DOI: 10.35681/1560-9189.2019.21.4.199268

УДК 004.81:004.7.056.5

О. В. Салієва, Ю. Є. Яремчук
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі

Розроблено когнітивну модель, яка відображає рівень захищеності комп'ютерної мережі при впливі на неї потенційних загроз. Сформовано матрицю взаємовпливів концептів нечіткої когнітивної карти та розраховано основні системні показники, такі як: консонанс, дисонанс і вплив концептів на систему. Аналіз даних показників дозволив виявити найбільш небезпечні загрози мережевій безпеці, що, у свою чергу, надає можливість вчасно провести відповідні заходи для послаблення ступеню негативних наслідків або ж запобігти їм.

Ключові слова: *інформаційна безпека, загрози безпеці, комп'ютерна мережа, когнітивне моделювання, нечітка когнітивна карта.*

Вступ

Сучасне життя неможливо уявити без використання комп'ютерних мереж, які надають своїм користувачам безліч можливостей, зокрема: інтерактивність, спільний доступ до даних, швидкий обмін текстовою, звуковою та відеоінформацією у реальному часі, оперативний зворотній зв'язок, сумісне використання технічних ресурсів та ін. [1]. Для належного функціонування мережі та надійного забезпечення усіх вищеперерахованих послуг особлива увага приділяється організації мережевої безпеки. Адже комп'ютерні мережі та їхні ресурси постійно перебувають під загрозою зараження шкідливим програмним забезпеченням чи здійсненням різних типів мережевих атак. Унаслідок цих атак зловмисники можуть отримати несанкціонований доступ до інформаційних ресурсів, здійснити крадіжку, знищення або псування даних, порушити функціонування та доступність сервісу, отримати контроль над роботою усієї системи. Щоб попередити вищезазначені дії, необхідно проаналізувати вплив можливих загроз на систему, оцінити силу їхньої дії, виділивши найвагоміші із них.

Вирішення даного питання можливе за допомогою методів статистичного аналізу, зокрема, дисперсійного та кореляційно-регресійного аналізу [2]. Проте дані методи потребують складних розрахунків, наявності достатньо повної статистичної інформації, тривалого часу для опрацювання необхідних даних. У зв'язку з

цим варто звернути увагу на когнітивний підхід, який надає можливість вирішувати задачі, що не піддаються строгій формалізації, наглядно представляти досліджувану систему або проблему, використовувати неповну, нечітку інформацію та суб'єктивні судження експертів предметної області, будувати гнучкі, конструктивні моделі, які адекватно реагують на зміни.

Метод когнітивного моделювання базується на побудові нечіткої когнітивної карти (НКК), вперше запропонованої у 1986 році Бартом Коско [3]. Під нечіткою когнітивною картою розуміється математична модель досліджуваної системи, що представлена у вигляді орієнтованого графа, вершинами якого є множина факторів (концептів), які відображають найбільш вагомі, з точки зору вивчення даної проблеми, фактори. А направлені дуги графа — причинно-наслідкові (або каузальні) зв'язки між концептами, причому ваги цих зв'язків визначають силу впливу концептів один на одного [5].

На сьогодні існують різні модифікації НКК для моделювання складних систем, вони відрізняються способами подання та методами їхнього аналізу. Найпоширенішими видами когнітивних карт є [5, 6]:

— знакові когнітивні карти;
— НКК Коско;
— модифіковані НКК Коско;
— нечіткі реляційні когнітивні карти;
— нечіткі продукційні когнітивні карти;
— НКК Силова.

Особливий інтерес представляють НКК, запропоновані В.Б. Силовим [7], які базуються на формалізованому представленні системи у вигляді

$$НКК = \langle C, F, W \rangle, \tag{1}$$

де $C = \{C_i\}$ — множина концептів; $F = \{F_i\}$ — множина зв'язків між концептами; $W = \{W_{ij}\}$ — множина ваг дуг (зв'язків).

Причому зв'язки між концептами в НКК Силова можуть бути як додатними — такими, що підсилюють вплив концепту C_i на концепт C_j ($W_{ij} \succ 0$), так і від'ємними — такими, які послаблюють вплив концепту C_i на концепт C_j ($W_{ij} \prec 0$), тобто $W_{ij} \in [-1; 1]$. Проблема опрацювання від'ємних впливів вирішується шляхом подвоєння потужності множини концептів і роздільного опрацювання додатних і від'ємних впливів. А відношення між концептами НКК розглядаються як елементи нечіткої матриці суміжності для графа НКК. Крім того, нечіткі значення вихідних концептів отримуються із використанням характерних для нечіткої логіки операцій *T*-норм над нечіткими значеннями вхідних концептів і ваг впливу [5].

НКК Силова мають ряд переваг над вищезазначеними когнітивними картами, зокрема, є точнішими, ніж класичні знакові когнітивні карти, дають змогу враховувати силу причинно-наслідкових зв'язків і опосередковані взаємовпливи концептів на систему та системи на концепти. У той же час значення концептів нечітких когнітивних моделей Коско є чіткими числами, що обмежує їхні можливості, а нечіткі продукційні або реляційні когнітивні карти недостатньо опрацьовані і в деяких ситуаціях неадекватно описують досліджувану систему.

Методологія когнітивного моделювання розвивається у напрямку вдосконалення апарату аналізу та моделювання ситуації. У роботах [3, 4] запропоновано моделі прогнозування розвитку ситуації.

Таким чином, актуальним є дослідження впливу загроз на рівень безпеки системи захисту інформації і, зокрема, комп'ютерної мережі, та визначення найвпливовіших із них на основі когнітивного моделювання.

Мета роботи

Розробити модель для аналізу впливу загроз на рівень захищеності комп'ютерної мережі, використовуючи когнітивний підхід.

Постановка задачі

Для досягнення поставленої мети необхідно:

— побудувати НКК предметної області;

— сформувати матрицю взаємовпливів;

— розрахувати основні системні показники НКК;

— визначити найвагоміші концепти досліджуваної системи;

— згенерувати можливі сценарії, які продемонструють відносну зміну рівня захищеності мережі залежно від сили впливу концептів.

Визначення загроз безпеці комп'ютерної мережі

Для забезпечення захисту комп'ютерних мереж, насамперед, необхідно провести системний аналіз можливих загроз мережевій безпеці.

Загрози характеризують можливі дії, які можуть бути здійсненні по відношенню до системи. Вони мають прояви у різноманітних формах, але найпоширенішими є такі [8]:

— випадкові: особа, яка не ознайомлена з відповідним регламентом і політикою, або через неналежний догляд, створює випадковий ризик;

— несанкціоновані зміни: оновлення, виправлення та інші зміни в операційних системах, програмних додатках, конфігураціях, можливостях взаємодії та обладнанні можуть створити несподівану загрозу безпеці систем промислової автоматики та контролю або відповідного промислового процесу.

Фактор загрози — поняття, яке використовується для опису суб'єкта, що становить собою загрозу. Факторами загроз можуть бути як зловмисники, так і порушники. Прикладами таких факторів є [8]:

— інсайдер: довірена особа, співробітник, підрядник або постачальник, які володіють інформацією, що, як правило, не відома на загал. Інсайдер може представляти собою загрозу навіть без злих намірів;

— аутсайдер: особа або група осіб, які не мають права внутрішнього доступу.

З метою виявлення загальних тенденцій зміни мережевої безпеки дослідимо корпоративну мережу із загальними характеристиками.

Розглянемо перелік можливих загроз, реалізація яких призведе до негативних наслідків функціонування мережі [9–12].

1. Scan Attacks — пошук можливих вразливостей системи:

1) Packet sniffers — перехоплення та аналіз трафіка;

2) Ping sweeps — знаходження IP-адрес працюючих комп'ютерів;

3) Port scanner — сканування відкритих TCP- та UDP-портів;

4) Phishing — спосіб отримання необхідної інформації безпосередньо у користувачів комп'ютерної мережі.

2. Web Attacks:

1) Cross-Site Scripting (XSS) — зловмисний збір інформації користувача, через сторінки веб-додатку;

2) SQL Injection — один із поширених способів зламу сайтів і програм, що працюють з базами даних, заснований на впровадженні у запит довільного SQL-коду;

3) Path Traversal — обробка зловмисником HTTP-запитів, для того, щоби обійти контролі доступу та перейти до інших каталогів і файлів у системі.

3. Spoofing — підміна довіреного суб'єкта:

1) IP-spoofing — використання чужої IP-адреси відправника з метою обману системи безпеки;

2) DNS-spoofing — зміна даних кешу доменних імен з метою присвоєння помилкової IP-адреси;

3) DHCP-spoofing — підміна шлюзу за замовчуванням (default gateway).

