

## **ПІДХОДИ ТА МЕТОДИ АДАПТИВНОГО УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

*Решетняк П.Ю., науковий керівник Семко В.В.*

Об'єкти критичної інфраструктури (ОКІ) дедалі частіше стають мішенню складних і динамічних кібератак з боку зловмисників, що діють на рівні державних спецслужб. Також, ОКІ у деяких галузях мають специфічні формалізовані жорсткі вимоги щодо забезпечення належного рівня кібербезпеки. Більш того, деякі галузеві інформаційно-комунікаційні системи (ІКС) мають притаманні тільки для цієї галузі загрози та вразливості. В таких умовах традиційні підходи до оцінювання ризиків кібербезпеки (наприклад, NIST SP 800-30, ISO/IEC 27005, FAIR тощо) демонструють обмеження у точності, адаптивності та здатності враховувати реальні бізнес-наслідки [1]. Зокрема, існуючі методики:

1. Опираються переважно на статичні або якісні оцінки.
2. Не враховують галузеву специфіку (наприклад, загрози, пов'язані з атаками на сигнальну мережу в телекомунікаційній сфері).
3. Погано масштабуються в умовах зростання складності систем.
4. Не забезпечують достатньої прозорості у прийнятті рішень щодо захисту критичних сервісів.

Аналіз останніх досліджень та публікацій вказує на активний розвиток напрямку динамічної оцінки ризиків, що використовують підходи та методи штучного інтелекту, машинного навчання, нейронних мереж, а також методик кількісної оцінки ризиків [2]. Однак, на даний момент, перевірка ефективності запропонованих методів обмежується результатами прикладів симуляцій та точкових сценаріїв, що не завжди коректно масштабуються на великі інфраструктурні середовища.

Метою дослідження є розробка методу адаптивного динамічного аналізу ризиків кібербезпеки ОКІ у сфері телекомунікацій, що поєднує кількісну обробку даних, формалізоване знання про інфраструктуру та здатність враховувати бізнес-контекст.

Для досягнення цієї мети передбачено виконання таких завдань:

1. Розробити багаторівневу онтологічну модель телекомунікаційної інфраструктури, яка формалізує взаємозв'язки між активами, сервісами та бізнес-послугами, а також відображає вразливості, загрози та інші об'єкти ризику.
2. Розробити метод пропагації ризиків в ієрархічній онтологічній моделі, який забезпечує формалізовану передачу ризику з інфраструктурного рівня на рівень бізнес-послуг та дозволяє виконувати кількісну оцінку ризику для критичних сервісів [3].
3. Розробити гібридний метод оцінки ризиків кібербезпеки, який поєднує кількісну обробку даних (з використанням Бассової нейронної мережі (BNN)) з якісною експертною оцінкою та логікою прийняття рішень (на основі нечіткої логіки) у динамічному середовищі з високим рівнем невизначеності [4].

Запропоновано гібридну модель, у якій BNN використовується для прогнозування ймовірності кіберінцидентів на основі даних моніторингу, а нечітка логіка — для формалізації знань експертів, оцінки контексту та підтримки прийняття рішень при невизначеності. Компоненти взаємодіють або каскадно (fuzzy → BNN), або паралельно (BNN + Fuzzy → агрегований ризик). Такий підхід дозволяє:

1. Забезпечити адаптивність до нових загроз (шляхом постійного донавчання BNN та вдосконалення і доповнення правил нечіткої логіки).

2. Працювати з неповними або нечіткими даними (наприклад, обробляти такі ознаки як «ступінь довіри до джерела», «вірогідність індикатора загрози», «ефективність активного контролю» тощо).
3. Прогнозувати монетарний вплив ризиків на критичні послуги, з урахуванням бізнес-контексту та можливих порушень SLA.
4. Зберігати інтерпретованість рішень для інженерів, аналітиків безпеки та керівництва.

Особливістю методу є також онтологічна формалізація структури ІКС: модель підтримує ієрархію «актив → сервіс → послуга» та містить механізми пропагачії ризику між рівнями (наприклад, через графовий або на основі нечітких правил). Це дозволяє інтегрувати технічні дані з бізнес-метриками, отримуючи оцінку ризику у фінансових показниках та розробляти сценарії оптимального реагування.

Результатом дослідження є запропонований метод динамічного аналізу ризику, що дозволяє враховувати ієрархію активів, адаптивно реагувати на нові загрози, використовувати як точні дані, так й експертні судження, забезпечуючи точність, стійкість і пояснюваність. Запропоноване поєднання BNN, нечіткої логіки та онтологічного підходу формує основу для інтелектуальної системи підтримки прийняття рішень, здатної забезпечити обґрунтовану пріоритезацію ризиків, оцінку збитків, планування інвестицій та стратегічне управління кібербезпекою ОКІ.

#### **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
2. Maaloul A., Zhioua S., Cuppens F. (2022). A Bayesian approach to risk assessment in cybersecurity. *Computers & Security*, 115, 102613.
3. Granadillo G., Simoens K., Doynikova E. (2021). Towards Risk Propagation Modelling in Cyber-Physical Systems. *Critical Information Infrastructures Security*.
4. Rejeb A., Simske S., Keogh J. G., Treiblmaier H., Zailani S. (2023). Fuzzy logic in cyber-risk management: A review. *Journal of Intelligent & Fuzzy Systems*, 44(3), 3365–3380.

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І  
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ  
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



**ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ  
АСПЕКТИ РОЗРОБКИ  
КОМП'ЮТЕРНИХ СИСТЕМ**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ  
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ  
СТУДЕНТІВ І АСПІРАНТІВ  
*24 квітня 2025 року***

**Київ 2025**

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

*Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів*