



**ПОЛТАВСЬКА  
ПОЛІТЕХНІКА**

Міністерство освіти і науки України  
Національний університет  
«Полтавська політехніка імені Юрія Кондратюка»

# **ЗБІРНИК НАУКОВИХ ПРАЦЬ**

**78-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ  
ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ  
ПРАЦІВНИКІВ, АСПІРАНТІВ ТА  
СТУДЕНТІВ УНІВЕРСИТЕТУ**

# **І ТОМ**



**15 – 22 травня 2026 року  
Полтава**

## **АДАПТИВНІ МОДЕЛІ ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ**

Стрімкий розвиток цифрових технологій, зростання обсягів передаваних даних і масштабування телекомунікаційних мереж формують новий рівень вимог до забезпечення інформаційної безпеки. Телекомунікаційні мережі сьогодні виступають основою функціонування державних, промислових, енергетичних, транспортних та фінансових систем, що відносить їх до об'єктів критичної інфраструктури. У зв'язку з цим будь-які порушення їхньої роботи внаслідок кібератак можуть призводити до значних економічних втрат, витоку конфіденційної інформації та порушення стабільності функціонування суспільства.

Традиційні засоби захисту інформації, зокрема міжмережеві екрани, антивірусні системи та системи виявлення вторгнень, переважно базуються на сигнатурному підході. Такий підхід передбачає ідентифікацію загроз на основі заздалегідь відомих шаблонів атак. Однак у сучасних умовах він демонструє обмежену ефективність, оскільки не здатний своєчасно виявляти нові, модифіковані або цілеспрямовані атаки, включаючи атаки нульового дня та складні багаторівневі вторгнення (АРТ). Зростаюча складність кіберзагроз обумовлює необхідність переходу до більш адаптивних та інтелектуальних методів захисту.

Одним із найбільш перспективних напрямів є поведінковий аналіз мережевого трафіку. Його сутність полягає у формуванні моделей нормального функціонування мережі та подальшому виявленні аномалій, що можуть свідчити про наявність кіберзагроз. На відміну від сигнатурних методів, поведінковий підхід дозволяє ідентифікувати раніше невідомі атаки, внутрішні загрози та приховані вторгнення. Крім того, він ефективно застосовується в умовах розвитку хмарних обчислень, Інтернету речей та розподілених мережевих інфраструктур.

Разом з тим впровадження поведінкового аналізу пов'язане з рядом науково-технічних проблем. Однією з ключових є висока динамічність мережевого трафіку, що ускладнює побудову адекватних моделей нормальної поведінки. Іншою проблемою є необхідність забезпечення високої точності виявлення аномалій при мінімізації кількості хибних спрацьовувань, які можуть значно ускладнювати роботу систем моніторингу безпеки. Також важливим є питання масштабованості рішень у зв'язку зі зростанням кількості підключених пристроїв і обсягів даних.

Для вирішення зазначених проблем доцільним є використання гібридних підходів, що поєднують методи статистичного аналізу,

машинного навчання та нейронних мереж. Застосування алгоритмів кластеризації, класифікації та глибокого навчання дозволяє більш точно моделювати поведінку мережі та ефективно виявляти відхилення від нормального стану. Особливу увагу слід приділяти адаптивним алгоритмам, здатним до самонавчання та оновлення моделей у процесі функціонування системи.

Перспективним напрямом досліджень є також створення комплексних систем моніторингу мережевого трафіку, які враховують часові залежності, контекст взаємодій та кореляційні зв'язки між подіями. Такі системи повинні функціонувати у режимі реального часу, забезпечувати обробку великих масивів даних і бути інтегрованими з існуючими засобами інформаційної безпеки підприємств.

Запропонований підхід до підвищення ефективності кіберзахисту телекомунікаційних мереж базується на поєднанні поведінкового аналізу та інтелектуальних методів обробки даних. Його реалізація дозволяє підвищити точність виявлення кіберзагроз, зменшити кількість хибних спрацьовувань, а також забезпечити адаптивність системи до змін у мережевому середовищі.

Практичне значення отриманих результатів полягає у можливості їх застосування в діяльності провайдерів телекомунікаційних послуг, операторів хмарних сервісів, а також у державних і приватних організаціях, що працюють із критичною інфраструктурою. Впровадження інтелектуальних систем аналізу мережевого трафіку сприятиме підвищенню загального рівня інформаційної безпеки та стійкості до сучасних кіберзагроз.

Таким чином, дослідження інтелектуальних методів поведінкового аналізу є актуальним напрямом розвитку кібербезпеки та відповідає сучасним викликам цифрової трансформації. Отримані результати можуть стати основою для створення нових ефективних систем захисту телекомунікаційних мереж.

#### *Література:*

1. Барабаш О. В., Литвинов В. В. *Кібербезпека інформаційних та телекомунікаційних систем : навч. посіб.* Київ : НАУ, 2020. 256 с.
2. Толюпа С. В., Пархоменко І. В. *Аналіз мережевого трафіку та виявлення аномалій у телекомунікаційних системах. Системи управління, навігації та зв'язку.* 2021. № 1. С. 112–118.
3. Géron A. *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow.* 3rd ed. Sebastopol : O'Reilly Media, 2022. 850 p.
4. Buczak A. L., Guven E. *A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials.* 2016. Vol. 18, No. 2. P. 1153–1176.
5. Ahmad Z., Shahid Khan A., Shiang C. W. *Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches. Transactions on Emerging Telecommunications Technologies.* 2021. Vol. 32, No. 1.