Sylabus przedmiotu / modułu kształcenia	
Nazwa przedmiotu/modułu kształcenia:	**Inteligentne systemy bezpieczeństwa komputerowego**
Nazwa w języku angielskim:	Intelligent cybersecurity systems
Język wykładowy:	polski
Kierunek studiów, dla którego przedmiot jest oferowany:	informatyka
Jednostka realizująca:	Instytut Informatyki
Rodzaj przedmiotu/modułu kształcenia (obowiązkowy/fakultatywny):	fakultatywny
Poziom modułu kształcenia (np. pierwszego lub drugiego stopnia, jednolitych magisterskich):	drugiego stopnia
Rok studiów:	pierwszy
Semestr:	drugi
Liczba punktów ECTS:	3
Imię i nazwisko koordynatora przedmiotu:	dr Piotr Świtalski
Imię i nazwisko prowadzących zajęcia:	dr Piotr Świtalski
Założenia i cele przedmiotu:	Założeniem tego przedmiotu jest znajomość przez słuchaczy zagadnień związanych z bezpieczeństwem komputerowym oraz metodami sztucznej inteligencji. Celem przedmiotu jest zaznajomienie studentów z nowoczesnymi metodami sztucznej inteligencji stosowanymi w bezpieczeństwie komputerowym, m.in.: ● metodami wykrywania anomalii, ● metodami wykrywania złośliwego oprogramowania, ● metodami wykrywania luk w oprogramowaniu, ● wprowadzeniem do generatywnych sieci przeciwstawnych oraz transformerów.

Symbol efektu	**Efekty uczenia się**	**Symbol efektu kierunkowego**
	WIEDZA **Student zna i rozumie:**	
W_01	inteligentne metody wykrywania ataków w dziedzinie bezpieczeństwa komputerowego	**W_S02, W_S03**
W_02	metody sztucznej inteligencji w systemach bezpieczeństwa komputerowego	**W_S02, W_S04**
	UMIEJĘTNOŚCI **Student potrafi:**	
U_01	zaimplementować prosty system detekcji anomalii	**U_S04, U_S06**
U_02	posługiwać się rozwiązaniami z dziedziny sztucznej inteligencji w bezpieczeństwie komputerowym	**U_S02**

Forma i typy zajęć:	studia stacjonarne: wykłady (20 godz.), ćwiczenia laboratoryjne (24 godz.) studia niestacjonarne: wykłady (10 godz.), ćwiczenia laboratoryjne (15 godz.)

Wymagania wstępne i dodatkowe:
Warunkiem uczestnictwa w zajęciach jest znajomość podstaw bezpieczeństwa komputerowego oraz metod sztucznej inteligencji.

Treści modułu kształcenia:

Treści dotyczące wykładu:

