

Metody modelowania zagrożeń i wykrywania podatności w sieciach 5G.

Rozprawa doktorska

Autor: mgr inż. Wiktor Sędkowski

Promotor: dr hab. inż. Rafał Stanisławski, prof. PO

Streszczenie: Niniejsza rozprawa koncentruje się na usystematyzowaniu technik i procesów związanych z automatyzacją procesu modelowania zagrożeń i wykrywania luk w nowoczesnych, dynamicznych systemach, takich jak sieci 5G. Ewolucja technologii 5G w kierunku bardziej otwartych struktur skoncentrowanych na protokole internetowym (IP) odróżnia ją od tradycyjnych zamkniętych sieci 3G czy 4G. Dynamiczny charakter architektury 5G wiąże się z nowymi zagrożeniami bezpieczeństwa, wymagając innowacyjnego podejścia do procesu modelowania zagrożeń, gdyż automatyzacja procesu modelowania potencjalnych zagrożeń pozostaje poważnym wyzwaniem dla dostawców usług i ekspertów ds. cyberbezpieczeństwa. Proponowane w niniejszej pracy rozwiązania automatyzują proces przewidywania podatności i modelowania zagrożeń w złożonych systemach, takich jak sieci 5G. Przeprowadzone badania wykazały, że możliwe jest skuteczne modelowanie i priorytetyzacja zagrożeń w systemach o zmiennej strukturze. Uzyskane wyniki potwierdzają, że algorytmy obliczeniowe mogą efektywnie modelować i priorytetyzować zagrożenia w czasie rzeczywistym. Analizy porównawcze przedstawione w pracy wskazują, że sztuczna inteligencja może być użyteczna w przewidywaniu podatności, generowaniu diagramów związanych z zagrożeniami oraz w tworzeniu opisów modeli zagrożeń.

Słowa kluczowe: Cyberbezpieczeństwo, modelowanie zagrożeń, sieci 5G, wykrywanie podatności, automatyzacja, sztuczna inteligencja, bezpieczeństwo sieci, ograniczanie ryzyka