© Saliieva O., Yaremchuk Yu. Determining the level of security of the information security system based on cognitive modeling // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 1, pp. 42-49.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.26.14669

ВИЗНАЧЕННЯ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ КОГНІТИВНОГО МОДЕЛЮВАННЯ

Ольга Салієва, Юрій Яремчук

Вінницький національний технічний університет

САЛІЄВА Ольга Володимирівна

Рік та місце народження: 1982 рік, м. Вінниця, Україна.
Освіта: Вінницький державний педагогічний інститут ім. М. Коцюбинського, 2004 рік; Вінницький національний технічний університет, 2018 рік.
Посада: аспірантка кафедри менеджменту та безпеки інформаційних систем з 2016 року.
Наукові інтереси: нечітка математика, безпека інформаційних систем.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на наукових конференціях, свідоцтва про реєстрацію авторського права на твір.
E-mail: salieva8257@gmail.com.
Orcid ID: 0000-0003-2388-7321.

ЯРЕМЧУК Юрій Євгенович, д.т.н., професор

Рік та місце народження: 1974 рік, м. Вінниця, Україна.
Освіта: Вінницький національний технічний університет, 1996 рік.
Посада: директор Центру інформаційних технологій та захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем, з 2010 року.
Наукові інтереси: криптографічний та стеганографічний захист інформації, технічний захист інформації, безпека інформаційних систем.
Публікації: понад 270 публікацій, у тому числі 2 монографії, 140 статей у наукових фахових виданнях, 20 підручників та навчальних посібників, автор 20-ти патентів на корисну модель та 20-х свідоцтв про реєстрацію авторського права на твір.
E-mail: yurevyar@vntu.edu.ua.
Orcid ID: 0000-0002-6303-7703.

Анотація. *У даній статті було розглянуто підходи до вирішення проблеми оцінювання рівня захищеності системи захисту інформації в умовах реалізації загроз. Запропоновано когнітивну модель на основі нечіткої когнітивної карти, яка дозволяє визначати рівень захищеності системи захисту інформації. Для побудови нечіткої когнітивної карти сформовано множину концептів та визначено причинно-наслідкові зв'язки між ними. Здійснено оцінювання структурно-топологічних властивостей нечіткої когнітивної карти. Зокрема, визначено такі показники структурної складності нечіткої когнітивної карти як: щільність, складність, центральність концепту та індекс ієрархії. Побудовано матрицю взаємовпливів концептів, на основі якої визначено кількісні значення основних системних показників: консонансу, дисонансу, впливу факторів. Проаналізувавши дані показники, було визначено найвагоміші загрози безпеці досліджуваної системи. Проведено сценарне моделювання впливу даних загроз на рівень захищеності системи захисту інформації. На основі даних отриманих у результаті запуску сценаріїв можна розробити чіткий план організації підвищення рівня захищеності системи захисту інформації, вчасно провести необхідні заходи, що допоможуть запобігти, локалізувати, усунути або ж зменшити силу впливу ймовірних загроз інформаційній безпеці.*

Ключові слова: *інформаційна безпека, загрози безпеці, когнітивне моделювання, нечітка когнітивна карта.*

Вступ

Важливим фактором розвитку сучасного суспільства є забезпечення захищеності інформаційних систем, які є ключовими елементами будь-яких процесів незалежно від сфери людської діяльності. При цьому особлива увага приділяється аналізу потенційних загроз інформаційній безпеці, реалізація яких

призводить до матеріальних, фінансових, репутаційних та інших збитків. Моделювання даних загроз, ступінь їх впливу на рівень захищеності займає провідне місце при проектуванні системи захисту інформації.

Для дослідження рівня захищеності системи захисту інформації в умовах реалізації загроз існують різні підходи, зокрема, оцінювання ризиків: методи пов'язані з якісним оцінюванням рівня ризиків (FRAP, OCTAVE та ін.), кількісні методи (RiskWatch, ГРИФ та ін.), методи, які використовують змішане оцінювання (CRAMM, MSAT та ін.); визначення актуальних загроз (наприклад, [1]).

Оскільки вирішення задачі рівня захищеності системи захисту безпосередньо пов'язане з людським фактором і характеризується високим ступенем невизначеності і складності формалізації загроз, то доцільно звернути увагу на методи когнітивного моделювання. Дані методи базуються на використанні нечітких когнітивних карт (НКК), яким властива простота, наочність, гнучкість, конструктивність, адаптація до невизначеності вхідних даних, використання знань і досвіду експертів предметної області.

