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):	Opracowanie systemu wykrywania ataków phishingowych z wykorzystaniem narzędzi sztucznej inteligencji Development of an Artificial Intelligence-Based System for Phishing Attack Detection
Zakres pracy i oczekiwane rezultaty praktyczne:	1 Analiza współczesnych technik phishingu: e-maile, strony WWW, wiadomości SMS, ataki spear-phishing i vishing. 2 Przegląd narzędzi sztucznej inteligencji wykorzystywanych do detekcji phishingu. 3 Przygotowanie zestawu danych (np. PhishTank, open-source datasets, własne zbiory URL i e-maili). 4 Implementacja modułu ekstrakcji cech. 5 Budowa systemu detekcji składającego się z: – modułu analizy tekstowej, – modułu analizy strukturalnej, – klasyfikatora SI. 6 Testy skuteczności różnych algorytmów oraz ich porównanie przy użyciu metryk PR-AUC, F1, precyzja, czułość. 7 Opracowanie demonstracyjnej aplikacji (CLI/web) umożliwiającej klasyfikację nowych próbek phishingowych.
Aspekt naukowy, problemowy, innowacyjny pracy:	Praca dotyczy jednego z najczęstszych i najbardziej niebezpiecznych rodzajów cyberataków. Aspekt innowacyjny obejmuje: – integrację różnych typów cech (tekstowych, strukturalnych, reputacyjnych) w jednym modelu, – empiryczną ocenę odporności systemu na nowe formy phishingu generowane przez modele językowe, – możliwość zaproponowania hybrydowego modelu zwiększającego skuteczność detekcji i redukującego fałszywe alarmy.
*Oprogramowanie, język programowania, środowisko systemowe:	
*Środowisko uruchomieniowe	
Dodatkowe wymagania i uwagi:	– Wskazana implementacja porównania co najmniej dwóch grup modeli: klasyczne ML oraz modele głębokie NLP. – Mile widziane testy odporności na perturbacje (np. lekkie modyfikacje tekstu przez atakującego). – Zalecana implementacja wizualizacji wyników i procesu klasyfikacji.
*Literatura:	

*pola opcjonalne