https://doi.org/10.31649/1997-9266-2020-151-4-98-104

УДК 004.7.056.5:004.81

**О. В. Салієва**[1]
**Ю. Є. Яремчук**[1]

# ДОСЛІДЖЕННЯ ДОСТОВІРНОСТІ ВПЛИВУ ЗАГРОЗ НА РІВЕНЬ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ, ВИЗНАЧЕНОГО ЗА СЦЕНАРНИМ МОДЕЛЮВАННЯМ НА ОСНОВІ КОГНІТИВНОГО ПІДХОДУ

[1]Вінницький національний технічний університет

*Стрімкий розвиток комп'ютерних мереж надає сучасному суспільству безліч нових можливостей, забезпечує надання різноманітних послуг в усіх сферах людської діяльності. Тому необхідно враховувати вагомість надійного і безпечного функціонування комп'ютерних мереж та приділяти значну увагу забезпеченню належного рівня їхньої захищеності. Визначаючи актуальність цього питання, проведено дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі за сценарним моделюванням на основі когнітивного підходу. Методика досліджень базується на використанні множинного регресійного аналізу, який дозволяє проаналізувати зв'язок між декількома незалежними змінними (загрозами) та цільовою змінною (захищеність комп'ютерної мережі).*

*Для досягнення поставленої мети сформовано аналітичний вираз лінійної кореляційної залежності, що існує між цільовою змінною відносно таких загроз як: шкідливі програми, фізичний вплив на мережу з боку зловмисника та ненавмисні дії, помилки користувачів мережі.*

*Оцінено адекватність запропонованої регресійної моделі за допомогою коефіцієнта детермінації, який є мірою якості рівняння регресії.*

*Визначено значення стандартизованого коефіцієнта регресії та коефіцієнта еластичності, які є необхідними для порівняння впливу кожної загрози окремо на рівень захищеності комп'ютерної мережі. Отримані значення коефіцієнтів, проаналізовано та зроблено висновок, що серед досліджуваних загроз найбільше знижують рівень захищеності ненавмисні дії, помилки користувачів мережі, а найменше — фізичний вплив на мережу з боку зловмисника. Такий результат збігається з отриманим авторами за сценарним моделюванням на основі когнітивного підходу, що, у свою чергу, свідчить про достовірність впливу визначених загроз на рівень захищеності комп'ютерної мережі.*

**Ключові слова:** комп'ютерна мережа, загроза, захищеність, когнітивний підхід, нечітка когнітивна карта, множинний регресійний аналіз.

