

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

KARTA OPISU PRZEDMIOTU

Wydział		Informatyki	
Kierunek		Informatyka	
Specjalność		Programowanie, Sieci komputerowe i systemy teleinformatyczne	
Semestr	II	Program studiów, dla którego obowiązuje sylabus	2024/2025
Stopień studiów	II		

Nazwa przedmiotu	Bezpieczeństwo i niezawodność sieci informatycznych i informacyjnych			
Kod przedmiotu	BiNSiII			
Łączna liczba godzin	60	Tryb	stacjonarny	niestacjonarny
Profil kształcenia	Ogólnoakademicki (A)		Praktyczny (P)	
Forma zajęć	wykład + laboratorium			
Język przedmiotu	polski			
Liczba punktów ECTS	5 (3+2)			

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

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

Wymagania wstępne	Znajomość zasad działania i konfiguracji sieci komputerowych, adresacji IP, architektur sieciowych, protokołów sieciowych.
Założenia i cele przedmiotu	Zaznajomienie studentów z zagrożeniami bezpieczeństwa (w tym dostępności) w sieciach informatycznych oraz z zasadą działania i konfiguracją mechanizmów bezpieczeństwa, w tym narzędzi kryptograficznych.
Metody dydaktyczne	<ol style="list-style-type: none"> 1. Wykład – w formie tradycyjnej lub prezentacji multimedialnej 2. Laboratorium – w trakcie którego studenci analizują i rozwiązują problemy/zadania, wykorzystując symulatory sieciowe oraz narzędzia zapewniania i testowania bezpieczeństwa

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

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. Zagrożenia bezpieczeństwa informacji i niezawodności sieci informatycznych. W02. Metody i środki ochrony systemów, w tym z zakresu kryptograficznych.	K_W04	P7S_WG_INŻ
UMIEJĘTNOŚCI – absolwent potrafi:	U01. Podjąć środki sprzętowe i programowe w celu zapewnienia ciągłości działania oraz bezpieczeństwa sieci informatycznych. U02. Ocenic bezpieczeństwo systemu informatycznego, korzystając z powszechnie dostępnych narzędzi.	K_U01 K_U06 K_U08 K_U09 K_U11	P7S_UW P7S_UW_INŻ P7S_KK
KOMPETENCJE SPOŁECZNE – absolwent jest gotów do	K01. Pracy w zespole i włączania się w organizację jego działań. K02. Krytycznej oceny możliwości urządzeń i rozwiązań sieciowych w obszarze bezpieczeństwa.	K_K04 K_K05	P7S_UO P7S_KK

Treści programowe		
Lp.	Tematyka zajęć	Liczba godzin
Forma zajęć – wykład		
1	Wprowadzenie, podstawowe pojęcia i definicje, atrybuty bezpieczeństwa.	2
2	Zagrożenia i podatności systemów informatycznych.	4
3	Kryptografia: algorytmy symetryczne i asymetryczne, funkcje skrótu, podpis cyfrowy.	4
4	Dystrybucja kluczy, infrastruktura klucza publicznego.	4
5	Bezpieczne usługi sieciowe, wirtualne sieci prywatne.	4
6	Niezawodność systemów informatycznych.	4
7	Filtrowanie ruchu sieciowego, zapory ogniowe.	4
8	Aspekty organizacyjne i prawne bezpieczeństwa i niezawodności.	4
Forma zajęć – laboratorium		
1	Analiza bezpieczeństwa usług internetowych.	4
2	Bezpieczeństwo i niezawodność infrastruktury sieciowej.	4
3	Zagrożenia i podatności sieci komputerowych.	4
4	Bezpieczeństwo systemów operacyjnych.	4

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

5	Narzędzia kryptograficzne: szyfrowanie i deszyfrowanie, podpisywanie i weryfikacja podpisów cyfrowych.	4
6	Konfiguracja bezpiecznych usług sieciowych.	5
7	Filtrowanie ruchu sieciowego. Zaliczenie.	5

Forma i warunki zaliczenia przedmiotu	Egzamin pisemny z wykładu. Wykonanie sprawozdań w ramach laboratorium.	
Metody weryfikacji efektów uczenia się		Nr efektu uczenia się z sylabusu
	Egzamin pisemny	W01-W02
	Ocena sprawozdań wykonanych w ramach laboratorium	U01-U02, K01

Literatura podstawowa	<ol style="list-style-type: none"> 1. W. Stallings, <i>Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii</i>, Helion, Gliwice 2012. 2. E. Cole, R. Krutz, J. Conle, <i>Bezpieczeństwo sieci: biblia</i>, Helion, Gliwice 2005. 3. L. Dostálek, <i>Bezpieczeństwo protokołu TCP/IP: kompletny przewodnik</i>, PWN, Warszawa 2006.
Literatura uzupełniająca	<ol style="list-style-type: none"> 1. M. Serafin, <i>Sieci VPN: zdalna praca i bezpieczeństwo danych</i>, wyd. Helion, Gliwice 2010. 2. A. Lockhart, <i>125 sposobów na bezpieczeństwo sieci</i>, Helion, Gliwice 2007.

Nakład pracy studenta	
	Liczba godzin
Zajęcia dydaktyczne	60
Przygotowanie się do zajęć	20
Studiowanie literatury	10
Udział w konsultacjach	5
Przygotowanie projektu / eseju / prezentacji itp.	-
Przygotowanie się do egzaminu / zaliczenia	30
Inne	-
ŁĄCZNY nakład pracy studenta w godz.	125
Liczba punktów ECTS	5