МАТЕРІАЛИ

ІІІ Міжнародної науково-практичної конференції “КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ІНСТИТУЦІЙ ТА ПОДОЛАННЯ КРИЗОВИХ СТАНІВ”

(Том 1)

14 листопада 2024 року

Київ – Прага – Таллінн – Тернопіль

Владислав МАЙСТРЕНКО;
Дмитро ЛАНДЕ, д.т.н., професор

МОДЕЛЬ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ

Анотація. Метою дослідження є створення ефективної моделі на основі нейронних мереж, зокрема архітектури трансформерів, для виявлення та нейтралізації кіберзагроз у державних інституціях. Модель забезпечує високоточне виявлення аномалій у мережевому трафіку, що підвищує рівень кібербезпеки державних систем.

Summary. The aim of the research is to develop an effective model based on neural networks, particularly transformer architecture, for detecting and neutralizing cyber threats in government institutions. The proposed model ensures high-accuracy anomaly detection in network traffic, enhancing cybersecurity in state systems.

Ключові слова: кібербезпека, нейронні мережі, трансформери, аномалії, державні інституції.

Основними завданнями дослідження є: дослідження можливостей трансформерів для виявлення аномалій у мережевому трафіку, розробка моделі на основі трансформерів для моніторингу трафіку та виявлення загроз, валідація моделі на реальних даних.

Запропонована модель на основі трансформерів дозволяє ефективно аналізувати великі обсяги мережевого трафіку завдяки здатності до обробки послідовних даних і виявлення аномалій. Використання механізму самоуваги в архітектурі трансформерів дозволяє моделі фокусуватися на важливих аспектах трафіку, що значно підвищує точність у виявленні потенційних загроз.

Розроблена система забезпечує адаптивний підхід до кіберзахисту, що дозволяє не лише своєчасно виявляти атаки, але й передбачати потенційні загрози на основі аналізу поведінкових моделей. Ця інновація значно підвищує ефективність кібербезпеки державних установ, знижуючи ризики витоку даних і збоїв у критично важливих системах.

Висновки. Розробка нових нейромережевих підходів до кіберзахисту, зокрема на основі трансформерів, дозволяє значно підвищити ефективність виявлення кібератак. Така модель має потенціал для впровадження в реальні системи державних інституцій і може стати основою для подальших досліджень у сфері кібербезпеки.