## Вступ

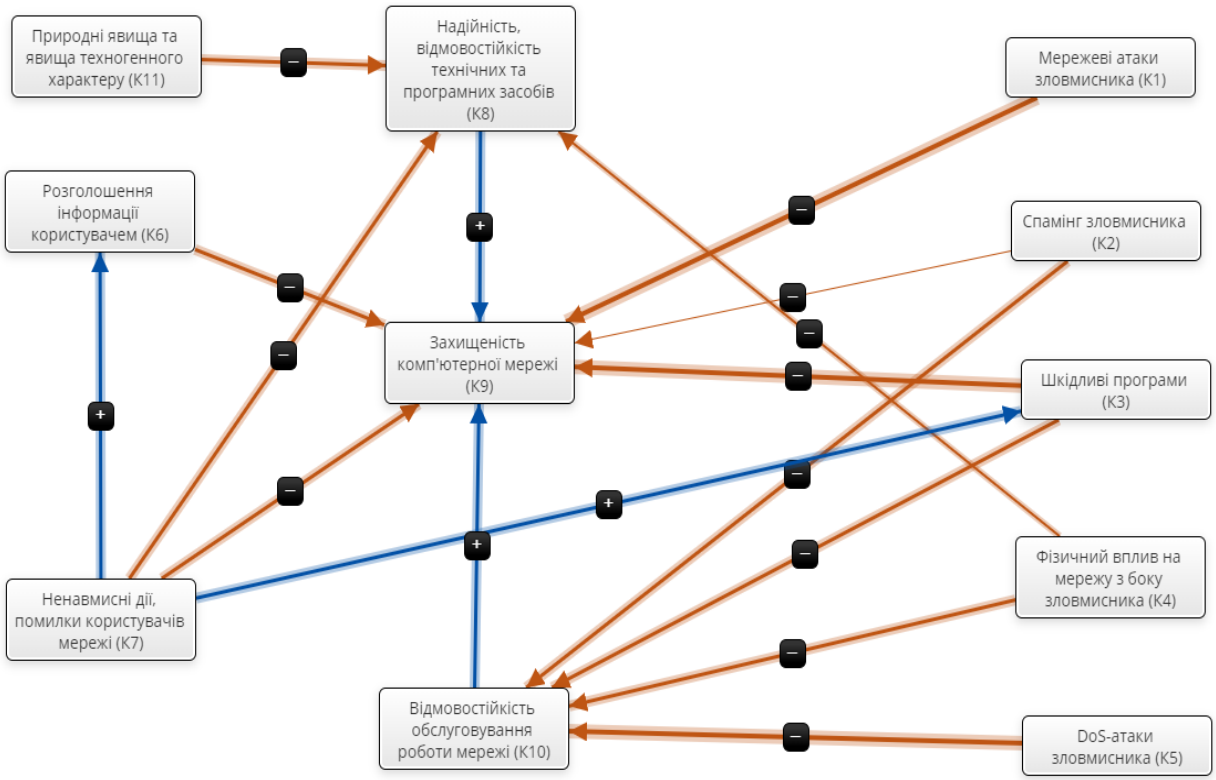
Комп'ютерні мережі (КМ) є невід'ємною частиною усіх сфер сучасного суспільного життя, адже вони створюють єдиний інформаційний простір для користувачів, задовольняючи їхні інформаційні потреби. Для ефективного та надійного функціонування КМ варто приділити значну увагу аналізу, оцінюванню та підвищенню рівня їхньої захищеності. В працях багатьох вчених розв'язуються такі задачі. Зокрема, у роботі [1] проводиться аналіз захищеності КМ на етапах проектування і експлуатації на основі розробки і використання моделей комп'ютерних атак, порушника, аналізованої КМ, формування дерева атак, оцінки рівня захищеності і методики аналізу захищеності КМ. Автори роботи [2] пропонують методику оцінювання захищеності КМ на основі логіко-лінгвістичного підходу та апарату нечіткої логіки. У роботі [3] запропоновано класифікацію методів тестування на проникнення для оцінювання захищеності комп'ютерних систем. Автори праці [4] розглянули підхід, який об'єднує множину моделей і методику, для реалізації детального аналізу захищеності КМ на етапах експлуатації і проектування, який базується на імітації дій порушника, побудові і аналізу графу загроз. У роботі [5] на основі когнітивного підходу проаналізовано вплив загроз на рівень захищеності КМ, визначено найвагоміші загрози та проведено сценарне моделювання для отримання прогнозів розвитку ситуації, у результаті якого визначено від-

носну зміну рівня захищеності КМ. Актуальним є дослідження, пов'язане зі встановленням достовірності отриманих результатів. Розв'язання цієї задачі можливе за допомогою методів статистичного аналізу, зокрема, за допомогою множинного регресійного аналізу, який дозволяє проаналізувати зв'язок між декількома незалежними змінними та цільовою (залежною) змінною [6].

*Метою роботи* є встановлення достовірності впливу загроз на рівень захищеності КМ, визначеного за сценарним моделюванням на основі когнітивного підходу, що дозволяє зменшити час обробки вхідних даних та покращити наочність їх представлення.

## Визначення впливу загроз на рівень захищеності КМ за допомогою множинного регресійного аналізу

Розглянемо когнітивну модель, запропоновану у роботі [5], для аналізу впливу загроз на рівень захищеності КМ (рис.).