НКК складної системи (проблеми) являє собою орієнтований граф, вершини якого (концепти) представляють системні змінні, а дуги – причинно-наслідкові зв'язки між концептами, причому ваги цих зв'язків визначають силу впливу концептів один на одного [2]. Дослідженню НКК присвячені праці таких вчених як Коско Б., Силов В. Б., Робертс Ф. С., Борисов В. В., Федулов А. С., Толмен Дж. та ін.

На сьогодні існує багато різновидів НКК: знакові когнітивні карти [3], НКК Коско [4], НКК Силова [5], нечіткі узагальнені когнітивні карти [6], реляційні НКК [7], продукційні НКК [8], інтервальні («сірі») НКК [9], нейтрософські НКК [10], динамічні когнітивні карти [11] та інші [12]. Вони відрізняються способом представлення відношень між концептами, значень концептів та алгоритмів, що забезпечують передачу впливу за когнітивною картою.

Питанням застосування НКК для вирішення задач інформаційної безпеки приділяється достатня увага, зокрема, у роботах [13-19].

У [13-15] для аналізу інформаційних загроз та визначення ризиків безпеці автори запропонували когнітивні моделі, використовуючи НКК Коско, Силова, які описують вплив потенційних загроз на досліджувану систему. Дані НКК базуються на доволі легкому моделюванні та швидкому обчисленні. Хоча варто зауважити, що для комплексного оцінювання впливу декількох факторів на один концепт використовується операція пошуку максимуму серед ваг впливу, що не завжди відображає ймовірність реалізації атаки на даний концепт.

Автор праці [16] для оцінювання стану захищеності даних в умовах можливої реалізації інформаційних загроз пропонує нечітку когнітивну модель, яка складається з шести ієрархічних рівнів. Вхідними даними моделі є лінгвістичні оцінки стану засобів захисту інформації. На основі цих оцінок розраховуються значення концептів на вищих рівнях. Недоліком даної моделі є те, що для визначення ступеня впливу концептів один на одного використовується метод експертних оцінок «Дельфі», який є трудомістким і потребує значних часових затрат.

У роботі [17] для оцінювання ризиків інформаційній безпеці використовують нечіткі продукційні когнітивні карти. Особливістю даних карт є те, що значення концептів виражають через нечіткі лінгвістичні змінні, для опису впливів між концептами використовують базу нечітких продукційних правил, при передаванні впливу когнітивною картою використовується алгоритм нечіткого виведення типу Мамдані, а для операції агрегування застосовується операція нечіткого додавання з перенесенням. Зазначимо, що нечіткі продукційні когнітивні карти мають додаткові переваги порівняно з НКК Коско, хоча одночасно характеризуються трудомісткістю та складністю реалізації, адже потребують використання великої кількості правил.

Для вирішення задачі оцінювання інформаційних ризиків у [18] автори скористалися апаратом нечітких сірих когнітивних карт, які відрізняються від звичайних НКК тим, що для встановлення впливів між концептами використовують «сірі» (інтервальні) числа. Перевагами застосування НКК даного типу є те, що вони дозволяють перейти від точкових оцінок думок експертів до інтервальних і, як наслідок, до отримання інтервальних оцінок кінцевих результатів, які є більш логічними й достовірними. Проте нечіткі «сірі» когнітивні карти характеризуються високою складністю обчислювальної реалізації.

У роботі [19] було запропоновано когнітивну модель, яка дозволяє аналізувати вплив загроз на рівень захищеності комп'ютерної мережі, але не розглядає задачу оцінювання стану захищеності системи у цілому. Тому актуальним є дослідження пов'язане з визначенням рівня захищеності системи захисту інформації на основі когнітивного підходу.

Мета роботи

Побудувати когнітивну модель для дослідження рівня захищеності системи захисту інформації.

Постановка задачі

Для досягнення поставленої мети необхідно:

– визначити структуру НКК предметної області (тобто склад її концептів та причинно-наслідкові зв'язки між ними);

– визначити силу впливу між кожною парою концептів;

– побудувати модель на основі НКК для визначення рівня захищеності досліджуваної системи;

– розрахувати основні системні показники розробленої НКК;

– провести сценарне моделювання для визначення відносної зміни рівня захищеності системи захисту інформації.

Розробка когнітивної моделі на основі НКК для ідентифікації рівня захищеності системи захисту інформації

В якості об'єкта дослідження оберемо систему захисту інформації із загальними характеристиками, щоб виявляти загальні тенденції зміни рівня захищеності при впливі потенційних загроз.