4. Атаки, спрямовані на отримання доступу до системи:

1) Password Attacks — злам паролю;

2) Trust Exploitation — компрометація довіреного хоста, використовуючи його для атак на інші хости у мережі;

3) атака man-in-the-middle — компрометація каналу зв'язку, при якому зловмисник здійснює втручання у протокол передавання даних, видаляючи або змінюючи інформацію.

5. Перехоплення сеансу (session hijacking) — використання поточного комп'ютерного сеансу для отримання несанкціонованого доступу до інформації або послуг у комп'ютерній мережі.

6. Compromised-Key Attack — перехоплення секретного ключа.

7. Спамінг — зловживання можливостями електронної пошти.

8. Атака відмови в обслуговуванні (Denial of Service, DoS) — лавинна маршрутизація пакетів, що призводить до перевантаження мережі і, як наслідок, робить її недоступною.

9. Шкідливе програмне забезпечення (trojan, worms, virus, botnet та ін.) — спрямоване на перешкоджання роботи мережі, збір конфіденційної інформації або отримання доступу до приватних комп'ютерних систем.

10. Фізичний вплив на мережу з боку зловмисника — призводить до руйнування або виведення з ладу фізичних компонентів, таких як апаратне забезпечення, пристрої, призначені для зберігання програмного забезпечення, з'єднувальні елементи, датчики, контролери.

11. Розголошення інформації — умисні або необережні дії користувача, внаслідок яких особа, що не має доступу до даної інформації, ознайомлюється з нею.

12. Ненавмисні дії, помилки користувачів мережі — включають у себе дії, що здійснюються випадково, через незнання, неуважність або недбалість, з цікавості, але без злого умислу.

13. Природні явища та явища техногенного характеру (аварії, урагани, землетруси, пожежі і т.п.).

Для побудови НКК, яка визначає стан безпеки комп'ютерної мережі, насамперед, необхідно сформувати з вищезазначеного переліку множину найбільш вагомих з точки зору вивчення даної проблеми концептів. У результаті опитування та узгодження думок групи експертів даної предметної області було визначено такі концепти:

K_1 — мережеві атаки зловмисника (Scan Attacks, Web Attacks, Spoofing, атаки, спрямовані на отримання доступу до системи, перехоплення сеансу та Compromised-Key Attack);

K_2 — спамінг зловмисника;

K_3 — шкідливі програми;

K_4 — фізичний вплив на мережу з боку зловмисника;

K_5 — DoS-атаки зловмисника;

K_6 — розголошення інформації користувачем;

K_7 — ненавмисні дії, помилки користувачів мережі;

K_8 — надійність, відмовостійкість технічних і програмних засобів;

K_9 — захищеність комп'ютерної мережі;

K_{10} — відмовостійкість обслуговування роботи мережі;

K_{11} — природні явища та явища техногенного характеру.

Як при розробці комп'ютерної мережі, так і при встановленні політики мережевої безпеки, можна моделювати атаки, змінюючи значення сили впливу досліджуваних концептів на систему, з метою оцінювання наслідків від їхньої можливої реалізації.

Розробка і аналіз НКК ідентифікації стану безпеки комп'ютерної мережі

Когнітивні моделі дозволяють здійснювати аналіз досліджуваної ситуації за допомогою вивчення структури взаємних впливів концептів когнітивної карти та динамічного аналізу, який полягає у генерації можливих сценаріїв її розвитку [7].

Після того як був сформований перелік концептів, визначимо значення сили впливу між кожною парою концептів шляхом статистичної обробки даних, отриманих у результаті експертного опитування.

Для цього задамо нечітку лінгвістичну шкалу, що являє собою впорядковану множину лінгвістичних значень (термів) оцінок настання ймовірних наслідків, отриманих у результаті дії одного концепту на інший:

СИЛА ЗВ'ЯЗКУ = {Не впливає; Дуже слабка; Слабка; Середня; Сильна; Дуже сильна}.

Кожному із цих значень ставиться у відповідність деякий числовий діапазон, що належить відрізку [0, 1] для додатних зв'язків і відрізку [–1, 0] для від'ємних зв'язків (табл. 1).

Моделювання і аналіз НКК предметної області будемо проводити, використовуючи програмне забезпечення Mental Modeler [13]. НКК, яка ілюструє множинні причинно-наслідкові зв'язки та характер взаємодії визначених факторів, зображена на рис. 1.