Нечітка когнітивна карта аналізу впливу загроз на рівень захищеності КМ

У результаті дослідження цієї моделі визначено найвагоміші концепти системи: шкідливі програми $(K_3)$, фізичний вплив на мережу з боку зловмисника $(K_4)$, ненавмисні дії, помилки користувачів мережі $(K_7)$ та досліджено відносну зміну цільового концепта — захищеність комп'ютерної мережі $(K_9)$ за максимально негативного впливу кожної з загроз окремо. Внаслідок чого виявлено, що зі збільшенням значення концепта $K_7$ захищеність досліджуваної системи послабиться на 0,06; зі збільшенням концепта $K_3$ — на 0,05, а зі збільшенням концепта $K_4$ — на 0,01.

Для перевірки отриманих результатів використаємо дані, отримані в результаті моделювання десяти різних сценаріїв, що відображають відносну зміну захищеності КМ з заданими значеннями найвагоміших концептів (табл. 1).

Таблиця 1

**Значення досліджуваних концептів під час моделювання *i*-го сценарію**

| $i$ | $K_{i3}$ | $K_{i4}$ | $K_{i7}$ | $K_{i9}$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | –0,1 |
| 2 | 0,8 | –0,4 | 1 | –0,07 |
| 3 | 0,7 | 0,3 | 0,9 | –0,06 |

Продовження табл.1

| $i$ | $K_{i3}$ | $K_{i4}$ | $K_{i7}$ | $K_{i9}$ |
|---|---|---|---|---|
| 4 | 0,6 | 0,2 | 0,8 | –0,03 |
| 5 | –0,5 | 0,1 | 0,5 | 0,21 |
| 6 | 1 | 0,5 | –0,4 | 0,05 |
| 7 | –0,3 | 0,7 | 0,5 | 0,15 |
| 8 | 0,4 | –0,2 | 0,3 | 0,06 |
| 9 | 0,2 | –0,8 | 0,9 | 0,03 |
| 10 | –1 | –1 | –1 | 0,63 |

Припускаючи, що між концептами існує лінійна кореляційна залежність, знайдемо її аналітичний вираз (рівняння регресії $K_9$ відносно $K_3$, $K_4$ та $K_7$) [7].

Позначимо $Y = \begin{pmatrix} -0{,}1 \\ -0{,}07 \\ -0{,}06 \\ -0{,}03 \\ 0{,}21 \\ 0{,}05 \\ 0{,}15 \\ 0{,}06 \\ 0{,}03 \\ 0{,}63 \end{pmatrix}$, $K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0{,}8 & -0{,}4 & 1 \\ 1 & 0{,}7 & 0{,}3 & 0{,}9 \\ 1 & 0{,}6 & 0{,}2 & 0{,}8 \\ 1 & -0{,}5 & 0{,}1 & 0{,}5 \\ 1 & 1 & 0{,}5 & -0{,}4 \\ 1 & -0{,}3 & 0{,}7 & 0{,}5 \\ 1 & 0{,}4 & -0{,}2 & 0{,}3 \\ 1 & 0{,}2 & -0{,}8 & 0{,}9 \\ 1 & -1 & -1 & -1 \end{pmatrix}$.

Рівняння множинної регресії матиме вигляд

$$\hat{y} = K_0' b, \tag{1}$$

де $\hat{y}$ — групова (умовна) середня змінної $Y$ при заданому векторі значень $K_0' = \left(1\ K_{10}\ K_{20} \ldots K_{p0}\right)$;

$b = \left(K'K\right)^{-1} K'Y$.

Для зручності обчислень складемо допоміжну таблицю (табл. 2).