При комплексному підході до захищеності досліджуваної системи на основі когнітивної моделі, насамперед, необхідно сформувати множину концептів

– найвагоміших факторів з точки зору вивчення даної проблеми. Аналізуючи дані отримані в результаті експертного опитування, для побудови НКК аналізу стану захищеності системи захисту інформації було сформовано такі концепти:

– K_1 – захист від витоку технічними каналами. Зауважимо, що технічні канали включають канали побічних електромагнітних випромінювань і наводок, акустичні, віброакустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали [20];

– K_2 – захист каналу передавання інформації. До таких каналів можна віднести лінії технічних засобів передавання інформації й систем їх життєзабезпечення (мережа електроживлення, заземлення, пожежна й охоронна сигналізація, системи опалення, водопостачання, вентиляції тощо), що проходять через периметр контрольованої зони і виходять за її межі;

– K_3 – *розголошення інформації персоналом. Розголошення виражається у повідомленні, передаванні, наданні, пересиланні, опублікуванні, втраті і у інших формах обміну і дій з діловою та науковою інформацією [21];*

– K_4 – фізичний захист. Фізичний несанкціонований доступ до приміщення організації, у кабінети і серверні кімнати, до обладнання, паперових документів, запам'ятовуючих пристроїв, носіїв інформації і т. п. може призвести до їх крадіжки або ж пошкодження [22];

– K_5 – НСД до інформації зловмисником. Несанкціонований доступ може здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування неправдивої інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів [20];

– K_6 – *організаційне забезпечення захисту інформації. Даний концепт забезпечує організацію охорони, режиму, роботу з кадрами, з документами; використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх і зовнішніх загроз підприємницької діяльності тощо [21];*

– K_7 – *ненавмисні дії, помилки обслуговуючого персоналу. Дана загроза включає у себе дії, що здійснюються випадково, через відсутність необхідних знань, неуважність або недбалість, з цікавості, але без злого умислу;*

– K_8 – надійність, відмовостійкість технічних та програмних засобів. Досліджувана система має бути захищена від фізичних відмов обладнання, забезпечуючи працездатність компонентів програмно-технічної платформи та оперативне відновлення резервних копій;

– K_9 – нормативно-правове забезпечення захисту. Нормативно-правове забезпечення регламентує та визначає порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації (КСЗІ); права, обов'язки й відповідальність персоналу роботи яких пов'язані з інформаційною безпекою; етапи створення КСЗІ [23];

– K_{10} – природні явища та явища техногенного характеру. До цієї загрози можуть відноситись вибух, аварія, пожежа, затоплення, ураган, землетрус і т .п.;

– K_{11} – захищеність системи захисту інформації. Для підвищення рівня захищеності системи захисту інформації важливо здійснити аналіз потенційних загроз, виділивши найвагоміші з них.

Наступним кроком є визначення сили зв'язку, яка визначає вплив одного концепта на інший та визначається лінгвістичними термами.

Причому зв'язки між концептами у НКК можуть бути як додатними — такими, що підсилюють вплив концепту K_i на концепт K_j ($w_{ij} \succ 0$), так і від'ємними — такими, які послаблюють вплив концепту K_i на концепт K_j ($w_{ij} \prec 0$), тобто $w_{ij} \in [-1; 1]$.

Для вирішення поставленої задачі задамо нечітку лінгвістичну шкалу:
СИЛА ЗВ'ЯЗКУ = {Не впливає; Дуже слабка; Слабка; Середня; Сильна; Дуже сильна}.

Кожному з цих термів поставимо у відповідність числовий діапазон, що належить відрізку [0, 1] для додатних зв'язків:

$$w_{ij} = \begin{Bmatrix} 0, & \text{не впливає;} \\ (0; 0{,}15], & \text{дуже слабка;} \\ (0{,}15; 0{,}35], & \text{слабка;} \\ (0{,}35; 0{,}6], & \text{середня;} \\ (0{,}6; 0{,}85], & \text{сильна;} \\ (0{,}85; 1], & \text{дуже сильна} \end{Bmatrix},$$

та аналогічний числовий діапазон взятий з протилежними знаками, що належить відрізку [-1, 0] для від'ємних зв'язків.

На основі опрацювання даних, отриманих у результаті експертного опитування встановимо силу зв'язку між кожною парою концептів, яка співвідноситься числовій оцінці.

Розробка експертами в галузі інформаційної безпеки структури знань про систему захисту, списку концептів та сили зв'язку між ними дозволяє побудувати НКК ідентифікації стану захищеності системи захисту інформації (рис. 1).

