УДК 519.233.5:004.81.056.6(045)

[0000-0003-2388-7321] **О. В. Салієва,** *асистент,*
e-mail: salieva8257@gmail.com
[0000-0002-6303-7703] **Ю. Є. Яремчук,** *д.т.н., професор*
e-mail: yurevyar@vntu.edu.ua
Вінницький національний технічний університет
вул. Хмельницьке шосе, 95, м. Вінниця, 21021, Україна

ДОСЛІДЖЕННЯ ДОСТОВІРНОСТІ ВПЛИВУ ЗАГРОЗ НА РІВЕНЬ ЗАХИЩЕНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА РЕЗУЛЬТАТАМИ КОГНІТИВНОГО МОДЕЛЮВАННЯ

У роботі проведено дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об'єкта критичної інфраструктури, визначеного за сценарним моделюванням на основі когнітивного підходу. Водночас застосовано апарат множинного регресійного аналізу, який дає можливість простежити зв'язок між загрозами та захищеністю досліджуваних систем, оцінивши ступінь ймовірного впливу. Сформовано аналітичні вирази лінійної кореляційної залежності між найвагомішими концептами кожної когнітивної моделі та захищеністю відповідної досліджуваної системи. З метою порівняння впливу загроз на захищеність об'єкта критичної інфраструктури та системи захисту інформації, отриманого за результатами когнітивного моделювання, визначено стандартизовані коефіцієнти регресії та коефіцієнти еластичності. Проведений аналіз отриманих значень цих показників дав змогу підтвердити достовірність впливу загроз на рівень захищеності досліджуваних систем.

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

Вступ. Сучасний інформаційний простір зазнає впливу найрізноманітніших загроз, реалізація яких може призвести до вкрай негативних наслідків. Тому дослідження впливу загроз на рівень захищеності систем є актуальним та важливим науковим завданням, яке характеризується високим ступенем невизначеності та складністю строгої формалізації. Для його вирішення доцільно скористатися когнітивним підходом, який базується на побудові нечітких когнітивних карт [1-6]. Так, у роботі [7] автори запропонували методику оцінювання рівня інформаційної безпеки на основі нечіткої когнітивної моделі, яка складається із шести рівнів ієрархії.

Автор праці [8] для проведення аналізу та оцінювання ризиків інформаційній безпеці використав нечітку когнітивну карту і нечітку продукційну модель у складі нечіткої гібридної моделі.

У [9] розглянуто задачу підвищення достовірності оцінок показників забезпечення інформаційної безпеки на основі побудови когнітивних моделей, пов'язаних з процесом формування та розвитку різних типів загроз.

У роботах [10-12] запропоновано та проаналізовано когнітивні моделі для оцінювання рівня захищеності комп'ютерної мережі (КМ), системи захисту інформації (ЗІ) та об'єкта критичної інфраструктури (КІ) відповідно. Визначено найвагоміші загрози і проведено сценарне моделювання, в результаті якого встановлено відносну зміну рівня захищеності досліджуваних систем при впливі кожної із найвагоміших загроз. Достовірність отриманого результату впливу загроз на рівень захищеності КМ підтверджено у роботі [13]. Тому цікавим є проведення аналогічного дослідження відносно систем ЗІ та об'єкта КІ на основі множинного регресійного аналізу[14].

Метою дослідження є встановлення достовірності впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ, отриманого за результатами когнітивного моделювання.

Для досягнення поставленої мети необхідно вирішити такі ***завдання:***

– визначити експериментальні дані за сценарним моделюванням на основі когнітивного підходу;

– для кожної з когнітивних моделей знайти аналітичний вираз лінійної кореляцій-

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251

ної залежності, яка існує між досліджуваними концептами;

– визначити коефіцієнти регресії та коефіцієнти еластичності;

– на основі значень коефіцієнта регресії та коефіцієнта еластичності порівняти вплив найвагоміших концептів на захищеність досліджуваних систем.

Визначення впливу загроз на рівень захищеності системи ЗІ на основі множинного регресійного аналізу

Розглянемо когнітивну модель, запропоновану у роботі [11], для визначення впливу загроз на рівень захищеності системи ЗІ (рисунок 1).