Таблиця 2

**Допоміжні дані**

| $i$ | $K_{i3}$ | $K_{i4}$ | $K_{i7}$ | $y_i$ | $K_{i3}^2$ | $K_{i4}^2$ | $K_{i7}^2$ | $K_{i3}K_{i4}$ | $K_{i3}K_{i7}$ | $K_{i4}K_{i7}$ | $y_iK_{i3}$ | $y_iK_{i4}$ | $y_iK_{i7}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | –0,1 | 1 | 1 | 1 | 1 | 1 | 1 | –0,1 | –0,1 | –0,1 |
| 2 | 0,8 | –0,4 | 1 | –0,07 | 0,64 | 0,16 | 1 | –0,32 | 0,8 | –0,4 | –0,056 | 0,028 | –0,07 |
| 3 | 0,7 | 0,3 | 0,9 | –0,06 | 0,49 | 0,09 | 0,81 | 0,21 | 0,63 | 0,27 | –0,042 | –0,018 | –0,054 |
| 4 | 0,6 | 0,2 | 0,8 | –0,03 | 0,36 | 0,04 | 0,64 | 0,12 | 0,48 | 0,16 | –0,018 | –0,006 | –0,024 |
| 5 | –0,5 | 0,1 | 0,5 | 0,21 | 0,25 | 0,01 | 0,25 | –0,05 | –0,25 | 0,05 | –0,105 | 0,021 | 0,105 |
| 6 | 1 | 0,5 | –0,4 | 0,05 | 1 | 0,25 | 0,16 | 0,5 | –0,4 | –0,1 | 0,05 | 0,025 | –0,02 |
| 7 | –0,3 | 0,7 | 0,5 | 0,15 | 0,09 | 0,49 | 0,25 | –0,21 | –0,15 | 0,35 | –0,045 | 0,105 | 0,075 |
| 8 | 0,4 | –0,2 | 0,3 | 0,06 | 0,16 | 0,04 | 0,09 | –0,08 | 0,12 | –0,06 | 0,024 | –0,012 | 0,018 |
| 9 | 0,2 | –0,8 | 0,9 | 0,03 | 0,04 | 0,64 | 0,81 | –0,16 | 0,18 | –0,72 | 0,006 | –0,024 | 0,027 |
| 10 | –1 | –1 | –1 | 0,63 | 1 | 1 | 1 | 1 | 1 | 1 | –0,63 | –0,63 | –0,63 |
| Σ | 2,9 | 0,4 | 4,5 | 0,87 | 5,03 | 3,72 | 6,01 | 2,01 | 3,41 | 1,55 | –0,916 | –0,611 | –0,673 |

У цьому випадку $K'K = \begin{pmatrix} i & \sum K_{i3} & \sum K_{i4} & \sum K_{i7} \\ \sum K_{i3} & \sum K_{i3}^2 & \sum K_{i3}K_{i4} & \sum K_{i3}K_{i7} \\ \sum K_{i4} & \sum K_{i3}K_{i4} & \sum K_{i4}^2 & \sum K_{i4}K_{i7} \\ \sum K_{i7} & \sum K_{i3}K_{i7} & \sum K_{i4}K_{i7} & \sum K_{i7}^2 \end{pmatrix}$.

Тому $(K'K)^{-1} = \begin{pmatrix} 10 & 2,9 & 0,4 & 4,5 \\ 2,9 & 5,03 & 2,01 & 3,41 \\ 0,4 & 2,01 & 3,72 & 1,55 \\ 4,5 & 3,41 & 1,55 & 6,01 \end{pmatrix}^{-1} = \begin{pmatrix} 0,158 & -0,035 & 0,048 & -0,111 \\ -0,035 & 0,377 & -0,136 & -0,152 \\ 0,048 & -0,136 & 0,359 & -0,051 \\ -0,111 & -0,152 & -0,051 & 0,349 \end{pmatrix}$.