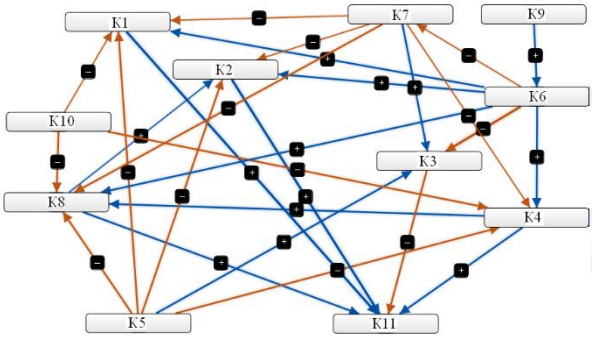

Рис. 1. Нечітка когнітивна карта дослідження стану захищеності системи захисту інформації

Моделювання виконано з використанням засобів програмного забезпечення Mental Modeler [24].

Проаналізувавши причинно-наслідкові зв'язки між концептами, зауважимо, що розроблена НКК містить:

– три концепти типу «Driver» – впливають на інші концепти, а на них не впливає жодний з концептів системи;

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

– сім концептів типу «Ordinary» – звичайні, проміжні концепти, які впливають і на яких впливають деякі концепти системи.

Матриця $W = \left\lfloor w(K_i, K_j) \right\rfloor_{n \times n}$ взаємовпливів концептів даної НКК матиме такий вигляд (табл. 1).

Таблиця 1

Матриця взаємовпливів концептів НКК предметної області

	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11
K1	0	0	0	0	0	0	0	0	0	0	0,9
K2	0	0	0	0	0	0	0	0	0	0	0,85
K3	0	0	0	0	0	0	0	0	0	0	-0,75
K4	0	0	0	0	0	0	0	0,5	0	0	0,7
K5	-0,55	-0,7	0,82	-0,75	0	0	0	-0,55	0	0	0
K6	0,7	0,65	-0,9	0,8	0	0	-0,3	0,7	0	0	0
K7	-0,45	-0,3	0,58	-0,42	0	0	0	-0,55	0	0	0
K8	0	0,25	0	0	0	0	0	0	0	0	0,55
K9	0	0	0	0	0	0,55	0	0	0	0	0
K10	-0,35	0	0	-0,5	0	0	0	-0,82	0	0	0
K11	0	0	0	0	0	0	0	0	0	0	0

Для визначення структурно-топологічних властивостей отриманої НКК скористаємось такими показниками структурної складності НКК:

а) щільність НКК – показує ступінь зв'язності графа, який відображає дану НКК:

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

де m – загальна кількість зв'язків НКК, а n – загальна кількість концептів НКК.

У нашому випадку $n = 11, m = 27$, підставивши відповідні значення у формулу (1), отримаємо, що $d = 0{,}25$. Дане значення вказує на достатньо велику кількість зв'язків між концептами, тобто на високу щільність розробленої НКК.

б) центральність концепта – характеризує ступінь взаємодії *i*-го концепта НКК з його сусідами:

– вихідна центральність – показує сукупну силу зв'язків (w_{ij}), що виходять з аналізованого концепта K_i:

$$od_i = \sum_{j=1}^{n} w_{ij};$$

– вхідна центральність – показує сукупну силу зв'язків (w_{ij}), що входять до аналізованого концепта K_i:

$$id_i = \sum_{j=1}^{n} w_{ij};$$

– загальна центральність концепта:

$$td_i = od_i + id_i. \qquad (2)$$

Розрахунок показників центральності показав, що найбільш високу структурну значимість має концепт K_6 $(td_6 = 4{,}6)$, а також концепти K_8, K_{11}, K_4, K_5 (показники $td_8, td_{11}, td_4, td_5$ рівні відповідно 3,92; 3,75; 3,67; 3,36). Дані концепти акумулюють найбільшу кількість зв'язків від інших концептів, тобто відіграють роль своєрідних центрів впливу в НКК для аналізу рівня захищеності системи захисту інформації.

в) складність – представляє собою співвідношення кількості концептів типу «Receiver» до концептів типу «Driver». Чим більше значення даного коефіцієнта, тим складніші карти, оскільки припускається, що вони містять більше корисних результатів та менше контрольованих впливів на зовнішнє середовище.

Для розробленої НКК предметної області отримаємо співвідношення: $\frac{1}{3} \approx 0{,}33$, що вказує на недостатньо складні системи мислення.

г) індекс ієрархії (*h*):

$$h = \frac{12 \cdot \sigma_{od}^2}{n^2 - 1}, \qquad (3)$$

де $\sigma_{od}^2 = \frac{\sum_{i=1}^{n} (od_i - \mu_{od})^2}{n}$, $\mu_{od} = \frac{\sum_{i=1}^{n} od_i}{n}$.

