
– низький рівень виявлення атак;
– самоорганізація зловмисників у злочинні угруповання;
– нарощування ресурсів зловмисників;
– застарілість використовуваного програмного та апаратного забезпечення.

Сценарій реалізації DDoS-атаки як загрози безпеці держави

1-й пріоритет:

– недосконалість законодавчої бази (правовий аспект);

– відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект);
– легковажне ставлення до інформаційної безпеки;
– застарілість використовуваного програмного та апаратного забезпечення;

2-й пріоритет:

– агресія держав;
– незадовільна робота влади;
– відсутність достатнього фінансування державних структур, що займаються проблемами інформаційної безпеки;
– безкарність за проведення атак;
– низький рівень виявлення атак;
– самоорганізація зловмисників у злочинні угруповання;
– низький рівень кваліфікації співробітників;

3-й пріоритет:

– внутрішня політична боротьба;
– сприятливі умови для реалізації DDoS-атак;
– доступність інформації про можливість реалізації DDoS-атаки;
– нарощування ресурсів зловмисників.

Висновки

В результаті проведення аналізу для кожного зі сценаріїв реалізації DDoS-атак, визначено перелік головних факторів, розподіл пріоритетів базисних факторів та їх доцільність розгляду. На основі отриманих результатів сформовано рекомендації щодо запобігання реалізації DDoS-атак.

Дослідження сценаріїв реалізації DDoS-атак показало, що отримані пріоритети для об'єктів захисту різних рівнів – особи, суспільства, держави – містять певні спільні фактори з найвищим пріоритетом:

– недосконаліть законодавчої бази (правовий аспект);
– відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект);

Обрані технології та методи використовуються вперше для вирішення визначених завдань та цілей проведеного дослідження. Перспективним напрямом подальшого дослідження можна вважати вирішення управлінських завдань вдосконалення існуючої системи забезпечення кібернетичної безпеки.

СПИСОК ЛІТЕРАТУРИ

1. Качинський А.Б., Ткач В.М., Поденко А.А. Ієрархія факторів типових сценаріїв реалізації DDOS-атак. Частина 1 // Математическое моделирование в экономике. – 2017. – № 1–2.
2. DDoS-атаки. Причины возникновения, классификация и защита от DDoS-атак [Електронний ресурс] / efsol.ru – 2015. – Режим доступу до ресурсу: http://efsol.ru/articles/ddos-attacks.html
3. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.

Стаття надійшла до редакції 24.01.2017.