Таблиця 1. Відповідність числового діапазону деякому лінгвістичному значенню сили зв'язку між концептами

Лінгвістичне значення	**Числовий діапазон**
Не впливає	0
Дуже слабка	(0; 0,15]
Слабка	(0,15; 0,35]
Середня	(0,35; 0,6]
Сильна	(0,6; 0,85]
Дуже сильна	(0,85, 1]

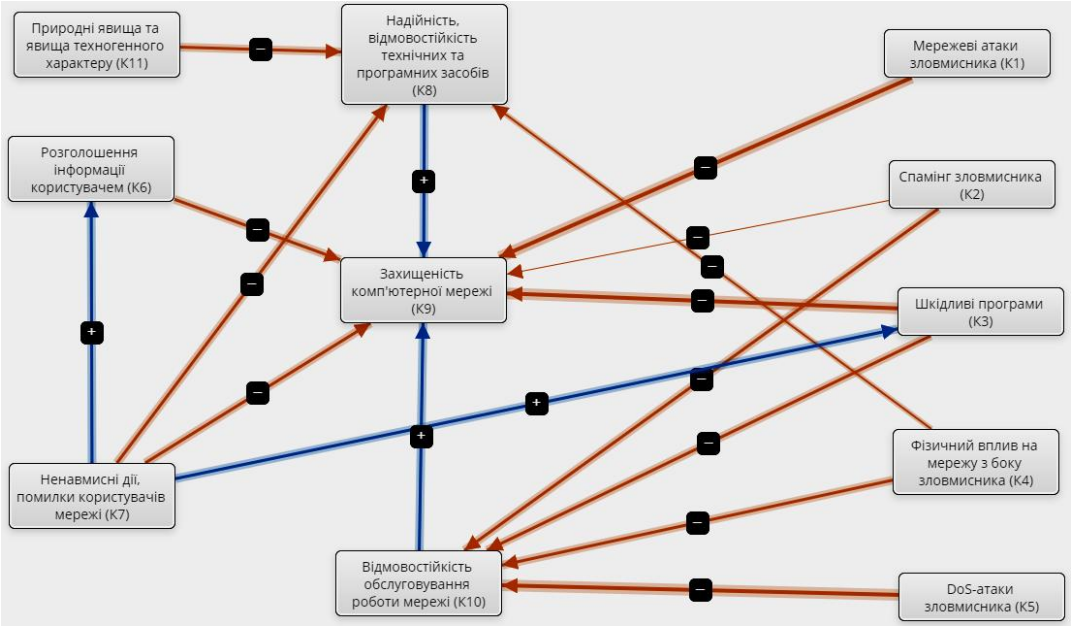

Рис. 1. Нечітка когнітивна карта дослідження стану мережевої безпеки

Побудована НКК складається з одинадцяти концептів:

1) шість концептів типу «Driver» — впливають на інші концепти, а на них не впливає жодний з концептів системи;

2) один концепт типу «Receiver» — на нього впливають концепти системи, а він не впливає ні на жоден з них;

3) чотири концепти типу «Ordinary» — звичайні, проміжні концепти, які впливають, і на яких впливають деякі концепти системи.

Для визначення складності розробленої НКК, обчислимо щільність зв'язків, використавши формулу

$$d = \frac{m}{n(n-1)}, \tag{2}$$

де m — кількість зв'язків, а n — кількість концептів.

У нашому випадку $n = 11, m = 16$, підставивши відповідні значення у формулу (2), отримаємо, що $d = 0{,}15$. Це вказує на достатню складність розробленої когнітивної моделі.

Для виконання аналізу НКК необхідно врахувати весь опосередкований взаємовплив концептів один на одного. Для цього на підставі побудованої когнітивної карти формується матриця взаємовпливу концептів один на одного (табл. 2).

Таблиця 2. Матриця взаємовпливів концептів НКК предметної області

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
K_1	0	0	0	0	0	0	0	0	–0,85	0	0
K_2	0	0	0	0	0	0	0	0	–0,15	–0,5	0
K_3	0	0	0	0	0	0	0	0	–0,9	–0,61	0
K_4	0	0	0	0	0	0	0	-0,38	0	–0,75	0
K_5	0	0	0	0	0	0	0	0	0	–0,98	0
K_6	0	0	0	0	0	0	0	0	–0,75	0	0
K_7	0	0	0,5	0	0	0,58	0	–0,55	–0,65	0	0
K_8	0	0	0	0	0	0	0	0	0,55	0	0
K_9	0	0	0	0	0	0	0	0	0	0	0
K_{10}	0	0	0	0	0	0	0	0	0,55	0	0
K_{11}	0	0	0	0	0	0	0	–0,82	0	0	0

