

## СИНТЕЗ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

### SYNTHESIS OF A DECISION-MAKING SUPPORT SYSTEM FOR ASSESSING THREATS TO THE INFORMATION SECURITY OF AN ENTERPRISE

Оксана Жигаревич, Василь Шлапа

*Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна*

**Abstract.** *In today's dynamic and interconnected world, information security (IS) has become paramount for enterprises of all sizes. The ever-evolving landscape of cyber threats poses a significant challenge to organizations, demanding robust and adaptable security measures. A decision support system (DSS) specifically designed for assessing IS threats can serve as a valuable tool for enterprises seeking to enhance their cybersecurity posture.*

В сучасному світі інформаційна безпека підприємств стає все більш актуальною. Зростання кількості та складності кіберзагроз робить необхідною розробку ефективних систем для їх оцінки та нейтралізації. Система підтримки прийняття рішень (СППР) може стати потужним інструментом для оцінки загроз інформаційної безпеки підприємства. СППР дозволяє систематизувати процес оцінки ризиків, приймати обґрунтовані рішення щодо захисту інформаційних активів та оптимізувати витрати на інформаційну безпеку.

Існує багато методів оцінки загроз інформаційної безпеки, які можна поділити на кількісні та якісні. Кількісні методи дозволяють оцінити ризики за допомогою числових показників, таких як ймовірність виникнення загрози та її вплив на інформаційні активи. Якісні методи ґрунтуються на експертних оцінках та описових даних. Найбільш поширеними моделями оцінки ризиків є COBIT, NIST, ISO 27001. Ці моделі пропонують комплексний підхід до оцінки інформаційних ризиків та розробки заходів щодо їх нейтралізації.

Методика синтезу системи підтримки прийняття рішень включає в себе кілька ключових етапів, що охоплюють аналіз, проектування, розробку та тестування системи. Спочатку проводиться ретельний аналіз вимог, який включає вивчення проблеми, збір даних від користувачів та аналіз потреб зацікавлених сторін. Після цього здійснюється проектування системи, де визначається архітектура, моделюються бізнес-процеси та вибираються відповідні технології. На етапі розробки відбувається безпосереднє програмування та інтеграція компонентів системи. Завершальним етапом є тестування, яке включає перевірку функціональності, продуктивності та відповідності системи заданим вимогам. Важливим аспектом методики є постійний зворотний зв'язок з користувачами та можливість адаптації системи до змінюваних умов і потреб.

У сучасному світі інформаційна безпека підприємств стає все більш актуальною. Зростання кількості та складності кіберзагроз робить необхідною розробку ефективних систем для їх оцінки та нейтралізації. Система підтримки прийняття рішень (СППР) може стати потужним інструментом для оцінки загроз інформаційної безпеки підприємства. СППР дозволяє систематизувати процес оцінки ризиків, приймати обґрунтовані рішення щодо захисту інформаційних активів та оптимізувати витрати на інформаційну безпеку.

#### Бібліографія

1. Інформаційна безпека: теорія та практика (2023), автори: В.М. Гриценко, О.В. Олійник, С. 310-325.
2. «Управління інформаційними ризиками: методи та інструменти» (2022), О.С. Петренко, О.О. Сидоренко, С. 180-195.