Перемножуючи цю матрицю на вектор $K'Y = \begin{pmatrix} \sum y_i \\ \sum y_i K_{i3} \\ \sum y_i K_{i4} \\ \sum y_i K_{i7} \end{pmatrix} = \begin{pmatrix} 0,87 \\ -0,916 \\ -0,611 \\ -0,673 \end{pmatrix}$, отримаємо:

$$b = \begin{pmatrix} 0,22 \\ -0,19 \\ -0,02 \\ -0,16 \end{pmatrix}. \qquad (2)$$

Враховуючи (1) та (2), складемо рівняння множинної регресії:

$$\hat{y} = 0,22 - 0,19K_3 - 0,02K_4 - 0,16K_7.$$

Оцінимо адекватність регресійної моделі за допомогою коефіцієнта детермінації $\left(R^2\right)$, який є мірою якості рівняння регресії, характеристикою його прогностичної сили

$$R^2 = \frac{b'X'Y' - n\overline{y^2}}{Y'Y - n\overline{y^2}}.$$

Зазначимо, що коефіцієнт детермінації характеризує частку варіації залежної змінної, зумовленої регресією або мінливістю незалежних змінних; чим ближче $R^2$ до одиниці, тим краще регресія описує залежність між незалежними змінними та залежною змінною.

Обчислимо добуток векторів

$$b'X'Y = \begin{pmatrix} 0,22 & -0,19 & -0,02 & -0,16 \end{pmatrix} \begin{pmatrix} 0,87 \\ -0,916 \\ -0,611 \\ -0,673 \end{pmatrix} = 0,485.$$

Крім того, $Y'Y = \sum_{i=1}^{10} y_i^2 = 0,4899.$

Визначимо множинний коефіцієнт детермінації:

$$R^2 = \frac{0,485 - 10 \cdot 0,087^2}{0,4899 - 10 \cdot 0,087^2} = 0,98.$$

Коефіцієнт детермінації $R^2 = 0,98$ свідчить про те, що варіація залежної змінної $Y$ — захищеність комп'ютерної мережі на 98 % пояснюється мінливістю включених в модель незалежних змінних $K_3$ — шкідливі програми, $K_4$ — фізичний вплив на мережу з боку зловмисника та $K_7$ — ненавмисні дії, помилки користувачів мережі.

Для порівняння впливу кожного з найвагоміших концептів окремо на захищеність КМ використаємо стандартизовані коефіцієнти регресії $b'_j$ та коефіцієнти еластичності $E_j$ $(j = 1, 2, ..., p)$:

$$b'_j = b_j \frac{s_{kj}}{s_y}, \qquad (3)$$

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

$$E_j = b_j \frac{\overline{K}_j}{\overline{y}}. \quad (4)$$

Стандартизований коефіцієнт регресії $b'_j$ показує на скільки величин $s_y$ зміниться в середньому залежна змінна $Y$ зі збільшенням тільки *j*-ї незалежної змінної на $s_{k\,j}$, а коефіцієнт еластичності $E_j$ — на скільки відсотків (від середнього значення) зміниться в середньому $Y$ зі збільшенням тільки $K_j$ на 1 %.

Використовуючи формули (3) та (4), обчислимо ці коефіцієнти.

$$b'_1 = -0{,}19\frac{0{,}65}{0{,}04} = -3{,}09; \quad b'_2 = -0{,}02\frac{0{,}62}{0{,}04} = -0{,}31; \quad b'_3 = -0{,}16\frac{1{,}51}{0{,}04} = -6{,}08;$$

$$E_1 = -0{,}19\frac{0{,}29}{0{,}087} = -0{,}63; \quad E_2 = -0{,}02\frac{0{,}04}{0{,}087} = -0{,}008; \quad E_3 = -0{,}16\frac{0{,}45}{0{,}087} = -0{,}83.$$

Таким чином, збільшення значення концептів шкідливі програми $(K_3)$, фізичний вплив на мережу з боку зловмисника $(K_4)$ та ненавмисні дії, помилки користувачів мережі $(K_7)$, на одне $S_{K3}$ або $S_{K4}$, або $S_{K7}$ послабить в середньому захищеність КМ відповідно на $3{,}09S_y$ або на $0{,}31S_y$, або на $6{,}08S_y$, а збільшення цих змінних на 1 % (від своїх середніх значень) призведе в середньому до послаблення захищеності КМ відповідно на 0,63 %, 0,008 % та 0,83 %.