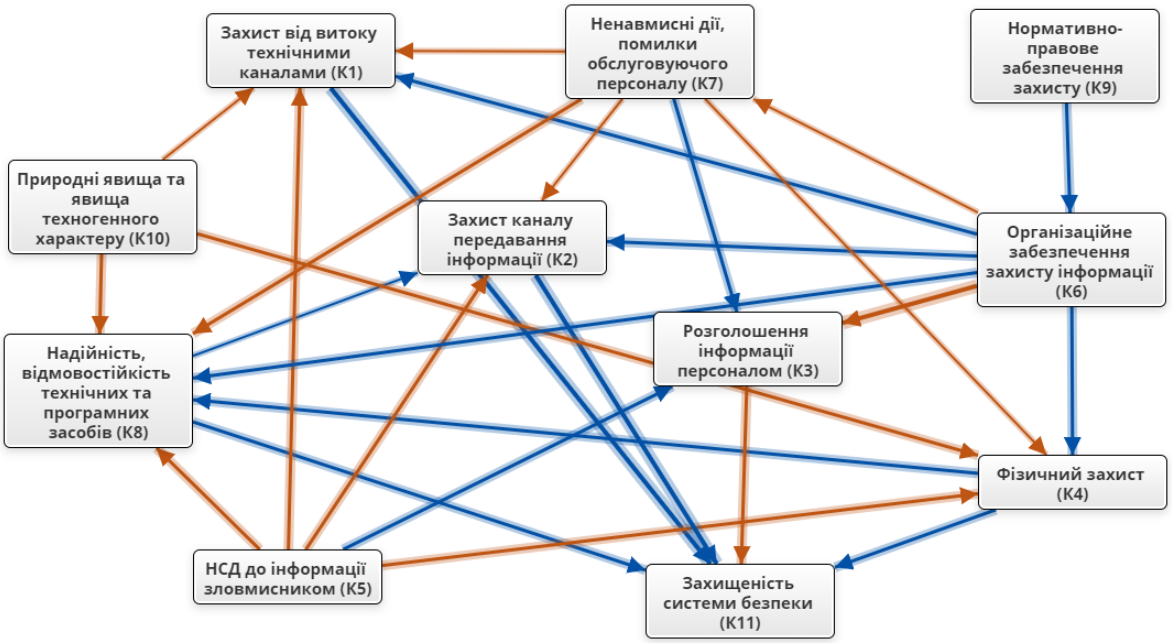

Рисунок 1 – Когнітивна модель дослідження стану захищеності системи ЗІ

У результаті дослідження цієї моделі було визначено її найвагоміші концепти: фізичний захист (K_4), НСД до інформації зловмисником (K_5) та організаційне забезпечення ЗІ (K_6). За допомогою сценарного моделювання встановлено, що при максимально негативному впливі кожного з цих концептів окремо захищеність системи безпеки (K_{11}) погіршиться відповідно на 0,26; 0,23 та 0,07.

Порівняємо вплив найвагоміших концептів на захищеність досліджуваної системи за допомогою регресійного аналізу [15].

Для досягнення поставленої мети змоделюємо десять різних сценаріїв, що відображають відносну зміну захищеності системи безпеки при заданих значеннях обраних концептів (таблиця 1).

Таблиця 1 – **Значення досліджуваних концептів, отримані в результаті сценарного моделювання**

i	K_{i4}	K_{i5}	K_{i6}	K_{i11}
1	1	1	1	0,08
2	0,9	-0,1	0,7	0,13
3	-0,1	-0,3	-0,1	-0,08
4	1	-0,2	1	0,16
5	-0,2	0,3	0,9	-0,04
6	0,8	0,2	-0,3	-0,01
7	1	-0,1	-0,2	0,06
8	-0,3	-0,5	0,8	0,01
9	0,7	0,8	0,9	0,05
10	0,5	-0,3	-0,1	0,02

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251

Припускаючи, що між концептами існує лінійна кореляційна залежність, знайдемо її аналітичний вираз (рівняння регресії K_{11} відносно K_4, K_5 та K_6).Позначимо:

$$Y = \begin{pmatrix} 0.08 \\ 0.13 \\ -0.08 \\ 0.16 \\ -0.04 \\ -0.01 \\ 0.06 \\ 0.01 \\ 0.05 \\ 0.02 \end{pmatrix}, \quad K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0.9 & -0.1 & 0.7 \\ 1 & -0.1 & -0.3 & -0.1 \\ 1 & 1 & -0.2 & 1 \\ 1 & -0.2 & 0.3 & 0.9 \\ 1 & 0.8 & 0.2 & -0.3 \\ 1 & 1 & -0.1 & -0.2 \\ 1 & -0.3 & -0.5 & 0.8 \\ 1 & 0.7 & 0.8 & 0.9 \\ 1 & 0.5 & -0.3 & -0.1 \end{pmatrix}.$$

Для зручності обчислень складемо допоміжну таблицю (таблиця 2).

