**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»**

# ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XI Всеукраїнської науково-практичної конференції

**«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:**

**ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»**

18 грудня 2025 року


**Полтава 2025**

**УДК 004.056.53:004.738.5**
***О.В. Шефер**, д.т.н., професор,*
***Д.Р. Олексієнко**, аспірант*
*Національний університет «Полтавська політехніка імені Юрія Кондратюка»*

# АДАПТИВНІ МЕТОДИ ВИЯВЛЕННЯ АНОМАЛІЙ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ

Стрімкий розвиток цифрових технологій, зростання обсягів даних та масштабування телекомунікаційних мереж створюють нові можливості для соціально-економічного розвитку, проте одночасно формують широкий спектр загроз інформаційній безпеці. Телекомунікаційні мережі сьогодні є критичною інфраструктурою, що забезпечує функціонування державних, промислових, енергетичних, транспортних та фінансових систем [1, 2]. Порушення їхньої роботи внаслідок кібератак може призвести до значних фінансових збитків, витоку конфіденційних даних, руйнування технологічних процесів і навіть загроз національній безпеці. З огляду на це пошук нових методів і засобів кіберзахисту телекомунікаційних мереж набуває стратегічного значення.

Традиційні засоби захисту – фаєрволи, системи запобігання вторгненням, антивірусні рішення – переважно ґрунтуються на сигнатурних підходах, тобто виявляють загрози за заздалегідь відомими шаблонами. Такий підхід є ефективним лише щодо відомих атак і не здатний своєчасно виявляти нові, модифіковані чи цілеспрямовані загрози (APT), які активно застосовуються у сучасному кіберпросторі. Динамічність, різноплановість та інтелектуальна складність сучасних атак зумовлюють необхідність застосування методів, здатних реагувати на нетипову поведінку, а не лише на фіксовані ознаки шкідливості [3].

Поведінковий аналіз мережевого трафіку є одним з найбільш перспективних напрямів сучасного кіберзахисту. Він базується на формуванні моделей нормальної активності мережі та виявленні аномалій, що можуть бути індикаторами кібератак. Такий підхід дозволяє виявляти атаки нульового дня, приховані вторгнення, внутрішні загрози, а також складні багатоступеневі атаки, які важко детектувати сигнатурними інструментами. Важливим фактором є й те, що поведінковий аналіз добре масштабується в умовах збільшення кількості підключених пристроїв, розширення периферійних мереж, переходу підприємств до хмарних технологій та розвитку концепції Інтернету речей (IoT).

Попри значні досягнення в цій сфері, існує низка наукових проблем, що потребують подальшого опрацювання [4]. По-перше, складність мережевого трафіку та високий рівень його динамічності унеможливлюють

пряме використання класичних методів статистичного аналізу, що вимагає розроблення нових гібридних методів на основі машинного навчання та нейронних мереж. По-друге, зростає потреба у підвищенні точності виявлення аномалій, адже велика кількість хибних спрацьовувань знижує ефективність системи кіберзахисту та ускладнює роботу фахівців. По-третє, сучасні телекомунікаційні мережі мають складну розподілену структуру, а отже методи аналізу мають адаптуватися до багаторівневих топологій, різнорідних протоколів і вимог до пропускної здатності.

Актуальною також є проблема інтеграції поведінкового аналізу з існуючими системами інформаційної безпеки підприємств. Необхідні нові підходи до створення апаратних та програмних модулів, здатних працювати у режимі реального часу, забезпечувати швидку обробку великих масивів даних (big data) та ефективно функціонувати в умовах обмежених ресурсів. Значної уваги потребують і методи комплексного аналізу трафіку, що враховують контекст взаємодій, часові залежності та кореляційні зв'язки між подіями. У цьому контексті перспективним напрямом є розроблення архітектур систем мережевого моніторингу з підтримкою самонавчання та адаптивного реагування на загрози.

Дослідження спрямоване на вирішення важливої науково-прикладної проблеми – підвищення ефективності захисту телекомунікаційних мереж шляхом застосування інтелектуальних методів поведінкового аналізу трафіку та розроблення новітніх технічних засобів для їх впровадження.

## ЛІТЕРАТУРА:

*1. Барабаш, О. В., Маркова, І. М. Захист інформації в телекомунікаційних мережах: підручник. Львів: Львівська політехніка, 2021. 406 с.*

*2. Козік, В. В., Романенко, В. Г. Кібербезпека телекомунікаційних систем: монографія. Київ: ДУТ, 2020. 312 с.*

*3. Kim, S., Lee, S., & Kim, H. Detecting Zero-day Malware Using Behavioral Analysis and Machine Learning.* International Journal of Security and Networks*, 2020, 15(2), pp. 65–76.*

*4. Koukoulis, I., Syrigos, I., & Korakis, T. (2025).* Self-supervised transformer-based contrastive learning for intrusion detection systems. *arXiv preprint.*

## ADAPTIVE METHODS FOR ANOMALIES DETECTION IN TELECOMMUNICATION NETWORKS BASED ON BEHAVIORAL ANALYSIS

***O. Shefer**, Doctor of Science, professor,*
***D. Oleksiienko**, postgraduate*
*National University "Yuri Kondratyuk Poltava Polytechnic"*