З аналізу значень обох показників випливає, що серед найвагоміших концептів досліджуваної системи ненавмисні дії, помилки користувачів мережі найбільше знижують рівень захищеності КМ, в той час як фізичний вплив на мережу з боку зловмисника послаблює захищеність мережі найменше. Це, у свою чергу, підтверджує достовірність результатів отриманих в наслідок проведеного сценарного моделювання у роботі [5].

## Висновки

З використанням множинного регресійного аналізу досліджено достовірність впливу найвагоміших загроз на рівень захищеності КМ. Цей вплив визначено за сценарним моделюванням на основі когнітивного підходу. Складено рівняння регресії $K_9$ — захищеність КМ відносно $K_3$ — шкідливі програми, $K_4$ — фізичний вплив на мережу з боку зловмисника та $K_7$ — ненавмисні дії, помилки користувачів мережі. Обчислено значення коефіцієнта детермінації ($R^2 = 0{,}98$), яке свідчить про адекватність регресійної моделі. Для порівняння впливу досліджуваних загроз на рівень захищеності КМ, визначено стандартизовані коефіцієнти регресії та коефіцієнти еластичності. Аналіз даних показників доводить, що серед найвагоміших загроз найбільше знижують рівень захищеності КМ ненавмисні дії, помилки користувачів мережі, а найменше — фізичний вплив на мережу з боку зловмисника.

Отже, проведене дослідження підтверджує достовірність впливу найвагоміших загроз на рівень захищеності КМ визначеного за сценарним моделюванням на основі когнітивного підходу.

Отримані результати варто враховувати в процесі організації захисту КМ, адже вони сприятимуть вчасному проведенню необхідних заходів, спрямованих на попередження та запобігання впливу цих загроз на безпечне функціонування мережі.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] О. А. Мясіщев, О. О. Мартинюк, і Н. М. Гіневська, «Аналіз захищеності комп'ютерних мереж на основі побудови дерева атак,» *Вісник Хмельницького національного університету*, № 5, с. 243-246, 2016.

[2] П. М. Гроза, і А. В. Варига, «Оцінка захищеності комп'ютерної мережі на основі нечіткої логіки,» *у Матеріалах II Всеукраїнської науково-технічної конференції «Проблеми інфокомунікацій»*, м. Полтава, 2018 р. [Електронний ресурс]. Режим доступу: http://reposit.pntu.edu.ua/handle/PoltNTU/5550 .

[3] В. В. Кальченко, «Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем,» *Системи управління, навігації та зв'язку*, т. 4 (50), с. 109-114, 2018.

[4] В. І. Чорненький, О. В. Сєлюков, В. О. Осипа, О. В. Глінський, і В. І. Щерба, «Вдосконалення методу підвищення інформаційної безпеки комп'ютерних мереж на основі формування правил політики безпеки,» *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, вип. № 61, с. 157-168, 2018.

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

[6] Р. М. Літнарович, *Побудова і дослідження математичної моделі за джерелами експериментальних даних методами регресійного аналізу*, Рівне: МЕГУ, 2011, 140 с.

[7] Н. Ш. Кремер, *Теория вероятностей и математическая статистик*. Москва, РФ: Юрайт, 2019, 538 с.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Стаття надійшла до редакції 10.09.2020

***Салієва Ольга Володимирівна*** — аспірантка кафедри менеджменту та безпеки інформаційних систем;

***Яремчук Юрій Євгенович*** — д-р техн. наук, професор, професор кафедри менеджменту та безпеки інформаційних систем, директор Центру інформаційних технологій і захисту інформації, e-mail: yurevyar@gmail.com .

