

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

KARTA OPISU PRZEDMIOTU

Wydział		Informatyki	
Kierunek		Informatyka	
Specjalność			
Semestr	VI	Program studiów, dla którego obowiązuje sylabus	2024/2025
Stopień studiów	I		

Nazwa przedmiotu	Metody audytu i walidacji bezpieczeństwa			
Kod przedmiotu	MAIWB			
Łączna liczba godzin	30	Tryb	stacjonarny	niestacjonarny
Profil kształcenia	Ogólnoakademicki (A)		Praktyczny (P)	
Forma zajęć	laboratorium			
Język przedmiotu	polski			
Liczba punktów ECTS	2			

Prowadzący zajęcia	
Forma prowadzonych zajęć	Laboratorium
Wymiar zajęć	30 h
Stopień (tytuł) naukowy	
Imię	
Nazwisko	

Wymagania wstępne	Podstawowa wiedza z zakresu informatyki i technologii informacyjnych, umiejętność obsługi systemów operacyjnych Windows i Linux, znajomość podstaw programowania i algorytmiki oraz podstawowych zasad działania sieci komputerowych.
Założenia i cele przedmiotu	Przedmiot ma na celu zapoznanie studentów z metodami oceny bezpieczeństwa systemów informatycznych poprzez audyty, testy penetracyjne oraz analizę podatności. Studenci poznają standardy i normy, sposoby raportowania wyników oraz formułowania rekomendacji. Celem jest uzyskanie umiejętności praktycznych w planowaniu i przeprowadzaniu audytów, a także w interpretacji ich wyników i wdrażaniu działań naprawczych.
Metody dydaktyczne	<ol style="list-style-type: none"> 1. Prezentacje multimedialne. 2. Pokazy przykładowych rozwiązań problemów. 3. Rozwiązywanie zadań praktycznych.

Efekty uczenia się (odniesienie do charakterystyk poziomów Polskiej Ramy Kwalifikacji)		Odniesienie do efektów dla kierunku	Odniesienie do efektów uczenia się wg Polskiej Ramy Kwalifikacji
WIEDZA – absolwent zna i rozumie:	W01. Metody nadzorowania, zabezpieczania i walidacji bezpieczeństwa systemów teleinformatycznych, w tym znaczenie audytów i	K_W06 K_W16	P6S_WG P6S_WG_INŻ

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

	<p>testów penetracyjnych.</p> <p>W02. Strukturę i zasady zarządzania projektami audytowymi, w tym tworzenie planów, harmonogramów oraz wykorzystanie narzędzi do analizy ryzyka.</p> <p>W03. Zagrożenia oraz aspekty prawne i etyczne towarzyszące przeprowadzaniu testów penetracyjnych i analiz podatności.</p> <p>W04. Zasady ochrony własności intelektualnej oraz normy prawne, które należy uwzględnić podczas audytów bezpieczeństwa (np. ujawnianie luk i ich dokumentacja).</p> <p>W05. Metody projektowania i oceny systemów informatycznych pod kątem spełnienia standardów i wymagań bezpieczeństwa, z uwzględnieniem wyników audytów.</p>	<p>K_W22 K_W18 K_W24</p>	
UMIEJĘTNOŚCI – absolwent potrafi:	<p>U01. Pozyskiwać informacje z norm, standardów i literatury fachowej, aby tworzyć kompletne plany audytu bezpieczeństwa.</p> <p>U02. Zaplanować i przeprowadzić testy penetracyjne oraz analizę podatności, a następnie opracować rekomendacje dotyczące poprawy zabezpieczeń.</p> <p>U03. Formułować hipotezy i weryfikować je poprzez eksperymenty i testy z wykorzystaniem odpowiednich narzędzi audytowych.</p> <p>U04. Efektywnie pracować w zespole audytowym, przydzielając zadania, zarządzając czasem i komunikując wyniki członkom zespołu.</p> <p>U05. Przygotować dokumentację wyników audytu i raport końcowy, zawierający analizę, wnioski oraz rekomendacje dla interesariuszy.</p>	<p>K_U01 K_U02 K_U03 K_U04 K_U09 K_U13</p>	<p>P6S_UW P6S_UW_INŻ P6S_UO P6S_KK P6S_UK</p>
KOMPETENCJE SPOŁECZNE – absolwent jest gotów do	<p>K01. Pracy w zespole, przyjmując w nim różne role.</p> <p>K02. Krytycznej oceny możliwości urządzeń sieciowych i systemów i dostępnych na rynku IT.</p> <p>K03. Ciągłego samokształcenia się w celu dostosowywania się do dynamicznie zmieniających się technologii.</p>	<p>K_K04 K_K05 K_K06</p>	<p>P6S_UO P6S_KR P6S_KK</p>

Lp.	Tematyka zajęć	Liczba godzin
Forma zajęć – laboratorium		
1	Podstawy audytu bezpieczeństwa. Cele audytu, standardy i normy (ISO/IEC 27001).	4
2	Planowanie i przeprowadzanie audytu. Metodologie audytu, tworzenie planu audytu,	6

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

	zbieranie danych.	
3	Testy penetracyjne. Rodzaje testów penetracyjnych, narzędzia i techniki, etyka testowania.	6
4	Analiza podatności. Wykorzystanie skanerów podatności, interpretacja wyników, ocena ryzyka	6
5	Raportowanie i rekomendacje. Tworzenie raportów z audytu, przedstawianie wyników, zalecenia naprawcze.	4
6	Przegląd studiów przypadków. Analiza realnych incydentów bezpieczeństwa, wnioski i najlepsze praktyki. Zaliczenie.	4

Forma i warunki zaliczenia przedmiotu	Wykonanie projektów. Częstkowe prezentacje, zdawanie raportów, obrona projektów.	
Metody weryfikacji efektów uczenia się		Nr efektu uczenia się z sylabusu
	Ocena projektów i częściowych prezentacji.	W01-W05, U01-U05, K01-K03

Literatura podstawowa	<ol style="list-style-type: none"> 1. R. Kurose, <i>Sieci komputerowe. Ujęcie całościowe</i>, Helion, Gliwice 2017. 2. W. Kabaciński, M. Żal, <i>Sieci telekomunikacyjne</i>, Warszawa 2008. 3. D. E. Comer, <i>Sieci komputerowe i intersieci</i>, Helion, Gliwice 2012. 4. E. Cole, R. Krutz, J. Conle, <i>Bezpieczeństwo sieci: biblia</i>, Helion, Gliwice 2005.
Literatura uzupełniająca	<ol style="list-style-type: none"> 1. S. A. Tanenbaum, M. Steen, <i>Systemy rozproszone Zasady i paradygmaty</i>, WNT, Warszawa 2006. 2. B. Dunsmore, T. Skandier, <i>Cisco, technologie telekomunikacyjne</i>, MIKOM, Warszawa 2008.

Nakład pracy studenta	
	Liczba godzin
Zajęcia dydaktyczne	30
Przygotowanie się do zajęć	5
Studiowanie literatury	5
Udział w konsultacjach	2
Przygotowanie projektu / eseju / prezentacji itp.	18
Przygotowanie się do egzaminu / zaliczenia	-
Inne	-
ŁĄCZNY nakład pracy studenta w godz.	60
Liczba punktów ECTS	2