УДК 004.056:004.052

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

ІЄРАРХІЯ ФАКТОРІВ ТИПОВИХ СЦЕНАРІЇВ РЕАЛІЗАЦІЇ DDOS-АТАК (*частина І*)

Анотація. *Запропоновано методологію ієрархічної структуризації когнітивних карт, що дозволяє визначити пріоритетність усунення причинних факторів для запобігання реалізації DDoS-атак.*
Ключові слова: *DDoS-атака, особа, суспільство, держава, когнітивні карти, ієрархія факторів, метод аналізу ієрархій.*

Вступ

Стрімкий розвиток новітніх технологій та інформатизації суспільства зумовлює появу не лише можливостей, але й загроз різних рівнів: від персональних – до загроз суспільству або державі. Зокрема, гостро постає проблема захисту від DDoS-атак. Особливої уваги потребує питання організації механізмів запобігання їм, оскільки своєчасне виявлення загрозливих факторів дозволяє не лише зберегти стабільність інформаційних систем різних рівнів, але й уникнути значних матеріальних витрат на відновлення їх нормального функціонування.

1. Сучасний стан речей

DDoS-атака – «розподілена відмова в обслуговуванні» (англ. – Distributed Denial-of-service attack) – спрямована на обчислювальну систему, з метою створення таких умов, за яких користувачі системи не можуть отримати доступ до деяких ресурсів або сервісів [1]. Враховуючи загрозу, що становлять DDoS-атаки, гостро постає потреба в розробці типових сценаріїв реалізації DDoS-атак, для побудови когнітивних карт, що є основою для прогнозування DDoS-атак різної природи, а також визначення рекомендацій щодо організації процесу запобігання їм.

На разі DDoS-атаки за характером використовуваних програмно-апаратних механізмів можна класифікувати наступним чином [2]:

1. Насичення смуги пропускання.
2. Атака на вичерпання системних ресурсів.
3. Недостатня перевірка даних користувача.
4. Атаки другого роду.
5. HTTP-flood.
6. ICMP-flood (Smurf-атака).
7. UDP-flood (атака Fraggle).
8. SYN-flood.
9. Надсилання «важких пакетів».
10. Переповнення серверу log-файлами.
11. Помилки програмного коду.
12. Недоліки в програмному коді.

Лабораторія Касперського у своєму квартальному звіті про загрози від 27 січня 2016 року надає таку інформацію щодо статистики розподілу DDoS-атак за типом механізмів, що використовуються (рис. 1) [3].

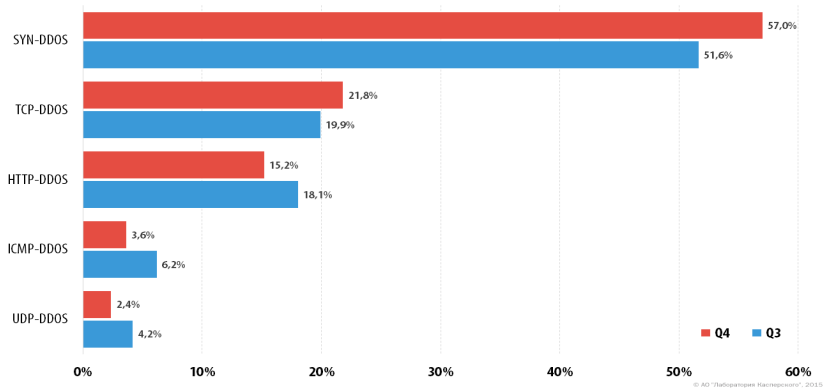

Рисунок 1 – Розподілення DDoS-атак за типами, 3-й та 4-й квартали 2015 року

Використавши дані, подані на рис. 1, отримали такі функції розподілу величин DDoS-атак за типами для 3-го та 4-го кварталів 2015 року (рис. 2):

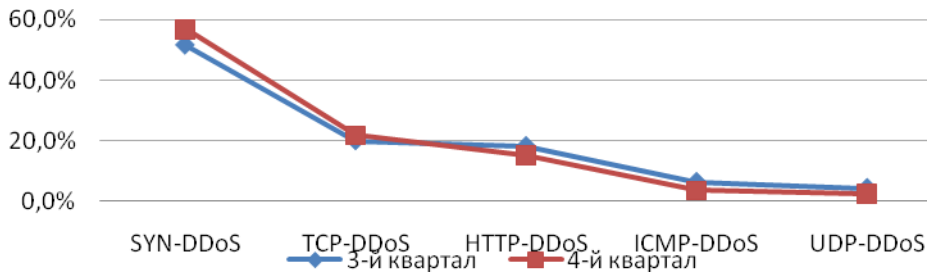

Рисунок 2 – Функції розподілу DDoS-атак за типами
для 3-го та 4-го кварталів 2015 року

Дані статистики свідчать про те, що серед зловмисників найбільш популярними методами проведення DDoS-атак є SYN-, TCP- та HTTP-DDoS.

