Zgłoszenie tematu pracy dyplomowej **:: STUDIA II STOPNIA ::**

rok akademicki 2025/26

Promotor:	**dr hab. inż. Serhii Semenov, prof. UKEN**
Temat pracy magisterskiej (j. polski, j.angielski):	Badanie algorytmów uczenia maszynowego w procesie wykrywania wirusów komputerowych *Investigation of Machine Learning Algorithms for Computer Virus Detection*
Zakres pracy i oczekiwane rezultaty praktyczne:	1 Analiza współczesnych zagrożeń malware (wirusy, trojany, ransomware, spyware) oraz sposobów ich działania. 2 Przegląd metod detekcji z wykorzystaniem uczenia maszynowego. 3 Implementacja klasycznych algorytmów ML. 4 Implementacja algorytmów głębokiego uczenia. 5 Przygotowanie i czyszczenie zbiorów danych (np. EMBER dataset, VirusShare, Malicia dataset). 6 Badania porównawcze skuteczności algorytmów przy użyciu metryk: Accuracy, F1, Precision, Recall, PR-AUC. 7 Analiza odporności modeli na techniki unikania detekcji, takie jak packery, obfuskacja kodu, modyfikacje struktury PE. 8 Opracowanie rekomendacji dotyczących budowy systemów antywirusowych opartych na ML.
Aspekt naukowy, problemowy, innowacyjny pracy:	Praca obejmuje jedno z najważniejszych zagadnień cyberbezpieczeństwa – detekcję złośliwego oprogramowania. Aspekty innowacyjne: – wykorzystanie głębokiego uczenia do analizy plików binarnych i ciągów instrukcji, – porównanie podejść statycznych i dynamicznych w kontekście ML, – ocena podatności modeli na ataki adversarial malware (próby celowej modyfikacji próbki w celu oszukania klasyfikatora), – możliwość budowy hybrydowego modelu łączącego cechy statyczne i dynamiczne.
*Oprogramowanie, język programowania, środowisko systemowe:	
*Środowisko uruchomieniowe	
Dodatkowe wymagania i uwagi:	– Wymagane szczególne środki ostrożności przy pracy z próbkami malware (analiza tylko w środowisku izolowanym). – Zalecane porównanie cech statycznych i dynamicznych. – Mile widziane badanie odporności modeli na obfuskację i packery.
*Literatura:	

*pola opcjonalne