Після чого досліджуються поведінка і стійкість побудованої карти. Це дозволяє зробити операція нечіткого транзитивного замикання. Використовуючи дану операцію, від когнітивної матриці можна перейти до транзитивно замкненої когнітивної матриці Z, елементами якої є пари $(z_{ij}, \overline{z_{ij}})$, за допомогою якої можуть бути розраховані основні системні показники НКК — консонанс, дисонанс і вплив концептів на систему, обчислення яких засноване на порівнянні контурів, утворених з концептів карти за критерієм відповідності, балансу та ступеню впливу [7].

Розраховані кількісні показники НКК аналізу стану захищеності комп'ютерної мережі відображено на рис. 2.

Component	Indegree	Outdegree	Centrality
Надійність, відмовостійкість технічних та програмних засобів	1.75	0.55	2.3
Природні явища та явища техногенного характеру	0	0.82	0.82
Захищеність комп'ютерної мережі	4.3999999999999995	0	4.3999999999999995
Мережеві атаки зловмисника	0	0.85	0.85
Шкідливі програми	0.5	1.51	2.01
Спамінг зловмисника	0	0.65	0.65
Фізичний вплив на мережу з боку зловмисника	0	1.13	1.13
DoS-атаки зловмисника	0	0.98	0.98
Ненавмисні дії, помилки користувачів мережі	0	2.2800000000000002	2.2800000000000002
Розголошення інформації користувачем	0.58	0.75	1.33
Відмовостійкість обслуговування роботи мережі	2.84	0.55	3.3899999999999997

Рис. 2. Основні показники НКК предметної області

Проаналізувавши значення даних показників можна визначити найвагоміші концепти досліджуваної системи. Це ті концепти, що мають найбільше значення консонансу та впливу, тобто: K_3 — шкідливі програми; K_4 — фізичний вплив на мережу з боку зловмисника; K_7 — ненавмисні дії, помилки користувачів мережі. Також доцільно зазначити, що найменший вплив на роботу мережі має такий концепт як K_2 — спамінг зловмисника.

Для отримання прогнозів розвитку ситуації визначимо відносну зміну концептів системи при максимальному значенні впливу на них найвагоміших факторів. Тобто змоделюємо наступні три сценарії.

1. Розглянемо, як зміниться стан системи при збільшенні значення концепту K_3 — шкідливі програми.

До шкідливих програм належать: троянські та шпіонські програми, черв'яки, віруси, логічні бомби та деякі інші види програм, спрямовані на порушення інформаційної безпеки. Ці програми можуть проникати на атаковані комп'ютери різними шляхами. Найчастіше це відбувається, коли користувач завантажує файли із неперевірених джерел (змінних носіїв чи веб-сайтів) або безпечно відкриває підозрілий файл, який надходить йому на електронну пошту. Існують і більш небезпечні представники шкідливих програм, що мають власні механізми «розмноження», копії таких програм розповсюджуються на комп'ютери у мережі без участі користувачів [9].

У досліджуваній системі концепт K_3 — шкідливі програми безпосередньо впливає на K_{10} — відмовостійкість обслуговування роботи мережі та K_9 — захищеність комп'ютерної мережі.

У результаті максимального збільшення значення впливу шкідливих програм відмовостійкість обслуговування роботи мережі знизиться на 0,04, а захищеність комп'ютерної мережі — на 0,05 (рис. 3).