2. Сценарій реалізації DDoS-атаки як загрози безпеці особи

Оскільки персональні ресурси користувачів мережі зазвичай не мають належного захисту та потужності, щоб протидіяти DDoS-атаці, тому у більшості ситуацій, в яких DDoS-атака здійснюється на особистість, веб-сайт людини або ж власне персональний комп'ютер, причинами можуть бути особиста неприязнь зловмисника, розвага або ж використання особистості в якості тренувальної мішені.

Окремо можна говорити про використання комп'ютерів користувачів як засобу реалізації DDoS-атаки, перетворення ресурсів користувачів в так звані «зомбі-комп'ютери». Зазвичай, «зомбування» здійснюється за допомогою троянської програми, що встановлює необхідне зловмиснику фонове

завдання. В середньому, інтенсивність DDoS-атаки, що відповідає даному сценарію, складає 100 Мбіт/с. Це еквівалентно, наприклад, тому, що на сайт зайшли 1000 користувачів і вони кожну секунду оновлюють сторінку.

Побудуємо когнітивну модель, яка дозволить проаналізувати проведення DDoS-атак під час зміни різних факторів, що впливають на неї. Для виділення факторів даного сценарію застосуємо PEST-аналіз [4, 5] та отримаємо такі результати:

Політичні:

– недосконаліть законодавчої бази (правовий фактор);

– відсутність налагоджених процедур виявлення кіберзлочинців (організаційний фактор).

Економічні:

– попит на DDoS-атаки (провокація зловмисника на здійснення DDoS-атаки);

– отримання легкого прибутку (грошовий інтерес зловмисників).

Соціальні:

– безкарність за проведення атак;

– низький рівень виявлення атак;

– доступність інформації про можливість реалізації DDoS-атаки;

– недостатня обізнаність звичайних користувачів.

Технічні:

– невідповідна захищеність користувацьких ресурсів;

– нарощування ресурсів зловмисників.

Підсумовуючи, отримуємо такий перелік факторів, які характеризують DDoS-атаки на особу, та їх умовні позначення (табл. 1).

Кожен із зазначених факторів певним чином пов'язаний з іншими (одним або декількома). Для відображення зв’язків між ними будується когнітивна карта даної проблемної ситуації.

Таблиця 1 – Перелік факторів DDoS-атаки

Позначення фактору	Зміст фактору
x_1	недосконаліть законодавчої бази (правовий аспект)
x_2	відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект)
x_3	провокація зловмисника до реалізації DDoS-атаки
x_4	грошовий інтерес зловмисників
x_5	безкарність за проведення атак
x_6	низький рівень виявлення атак
x_7	доступність інформації про можливість реалізації DDoS-атаки
x_8	недостатня обізнаність звичайних користувачів
x_9	невідповідна захищеність користувацьких ресурсів
x_{10}	нарощування ресурсів зловмисниками

За факторами, поданими в табл. 1, будуємо направлений граф причинно-наслідкових відношень, який відображає сценарій проходження DDoS-атаки на особу (рис. 3).

Опис множини факторів сценарію можна реалізувати у двох взаємопов'язаних формах: у вигляді бінарної матриці та у вигляді направленого графа [6]. Для побудови бінарної матриці, що може бути представлена у вигляді матриці досяжності, спочатку порахуємо матрицю залежності.

