

**О. В. Салієва**

*асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет*

## **ВИЗНАЧЕННЯ ВПЛИВУ ЗАГРОЗ НА РІВЕНЬ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗА КОГНІТИВНОЮ МОДЕЛЛЮ НА ОСНОВІ РЕГРЕСІЙНОГО АНАЛІЗУ**

Сучасна суспільна діяльність усіх своїх проявах характеризується масовим використанням комп'ютерних мереж (КМ), які надають безліч можливостей та задовольняють різноманітні інформаційні потреби людства. Тому вагоме місце посідає питання щодо забезпечення належного рівня їхньої захищеності. Оскільки дана задача має суб'єктивний характер та описується як кількісними так і якісними факторами впливу на мережеву безпеку, то для її вирішення доцільно скористатися когнітивним підходом, який базується на побудові нечіткої когнітивної карти [1, с. 94].

У роботі [4, с.28-39] запропоновано когнітивну модель, яка дозволяє визначити вплив загроз на рівень захищеності КМ, встановити такі найвагомші загрози як: шкідливі програми, фізичний вплив на мережу з боку зловмисника та ненавмисні дії, помилки користувачів мережі. Для отримання прогнозів розвитку ситуації проведено сценарне моделювання, у результаті якого визначено відносну зміну рівня захищеності КМ.

Враховуючи актуальність даної проблеми, у роботі [3, с.98-104] здійснено подальше дослідження розробленої когнітивної моделі, яке полягає у встановленні достовірності впливу загроз на рівень захищеності КМ визначеного за сценарним моделюванням на основі когнітивного підходу.

Для досягнення поставленої мети використано методи множинного регресійного аналізу [2, с. 457], на основі яких сформовано аналітичний вираз лінійної кореляційної залежності, що існує між захищеністю КМ та найвагомшими концептами

системи.

Оцінено адекватність запропонованої регресійної моделі за допомогою коефіцієнта детермінації ( $R^2 = 0,98$ ), який свідчить про те, що варіація залежної змінної (захищеність КМ) на 98% пояснюється мінливістю включених в модель незалежних змінних (шкідливі програми, фізичний вплив на мережу з боку зловмисника та ненавмисні дії, помилки користувачів мережі).

Для визначення впливу кожної загрози окремо на рівень захищеності КМ обчислено значення стандартизованого коефіцієнта регресії та коефіцієнта еластичності. Зокрема, встановлено, що збільшення значення концептів: шкідливі програми, фізичний вплив на мережу з боку зловмисника та ненавмисні дії, помилки користувачів мережі (від своїх середніх значень) призведе в середньому до послаблення захищеності КМ відповідно на 0,63%, 0,008% та 0,83%.

Таким чином, найбільше знижують рівень захищеності КМ ненавмисні дії, помилки користувачів мережі, а найменше – фізичний вплив на мережу з боку зловмисника. Даний результат збігається з тим, що був отриманий за проведенням сценарним моделюванням на основі когнітивного підходу [4], що, у свою чергу, свідчить про достовірність впливу визначених загроз на рівень захищеності КМ.

#### **Список використаних джерел:**

1. Силов В. Б. Принятие стратегических решений в нечеткой обстановке, М.: ИНПРО, РЕС, 228 с, 1995.
2. Кремер Н. Ш. Теория вероятностей и математическая статистика. Москва: Юрайт, 2019, 538 с.
3. Салієва О. В., Яремчук Ю. Є. Дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі, визначеного за сценарним моделювання на основі когнітивного підходу. *Вісник Вінницького політехнічного інституту*. 2020. №4. С. 98-104.
4. Салієва О. В., Яремчук Ю. Є. Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі. *Рєєстрація, зберігання і обробка даних*. 2019. №4. С. 28-39.

**Науковий керівник: Ю. Є. Яремчук**, д.т.н., професор,  
Вінницький національний технічний університет