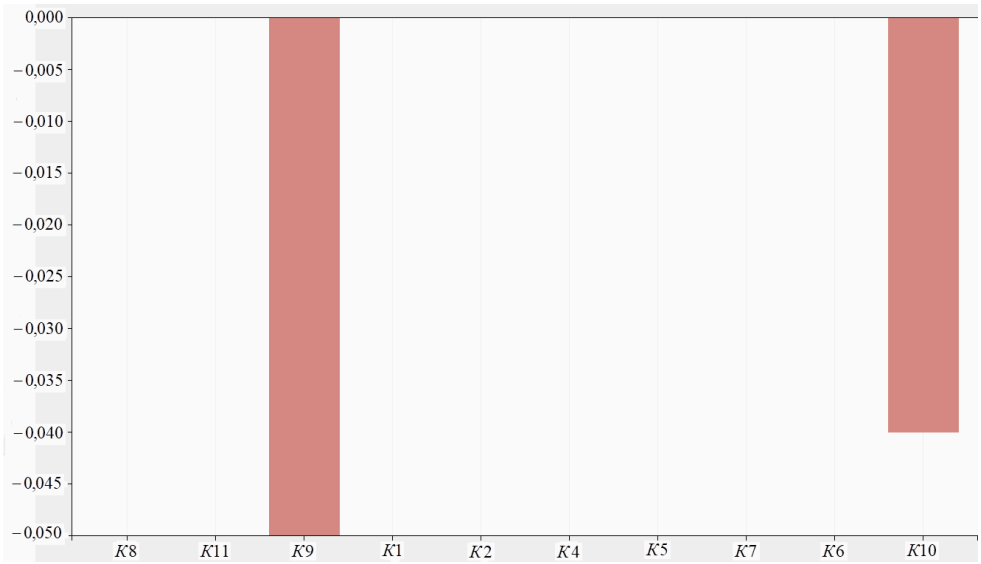

Рис. 3. Сценарій, що відображає реакцію системи на максимально негативні зміни концепту K_3 — шкідливі програми

Для запобігання або попередження негативної дії сучасних шкідливих програм доцільно регулярно оновлювати програмне забезпечення, включаючи операційну систему та усі додатки, використовувати надійні антивірусні програми, створювати резервні копії, які зберігаються на жорсткому диску в автономному режимі тощо.

2. Змоделюємо наступну ситуацію, яка відображатиме зміни у системі при підвищені значення такого концепту як K_4 — фізичний вплив на мережу з боку зловмисника.

У даному випадку важливе місце посідають фізичні засоби захисту мережі, які призначені для створення перешкод на шляху потенційного зловмисника, який може несанкціоновано проникнути в приміщення, вчинити акт вандалізму, здійснити крадіжку та інші дії, які негативно вплинуть на роботу мережі.

Концепт K_4 — фізичний вплив на мережу з боку зловмисника має безпосередній вплив на такі концепти системи як: K_8 — надійність, відмовостійкість технічних і програмних засобів, K_{10} — відмовостійкість обслуговування роботи мережі, та опосередковано впливає на K_9 — захищеність комп'ютерної мережі. Дослідимо відносні зміни значень цих концептів (рис. 4).

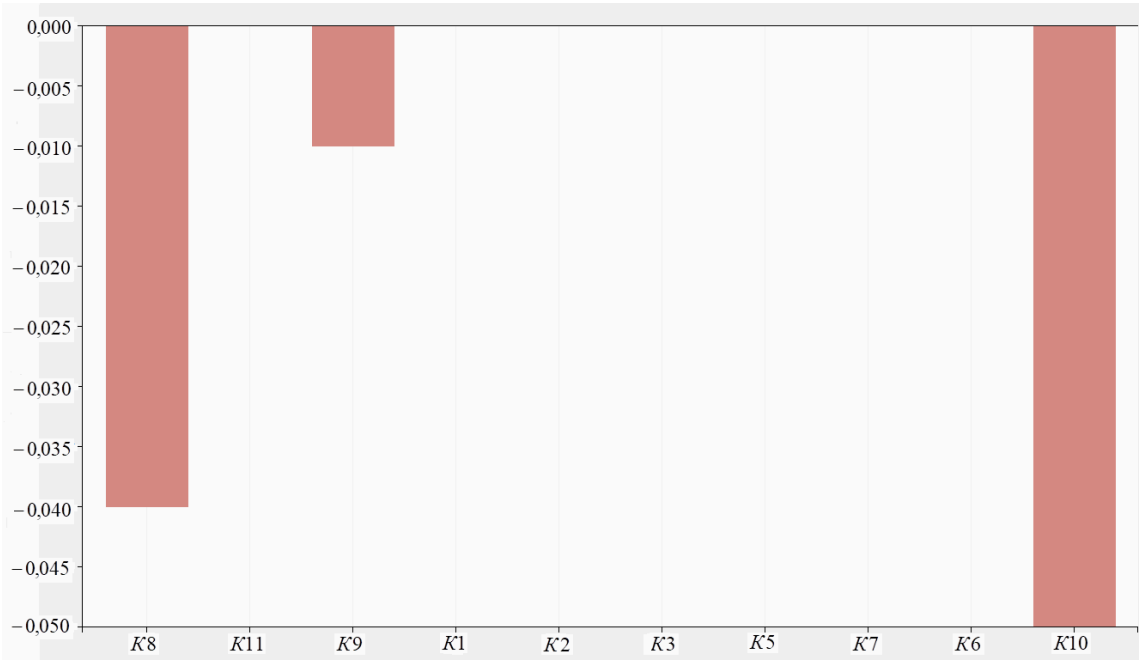

Рис. 4. Сценарій, що відображає реакцію системи на максимально негативні зміни концепту K_4 — фізичний вплив на мережу з боку зловмисника