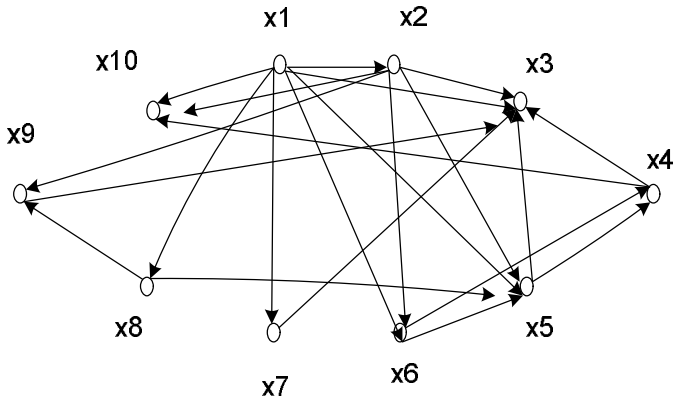

Рисунок 3 – Когнітивна карта для сценарію реалізації DDoS-атаки як загрози безпеці особи

Матриця залежності *B* заповнюється наступним чином. Якщо множина вершин H визначена, тоді за допомогою бінарного відношення «залежить від» можна заповнити матрицю так, що відповідь «так» фіксують одиницею, а відповідь «ні» фіксують нулем, тобто елемент b_{ij} матриці визначається таким чином [6]:

$$b_{ij} = \begin{cases} 1, \text{якщо } i \text{ залежить від } j \\ 0, \text{якщо } i \text{ не залежить від } j. \end{cases}$$

Отримані результати заносимо в табл. 2.

Таблиця 2 – Матриця залежності для сценарію реалізації DDoS-атаки як загрози безпеці особи

№	1	2	3	4	5	6	7	8	9	10
1	1	1	1	0	1	1	1	1	0	1
2	0	1	1	0	1	1	0	0	1	1
3	0	0	1	0	0	0	0	0	0	0
4	0	0	1	1	0	0	0	0	0	1
5	0	0	1	1	1	0	0	0	0	0
6	0	0	0	1	1	1	0	0	0	0
7	0	0	1	0	0	0	1	0	0	0
8	0	0	0	0	1	0	0	1	1	0
9	0	0	1	0	0	0	0	0	1	0
10	0	0	0	0	0	0	0	0	0	1

Матрицю досяжності D можна побудувати простішим шляхом, безпосередньо за вихідним направленням графу. Заповнення матриці бінарними елементами здійснюється за рядком (зліва направо) за правилом:

$$d_{ij} = \begin{cases} 1, \text{якщо з } i \text{ можна потрапити в } j \\ 0, \text{в іншому випадку.} \end{cases}$$

Дані заносимо в табл. 3. Використовуючи матрицю досяжності, будуємо таблицю, яка є першою ітерацією аналізу (табл. 4).

Таблиця 3 – Матриця досяжності для сценарію реалізації DDoS-атаки як загрози безпеці особи

№	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	0	1	1	1	1	1	0	0	1	1
3	0	0	1	0	0	0	0	0	0	0
4	0	0	1	1	0	0	0	0	0	1
5	0	0	1	1	1	0	0	0	0	1
6	0	0	1	1	1	1	0	0	0	1
7	0	0	1	0	0	0	1	0	0	0
8	0	0	1	1	1	0	0	1	1	0
9	0	0	1	0	0	0	0	0	1	0
10	0	0	0	0	0	0	0	0	0	1

Дана матриця досяжності дозволяє розділити всю множину вершин H на підмножину рівнів. Для цього всі вершини поділяють на досяжні та передуючі.

Вершину h_i називають досяжною з вершини h_j, якщо в орієнтованому графі існує шлях з h_j в h_i. Позначимо підмножину вершин цього шляху через $R(h_i)$. Вершину h_j називають передуючою вершиною до h_i, якщо можливе досягнення h_i з h_j. Позначимо підмножину вершин цього шляху через $A(h_i)$. $A(h_i) = R(h_i) \cap A(h_i)$ ($\cap$ – знак перетину або суміщення) недосяжні з будь-якої з вершин множини H, що залишилися, і, відповідно, може позначатись як рівень ієрархії [6].

Таблиця 4 – Перша ітерація аналізу ієрархії факторів

h_i	$R(h_i)$	$A(h_i)$	$R(h_i) \cap A(h_i)$
1	1,2,3,4,5,6,7,8,9,10	1	1
2	2,3,4,5,6,9,10	1, 2	2
3	3	1,2,3,4,5,6,7,8,9	3
4	3,4,10	1,2,4,5,6,8	4
5	3,4,5,10	1,2,5,6,8	5
6	3,4,5,6,10	1,2,6	6
7	3,7	1,7	7

8	3,4,5,8,9	1,8	8
9	3,9	1,2,8,9	9
10	10	1,2,4,5,6,10	10

З табл. 4 видно, що рівність критеріїв $A(h_i) = R(h_i) \cap A(h_i)$ виконується для елемента 1. Як наслідок, він і є елементом першого рівня ієрархії.