1. **Wstęp do inteligentnych systemów bezpieczeństwa komputerowego.** Koncepcja bezpieczeństwa komputerowego. Źródła zagrożeń. Zastosowania sztucznej inteligencji (SI) w cyberbezpieczeństwie – metody i przykłady. Wyzwania dla SI.
2. **Nowoczesne technologie uwierzytelniania użytkowników.** Statyczne uwierzytelnienie. Hasła jednorazowe. Wieloetapowe uwierzytelnianie. Token. Proces uwierzytelniania. Asercje. Moduł TPM. Tokeny sprzętowe. FIDO. protokół UAF. FDO.
3. **Łańcuchy bloków w bezpieczeństwie komputerowym.** Historia łańcucha bloków. Typy łańcuchów bloków. Decentralizacja z użyciem łańcucha bloków. Typowe algorytmy. Metody decentralizacji. Łańcuch bloków. Inteligentne kontrakty. Platformy do decentralizacji. Bezpieczeństwo łańcuchów bloków.
4. **Wprowadzenie do metod SI cz. 1.** Metody uczenia maszynowego. Sieci LSTM.
5. **Wprowadzenie do metod SI cz. 2.** Autoenkodery. Generatywne sieci przeciwstawne (GAN). Transformery.
6. **Wykrywanie anomalii.** Systemy wykrywania włamań. Analiza behawioralna. Architektura inteligentnych systemów detekcji. Użycie metod SI do wykrywania anomalii.
7. **Wykrywanie złośliwego oprogramowania.** Metody wykrywania. Wykonanie kodu komputerowego. Analiza i klasyfikacja złośliwego oprogramowania. Przykład analizy złośliwego pliku. Użycie metod SI do wykrywania złośliwego oprogramowania.
8. **Wykrywanie luk w oprogramowaniu.** Metryki. Wykrywanie podatności w kodzie.
9. **Skanowanie podatności.** Fuzzing. Analiza statyczna (SAST). Analiza dynamiczna (DAST). Narzędzia: CodeQL, DeepCode, Microsoft Security Copilot. Użycie metod SI do wykrywania luk w kodzie.
10. **Identyfikacja użytkowników i zarządzanie dostępem.** Biometria behawioralna. Metody i przykłady. **Projektowanie uniwersalne w systemach inteligentnych.** Zasady projektowania uniwersalnego. Identyfikacja potrzeb osób ze szczególnymi potrzebami. Zastosowania sztucznej inteligencji w technologiach dla osób ze szczególnymi potrzebami.

Treści dotyczące laboratorium:

1. Delegowanie autoryzacji do zasobów w OAuth2. Implementacja.
2. Łańcuch bloków. Implementacja. Tworzenie bloku. Weryfikacja bloku.
3. Wprowadzenie do analizy danych. Ładowanie danych ze zbioru. Manipulacja danymi. Analiza danych. Przetwarzanie danych. Normalizacja danych. Wizualizacja danych.
4. Algorytmy uczenia maszynowego w wykrywaniu anomalii. Metody uczenia maszynowego: las izolacji i maszyny wektorów nośnych. Przykład dostrajania hiperparametrów.
5. Wykrywanie anomalii z użyciem modeli sieci neuronowych. Prosta sieć neuronowa na PyTorch i Keras.
6. Wykrywanie anomalii z użyciem architektury sieci LSTM. Uruchomienie przykładu dla zbioru danych nyc_taxi. Wykrywanie anomalii.
7. Wykrywanie spamu za pomocą sieci neuronowych. Przygotowywanie danych. Wizualizacja danych. Tokenizacja. Sekwencjonowanie i wypełnianie. Model klasyfikacji tekstu za pomocą modelu BiLSTM. Ocena modeli.
8. Autoenkodery. Przykład zastosowania. Detekcja ataku na karty kredytowe. Ocena modelu.
9. Generatywne sieci przeciwstawne. Detekcja anomalii za pomocą sieci GAN. Przykład. Ocena modelu.
10. Transformery. Detekcja anomalii za pomocą transformerów. Przykład. Ocena modelu.
11. Analiza behawioralna. Biometria behawioralna. Przykład modelu. Wykorzystanie metody w bezpieczeństwie komputerowym.
12. Analiza podatności kodu komputerowego. Wykorzystanie metod SI do analizy kodu**.**

Literatura podstawowa:

1. Adari S.K., Alla S.: Beginning Anomaly Detection Using Python-Based Deep Learning: Implement Anomaly Detection Applications with Keras and PyTorch, Apress, 2024
2. Géron A.: Uczenie maszynowe z użyciem Scikit-Learn i TensorFlow. Wydanie II, Helion, 2020
3. McIlwraith D., Marmanis H., Babenko D.: Inteligentna sieć. Algorytmy przyszłości. Wydanie II, Helion, 2017

Literatura dodatkowa:

1. Bashir I.: Blockchain. Zaawansowane zastosowania łańcucha bloków. Wydanie II, Helion, 2019
2. Reznik L.: Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security 1st Edition, Wiley, 2021

Planowane formy/działania/metody dydaktyczne:

Wykład tradycyjny wspomagany jest technikami multimedialnymi. Ćwiczenia laboratoryjne – zajęcia praktyczne z wykorzystaniem wybranych narzędzi programowych. Na stronie internetowej prowadzącego zamieszczane są materiały z problemami i zadaniami laboratoryjnymi.