Таблиця 2 – **Додаткові проміжні дані**

i	K_{i4}	K_{i5}	K_{i6}	y_i	K_{i4}^2	K_{i5}^2	K_{i6}^2	$K_{i4}K_{i5}$	$K_{i4}K_{i6}$	$K_{i5}K_{i6}$	y_iK_{i4}	y_iK_{i5}	y_iK_{i6}
1	1	1	1	0,08	1	1	1	1	1	1	0,08	0,08	0,08
2	0,9	-0,1	0,7	0,13	0,81	0,01	0,49	-0,09	0,63	-0,07	0,117	-0,013	0,091
3	-0,1	-0,3	-0,1	-0,08	0,01	0,09	0,01	0,03	0,01	0,03	0,008	0,024	0,008
4	1	-0,2	1	0,16	1	0,04	1	-0,2	1	-0,2	0,16	-0,032	0,16
5	-0,2	0,3	0,9	-0,04	0,04	0,09	0,81	-0,06	-0,18	0,27	0,008	-0,012	-0,036
6	0,8	0,2	-0,3	-0,01	0,64	0,04	0,09	0,16	-0,24	-0,06	-0,008	-0,002	0,003
7	1	-0,1	-0,2	0,06	1	0,01	0,04	-0,1	-0,2	0,02	0,06	-0,006	-0,012
8	-0,3	-0,5	0,8	0,01	0,09	0,25	0,64	0,15	-0,24	-0,4	-0,003	-0,005	0,008
9	0,7	0,8	0,9	0,05	0,49	0,64	0,81	0,56	0,63	0,72	0,035	0,04	0,045
10	0,5	-0,3	-0,1	0,02	0,25	0,09	0,01	-0,15	-0,05	0,03	0,01	-0,006	-0,002
$\sum$	5,3	0,8	4,6	0,38	5,33	2,26	4,9	1,3	2,36	1,34	0,47	0,07	0,345

Враховуючи дані таблиці 2, знайдемо $(K'K)^{-1}$:

$$(K'K)^{-1} = \begin{pmatrix} 10 & 5.3 & 0.8 & 4.6 \\ 5.3 & 5.33 & 1.3 & 2.36 \\ 0.8 & 1.3 & 2.26 & 1.34 \\ 4.6 & 2.36 & 1.34 & 4.9 \end{pmatrix}^{-1} =$$

$$= \begin{pmatrix} 0.34 & -0.28 & 0.18 & -0.24 \\ -0.28 & 0.48 & -0.23 & 0.095 \\ 0.18 & -0.23 & 0.65 & -0.23 \\ -0.24 & 0,095 & -0.23 & 0.44 \end{pmatrix}.$$

Перемножаючи цю матрицю на вектор

$$K'Y = \begin{pmatrix} 0.38 \\ 0.47 \\ 0.07 \\ 0.345 \end{pmatrix}, \text{ отримаємо } b = \begin{pmatrix} -0.07 \\ 0.14 \\ -0.08 \\ 0.092 \end{pmatrix}.$$

Таким чином, рівняння множинної регресії матиме вигляд

$$\hat{y} = -0.07 + 0.14K_4 - 0.08K_5 + 0.092K_6.$$

Для порівняння впливу кожного із найвагоміших концептів на захищеність системи ЗІ використаємо стандартизовані коефіцієнти регресії b'_j та коефіцієнти еластичності E_j $(j = 1, 2, \ldots, p)$:

$$b'_j = b_j \frac{s_{kj}}{s_y}, \qquad (1)$$

де $s_{kj}^2 = \frac{\sum (K_{ij} - \overline{K})^2}{i}$, $s_y^2 = \frac{\sum (y_i - \overline{y})^2}{i}$,

$$E_j = b_j \frac{\overline{K}_j}{\overline{y}}. \qquad (2)$$

Розрахуємо стандартизовані коефіцієнти регресії b'_j (1) і коефіцієнти еластичності E_j (2):

$$b'_1 = 0.14\frac{0.5}{0.07} = 1, \quad b'_2 = -0.08\frac{0.47}{0.07} = -0.54,$$

$$b'_3 = 0.092\frac{0.53}{0.07} = 0.7;$$

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251

$$E_1 = 0.14\frac{0.53}{0.038} = 1.95, \quad E_2 = -0.08\frac{0.08}{0.038} = -0.17,$$

$$E_3 = 0.092\frac{0.46}{0.038} = 1.11.$$

Проаналізувавши значення отриманих показників, можна зробити висновок, що збільшення значень концептів фізичний захист (K_4) та організаційне забезпечення ЗІ (K_6) на одне S_{K4} або S_{K6} посилить у середньому захищеність системи ЗІ відповідно на S_y або на $0.7S_y$, а збільшення цих змінних на 1 % (від своїх середніх значень) приведе у середньому до підвищення рівня захищеності відповідно на 1,95 % та 1,11 %. Водночас збільшення значення концепту НСД до інформації зловмисником (K_5) на S_{K5} призведе до послаблення захищеності у середньому на $0.54S_y$, а збільшення цього концепту на 1 % (від своїх середніх значень) призведе у середньому до зниження рівня захищеності системи ЗІ на 0,17 %.

