УДК 004.056.5 : 004.89
В. Ковальський; Є. Тиш, к. т. н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРОГНОЗУВАННЯ МЕРЕЖЕВИХ АНОМАЛІЙ У ХМАРНОМУ СЕРЕДОВИЩІ З ВИКОРИСТАННЯМ ГЕНЕРАТИВНИХ АЛГОРИТМІВ

UDC 004.056.5 : 004.89
V. Kovalskyi; Ie. Tysh, PhD.

PREDICTION OF NETWORK ANOMALIES IN A CLOUD ENVIRONMENT USING GENERATIVE ALGORITHMS

Стрімкий розвиток хмарних технологій упродовж останніх років суттєво змінив підходи до зберігання, обробки та передачі інформації. Переважна більшість інформаційних ресурсів сьогодні функціонує у розподілених хмарних середовищах, що забезпечують високу доступність, гнучкість та масштабованість обчислювальних процесів. Однак разом із очевидними перевагами такі технології створюють нові виклики у сфері кібербезпеки. Зі зростанням обсягу мережевого трафіку та кількості підключених пристроїв суттєво збільшується і кількість мережевих загроз, які вирізняються складністю, прихованою природою, динамічністю та здатністю до швидкої адаптації.

Традиційні сигнатурні методи виявлення атак, що ґрунтуються на порівнянні мережевих пакетів із відомими шаблонами загроз, в умовах сучасних кіберзагроз поступово втрачають свою ефективність. Такі підходи демонструють низьку здатність до розпізнавання нових, невідомих раніше атак, а також не забезпечують своєчасного реагування на складні багаторівневі атаки. У зв’язку з цим зростає актуальність використання інтелектуальних методів аналізу мережевого трафіку, здатних не лише фіксувати вже відомі загрози, але й прогнозувати потенційні аномальні стани.

У даній роботі досліджується підхід до прогнозування мережевих аномалій на основі генеративних алгоритмів машинного навчання. Генеративні моделі здатні відтворювати складні статистичні та часові закономірності у потоках мережевих даних, що дає змогу формувати реалістичні синтетичні сценарії мережевого навантаження. Такі моделі використовуються для побудови прогнозів нормальної поведінки трафіку, які надалі порівнюються з реальними показниками. Виявлені відхилення між прогнозованими та фактичними значеннями розглядаються як індикатори потенційної аномальної активності або початку кібератаки.

Запропонований підхід реалізується у хмарному середовищі, що забезпечує високу продуктивність обчислень, можливість гнучкого масштабування ресурсів та інтеграцію з існуючими системами моніторингу й кіберзахисту. Використання хмарної інфраструктури дозволяє здійснювати обробку великих обсягів даних у реальному часі, а також підвищує надійність та стійкість системи до збоїв.

Таким чином, поєднання генеративних алгоритмів машинного навчання з можливостями хмарних обчислень створює ефективний інструмент для прогнозування та своєчасного виявлення мережевих аномалій. Це дозволяє підвищити рівень захищеності інформаційних ресурсів, зменшити ризики успішних кібератак та сприяє формуванню сучасних інтелектуальних систем кібербезпеки.