УДК 004.75 : 004.8
В. Ковальський; Є. Тиш, к. т. н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ПРОГНОЗУВАННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ НА ОСНОВІ TIMEGAN У ХМАРНОМУ СЕРЕДОВИЩІ

UDC 004.75 : 004.8
V. Kovalskyi; Ie. Tysh, PhD.

INTELLIGENT SYSTEM FOR PREDICTING NETWORK TRAFFIC ANOMALIES BASED ON TIMEGAN IN A CLOUD ENVIRONMENT

Сучасні хмарні інфраструктури характеризуються високим рівнем динамічності, частою зміною топології мережі, масштабованістю ресурсів та суттєвою нерівномірністю навантаження. Такі особливості з одного боку забезпечують гнучкість, доступність та ефективність обчислювальних процесів, а з іншого – значно ускладнюють процеси моніторингу та забезпечення мережевої безпеки. Зростання обсягів переданих даних, кількості підключених користувачів і сервісів призводить до появи нових типів загроз, що відзначаються складною структурою, прихованою поведінкою та високим рівнем адаптивності до захисних механізмів.

Традиційні статистичні та сигнатурні методи виявлення мережевих атак, які базуються на порівнянні поточного трафіку з наперед заданими шаблонами або граничними значеннями параметрів, не здатні повною мірою забезпечити необхідну точність в умовах хмарних середовищ. Такі підходи є обмеженими у випадках появи нових, раніше невідомих загроз, а також демонструють низьку ефективність під час виявлення багаторівневих і повільно еволюціонуючих атак. У зв’язку з цим постає необхідність застосування інтелектуальних методів аналізу, заснованих на машинному навчанні та глибоких нейронних мережах.

У даній роботі запропоновано використання генеративної нейронної мережі типу TimeGAN для моделювання часових рядів мережевого трафіку та прогнозування його поведінки. TimeGAN поєднує переваги автокодувальників і генеративно-змагальних мереж, що дозволяє ефективно відтворювати як статистичні характеристики, так і часові залежності у даних. Модель навчається на історичних вибірках трафіку, формує внутрішнє подання його структури та генерує прогнозні значення параметрів мережевої активності.

Процес виявлення аномалій здійснюється шляхом порівняння згенерованих прогнозних даних із реальними потоками трафіку. Суттєві розбіжності між цими значеннями розглядаються як індикатори потенційної аномальної активності або початку кібератаки. Такий підхід дозволяє виявляти не лише вже відомі типи загроз, але й нові, раніше неописані сценарії атак, що є особливо важливим для сучасних хмарних середовищ.

Розроблена інтелектуальна система реалізується у хмарному середовищі, що забезпечує можливість гнучкого масштабування обчислювальних ресурсів залежно від поточного навантаження, а також підтримує обробку великих потоків даних у режимі реального часу. Використання хмарної інфраструктури підвищує надійність системи, забезпечує її доступність та спрощує інтеграцію з існуючими засобами моніторингу й кіберзахисту.