# РЕЦЕНЗІЯ

рецензента
кандидата технічних наук, доцента,
професора кафедри Технічних систем кіберзахисту
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій
**ПЕПИ Юрія Володимировича**
на дисертаційну роботу **РИЖАКОВА Миколи Миколайовича** на тему:
«Методи та моделі виявлення аномалій мережевого трафіку на об'єктах критичних інформаційних інфраструктур»,
подану на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – «Кібербезпека та захист інформації»

**Актуальність теми**

Як відомо, об'єкти критичної інфраструктури супроводжується зростанням обсягів даних, ускладненням топологій мереж та підвищенням вимог до безперервності сервісів. У таких умовах головним пріоритетом стає своєчасне виявлення аномальних станів мережевого трафіку, які можуть бути наслідком як цілеспрямованих атак, так і нетипових збоїв, помилок конфігурації мереж або непрацездатності обладнання. Відомі механізми моніторингу не завжди здатні забезпечити необхідну адаптивність і швидкість виявлення аномалій в умовах швидких змін поведінки трафіку. Актуальність роботи полягає в тому, що для об'єктів критичної інфраструктури важливий не лише факт «фіксація відхилень», а й оперативне визначення його небезпеки для процесів, тобто перехід від сигналу про аномалію до пріоритету інциденту за рівнем критичності та подальшої його інтерпретації. Запропонована в дисертації орієнтація на поєднання раннього детектування, прогнозу поведінки компонентів та семантичної інтерпретації подій є своєчасною та відповідає потребам сучасних центрів моніторингу кібербезпеки й оперативного реагування на кіберінциденти.

**Обґрунтованість наукових результатів, висновків та рекомендацій**

Наукові результати дисертації мають належний рівень обґрунтованості, оскільки базуються на логічно сформульованій постановці наукового завдання, чітко сформованих задач, визначенні мети, а також на коректному підборі математичного апарату й методів машинного навчання. Автор послідовно розглядає етапи формування ознак мережевого трафіку, побудови моделей, оцінювання відхилень і формування рішення щодо належності спостереження до нормального або аномального класу. Достовірність висновків забезпечується узгодженістю теоретичних положень із описаними процедурами експериментальної перевірки, а також тим, що запропоновані методи орієнтовані на експлуатацію в реальних

умовах (потоковість даних, необхідність встановлення адаптивних меж, обмеження часу прийняття рішення). Рекомендації щодо використання підходу в системах моніторингу та реагування є практично мотивованими і випливають із отриманих результатів, що вказує на практичну цінність проведеного дисертаційного дослідження.

**Новизна наукових результатів дослідження**

До найбільш суттєвих результатів, що визначають наукову новизну дисертації, слід віднести:

1. Системне поєднання реконструктивного аналізу та прогнозування для задач виявлення аномалій мережевого трафіку з використанням адаптивних меж аномальності, що підвищує робастність до природних коливань навантаження та змін режимів роботи мережі;
2. Формалізацію підходу до семантичної атрибуції аномальних подій, що дозволяє не обмежуватися числовим показником «ступеня аномальності», а перейти до інтерпретації події у прикладному контексті (тип/клас відхилення, можливі причини, пов'язані активи/сегменти);
3. Запропоновано механізм оцінювання критичності аномалій (ризик-орієнтована складова), який забезпечує пріоритизацію реакції в умовах великої кількості сигналів та дефіциту ресурсів реагування;
4. Розроблено узагальнену архітектурну модель інтелектуальної системи, в якій детектування, атрибуція та оцінювання критичності розглядаються як пов'язаний цикл обробки подій, придатний до інтеграції в контур SOC/SIEM.

У сукупності зазначені результати формують новий підхід до побудови систем виявлення аномалій саме для об'єктів критичної інфраструктури.

**Практична цінність отриманих результатів**

Практична цінність дисертації полягає у можливості застосування запропонованих моделей і процедур для підвищення ефективності моніторингу мережевих подій у критичних інфраструктурах. Важливим є те, що моделі і методи дозволяють:

- зменшити частку хибних спрацювань за рахунок адаптивного налаштування меж аномальності;
- виявляти відхилення на ранніх етапах завдяки прогнозному компоненту;
- виконувати ранжування подій за критичністю, що знижує навантаження на операторів SOC і прискорює реагування;
- формувати більш «операційно придатні» результати для інтеграції з системами SIEM/SOAR (подія + інтерпретація + рівень пріоритету).