Викреслюючи з таблиці 4 рядок з номером 1 та прибираючи з усіх послідовностей цифру 1, отримуємо другу ітерацію (табл. 5).

Таблиця 5 – Друга ітерація побудови ієрархії факторів

h_i	$R(h_i)$	$A(h_i)$	$R(h_i) \cap A(h_i)$
2	2,3,4,5,6,9,10	2	2
3	3	2,3,4,5,6,7,8,9	3
4	3,4,10	2,4,5,6,8	4
5	3,4,5,10	2,5,6,8	5
6	3,4,5,6,10	2,6	6
7	3,7	7	7
8	3,4,5,8,9	8	8
9	3,9	2,8,9	9
10	10	2,4,5,6,10	10

Повторюючи ітерації, отримуємо остаточно шість рівнів розподілу елементів, які представлені на рис. 4.

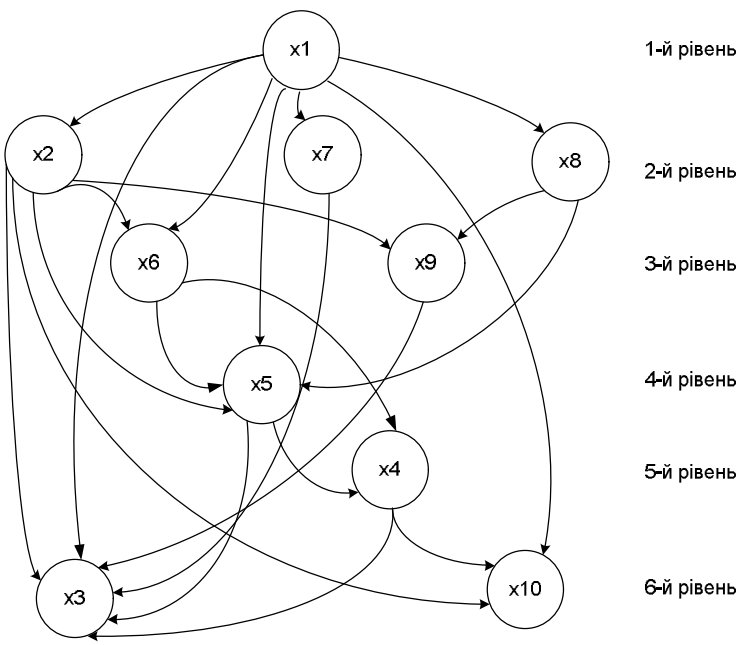

Рисунок 4 – Ієрархічно структурований граф для сценарію реалізації DDoS-атаки як загрози безпеці особи

За допомогою рис. 4 складаємо табл. 6 розподілу факторів за рівнями ієрархії.

Таблиця 6 – Ієрархічно структурований перелік факторів DDoS-атаки

Рівень ієрархії №	Позначення фактору	Зміст фактору
1	x_1	недосконаліть законодавчої бази (правовий аспект)
2	x_2	відсутність налагоджених процедур виявлення кіберзлочинців (організаційний аспект)
	x_7	доступність інформації про можливість реалізації DDoS-атаки
	x_8	недостатня обізнаність звичайних користувачів
3	x_6	низький рівень виявлення атак
	x_9	невідповідна захищеність користувацьких ресурсів
4	x_5	безкарність за проведення атак
5	x_4	грошовий інтерес зловмисників
6	x_3	провокація зловмисника до реалізації DDoS-атаки
	x_{10}	нарощування ресурсів зловмисниками

Отже, під час організації процесу реалізації механізмів запобігання загрозі DDoS-атаки для даного сценарію, в першу чергу необхідно продумати повне або часткове усунення факторів, що знаходяться на 1-му та 2-му ієрархічних рівнях. Тобто мінімізувати дію таких факторів, як: правовий аспект, організаційний аспект, доступність інформації про можливість реалізації DDoS-атаки та недостатня обізнаність звичайних користувачів.

3. Сценарій реалізації DDoS-атаки як загрози безпеці суспільства

За свідченнями правоохоронних органів України, масові DDoS-атаки на сайти українських банків, причинами виникнення яких є недобросовісна конкурентна боротьба між компаніями, шахрайство тощо, відбуваються кожного дня, причому зловмисники діють як з території нашої держави, так і з-за кордону, особливо із східних кордонів. Нині DDoS-атаки, які несуть загрозу суспільству, є найбільш популярними. Статистичні дослідження, наведені вище, свідчать про те, що найчастіше цілями атак стають ресурси інтернет-торгівлі, фінансового сектору та IT-компаній.

