SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA 2026/2027 - 2029/2030

Rok akademicki 2027/2028

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	*podstawy cyberbezpieczeństwa*
Kod przedmiotu*	
Nazwa jednostki prowadzącej kierunek	*Instytut Informatyki, Wydział Nauk Ścisłych i Technicznych*
Nazwa jednostki realizującej przedmiot	*Instytut Informatyki, Wydział Nauk Ścisłych i Technicznych*
Kierunek studiów	*sztuczna inteligencja*
Poziom studiów	*studia I stopnia*
Profil	*ogólnoakademicki*
Forma studiów	*stacjonarne*
Rok i semestr/y studiów	*rok II, semestr 4*
Rodzaj przedmiotu	*przedmiot kierunkowy*
Język wykładowy	*polski*
Koordynator	*dr inż. Marcin Ochab*
Imię i nazwisko osoby prowadzącej / osób prowadzących	*dr inż. Marcin Ochab*

***** - *opcjonalnie, zgodnie z ustaleniami w Jednostce*

1.1.Formy zajęć dydaktycznych, wymiar godzin i punktów ECTS

Semestr (nr)	Wykł.	Ćw.	Konw.	Lab.	Sem.	ZP	Prakt.	Inne (jakie?)	**Liczba pkt. ECTS**
4	15			15					2

1.2. Sposób realizacji zajęć

zajęcia w formie tradycyjnej

1.3 Forma zaliczenia przedmiotu (z toku)

wykład – zaliczenie bez oceny, laboratoria – zaliczenie z oceną

2.WYMAGANIA WSTĘPNE

podstawowe zagadnienia dotyczące systemów operacyjnych, programowania, sieci komputerowych

3. CELE, EFEKTY UCZENIA SIĘ, TREŚCI PROGRAMOWE I STOSOWANE METODY DYDAKTYCZNE

3.1 Cele przedmiotu

C1	Zapoznanie z podstawowymi zagadnieniami związanymi z bezpieczeństwem informacji i systemów informatycznych.
C2	Zapoznanie się z metodami zapobiegania podatnościom występującym w systemach informatycznych oraz realizacją potrzebnych zabezpieczeń.
C3	Kształtowanie świadomości potrzeby ciągłego kształcenia się w obszarze bezpieczeństwa informatycznego.
C4	Poznanie narzędzi pozwalających na analizę stanu bezpieczeństwa systemu.

3.2 Efekty uczenia się dla przedmiotu

EK (efekt uczenia się)	Treść efektu uczenia się zdefiniowanego dla przedmiotu	Odniesienie do efektów kierunkowych [1]
EK_01	Zna rodzaje cyberzagrożeń oraz podejścia i mechanizmy obronne przeciwko nim. Zna odpowiednie normy i dobre praktyki pod kątem cyberbezpieczeństwa stosowane w różnych systemach informatycznych.	K_W09
EK_02	Zna podstawowe narzędzia do testowania bezpieczeństwa systemów informatycznych oraz uwarunkowania prawne dotyczące ich stosowania	K_W12
EK_03	Potrafi analizować ryzyko wynikające z podatności związanych z bezpieczeństwem systemów informatycznych oraz wdrażać odpowiednie zabezpieczenia. Potrafi udokumentować przeprowadzone testy.	K_U09, K_U14

3.3 Treści programowe

A. Problematyka wykładu

Uwarunkowania prawne dotyczące testowania bezpieczeństwa systemów informatycznych
Istniejące klasyfikacje błędów dotyczących bezpieczeństwa systemów informatycznych
Najpopularniejsze podatności w aplikacjach internetowych
Sanityzacja danych po stronie frontend'u i backend'u
Bezpieczeństwo haseł po stronie użytkownika, mechanizm MFA.
Hashowanie i szyfrowanie
Testowanie złożoności haseł i hashy, uzyskiwanie i budowanie własnych słowników.
Szyfry symetryczne i asymetryczne
Podstawowe zagadnienia OSINT

B. Problematyka laboratoriów

Ataki na aplikacje internetowe oraz sposoby ich obrony.