При $h = 1$ система є повністю ієрархічною, при $h = 0$ – повністю демократичною. Демократичні системи більш адаптивні до змін зовнішнього середовища завдяки високому рівню їх інтеграції та зв'язності. У нашому випадку $h = 0{,}2$, що свідчить про високу демократичність досліджуваної системи.

У табл. 2 відображено кількісне значення основних системних показників розробленої НКК предметної області: консонансу, дисонансу та впливу концептів на систему.

Таблиця 2

Основні показники НКК предметної області

Component	Indegree	Outdegree	Centrality
K4	2.469999999	1.2	3.67
K1	2.050000000	0.9	2.95
K8	3.12	0.8	3.92
K9	0	0.55	0.55
K5	0	3.3699999999	3.36999999997
K11	3.750000000	0	3.75000000004
K2	1.900000000	0.85	2.75
K10	0	1.67	1.67
K6	0.55	4.05	4.6
K7	0.3	2.3	2.59999999996
K3	2.3	0.75	3.05

Проаналізувавши вищезазначені показники, визначимо найвпливовіші концепти досліджуваної системи (ті концепти, що мають найбільше значення консонансу (outdegree) та впливу на систему): K_6 – організаційне забезпечення захисту інформації, K_4 – фізичний захист, K_5 – НСД до інформації зловмисником. Відмітимо, що найменший рівень впливу на систему захисту інформації має концепт K_9 – нормативно-правове забезпечення захисту.

Аналіз запропонованої когнітивної моделі для встановлення рівня захищеності системи захисту інформації

На цьому етапі проведемо сценарне моделювання для визначення відносної зміни рівня захищеності системи при максимальному значенні впливу на неї найвагоміших концептів.

Сценарій 1. Стан концепта K_6 – організаційне забезпечення захисту інформації активується, приймаючи максимально можливе негативне значення.

Зауважимо, що організаційна складова захисту інформації відіграє значну роль при створенні надійного комплексного механізму безпеки. Адже більшість загроз обумовлюються не технічними аспектами, а діями зловмисників, необережністю чи помилками персоналу. Тому важливо отримати прогноз розвитку даної ситуації.

Концепт K_6 у розробленій НКК має безпосередній вплив на концепти: K_1 – захист від витоку технічними каналами, K_2 – захист каналу передавання інформації, K_3 – розголошення інформації персоналом, K_4 – фізичний захист, K_7 – ненавмисні дії, помилки обслуговуючого персоналу, K_8 – надійність, відмовостійкість технічних і програмних засобів та опосередкований вплив на K_{11} – захищеність системи захисту інформації. Тому при зміні значення K_6 спостерігатиметься така реакція досліджуваної системи (рис. 2).

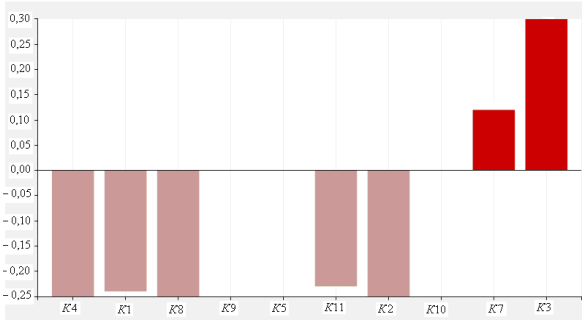

Рис. 2. Сценарій, що відображає реакцію системи на максимальні негативні зміни концепта K_6

Отримана стовпчаста діаграма показує, що при неналежній організації забезпечення захисту інформації спостерігатиметься збільшення значення концептів K_7 – ненавмисні дії, помилки обслуговуючого персоналу та K_3 – розголошення інформації персоналом, що, у свою чергу, призведе до зменшення захисту від витоку технічними каналами на 0,24, послаблення фізичного захисту, надійності, відмовостійкості технічних та програмних засобів, захисту каналу передавання інформації – кожного на 0,25 і, у цілому, рівень захищеності системи захисту інформації погіршиться на 0,23.

Для попередження негативних наслідків необхідно особливу увагу приділяти плануванню організаційних заходів, які мають здійснюватися спеціально створеною структурою, укомплектованою висококваліфікованими фахівцями з інформаційної безпеки.

Сценарій 2. Максимальне зменшення значення концепту K_4 – фізичний захист.

Фізична безпека спрямована на захист від таємного проникнення на територію і у приміщення сторонніх осіб; часового контролю перебування персоналу на робочому місці; організації і дотримання надійного пропускного режиму і т.п.