Побудуємо когнітивну модель, яка дозволить проаналізувати проведення DDoS-атак під час зміни різних факторів, що впливають на неї. Для даного сценарію застосуємо PEST-аналіз та отримаємо:

Політичні:

– правовий аспект – недосконаліть законодавчої бази (відсутність норм регулювання конкурентної боротьби);

– організаційний аспект – відсутність налагоджених процедур виявлення кіберзлочинців.

Економічні:

– сприятливе для реалізації DDoS-су конкурентне середовище;

– провокація зловмисників до реалізації DDoS-атак (попит на послуги зловмисників);

– грошовий інтерес зловмисника.

Соціальні:

– безкарність за проведення атак;

– низький рівень виявлення атак;

– самоорганізація зловмисників у злочинні угрупування;

– доступність інформації про можливість реалізації DDoS-атаки;

– недостатня обізнаність працівників компаній (як звичайних, так і технічних, економія на безпеці).

Технічні:

– нарощування ресурсів зловмисників (спричинене безконтрольною діяльністю в мережі Інтернет, зростанням заражених ресурсів користувачів і об'єднанням зловмисників у групи);

– застарілість використовуваного програмного та апаратного забезпечення.

Підсумовуючи, отримуємо такий перелік факторів, що характеризують DDoS-атаки на суспільство, та їх умовні позначення (табл. 7).

Таблиця 7 – Перелік факторів DDoS-атаки

Позначення фактору	Зміст фактору
y_1	правовий аспект (недосконалість законодавчої бази)
y_2	організаційний аспект (відсутність налагоджених процедур виявлення кіберзлочинців)
y_3	сприятливе для реалізації DDoS-су конкурентне середовище
y_4	провокація зловмисників до реалізації DDoS-атак
y_5	грошовий інтерес зловмисника
y_6	безкарність за проведення атак
y_7	низький рівень виявлення атак
y_8	самоорганізація зловмисників у злочинні угрупування
y_9	доступність інформації про можливість реалізації DDoS-атаки
y_{10}	недостатня обізнаність працівників компаній
y_{11}	нарощування ресурсів зловмисників
y_{12}	застарілість використовуваного програмного та апаратного забезпечення

Для відображення зв'язку між зазначеними факторами будується когнітивна карта даної проблемної ситуації. За факторами, поданими в табл. 7, будуємо направлений граф причинно-наслідкових відношень, який відображає сценарій проходження DDoS-атаки на суспільство (рис. 5).

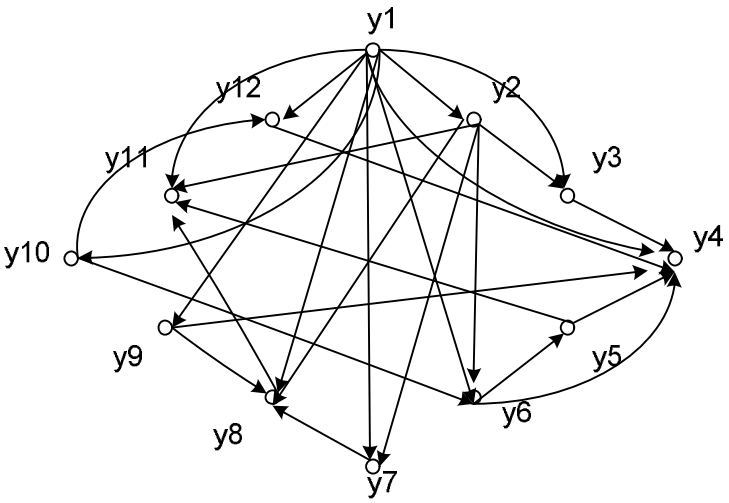

Рисунок 5 – Когнітивна карта для сценарію реалізації DDoS-атаки як загрози безпеці суспільства

Здійснюючи аналогічні для попереднього рівня операції, будуємо таблицю, що є першою ітерацією аналізу (табл. 8).