Таким чином, концепт фізичний захист (K_4) чинить більший вплив на захищеність системи ЗІ, ніж концепт організаційне забезпечення ЗІ (K_6), а концепт НСД до інформації зловмисником (K_5) має найменший вплив серед усіх найвагоміших концептів когнітивної моделі. Це, у свою чергу, підтверджує результати, отримані у роботі [11], внаслідок проведеного сценарного моделювання.

Визначення впливу загроз на рівень захищеності об'єкта КІ за допомогою множинного регресійного аналізу

Подібним чином проаналізуємо результати, отримані внаслідок дослідження когнітивної моделі для визначення рівня захищеності об'єкта КІ [12] (рисунок 2).

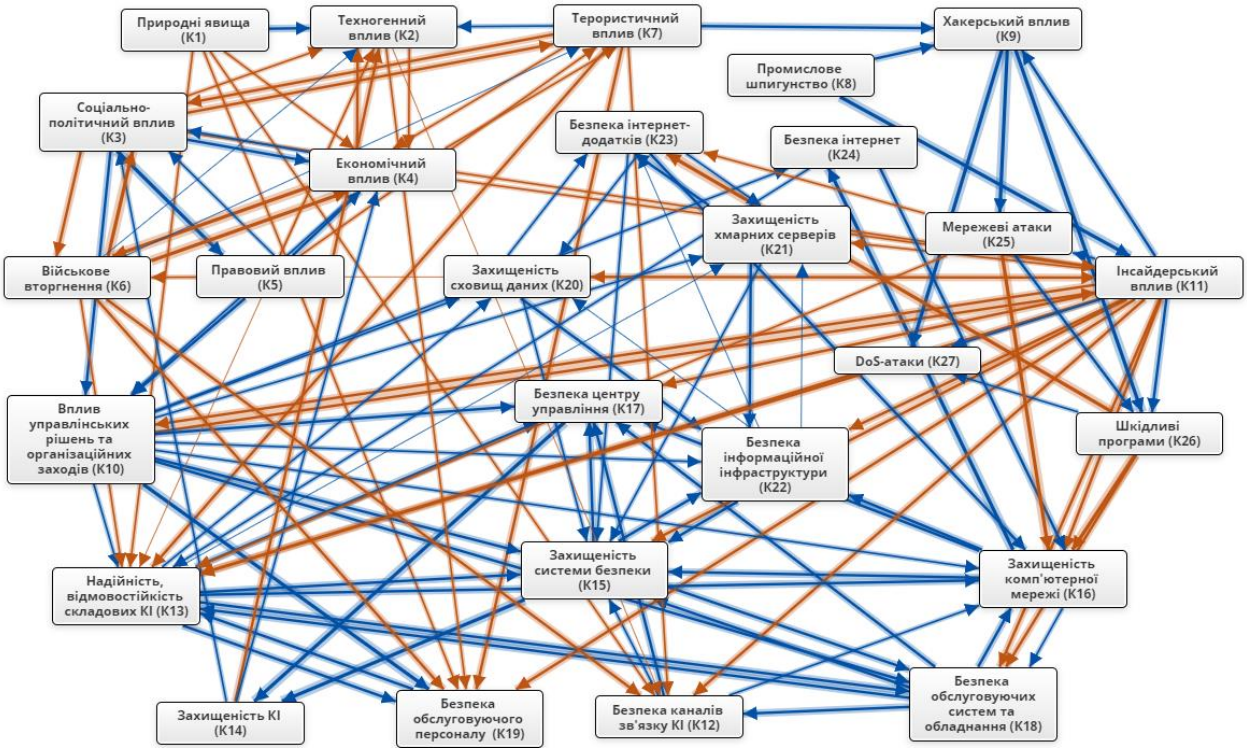

Рисунок 2 – Когнітивна модель для дослідження рівня захищеності об'єкта КІ

У цьому випадку найвагомішими концептами було визначено: інсайдерський вплив (K_{11}), захищеність системи безпеки (K_{15}) і захищеність КМ (K_{16}). Відзначимо, що при максимально негативному впливі кожного з цих концептів захищеність об'єкта КІ (K_{14}) погіршиться на 0,03; 0,44 та 0,06 відповідно.

З метою проведення дослідження змоделюємо 10 різних сценаріїв, що відображають відносну зміну захищеності об'єкта КІ при заданих значеннях найвагоміших концептів (таблиця 3).

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251

Таблиця 3 – **Значення досліджуваних концептів, отримані в результаті сценарного моделювання**

i	K_{i11}	K_{i15}	K_{i16}	K_{i14}
1	-1	1	1	0,02
2	-0,5	-0,7	0,8	-0,31
3	1	0,6	-0,9	-0,11
4	-0,2	-0,9	-0,7	-0,41
5	-0,1	-0,6	-0,2	-0,32
6	-0,9	-1	-1	-0,41
7	0,4	0,3	0,1	-0,11
8	0,6	-0,5	-0,1	-0,36
9	-0,8	-0,4	-0,9	-0,26
10	0,3	-0,8	-0,9	-0,44

Припускаючи, що між концептами існує лінійна кореляційна залежність, знайдемо її аналітичний вираз (рівняння регресії K_{14} відносно K_{11}, K_{15} та K_{16}). Здійснимо позначення:

$$Y = \begin{pmatrix} 0.02 \\ -0.31 \\ -0.11 \\ -0.41 \\ -0.32 \\ -0.41 \\ -0.11 \\ -0.36 \\ -0.26 \\ -0.44 \end{pmatrix}, \quad K = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & -0.5 & -0.7 & 0.8 \\ 1 & 1 & 0.6 & -0.9 \\ 1 & -0,2 & -0.9 & -0,7 \\ 1 & -0.1 & -0.6 & -0.2 \\ 1 & -0.9 & -1 & -1 \\ 1 & 0.4 & 0.3 & 0.1 \\ 1 & 0.6 & -0.5 & -0.1 \\ 1 & -0.8 & -0.4 & -0.9 \\ 1 & 0.3 & -0.8 & -0.9 \end{pmatrix}.$$

Для зручності обчислень складемо допоміжну таблицю (таблиця 4).

Таблиця 4 – **Додаткові проміжні дані**

i	K_{i11}	K_{i15}	K_{i16}	y_i	K_{i11}^2	K_{i15}^2	K_{i16}^2	$K_{i11}K_{i15}$	$K_{i11}K_{i16}$	$K_{i15}K_{i16}$	y_iK_{i11}	y_iK_{i15}	y_iK_{i16}
1	-1	1	1	0,02	1	1	1	-1	-1	1	-0,02	0,02	0,02
2	-0,5	-0,7	0,8	-0,31	0,25	0,49	0,64	0,35	-0,4	-0,56	0,155	0,217	-0,248
3	1	0,6	-0,9	-0,11	1	0,36	0,81	0,6	-0,9	-0,54	-0,09	-0,054	0,099
4	-0,2	-0,9	-0,7	-0,41	0,04	0,81	0,49	0,18	0,14	0,63	0,08	0,36	0,287
5	-0,1	-0,6	-0,2	-0,32	0,01	0,36	0,04	0,06	0,02	0,12	0,032	0,192	0,064
6	-0,9	-1	-1	-0,41	0,81	1	1	0,9	0,9	1	0,369	0,41	0,41
7	0,4	0,3	0,1	-0,11	0,16	0,09	0,01	0,12	0,04	0,03	-0,044	-0,033	-0,011
8	0,6	-0,5	-0,1	-0,36	0,36	0,25	0,01	-0,3	-0,06	0,05	-0,216	0,18	0,036
9	-0,8	-0,4	-0,9	-0,26	0,64	0,16	0,81	0,32	0,72	0,36	0,208	0,104	0,234
10	0,3	-0,8	-0,9	-0,44	0,09	0,64	0,81	-0,24	-0,27	0,72	-0,132	0,352	0,396
$\sum$	-1,2	-3	-2,8	-2,71	4,36	5,16	5,62	0,99	-0,81	2,81	0,342	1,748	1,287

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251

Таким чином, отримаємо обернену матрицю:

$$(K'K)^{-1} = \begin{pmatrix} 10 & -1.2 & -3 & -2.8 \\ -1.2 & 4.36 & 0.99 & -0.81 \\ -3 & 0.99 & 5.16 & 2.81 \\ -2.8 & -0.81 & 2.81 & 5.62 \end{pmatrix}^{-1} =$$

$$= \begin{pmatrix} 0.13 & 0.035 & 0.043 & 0.049 \\ 0.035 & 0.28 & -0.088 & 0.1 \\ 0.043 & -0.088 & 0.32 & -0.15 \\ 0.049 & 0{,}1 & -0.15 & 0.29 \end{pmatrix}.$$