У досліджуваній моделі концепт K_4 – фізичний захист має безпосередній вплив на концепти K_8 – надійність, відмовостійкість технічних та програмних засобів і K_{11} – захищеність системи захисту інформації та опосередкований вплив на K_2 – захист каналу передавання інформації. Максимально негативна зміна значення K_4 призведе до такої ситуації (рис. 3).

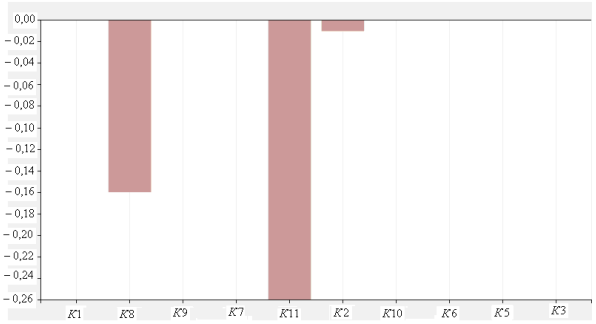

Рис. 3. Сценарій, що відображає реакцію системи на максимальні негативні зміни концепта K_4

Проаналізувавши отриману гістограму, можна зробити висновки щодо відносної зміни концептів розробленої НКК, на які впливає K_4. Зокрема, прослідковується зменшення надійності, відмовостійкості технічних та програмних засобів на 0,16, послаблення захисту каналу передавання інформації на 0,01 та захищеності системи захисту інформації – на 0,26.

Таким чином, щоб попередити вищезазначену ситуацію доцільно підсилити систему охорони периметра, відеоспостереження, охоронної сигналізації, контролю й управління доступом, систему збереження (сейфи, шафи тощо).

Сценарій 3. Максимальне посилення негативного значення концепта K_5 – НСД до інформації зловмисником.

Отримання НСД до інформації призводить до витоку даних, їх копіювання, модифікації, видалення, блокування доступу як до інформації так і до всієї системи, виведення її з ладу.

В побудованій НКК концепт K_5 – НСД до інформації зловмисником безпосередньо впливає на такі концепти: K_1 – захист від витоку технічними каналами, K_2 – захист каналу передавання інформації, K_3 – розголошення інформації персоналом, K_4 – фізичний захист, K_8 – надійність, відмовостійкість технічних та програмних засобів та має опосередкований вплив на K_{11} – захищеність системи захисту інформації. Реакцію системи на збільшення значення даного концепта зображено на рис. 4.

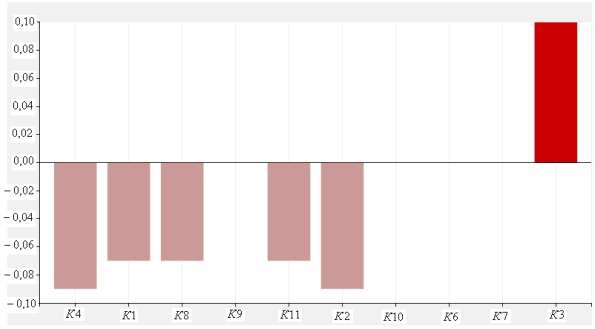

Рис. 4. Сценарій, що відображає реакцію системи на максимальні негативні зміни концепта K_5

У результаті моделювання даного сценарію бачимо, що розголошення інформації персоналом збільшиться, при цьому захист від витоку технічними каналами, надійність, відмовостійкість технічних й програмних засобів та захищеність системи захисту інформації послабляться на 0,07, а захист каналу передавання інформації та фізичний захист – на 0,09.

Щоб попередити наслідки вищезазначеного сценарію, варто підвищити заходи безпеки від НСД, використавши апаратні засоби захисту, систему контролю доступу до окремих документів, аутентифікацію, одноразові паролі тощо.

Отже, розроблена когнітивна модель для визначення рівня захищеності системи захисту інформації надає достатній ступінь деталізації, дозволяє враховувати наявність великої кількості альтернативних сценаріїв реалізації загроз.

Висновки

Таким чином, використовуючи когнітивний підхід, розроблено модель для визначення рівня захищеності системи захисту інформації. Здійснено структурно-топологічний аналіз побудованої НКК предметної області, внаслідок чого визначено найбільш структурно-значимі елементи: K_4 – фізичний захист, K_5 – НСД до інформації зловмисником, K_6 – організаційне забезпечення захисту інформації, K_8 – надійність, відмовостійкість технічних та програмних засобів, K_{11} – захищеність системи захисту інформації. Обчислено щільність ($d = 0{,}25$), що вказує на високу складність розробленої НКК.