Таблиця 8 – Перша ітерація аналізу ієрархії факторів

h_i	$R(h_i)$	$A(h_i)$	$R(h_i) \cap A(h_i)$
1	1,2,3,4,5,6,7,8,9,10,11,12	1	1
2	2,3,4,5,6,7,8,11	1,2	2
3	3,4	1,2,3	3
4	4	1,2,3,4,5,6,9,10,12	4
5	4,5,11	1,2,5,6,10	5
6	4,5,6,11	1,2,6,10	6
7	7,8	1,2,7	7
8	8,11	1,2,7,8,9	8
9	4,8,9	1,9	9
10	4,5,6,10,12	1,10	10
11	11	1,2,5,6,8,11	11
12	4,12	1,10,12	12

Повторюючи ітерації, отримуємо остаточно шість рівнів розподілу елементів, які представлені на рис. 6.

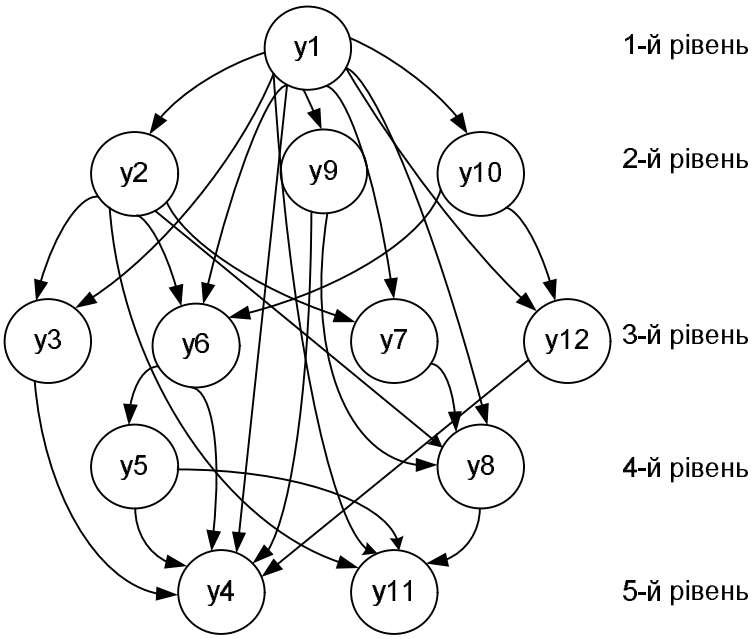

Рисунок 6 – Ієрархічно структурований граф для сценарію реалізації DDoS-атаки як загрози безпеці суспільства

За допомогою рис. 6 складаємо таблицю розподілу факторів за рівнями ієрархії (табл. 9).

Таблиця 9 – Ієрархічно структурований перелік факторів DDoS-атаки

Рівень ієрархії №	Позначення фактору	Зміст фактору
1	y_1	правовий аспект (недосконалість законодавчої бази)
2	y_2	організаційний аспект (відсутність налагоджених процедур виявлення кіберзлочинців)
	y_9	доступність інформації про можливість реалізації DDoS-атаки
	y_{10}	недостатня обізнаність працівників компаній
3	y_3	сприятливе для реалізації DDoS-атаки конкурентне середовище
	y_6	безкарність за проведення атак
	y_7	низький рівень виявлення атак
	y_{12}	застарілість використовуваного програмного та апаратного забезпечення
4	y_5	грошовий інтерес зловмисника
	y_8	самоорганізація зловмисників у злочинні угрупування
5	y_4	провокація зловмисників до реалізації DDoS-атак
	y_{11}	нарощування ресурсів зловмисників

Під час розв'язання проблеми реалізації DDoS-атаки для даного сценарію, в першу чергу необхідно продумати повне або часткове усунення факторів, що знаходяться на 1-му та 2-му ієрархічних рівнях. Тобто мінімізувати дію таких факторів, як: правовий аспект, організаційний аспект, доступність інформації про можливість реалізації DDoS-атаки та недостатня обізнаність працівників компаній.

4. Сценарій реалізації DDoS-атаки як загрози безпеці держави

Для України, зважаючи на досить складну політичну ситуацію, можна говорити про те, що проблема DDoS-атак, причиною яких є політична діяльність, досить актуальна та гостро відчутна. Варто також відзначити, що значна частка усіх DDoS-атак на державні структури припадає на веб-сайти місцевих органів влади або державних підприємств, яким майже не виділяються кошти на їх підтримку, на достойні зарплати адміністраторам та спеціалістам з безпеки. Загалом, підвищення уваги зловмисників до веб-ресурсів державних установ є світовим трендом [7].