На основі даної стовпчастої діаграми можна зробити висновок, що при збільшенні значення даного концепту захищеність комп'ютерної мережі зменшиться на 0,01, надійність, відмовостійкість технічних і програмних засобів — на 0,04, а відмовостійкість обслуговування роботи мережі — на 0,05. Тому особливу увагу потрібно звернути на підсилення фізичних засобів, що дозволять вирішити задачі,

пов'язані із захистом території, приміщень, обладнання та здійснення контрольованого доступу до них.

3. Дослідимо можливі зміни концептів при збільшенні негативного впливу на мережу компонента K_7 — ненавмисні дії, помилки користувачів мережі.

Ненавмисні дії, помилки користувачів, операторів і системних адміністраторів, які обслуговують мережу можуть призвести як до несправностей чи повної непрацездатності системи, так і до створення слабких місць, якими можуть скористатися зловмисники.

Концепт K_7 — ненавмисні дії, помилки користувачів мережі має безпосередній вплив на K_3 — шкідливі програми, K_6 — розголошення інформації користувачем, K_8 — надійність, відмовостійкість технічних і програмних засобів, K_9 — захищеність комп'ютерної мережі та опосередковано впливає на K_{10} — відмовостійкість обслуговування роботи мережі. Розглянемо відносні зміни значень цих концептів (рис. 5).

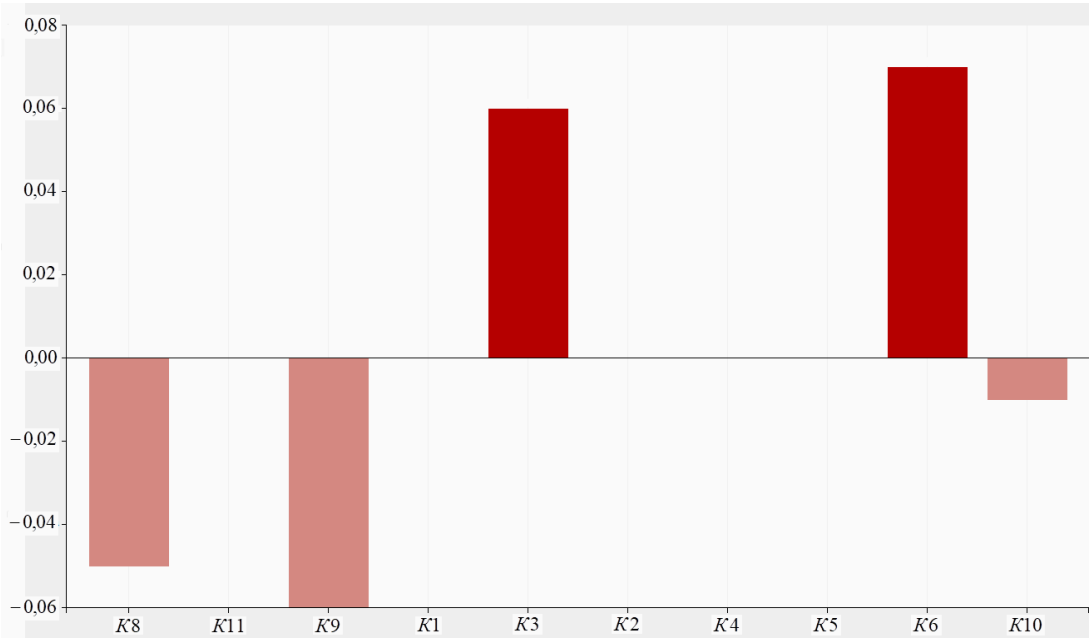

Рис. 5. Сценарій, що відображає реакцію системи на максимальні негативні зміни концепту K_7 — ненавмисні дії, помилки користувачів мережі

Отримана гістограма показує, що в результаті вищезазначених дій збільшиться значення таких концептів як K_3 — шкідливі програми та K_6 — розголошення інформації користувачем, що призведе до погіршення відмовостійкості обслуговування роботи мережі на 0,01, надійності, відмовостійкості технічних і програмних засобів — на 0,05 і, у свою чергу, захищеність комп'ютерної мережі зменшиться на 0,06. Таким чином, необхідно правильно організовувати роботу зі співробітниками, яка передбачає якісний підбір і розстановку персоналу, включаючи навчання правил роботи з конфіденційною інформацією, ознайомлення із заходами відповідальності за порушення правил захисту інформації, проведення

систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв, періодичне проходження навчання та ін.