На підставі сформованої матриці взаємовпливів визначено основні системні показники: консонанс, дисонанс та вплив концептів. Аналіз даних показників дозволив виділити найвагоміші концепти: K_6 – організаційне забезпечення захисту інформації, K_4 – фізичний захист, K_5 – НСД до інформації зловмисником та концепт, який має найменший вплив на систему – K_9 – нормативно-правове забезпечення захисту.

З метою визначення відносної зміни рівня захищеності предметної області проведено сценарне моделювання. Зокрема, досліджено, що максимально негативна зміна концепта K_6 – організаційне забезпечення захисту інформації призведе до зниження захисту від витоку технічними каналами на 0,24, послаблення фізичного захисту, надійності, відмовостійкості технічних та програмних засобів, захисту каналу передавання інформації – на 0,25 кожного і, в цілому, рівень захищеності системи захисту інформації погіршиться на 0,23.

Також вагоме місце для безпеки системи займає фактор K_4 – фізичний захист, у наслідок впливу якого прослідковується зниження надійності, відмовостійкості технічних та програмних засобів на 0,16, послаблення захисту каналу передавання інформації на 0,01 та захищеності системи захисту інформації – на 0,26. Порівняно не суттєво знизиться рівень захищеності (на 0,07) при негативному впливі концепта K_5 – НСД до інформації зловмисником.

На основі даних отриманих у результаті запуску вищезазначених сценаріїв можна розробити чіткий план організації підвищення рівня захищеності системи захисту інформації, вчасно провести необхідні заходи, що допоможуть запобігти, локалізувати, усунути або ж зменшити силу впливу ймовірних загроз інформаційній безпеці.

ЛІТЕРАТУРА

[1]. *Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. [Введ. 2008-02-14]*, М.: ФСТЭК России, 2008. 16 с.

[2]. В. Борисов, В. Круглов, А. Федулов, *Нечеткие модели и сети*, 2-е изд., стереотип, М.: Горячая линия, Телеком, 2012, 284 с.

[3]. Ф. Робертс, *Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам*, М.: Наука, 1986, 496 с.

[4]. B. Kosko, "Fuzzy Cognitive Maps", *International Journal* of *Man-Machine Studies*, Vol. 24, No. 1, pp. 65-75, 1986.

[5]. В. Силов, *Принятие стратегических решений в нечеткой обстановке*, М.: ИНПРО, РЕС, 228 с, 1995.

[6]. В. Борисов, А. Федулов, "Обобщенные нечеткие когнитивные карты", *Нейрокомпьютеры: разработка, применение*, №3, С. 3-20, 2004.

[7]. А. Федулов, "Нечеткие реляционные когнитивные карты", *Известия РАН. Теория и системы управления*, №1, С. 120-132, 2005.

[8]. J. Carvalho, "Rule Based Fuzzy Cognitive Maps: Fuzzy Causal Relations", *Computational Intelligence for Modeling, Control and Automation: Evolutionary Computation and Fuzzy Logic for Intelligent Control, Knowledge Acquisition and Information Retrieval*. [Electronic resource]. Online access: www.Inesc-id.pt/pt/indicadores/Ficheiros/1894.pdf.

[9]. J. Salmeron, "Modelling grey uncertainty with fuzzy grey cognitive maps", *Expert Syst. Appl.*, Vol. 37, No. 12, pp. 7581-7588, 2010.

[10]. V. Kandasamy, F. Smarandache, *Fuzzy Cognitive Maps and Neutrosophic Cognitive Maps*, Xiquan: Phoenix, 2003, 576 p.

[11]. Y. Miao, Z.Q. Liu, C.K. Siew, C.Y. Miao, "Dynamical cognitive network: An extension of fuzzy cognitive map", *IEEE Trans on Fuzzy Systems,* Vol. 9, No. 5, pp. 760-770, 2001.

[12]. E. Papageorgiou, I. Salmeron, Review of Fuzzy Cognitive Maps Research During the Last Decade", *IEEE Trans on Fuzzy Systems*, Vol. 21, No. 1, pp. 66-79, 2013.

[13]. В. Камаев, В. Натров, "Моделирование и анализ состояния информационной безопасности организации", *Известия тульского государственного университета. Технические науки*, № 3, С. 148-155, 2011.

[14]. Е. Степанова, И. Машкина, В. Васильев, "Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности", *Известия Южного федерального университета. Технические науки*, Т. 112, №11, С. 31-40, 2010.

[15]. P. Szwed, P. Skrzyński, "A new lightweight method for security risk assessment based on fuzzy cognitive maps", *International Journal of Applied Mathematics and Computer Science*, Vol. 24, No. 1, pp. 213-225, 2014.