Побудуємо когнітивну модель, яка дозволить проаналізувати проведення DDoS-атак під час зміни різних факторів, що впливають на неї. Для виділення факторів даного сценарію застосуємо PEST-аналіз та отримаємо:

Політичні:

– правовий аспект – недосконалість законодавчої бази;

– організаційний аспект – відсутність налагоджених процедур виявлення кіберзлочинців;

– внутрішня політична боротьба (сучасна геополітична ситуація);

– агресія держав (терористична діяльність, робота іноземних резидентів, яка направлена на підривання авторитету держави на міжнародній арені);

– незадовільна робота влади.

Економічні:

– відсутність достатнього фінансування державних структур та підрозділів, що займаються проблемами інформаційної безпеки;

– сприятливі умови для реалізації DDoS-атак (доступність та відносно низька вартість замовлення виконання атак).

Соціальні:

– безкарність за проведення атак;

– легковажне ставлення до інформаційної безпеки;

– самоорганізація зловмисників у злочинні угрупування;

– доступність інформації про можливість реалізації DDoS-атаки;

– низький рівень кваліфікації співробітників (як звичайних, так і технічних, економія на безпеці, дефіцит кваліфікованих кадрів).

Технічні:

– нарощування ресурсів зловмисників (спричинене безконтрольною діяльністю в мережі Інтернет, зростанням заражених ресурсів користувачів і об'єднанням зловмисників у групи);

– застарілість використовуваного програмного та апаратного забезпечення.

Підсумовуючи, отримуємо такий перелік факторів, що характеризують DDoS-атаки на державу, та їх умовні позначення (табл. 10). Для відображення зв'язку між ними будується когнітивна карта даної проблемної ситуації.

Таблиця 10 – Перелік факторів DDoS-атаки

Позначення фактору	Зміст фактору
z_1	недосконаліть законодавчої бази
z_2	відсутність налагоджених процедур виявлення кіберзлочинців
z_3	внутрішня політична боротьба
z_4	агресія держав
z_5	незадовільна робота влади
z_6	відсутність достатнього фінансування державних структур, що займаються проблемами інформаційної безпеки
z_7	сприятливі умови для реалізації DDoS-атак
z_8	безкарність за проведення атак
z_9	низький рівень виявлення атак
z_{10}	легковажне ставлення до інформаційної безпеки
z_{11}	самоорганізація зловмисників у злочинні угрупування
z_{12}	доступність інформації про можливість реалізації DDoS-атаки
z_{13}	низький рівень кваліфікації співробітників
z_{14}	нарощування ресурсів зловмисників
z_{15}	застарілість використовуваного програмного та апаратного забезпечення

За факторами, поданими в табл. 10, будуємо направлений граф причинно-наслідкових відношень, який відображає сценарій проходження DDoS-атаки на державу (рис. 7).

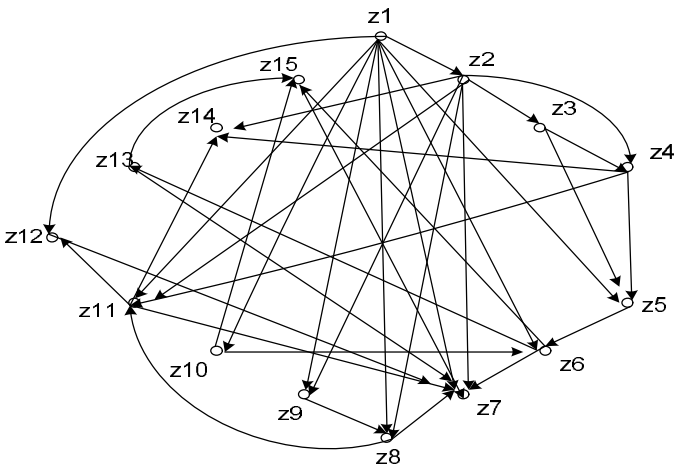

Рисунок 7 – Когнітивна карта для сценарію реалізації DDoS-атаки як загрози безпеці держави

Повторивши аналогічні до попередніх рівнів операції, отримуємо дев’ять рівнів розподілу елементів, що представлені на рис. 8.