[1] W przypadku ścieżki kształcenia prowadzącej do uzyskania kwalifikacji nauczycielskich uwzględnić również efekty uczenia się ze standardów kształcenia przygotowującego do wykonywania zawodu nauczyciela.

Zarządzanie kluczami publicznymi i prywatnymi.
Menedżery haseł. MFA.
Testowanie praktyczne złożoności haseł i algorytmów hashujących, pozyskiwanie słowników i ich modyfikacje.
Realizacja projektu zaliczeniowego.

3.4 Metody dydaktyczne

Wykład: wykład z prezentacją multimedialną.
Laboratorium: wykonywanie zadań praktycznych przy komputerze.

4. METODY I KRYTERIA OCENY

4.1 Sposoby weryfikacji efektów uczenia się

Symbol efektu	Metody oceny efektów uczenia się (np.: kolokwium, egzamin ustny, egzamin pisemny, projekt, sprawozdanie, obserwacja w trakcie zajęć)	Forma zajęć dydaktycznych (w, ćw, ...)
EK_01, EK_02	kolokwium	wykład
EK_03	projekt	laboratorium

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Zaliczenie wykładu uzyskiwane jest na podstawie kolokwium, weryfikującego znajomość zagadnień przedstawionych w ramach wykładu.
Efekty EK_01 i EK_02 uznaje się za zaliczone, gdy udzielone zostanie co najmniej 50% prawidłowych odpowiedzi na pytania przyporządkowane do każdego z nich.
Zaliczenie wykładu następuje, gdy EK_01 i EK_02 są zaliczone na „zal".

Zaliczenie laboratorium następuje na podstawie wykonanego projektu, dotyczącego wybranego tematu z zagadnień omawianych na laboratorium. Za projekt wystawiana jest ocena w skali 2.0 - 5.0 proporcjonalnie do uzyskanej liczby punktów, możliwych do zdobycia za wykonanie praktycznej części projektu oraz za dokumentację (opisującą zrealizowany projekt).

Efekt EK_03 jest uznany za zaliczony, gdy projekt wykonany przez studenta uzyska przynajmniej 50% możliwych punktów.
Ocena końcowa z laboratorium jest wystawiana na postawie oceny za efekt EK_03.

5. CAŁKOWITY NAKŁAD PRACY STUDENTA POTRZEBNY DO OSIĄGNIĘCIA ZAŁOŻONYCH EFEKTÓW W GODZINACH ORAZ PUNKTACH ECTS

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny z harmonogramu studiów	30
Inne z udziałem nauczyciela akademickiego	–

(udział w konsultacjach, egzaminie)	
Godziny niekontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	20
SUMA GODZIN	50
SUMARYCZNA LICZBA PUNKTÓW ECTS	**2**

** Należy uwzględnić, że 1 pkt ECTS odpowiada 25-30 godzin całkowitego nakładu pracy studenta.*

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

wymiar godzinowy	–
zasady i formy odbywania praktyk	–

7. LITERATURA

Literatura podstawowa:

1) Michał Bentkowski, Gynvael Coldwind, Artur Czyż, Rafał Janicki, Jarosław Kamiński, Adrian Michalczyk, Mateusz Niezabitowski, Marcin Piosek, Michał Sajdak, Grzegorz Trawiński, Bohdan Widła: Bezpieczeństwo aplikacji webowych, SECURITUM, 2019
2) Andrew Hoffman: Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach, Gliwice, Helion, 2021
3) Malcolm McDonald: Bezpieczeństwo aplikacji internetowych dla programistów. Rzeczywiste zagrożenia, praktyczna ochrona, Gliwice, Helion, 2021.
4) Bernardo Damele A. G., Miroslav Stampar: sqlmap user's manual, 2011

Literatura uzupełniająca:

1) Himanshu Sharma, Harpreet Singh, „Hands on Red Team Tactics A practical guide to mastering Red Team operations", 2018
2) David Kennedy et al., „Metasploit: the penetration tester's guide", 2011