Вінницький національний технічний університет, Вінниця

**O. V. Saliieva**[1]
**Yu. E. Yaremchuk**[1]

# Investigation of the Significance of the Impact of Threats on the Level of Security of a Computer Network Determined by Scenario Modeling Based on a Cognitive Approach

[1]Vinnytsia National Technical University

*The rapid development of computer networks provides modern society with many new opportunities, provides a variety of services in all areas of human activity. Therefore, it is important to consider the importance of reliable and secure operation of computer networks and pay close attention to ensuring the proper level of their security. To determine the relevance of this issue, a study was conducted on the significance of the impact of threats on the level of security of a computer network by scenario modeling based on a cognitive approach. The research methodology is based on the use of multiple regression analysis, which allows to analyze the relationship between several independent variables (threats) and the target variable (computer network security).*

*To achieve this goal, an analytical expression of the linear correlation that exists between the target variable in relation to such threats as: malware, physical impact on the network by an attacker and unintentional actions, errors of network users.*

*The adequacy of the proposed regression model is evaluated using the coefficient of determination, which is a measure of the quality of the regression equation.*

*The values of the standardized regression coefficient and the coefficient of elasticity, which are necessary to compare the impact of each threat separately on the level of security of the computer network, are determined. The obtained values of the coefficients were analyzed and it was concluded that among the studied threats the most reduce the level of security unintentional actions, errors of network users, and the least - the physical impact on the network by an attacker. This result coincides with the fact that it was obtained by conducting a scenario simulation based on a cognitive approach, which, in turn, indicates the reliability of the impact of certain threats on the level of security of the computer network.*

**Keywords**: computer network, threat, security, cognitive approach, fuzzy cognitive map, multiple regression analysis.

***Saliieva Olha V.*** — Post-Graduate Student of the Chair of Management and Security of Information Systems;

***Yaremchuk Yurii Ye.*** — Dr. Sc. (Eng.), Professor, Professor of the Chair of Management and Security of Information Systems, Head of the Center of Information Technologies and Information Security, e-mail: yurevyar@gmail.com

**О. В. Салиева**[1]
**Ю. Е. Яремчук**[1]

# Исследование достоверности влияния угроз на уровень защищенности компьютерной сети, определенного по сценарному моделированию на основе когнитивного подхода

[1]Винницкий национальный технический университет

*Стремительное развитие компьютерных сетей предоставляет современному обществу множество новых возможностей, обеспечивает предоставление различных услуг во всех сферах человеческой деятельности. Поэтому необходимо учитывать значимость надежного и безопасного функционирования компьютерных сетей и уделять значительное внимание обеспечению надлежащего уровня их защищенности. Определяя актуальность этого вопроса, проведено исследование достоверности влияния угроз на уровень защищенности компьютерной сети по сценарному моделированию на основе когнитивного подхода. Методика исследований базируется на использовании множественного регрессионного анализа, позволяющего проанализировать связь между несколькими независимыми переменными (угрозами) и целевой переменной (защищенность компьютерной сети).*

*Для достижения поставленной цели сформировано аналитический выражение линейной корреляционной зависимости, существующей между целевой переменной относительно таких угроз как: вредоносные программы, физическое воздействие на сеть со стороны злоумышленника и непреднамеренные действия, ошибки пользователей сети.*

*Оценена адекватность предложенной регрессионной модели с помощью коэффициента детерминации, который является мерой качества уравнения регрессии.*

*Определены значения стандартизированного коэффициента регрессии и коэффициента эластичности, необходимые для сравнения влияния каждой угрозы отдельно на уровень защищенности компьютерной сети. На основе анализа полученных значений коэффициентов сделан вывод, что среди исследуемых угроз больше снижают уровень защищенности непреднамеренные действия, ошибки пользователей сети, а меньше всего — физическое воздействие на сеть со стороны злоумышленника. Такой результат совпадает с полученным по сценарному моделированию на основе когнитивного подхода, что, в свою очередь, свидетельствует о достоверности влияния определенных угроз на уровень защищенности компьютерной сети.*

**Ключевые слова:** компьютерная сеть, угроза, защищенность, когнитивный подход, нечеткая когнитивная карта, множественный регрессионный анализ.

***Салиева Ольга Владимировна*** — аспирант кафедры менеджмента и безопасности информационных систем;

***Яремчук Юрий Евгеньевич*** — д-р техн. наук, профессор, профессор кафедры менеджмента и безопасности информационных систем, директор Центра информационных технологий и защиты информации, e-mail: yurevyar@gmail.com