Sposoby weryfikacji efektów uczenia się osiąganych przez studenta:

Symbol efektu	Metody weryfikacji efektów uczenia się
W_01	Efekt realizowany na egzaminie w formie pisemnej. Przykładowe pytanie: „W jaki sposób można wykrywać anomalie w ruchu sieciowym opierając się o metody SI?”.
W_02	Efekt realizowany na egzaminie w formie pisemnej. Przykładowe pytanie: „Jakimi sposobami możliwe jest wykrywanie podatności w kodzie? Opisz działanie sieci neuronowych w kontekście wykrywania podatności w kodzie”.
U_01	Efekt realizowany w trakcie zajęć laboratoryjnych. Przykładowe zadanie: „Zbuduj model do detekcji anomalii. Określ hiperparametry dla modelu i wykonaj trenowanie sieci. Przetestuj rozwiązanie. Wygeneruj metryki dla nauczonej sieci oraz pokaż matrycę pomyłek”.
U_02	Efekt realizowany w trakcie zajęć laboratoryjnych. Przykładowe zadanie: „Zbuduj narzędzie do analizy ataków SQL Injection na bazie DeepCode”.

Forma i warunki zaliczenia:

Moduł kończy się egzaminem. Ocena z przedmiotu składa się z dwóch ocen cząstkowych:

oceny z zajęć laboratoryjnych,

oceny z egzaminu końcowego.

Na ocenę z zajęć laboratoryjnych składają się oceny cząstkowe uzyskane na regularnych zajęciach z nauczycielem akademickim, za które można uzyskać sumarycznie 50 pkt. Zaliczenie zajęć laboratoryjnych możliwe po uzyskaniu co najmniej 51% liczby punktów z tej formy zaliczenia

Egzamin jest egzaminem pisemnym. Do egzaminu mogą przystąpić osoby, które uzyskały zaliczenie laboratorium. Na egzaminie można uzyskać maksymalnie 50 pkt. Egzamin będzie zaliczony w przypadku uzyskania co najmniej 51% liczby punktów z tej formy zaliczenia.

Ocena końcowa, w zależności od sumy uzyskanych punktów (maksymalnie 100 pkt) jest następująca (w nawiasach ocena wg skali ECTS):

- 0 – 50 pkt: niedostateczna (F),
- 51 – 60 pkt: dostateczna (E),

- 61 – 70 pkt: dostateczna plus (D),
- 71 – 80 pkt: dobra (C),
- 81 – 90 pkt: dobra plus (B),
- 91 – 100 pkt: bardzo dobra (A).

Bilans punktów ECTS:	
Studia stacjonarne	
Aktywność	Obciążenie studenta
Udział w wykładach	20 godz.
Udział w ćwiczeniach laboratoryjnych	24 godz.
Przygotowanie się do egzaminu	10 godz.
Udział w egzaminie	1 godz.
Przygotowanie się do ćwiczeń laboratoryjnych	18 godz.
Udział w konsultacjach z przedmiotu	2 godz.
Sumaryczne obciążenie pracą studenta	**75 godz.**
Punkty ECTS za przedmiot	**3 ECTS**
Studia niestacjonarne	
Aktywność	Obciążenie studenta
Udział w wykładach	10 godz.
Udział w ćwiczeniach laboratoryjnych	15 godz.
Przygotowanie się do egzaminu	19 godz.
Udział w egzaminie	1 godz.
Przygotowanie się do ćwiczeń laboratoryjnych	28 godz.
Udział w konsultacjach z przedmiotu	2 godz.
Sumaryczne obciążenie pracą studenta	**75 godz.**
Punkty ECTS za przedmiot	**3 ECTS**