УДК 004.056:004.75

МЕТОДИ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У ХМАРНИХ СЕРЕДОВИЩАХ НА ОСНОВІ АВТОЕНКОДЕРІВ

Фісенко Д. М., Мазепа А.Д., Пантєлєєв В.О
e-mail: dmytro.fisenko@nure.ua, artem.mazepa@nure.ua, vadym.pantielieiev@nure.ua
Науковий керівник – д.т.н., проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

This work examines methods for detecting cyber threats in cloud environments based on autoencoders. The rapid spread of cloud technologies today is leading to an increasing number of cyber threats aimed at cloud infrastructure. Traditional signature-based attack detection methods are limited in identifying new or modified threats, which could be solved by using advanced machine learning methods. The study considers the features of using autoencoders as deep learning models for anomaly detection in cloud environments. It is concluded that the use of autoencoders is a promising direction for improving the efficiency of cyber threat detection in cloud environments.

Стрімкий розвиток інформаційних технологій супроводжується активним використанням хмарних середовищ в різноманітних сферах діяльності. Водночас це також зумовлює зростання кількості кіберзагроз, спрямованих на порушення конфіденційності, цілісності та доступності інформації. В наш час найпоширенішими кіберзагрозами є несанкціонований доступ, витік даних, DDoS-атаки, компрометація облікових записів, а також експлуатація вразливостей. Методи виявлення кіберзагроз які основані на сигнатурному аналізі є ефективними лише для відомих атак і часто можуть пропускати нові або модифіковані атаки. У зв’язку з цим особливої актуальності набувають методи засновані на машинному навчанні, здатні виявляти аномальну поведінку в хмарних середовищах.

Одним із сучасних підходів виявлення кіберзагроз у хмарних середовищах є використання автоенкодерів. Автоенкодер це різновид штучної нейронної мережі який використовується для вирішення задач некерованого навчання. Метою його роботи являється кодування вхідних даних та подальше їх відновлення з мінімальною похибкою.

Принцип застосування автоенкодера у задачах кібербезпеки полягає в навчанні моделі на даних, що характеризують нормальне функціонування системи. У такому разі для нормальної активності похибка відновлення є незначною, тоді як для аномальних або потенційно шкідливих дій вона зростає. Це дає змогу використовувати величину похибки як індикатор можливої кіберзагрози. Такий підхід є особливо доцільним для хмарних середовищ, які характеризуються динамічністю, багатокористувацькою

архітектурою, великою кількістю мережевих вузлів і значними об’ємами журналів подій.

Перевагою використання автоенкодерів є можливість виявлення раніше невідомих атак без необхідності формування повного набору розмічених шкідливих даних. Це є значущою перевагою, оскільки в реальних умовах забезпечити наявність повної бази всіх можливих сценаріїв атак є вкрай складно. Крім того, автоенкодери дозволяють автоматизувати виділення інформативних ознак із великих масивів даних і можуть бути адаптовані до змін у хмарному середовищі шляхом повторного навчання.

Повна формула проходу через автоенкодер виглядає так:

$$\hat{x} = \phi(\sigma(x)),$$

де головна умова навчання:

$$\min_{\theta,\theta'} \sum L\left(x, \phi_{\theta}(\sigma_{\theta}(x))\right),$$

де θ – параметри енкодера, θ′ - параметри декодера.

У ході проведеного дослідження було проаналізовано методи виявлення кіберзагроз у хмарних середовищах на основі автоенкодерів. Використання даного підходу є перспективним напрямом розвитку сучасних систем кіберзахисту. Він забезпечує можливість виявлення аномальної активності, у тому числі невідомих атак, шляхом аналізу відхилень від нормального функціонування системи. Під час експерименту встановлено, що для нормальних подій похибка при відновленні даних залишалася в межах порогового значення, тоді як для аномальних подій її значення суттєво зростало. Це дало змогу ідентифікувати більшість аномальних станів як потенційно небезпечні.

Слід зазначити, що використання даного підходу сприяє підвищенню ефективності системи безпеки хмарного середовища, автоматизації обробки великих обсягів даних та вдосконаленню механізмів протидії кіберзагрозам.

Список використаних джерел:

1. Neto, E.C.P., Iqbal, S., Buffett, S. et al. Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. Artif Intell Rev 58, 340 (2025). https://doi.org/10.1007/s10462-025-11346-z

2. Syed, A., & Ahmad, M. I. (2025). Advanced Data Collection Techniques in Cloud Security: A Multi-Modal Deep Learning Autoencoder Approach. ArXiv. https://doi.org/10.20944/preprints202510.0767.v1

3. K. S, S.; Elumalai, T.; Rajamani, R.; Kumar, A.; Balusamy, B.; Yogarayan, S.; Prabu, K. An Unsupervised Cloud-Centric Intrusion Diagnosis Framework Using Autoencoder and Density-Based Learning. Future Internet 2026, 18, 54. https://doi.org/10.3390/fi18010054