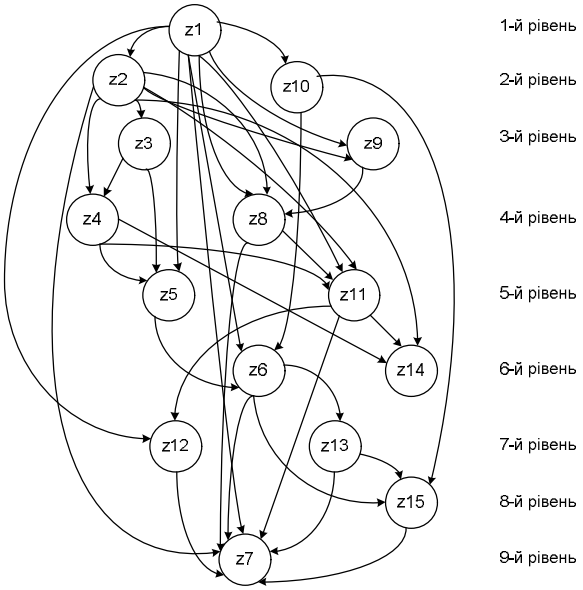

Рисунок 8 – Ієрархічно структурований граф для сценарію реалізації DDoS-атаки як загрози безпеці держави

За допомогою рис. 8 складаємо таблицю 11 розподілу факторів за рівнями ієрархії.

Таблиця 11 – Ієрархічно структурований перелік факторів DDoS-атаки

Рівень ієрархії	Позначення фактору	Зміст фактору
1	z_1	недосконаліть законодавчої бази
2	z_2	відсутність налагоджених процедур виявлення кіберзлочинців
	z_{10}	легковажне ставлення до інформаційної безпеки
3	z_3	внутрішня політична боротьба
	z_9	низький рівень виявлення атак
4	z_4	агресія держав
	z_8	безкарність за проведення атак
5	z_5	незадовільна робота влади
	z_{11}	самоорганізація зловмисників у злочинні угрупування
6	z_6	відсутність достатнього фінансування державних структур, що займаються проблемами інформаційної безпеки
	z_{14}	нарощування ресурсів зловмисників
7	z_{12}	доступність інформації про можливість реалізації DDoS-атаки
	z_{13}	низький рівень кваліфікації співробітників
8	z_{15}	застарілість використовуваного програмного та апаратного забезпечення
9	z_7	сприятливі умови для реалізації DDoS-атак

В межах реалізації механізмів запобігання DDoS-атаці для даного сценарію, в першу чергу необхідно продумати повне або часткове усунення факторів, що знаходяться на 1-му та 2-му ієрархічних рівнях. Тобто мінімізувати дію правового аспекту, організаційного аспекту та легковажного ставлення до інформаційної безпеки. За допомогою отриманих ієрархій проведено оцінку впливу характеристик рівнів один на одного із застосуванням методу аналізу ієрархій.

Висновки

Дослідження можливих сценаріїв реалізації DDoS-атак показало, що здійснення зловмисниками атак на ті чи інші об'єкти зумовлене низкою особливостей. Тому, основною методологією при моделюванні ситуацій має бути когнітивний аналіз, оскільки він дозволяє спрогнозувати розвиток подій, залежних від великої кількості взаємопов'язаних факторів.

Як результат виконання сценарного прогнозування реалізації DDoS-атак запропоновано класифікувати всі відомі на сьогоднішній день причини DDoS-атак з точки зору критеріїв головних об'єктів захисту національної безпеки – на рівнях особи, суспільства, держави. Розглянуті сценарії реалізації DDoS-атак на кожному з рівнів дають змогу спростити вибір методів запобігання DDoS-атакам залежно від специфічних особливостей об'єкта захисту.

Застосування алгоритму ієрархічної структуризації когнітивних карт дозволяє визначити пріоритетність усунення причинних факторів під час реалізації механізмів запобігання DDoS-атакам і є необхідною умовою для застосування методів аналізу впливів в отриманих графічних структурах.

СПИСОК ЛІТЕРАТУРИ

1. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.: ил.
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. Kaspersky Lab. Kaspersky Security Bulletin [Електронний ресурс] / Kaspersky Lab. – 2015. – Режим доступу до ресурсу: https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf.
4. Лапыгин Ю.Н. Теория организации. Учебник. – М.: ИНФРА-М, 2007. – 222 с.
5. Волкова В.Н., Денисов А.А. Теория систем. Учебное пособие. – М.: Высшая школа, 2006. – 511 с.: ил.
6. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.
7. Weckler A. Multiple government websites down as servers under DDoS attack [Електронний ресурс] / independent.ie – 2016. – Режим доступу до ресурсу: http://www.independent.ie/irish-news/news/multiple-government-websites-down-as-servers-under-ddos-attack-34387566.html

Стаття надійшла до редакції 08.12.16.