

## KARTA KURSU

Nazwa	<b>Wykrywanie anomalii sieciowych z użyciem uczenia maszynowego</b>
Nazwa w j. ang.	Detecting network anomalies using machine learning

Koordynator	Dr.hab. Serhii Semenov	Zespół dydaktyczny
Punktacja ECTS*	st. stacjonarne: 3 st. niestacjonarne: 3	

### Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z nowoczesnymi metodami wykrywania anomalii w danych sieciowych, ze szczególnym uwzględnieniem technik uczenia maszynowego i głębokiego uczenia. Studenci zdobędą wiedzę na temat rodzajów anomalii, metod ich identyfikacji oraz zastosowania algorytmów analitycznych do danych pochodzących z ruchu sieciowego, logów systemowych i środowisk IoT. Uczestnicy kursu nauczą się przetwarzać dane, budować modele detekcji, oceniać ich skuteczność oraz interpretować wyniki w kontekście praktycznych zastosowań w dziedzinie cyberbezpieczeństwa. Zajęcia mają charakter teoretyczno-praktyczny i przygotowują studentów do samodzielnego projektowania oraz wdrażania systemów wykrywających anomalie.

### Warunki wstępne

Wiedza	Student powinien posiadać podstawową wiedzę z zakresu: działania sieci komputerowych i protokołów komunikacyjnych (np. TCP/IP), podstaw statystyki i analizy danych, zasad działania systemów operacyjnych oraz logiki działania aplikacji sieciowych.
Umiejętności	Student powinien umieć: programować w języku Python (w stopniu podstawowym lub średnio zaawansowanym), korzystać z podstawowych bibliotek do analizy danych (np. NumPy, pandas, matplotlib), posługiwać się narzędziami do pracy z danymi (np. Jupyter Notebook, środowiska IDE).
Kursy	Rekomendowane wcześniejsze zaliczenie kursów z zakresu: podstaw programowania, wprowadzenia do SI, podstaw sieci komputerowych.

### Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student:  W01: Student zna pojęcia, typy oraz modele wykrywania anomalii w danych, ze szczególnym uwzględnieniem zastosowań w analizie ruchu sieciowego.	K_W01, K_W02, K_W04, K_W07

	W02: Student rozumie podstawowe i zaawansowane metody uczenia maszynowego oraz ich rolę w systemach detekcji anomalii.	K_W01, K_W03, K_W07
	W03: Student posiada wiedzę na temat źródeł danych sieciowych, procesu ekstrakcji cech i przygotowania danych do analizy.	K_W02, K_W04, K_W06

Umiejętności	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	Po zakończeniu kursu student: U01: Student potrafi wykorzystać algorytmy ML i DL (np. Isolation Forest, Autoencoder, LSTM) do wykrywania anomalii w danych sieciowych.	K_U01, K_U03, K_U04, K_U07
	U02: Student potrafi przygotować dane, przeprowadzić eksperymenty, ocenić skuteczność modelu oraz dokonać jego walidacji.	K_U05, K_U06, K_U09, K_U10
	U03: Student umie interpretować wyniki działania systemów wykrywania anomalii i wskazać ich zastosowanie w rzeczywistym środowisku cyberbezpieczeństwa.	K_U07, K_U11, K_U13

Kompetencje społeczne	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	Po zakończeniu kursu student: K01: Student rozumie znaczenie wczesnego wykrywania anomalii dla bezpieczeństwa systemów informatycznych i jest świadomy etycznych aspektów analizy danych.	K_K03, K_K04
	K02: Student jest gotów do pracy zespołowej w projektach z obszaru analizy danych i cyberbezpieczeństwa.	K_K01, K_K05
	K03: Student wykazuje potrzebę ciągłego doskonalenia się w zakresie nowoczesnych technologii wykrywania zagrożeń.	K_K02

#### Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	Z
Liczba godzin	10					30					

#### Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	Z
Liczba godzin	10					15					

## Opis metod prowadzenia zajęć

Zajęcia prowadzone są w formie wykładów oraz laboratoriów, z wykorzystaniem aktywizujących metod kształcenia.

Wykłady mają charakter problemowy i prezentacyjny – wprowadzają podstawowe pojęcia, klasyfikacje i techniki wykrywania anomalii, ze szczególnym uwzględnieniem zastosowań w cyberbezpieczeństwie.

Część materiału może być udostępniana w formie prezentacji lub materiałów e-learningowych.

Laboratoria prowadzone są w trybie praktycznym, zorientowanym na rozwiązywanie rzeczywistych problemów. Studenci pracują indywidualnie lub w małych zespołach, wykorzystując narzędzia programistyczne i środowiska analityczne (np. Python, scikit-learn, pandas, Jupyter Notebook). Zajęcia nastawione są na samodzielną analizę danych, implementację modeli detekcji anomalii oraz interpretację wyników.

## Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Zadania problemowe
W01					X			X					
W02					X			X					
W03					X			X					
U01					X			X					
U02					X			X					
U03					X			X					
K01					X			X					
K02					X			X					
K03					X			X					

Kryteria oceny	Warunkiem zaliczenia kursu jest:
	<ul style="list-style-type: none"> <li>uzyskanie pozytywnych ocen z zajęć laboratoryjnych (zaliczenie wszystkich obowiązkowych ćwiczeń),</li> <li>zaliczenie testu końcowego obejmującego materiał z wykładów.</li> </ul>
Kryteria oceny	Składniki oceny końcowej:
	<ul style="list-style-type: none"> <li><b>Aktywność i wykonanie zadań laboratoryjnych</b> – 60% Ocena obejmuje poprawność i kompletność realizowanych ćwiczeń, samodzielność oraz terminowość.</li> <li><b>Test końcowy z części teoretycznej (materiał wykładowy)</b> – 40% Pisemny test sprawdzający wiedzę z zakresu pojęć, metod oraz interpretacji wyników.</li> </ul>
Kryteria oceny	Skala ocen:
	<ul style="list-style-type: none"> <li>&lt; 50% – niedostateczny (2,0)</li> <li>50–59% – dostateczny (3,0)</li> <li>60–69% – dostateczny plus (3,5)</li> <li>70–79% – dobry (4,0)</li> <li>80–89% – dobry plus (4,5)</li> <li>90–100% – bardzo dobry (5,0)</li> </ul>

Uwagi	
-------	--

## Treści merytoryczne (wykaz tematów)

1. **Wprowadzenie do wykrywania anomalii w danych sieciowych**  
Definicje, klasyfikacja anomalii, znaczenie detekcji w kontekście bezpieczeństwa informatycznego.
2. **Źródła i charakterystyka danych sieciowych**  
Format danych (PCAP, NetFlow, logi), ekstrakcja cech, przygotowanie danych do analizy.
3. **Tradycyjne metody wykrywania anomalii**  
Podejścia statystyczne, progowe, analiza odchyłeń od normy.
4. **Uczenie maszynowe w detekcji anomalii**  
Modele nadzorowane i nienadzorowane, k-NN, SVM, Isolation Forest, Local Outlier Factor.
5. **Metody klasteryzacji i redukcji wymiarów**  
K-means, DBSCAN, analiza głównych składowych (PCA) w kontekście detekcji nietypowych obserwacji.
6. **Głębokie uczenie w analizie anomalii**  
Autoenkodery, sieci LSTM/GRU, wykrywanie anomalii w danych sekwencyjnych i czasowych.
7. **Analiza anomalii w danych rzeczywistych**  
Przykłady z logów systemowych, danych z systemów IDS/IPS (np. Zeek, Suricata) i środowisk IoT.
8. **Ocena skuteczności modeli detekcji**  
Metryki ewaluacji: precision, recall, F1-score, AUC; dobór parametrów i walidacja.
9. **Interpretowalność i wyjaśnialność modeli**  
Techniki zwiększające przejrzystość działania modeli ML i DL.
10. **Projektowanie prostych systemów wykrywających anomalie**  
Łączenie modeli, analiza wyników, przykłady wdrożeń w środowiskach testowych.

## Wykaz literatury podstawowej

1. Emmanuel Tsukerman Machine Learning for Cybersecurity Cookbook. Over 80 recipes on how to implement machine learning algorithms for building security systems using Python  
Wydawnictwo: Packt Publishing 346 c.
2. Moskalenko, V.; Kharchenko, V.; Semenov, S. Model and Method for Providing Resilience to Resource-Constrained AI-System. Sensors 2024, 24, 5951. <https://doi.org/10.3390/s24185951>
3. Meleshko, Yelyzaveta V., Mykola Yakymenko and Serhii Semenov. "A Method of Detecting Bot Networks Based on Graph Clustering in the Recommendation System of Social Network." International Conference on Computational Linguistics and Intelligent Systems (2021).

## Wykaz literatury uzupełniającej

1. R. Patelski and D. Pazderski, "Parameter Identifying Disturbance Rejection Control With Asymptotic Error Convergence," in IEEE Robotics and Automation Letters, vol. 9, no. 2, pp. 1035-1042, Feb. 2024, doi: 10.1109/LRA.2023.3339942.
2. Andreas Fried, Maximilian Stemmer-Grabow, and Julian Wachter. 2023. Register Allocation for Compressed ISAs in LLVM. In Proceedings of the 32nd ACM SIGPLAN International Conference on Compiler Construction (CC 2023). Association for Computing Machinery, New York, NY, USA, 122–132. <https://doi.org/10.1145/3578360.3580261>
3. Schummer, P.; del Rio, A.; Serrano, J.; Jimenez, D.; Sánchez, G.; Llorente, Á. Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation. AI 2024, 5, 2967-2983. <https://doi.org/10.3390/ai5040143>

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia stacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	15
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	10
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie)	
	Przygotowanie do egzaminu/zaliczenia	5
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia niestacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	15
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	10
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie)	10
	Przygotowanie do egzaminu/zaliczenia	5
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3