[16]. И. Ажмухамедов, О. Князева, "Оценка состояния защищенности данных организации в условиях возможности реализации угроз", *Управление и высокие технологии*, №3 (31), С. 24-39, 2015.

[17]. В. Васильев, А. Вульфин, М. Гузаиров, "Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт", *Информационные технологии*, Т. 24, №4, С. 266-273, 2018.

[18]. В. Васильев, А. Вульфин, М. Гузаиров, А. Кириллова, "Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт", *Информационные технологии*, Т. 24, №10, С. 657-664, 2018.

[19]. О. Салієва, Ю. Яремчук, "Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі", *Реєстрація, зберігання і обробка даних*, №4, С. 28-39, 2019.

[20]. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. [Чинний від 1997-01-01]. Київ, 1996. 20 с.

[21]. В. Ярочкин, *Информационная безопасность*, М.: Академический Проект; Гаудеамус, 2004, 544 с.

[22]. А. Астахов, *Искусство управления информационными рисками*, М.: ДМК Пресс, 2010, 312 с.

[23]. О. Юдін, *Інформаційна безпека. Нормативно-правове забезпечення*, К.: Видавництво Національного авіаційного університету «НАУ - друк», 2011, 640 с.

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

УДК 004[056.5::81]

Салиева О.В., Яремчук Ю.Е. Определение уровня защищенности системы защиты информации на основе когнитивного моделирования

Аннотация. *В данной статье были рассмотрены подходы к решению проблемы оценки уровня защищенности системы защиты информации в условиях реализации угроз. Предложено когнитивную модель на основе нечеткой когнитивной карты, которая позволяет определять уровень защищенности системы защиты информации. Для построения нечеткой когнитивной карты сформировано множество концептов и определены причинно-следственные связи между ними. Осуществлено оценивания структурно-топологических свойств нечеткой когнитивной карты. В частности, определены следующие показатели структурной сложности нечеткой когнитивной карты как: плотность, сложность, центральность концепта и индекс иерархии. Построено матрицу взаимовлияния концептов, на основе которой определены количественные значения основных системных показателей: консонанса, диссонанса, влияния факторов. Проанализировав данные показатели, были определены наиболее значимые угрозы безопасности исследуемой системы. Проведено сценарное моделирование влияния данных угроз на уровень защищенности системы защиты информации. На основе данных полученных в результате запуска сценариев можно разработать четкий план организации повышения уровня защищенности системы защиты информации, вовремя провести необходимые мероприятия, которые помогут предотвратить, локализовать, устранить или уменьшить силу воздействия возможных угроз информационной безопасности.*

Ключевые слова: *информационная безопасность, угрозы безопасности, когнитивное моделирование, нечеткая когнитивная карта.*

Saliieva O., Yaremchuk Yu. Determining the level of security of the information security system based on cognitive modeling

Abstract. *This article discusses approaches to solving the problem of assessing the level of security of the information security system in the context of threats. The analysis of application of different types of fuzzy cognitive maps for the decision of problems of information security is carried out. To identify general trends in the level of protection under the influence of potential threats, a system of information protection with general characteristics was chosen. A cognitive model based on a fuzzy cognitive map is proposed, which allows to determine the level of security of the information security system. To build a fuzzy cognitive map, many concepts have been formed - the most important factors in terms of studying this problem and the cause-and-effect relationships between them have been identified. The structural and topological properties of the fuzzy cognitive map are evaluated. In particular, such indicators of structural complexity*

of fuzzy cognitive map as: density, complexity, centrality of the concept and hierarchy index are determined. A matrix of mutual influences of concepts is constructed, on the basis of which quantitative values of the main system indicators are determined: consonance, dissonance, influence of factors. After analyzing these indicators, the most important threats to the security of the studied system were identified. Scenario modeling of the impact of these threats on the level of security of the information security system is carried out. Based on the data obtained from the launch of the developed scenarios, it is possible to prepare a clear plan for improving the security of the information security system, timely take the necessary measures to help prevent, localize, eliminate or reduce the impact of potential threats to information security.
Keywords: *information security, security threats, cognitive modeling, fuzzy cognitive map.*

Салієва Ольга Володимирівна, аспірантка кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.
Салиева Ольга Владимировна, аспирантка кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.
Saliieva Olha, graduate student of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.

Яремчук Юрій Євгенович, директор Центру інформаційних технологій та захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.
Яремчук Юрий Евгеньевич, директор Центра информационных технологий и защиты информации, профессор кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.
Yaremchuk Yurii, Director of the Center for Information Technologies and Information Protection, Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.

Отримано *6 квітня 2020 року*, затверджено редколегією *25 квітня 2020 року*