Перемножаючи цю матрицю на вектор

$$K'Y = \begin{pmatrix} -2.71 \\ 0.342 \\ 1.748 \\ 1.287 \end{pmatrix}, \text{ матимемо } b = \begin{pmatrix} -0.2 \\ -0.024 \\ 0.22 \\ 0.016 \end{pmatrix}.$$

Отже, складемо рівняння множинної регресії:

$$\hat{y} = -0.2 - 0.024K_{11} + 0.22K_{15} + 0.016K_{16}.$$

За допомогою формул (1)-(2) розрахуємо стандартизовані коефіцієнти регресії b'_j та коефіцієнти еластичності E_j:

$$b'_1 = -0.024\frac{0.65}{0.14} = -0{,}11, \quad b'_2 = 0.22\frac{0.65}{0.14} = 1.02,$$

$$b'_3 = 0.016\frac{0.69}{0.14} = 0.08;$$

$$E_1 = -0.024\frac{-0.12}{-0.271} = -0.01, \quad E_2 = 0.22\frac{-0.3}{-0.271} = 0.24,$$

$$E_3 = 0.016\frac{-0.28}{-0.271} = 0.017.$$

Аналіз розрахованих коефіцієнтів показав, що збільшення значень концептів захищеність системи безпеки (K_{15}) та захищеність КМ (K_{16}) на одне S_{K15} або S_{K16} посилить у середньому захищеність об'єкта КІ відповідно на $1.02S_y$ або на $0.08S_y$, а збільшення цих змінних на 1 % (від своїх середніх значень) приведе у середньому до підвищення рівня захищеності відповідно на 0,24 % та 0,017 %. Водночас збільшення інсайдерського впливу (K_{11}) на S_{K11} призведе до послаблення захищеності в середньому на $0.11S_y$, а збільшення цього концепту на 1 % (від своїх середніх значень) призведе у середньому до зниження рівня захищеності об'єкта КІ на 0,01 %.

Отримані дані підтверджують достовірність результатів, отриманих за сценарним моделюванням у роботі [12], а саме: встановлено, що захищеність системи безпеки (K_{15}) чинить більший вплив на захищеність КІ, ніж захищеність КМ (K_{16}), у той час як зростання інсайдерського впливу (K_{11}) найменшою мірою відобразиться на захищеності КІ.

Результати досліджень. На основі множинного регресійного аналізу визначено вплив найвагоміших загроз на рівень захищеності системи ЗІ та об'єкта КІ.

Зокрема, при дослідженні когнітивної моделі системи ЗІ встановлено, що збільшення значень концептів фізичний захист (K_4) та організаційне забезпечення ЗІ (K_6) на 1 % (від своїх середніх значень) приведе у середньому до підвищення рівня захищеності відповідно на 1,95 % та 1,11 %. Водночас збільшення значення концепту НСД до інформації зловмисником (K_5) знизить у середньому рівень захищеності на 0,17 %.

У свою чергу, дослідження когнітивної моделі об'єкта КІ показало, що підвищення захищеності системи безпеки (K_{15}) та КМ (K_{16}) на 1 % (від своїх середніх значень) підсилить у середньому рівень захищеності відповідно на 0,24 % та 0,017 %, а зростання інсайдерського впливу (K_{11}) призведе до зниження рівня захищеності об'єкта КІ на 0,01 %.

Зазначені результати підтверджують достовірність впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ, отриманого за результатами когнітивного моделювання.

Обговорення результатів. Аналізуючи отримані результати з наявними у роботі [13], слід відзначити, що вони дають можливість дослідити достовірність впливу загроз лише для КМ, у той час як результати цієї роботи підтверджують вірогідність впливу загроз для системи ЗІ та об'єкта КІ. Порівнюючи отримані результати з наявними у роботах [11] та [12], слід також зазначити, що в них визначався вплив загроз на захищеність системи ЗІ та об'єкта КІ на основі сценарного моделювання, тоді як у цьому дослідженні підтверджено достовірність впливу загроз на рівень захищеності досліджуваних систем на основі апарату множинного регресійного аналізу, що у

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251

цілому підвищило рівень достовірності впливу визначених загроз. Окрім того, результати цієї роботи дають можливість спрогнозувати розвиток ситуації для прийняття вчасних та ефективних управлінських рішень, спрямованих на підвищення захищеності системи ЗІ та об'єкта КІ.