Отже, розроблена НКК аналізу впливу загроз на рівень захищеності мережі відображає, головним чином, якісні тенденції розвитку ситуації та являється одним із засобів оптимізації робіт при налаштуванні захисту комп'ютерних мереж.

Висновки

Розроблено когнітивну модель для аналізу загроз безпеці комп'ютерних мереж. На основі матриці взаємовпливів концептів побудованої НКК розраховано основні системні показники: консонанс, дисонанс та вплив концептів. У результаті аналізу значень цих показників було визначено найвагоміші концепти системи: K_3 — шкідливі програми; K_4 — фізичний вплив на мережу з боку зловмисника; K_7 — ненавмисні дії, помилки користувачів мережі.

Посилюючи вплив даних концептів на мережу, змодельовано різні сценарії, у результаті запуску яких спостерігається відносна зміна рівня захищеності мережі. Так при максимальному впливі концепту K_3 — шкідливі програми, захищеність послабиться на 0,05, а відмостійкість обслуговування роботи мережі — на 0,04. Найбільше знизиться захищеність (на 0,06) при посилені впливу концепту K_7 — ненавмисні дії, помилки користувачів мережі, при цьому збільшиться значення таких концептів як K_3 — шкідливі програми та K_6 — розголошення інформації користувачем, що призведе до погіршення відмовостійкості обслуговування роботи мережі на 0,01, надійності, відмовостійкості технічних і програмних засобів — на 0,05. Якщо ж збільшити значення впливу концепту K_4 — фізичний вплив на мережу з боку зловмисника, то захищеність комп'ютерної мережі зменшиться на 0,01, надійність, відмовостійкість технічних і програмних засобів — на 0,04, а відмовостійкість обслуговування роботи мережі — на 0,05.

Результати даного дослідження надають можливість досліджувати та прогнозувати стан мережевої безпеки, що, у свою чергу, сприяє впровадженню необхідних механізмів попередження, захисту та контролю доступу на відповідних рівнях мережевої інфраструктури. Крім того, отримані висновки можна врахувати під час організації захисту корпоративної мережі.

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 5-е изд. Санкт-Петербург: Питер, 2017. 992 с.

2. Ниворожкина Л.И., Арженовский С.В., Рудяга А.А. Статистические методы анализа данных: учебник. — Москва: Риор, 2018. 320 с.

3. Kosko B. Fuzzy Cognitive Maps. *International Journal* of *Man-Machine Studies*. 1986. Vol. 24(1). P. 65–75.

4. Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам. Москва: Наука, 1986. 496 с.

5. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. 2-е изд., стереотип. Москва: Горячая линия – Телеком, 2012. 284 с.

6. Рыков А.С. Методы системного анализа: многокритериальная и нечеткая оптимизация, моделирование и экспертные оценки. Москва: Экономика, 1999. 316 с.

7. Силов В.Б. Принятие стратегических решений в нечеткой обстановке. Москва: ИНПРО – РЕС, 1995. 228 с.

8. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы.

9. Захарченко С.М., Трояновська Т.І., Бойко О.В. Основи побудови захищених мереж на базі обладнання компанії Cisco: навч. посіб. — Вінниця: ВНТУ, 2017. 136 с.

10. Перцев И.Ю., Зинькевич В.Н. Анализ существующих угроз компьютерной безопасности в сети. *Наука, образование и культура*. 2015. № 3. С. 9–12.

11. ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей.

12. Анализ угроз сетевой безопасности. Вход Your Private Network. URL: http: //ypn.ru/138/analysis-of-threats-to-network-security

13. Gray S.A., De Kok J.L., Helfgott A.E.R.,. O'Dwyer B, Jordan R., Nyaki A. Using fuzzy cognitive mapping as a participatory approach to analyze change, preferred states, and perceived resilience of social-ecological systems. *Ecology and Society*, 2015. **20**(2):11. URL: http://www.ecologyandsociety.org/vol20/iss2/art11

Надійшла до редакції 23.09.2019