Таким чином, робота має чітку прикладну спрямованість і може бути корисною для практичної модернізації або вдосконалення систем моніторингу кібербезпеки критичних інфраструктурних об'єктів.

**Зв'язок роботи з науковими програмами, планами та темами**

Тематика дисертації узгоджується з напрямами наукових досліджень у сфері кібербезпеки, захисту інформації та забезпечення стійкості критичної інфраструктури. Робота відповідає сучасним пріоритетам розвитку галузі інформаційних технологій і кіберзахисту, зокрема в частині інтелектуального аналізу телеметрії, виявлення аномалій та підтримки процесів реагування. Також дослідження пов'язане з науковими планами та тематикою профільних підрозділів університету, спрямованих на розроблення методів і технологій захисту інформаційних систем та мереж, що експлуатуються у критичних середовищах.

**Повнота викладу основних результатів дисертації у публікаціях**

Основні положення дисертації відображені у публікаціях здобувача, що свідчить про належну апробацію отриманих результатів у науковому середовищі. Тематика публікацій відповідає предметній області дослідження й охоплює ключові складові роботи: інтелектуальне виявлення аномалій, узагальнену модель системи, підходи до оцінювання аномальності та критичності подій.

Загалом рівень висвітлення результатів у наукових працях можна вважати достатнім для підтвердження авторського внеску та наукової новизни.

**Оцінка змісту дисертації та відповідність встановленим вимогам щодо оформлення**

Дисертація є цілісним завершеним науковим дослідженням, у якому витримано логіку викладу матеріалу: обґрунтування проблеми, аналіз існуючих підходів, постановка задачі, побудова моделей і методів, експериментальна перевірка та формування висновків. Структура роботи відповідає загальноприйнятим вимогам до дисертаційних досліджень, а матеріал подано зрозумілою мовою з графічною інтерпретацією.

Оформлення дисертації відповідає встановленим вимогам: використано науковий стиль викладення, наведено необхідні ілюстративні та аналітичні матеріали, результати сформульовано у вигляді висновків і положень, що виносяться на захист.

**Недоліки та зауваження**

Зупинимось на окремих зауваженнях:

1. Доцільно ширше подати аналіз чутливості результатів до вибору параметрів моделей (наприклад, розміру вікна, порогових значень, гіперпараметрів навчання), оскільки в процесі експлуатації об'єктів критичних інфраструктур ці налаштування суттєво впливають на стабільність детектування і змінюються досить швидко;

2. Бажано детально описати вимоги до ресурсів та продуктивності розробленого програмного застосунку (латентність обробки, пропускна здатність, режим роботи в реальному часі), що підвищило б практичну відтворюваність підходу для різних класів інфраструктур;

3. У частині семантичної атрибуції корисним було б подати більш формалізовану схему відповідностей «ознака/патерн → інтерпретація/клас події» (таблично або як набір правил), щоб спростити застосування методики сторонніми користувачами;

4. Перспективним доповненням було б розширений аналіз стійкості ML-компонентів до навмисних впливів (adversarial), що є актуальним саме для кібербезпекових систем.

Наведені зауваження не знижують загальної позитивної оцінки дисертації та можуть бути враховані автором у подальшій роботі.

**Висновок**

Дисертаційна робота Рижакова Миколи Миколайовича на тему «Методи та моделі виявлення аномалій мережевого трафіку на об'єктах критичних інформаційних інфраструктур» є завершеним самостійним дослідженням, що містить науково обґрунтовані результати, має елементи наукової новизни та характеризується практичною значущістю для задач кіберзахисту критичних інфраструктурних інформаційних мереж.

За змістом, рівнем обґрунтованості, новизною та практичною цінністю дисертація відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому Постановою Кабінету Міністрів України від 12 січня 2022 р. №44. Автор дисертаційної роботи заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – «Кібербезпека та захист інформації».

**Рецензент:**
професор кафедри Технічних
систем кіберзахисту Державного університету
інформаційно-комунікаційних технологій,
кандидат технічних наук, доцент Юрій ПЕПА

Підпис канд. техн. наук, доцента Ю. Пепи засвідчую.

Учений секретар
Державного університету інформаційно-
комунікаційних технологій Галина ЄНЧЕВА

«23» січня 2026 р.