Висновки. Таким чином, на основі множинного регресійного аналізу було доведено достовірність впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ, визначеного за результатами когнітивного моделювання. Для кожної із когнітивних моделей знайдено аналітичний вираз лінійної кореляційної залежності, яка існує між найвагомішими її концептами та захищеністю відповідної системи. Розраховано стандартизовані коефіцієнти регресії, які показують, на скільки величин зміниться в середньому залежна змінна при збільшенні тільки однієї незалежної змінної, та коефіцієнти еластичності, за допомогою яких простежується, на скільки відсотків (від середнього значення) зміниться у середньому залежна змінна при збільшенні незалежної змінної на 1 %. Проведений аналіз отриманих значень визначених показників дав змогу підтвердити достовірність впливу загроз на рівень захищеності досліджуваних систем.

Наукова новизна роботи полягає у використанні когнітивних моделей для дослідження впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ.

Практичною цінністю роботи є можливість застосування отриманих результатів для підвищення рівня захищеності досліджуваних систем.

Перспективним є подальше дослідження еволюційного розвитку усієї системи ЗІ при впливі на неї потенційних загроз на основі імпульсного моделювання.

Список використаних джерел

[1] B. Kosko, "Fuzzy cognitive maps", *International Journal of Man-Machine Studies*, vol. 24, no. 1, pp. 65-75, 1986.

[2] В. Б. Силов, *Принятие стратегических решений в нечеткой обстановке.* Москва, Россия: ИНПРО, РЕС, 1995.

[3] В. В. Борисов, В. В. Круглов, и А. С. Федулов, *Нечеткие модели и сети*, 2-е изд., стереотип. Москва, Россия: Горячая линия, Телеком, 2012.

[4] О. П. Кузнецов, А. А. Кулинич, и А. В. Марковский, "Анализ влияний при управлении слабоструктурированными ситуациями на основе когнитивных карт", *Человеческий фактор в управлении*, с. 313-344, 2006.

[5] E. Papageorgiou, and 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.

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

[7] И. М. Ажмухамедов, и О. М. Князева, "Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности", *Прикаспийский журнал: управление и высокие технологии*, № 3 (31), с. 24-39, 2015.

[8] Е. А. Зюзикова, "Использование нечеткой гибридной модели для анализа рисков информационной безопасности", *Научный журнал «Студенческий»*, № 11 (31), с. 5-7, 2018.

[9] Ш. Г. Магомедов, "Оценка степени влияния сопутствующих факторов на показатели информационной безопасности", *Российский технологический журнал,* т. 5, № 2, с. 47-56, 2017.

[10] О. В. Салієва,та Ю. Є. Яремчук, "Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі", *Реєстрація, зберігання і обробка даних*, т. 21, № 4, с. 28-39, 2019.

[11] О. В. Салієва, та Ю. Є. Яремчук, "Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання", *Безпека інформації*, № 1, с. 42-49, 2020.

[12] О. В. Салієва, та Ю. Є. Яремчук, "Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури", *Безпека інформації*, т. 26, № 2, с. 64-73, 2020.

[13] О. В. Салієва, та Ю. Є. Яремчук, "Дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі,

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251

визначеного за сценарним моделюванням на основі когнітивного підходу", *Вісник Вінницького політехнічного інституту,* № 4, с. 98-104, 2020.

[14] Р. М. Літнарович, *Побудова і дослідження математичної моделі за джерелами експериментальних даних методами регресійного аналізу*. Рівне, Україна: МЕГУ, 2011.

[15] Н. Ш. Кремер, *Теория вероятностей и математическая статистика*. Москва, Россия: Юрайт, 2019.

References

[1] B. Kosko, "Fuzzy cognitive maps", *International Journal of Man-Machine Studies*, vol. 24, no. 1, pp. 65-75, 1986.

[2] V. B. Silov, *Strategic decision-making in a fuzzy environment*. Moscow, Russia: INPRO, RES, 1995. [in Russian].

[3] V. V. Borisov, V. V. Kruglov, and A. S. Fedulov, *Fuzzy models and networks*, 2nd ed., Stereotype. Moscow, Russia: Goryachaya liniya. Telekom, 2012. [in Russian].

[4] O. P. Kuznetsov, A. A. Kulinich, and A. V. Markovskiy, "Analysis of influences in the management of weakly structured situations based on cognitive maps", *The human factor in management*, pp. 313-344, 2006. [in Russian].

[5] E. Papageorgiou, and 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.

[6] A. S. Fedulov, "Fuzzy relational cognitive maps", *Izvestiya RAN. Teoriyaisistemyupravleniya*, no. 1, pp. 120-132, 2005. [in Russian].

[7] I. M. Azhmukhamedov, and O. M. Knyazeva, "Assessment of the state of security of the organization's data in the context of the possibility of implementing threats to information security", *Prikaspiyski yzhurnal: upravleniye i vysokiye tekhnologii*, no. 3 (31), pp. 24-39, 2015. [in Russian].

[8] E. A. Zyuzikova, "Using a fuzzy hybrid model for the analysis of information security risks", *Nauchnyy zhurnal "Studencheskiy"*, no. 11 (31), pp. 5-7, 2018. [in Russian].

[9] Sh. G. Magomedov, "Assessment of the degree of influence of accompanying factors on information security indicators", *Rossiyskiy tekhnologicheskiy zhurnal*, vol. 5, no. 2, pp. 47-56, 2017. [in Russian].

[10] O. V. Saliieva, and Yu. E. Yaremchuk, "Development of a cognitive model for the analysis of the impact of threats on the level of security of a computer network", *Reiestratsiia, zberihannia i obrobka danykh*, vol. 21, no. 4, pp. 28-39, 2019. [in Ukrainian].

[11] O. V. Saliieva, and Yu. E. Yaremchuk, "Determination of the level of security of the information protection system based on cognitive modeling", *Bezpeka informatsii*, no. 1, pp. 42-49, 2020. [in Ukrainian].

[12] O. V. Saliieva, and Yu. E. Yaremchuk, "Cognitive model for studying the level of security of a critical infrastructure object", *Bezpeka informatsii*, vol. 26, no. 2, pp. 64-73, 2020. [in Ukrainian].

[13] O. V. Saliieva, and Yu. E. Yaremchuk, "Study of the reliability of the impact of threats on the level of security of a computer network, determined by scenario modeling based on a cognitive approach", *Visnyk Vinnytskoho politekhnichnoho instytutu*, no. 4, pp. 98-104, 2020. [in Ukrainian].

[14] R. M. Litnarovych, *Construction and research of a mathematical model based on sources of experimental data by regression analysis*, Rivne, Ukraine: MEGU, 2011. [in Ukrainian].

[15] N. Sh. Kremer, *Probability theory and mathematical statistics*, Moscow, Russia: Yurayt, 2019. [in Russian].

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251

O. V. Saliieva, *assistant,*
e-mail: salieva8257@gmail.com
Yu. E. Yaremchuk, *D.Sc., professor*
e-mail: yurevyar@vntu.edu.ua
Vinnytsia National Technical University,
Khmelnytske Shosse, 95, Vinnytsia, Ukraine

STUDY OF THE RELIABILITY OF THE IMPACT OF THREATS ON THE LEVEL OF SECURITY OF THE INFORMATION PROTECTION SYSTEM AND THE OBJECT OF CRITICAL INFRASTRUCTURE BASED ON THE RESULTS OF COGNITIVE MODELING

The rapid development of information technology has led to new challenges and threats to information security. Therefore, it is important to solve the problem of ensuring the proper level of security of systems when exposed to potential threats. Particular attention is paid to the safety of critical infrastructure and information protection systems, violations of the functioning of which can lead to large-scale consequences of a negative nature.

In this regard, the study of the reliability of the impact of threats on the level of security of the information protection system and the object of critical infrastructure determined by the script modeling on the basis of cognitive approach has been conducted. At the same time, the multiple regression analysis apparatus is used, which allows to trace the link between threats and the security of the investigated systems, assessing the degree of likely impact.

To achieve this goal, based on the researched cognitive models to assess the level of security of information protection systems and the object of critical infrastructure, analytical expressions of linear correlational dependence between the most important concepts of each model separately and the protection of the relevant systems are formed. In order to compare the impact of threats on the security of the information protection system and the object of critical infrastructure, standardized regression coefficients are defined, which show how much values the dependent variable will change on average while increasing only one independent variable and the elasticity ratios by which the average dependent variable will change by one percent. The analysis of the obtained values of these indicators has allowed to confirm the accuracy of the results obtained as a result of script modeling on a cognitive approach.

Keywords: *information security, security threats, cognitive modeling, fuzzy cognitive map, multiple regression analysis.*

Стаття надійшла 14.09.2020
Прийнято 18.10.2020

© О. В. Салієва, Ю. Є. Яремчук, 2020
DOI: 10.24025/2306-4412.3.2020.216251