

# AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

## KARTA OPISU PRZEDMIOTU

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

Nazwa przedmiotu	Bezpieczeństwo i niezawodność sieci informatycznych i informacyjnych			
Kod przedmiotu	BiNSiII			
Łączna liczba godzin	36	Tryb	stacjonarny	niestacjonarny
Profil kształcenia	Ogólnoakademicki (A)		Praktyczny (P)	
Forma zajęć	wykład + laboratorium			
Język przedmiotu	polski			
Liczba punktów ECTS	5 (3+2)			

Prowadzący zajęcia	
<b>Forma prowadzonych zajęć</b>	<b>Wykład</b>
<b>Wymiar zajęć</b>	<b>18 h</b>
<b>Stopień (tytuł) naukowy</b>	
<b>Imię</b>	
<b>Nazwisko</b>	

Prowadzący zajęcia	
<b>Forma prowadzonych zajęć</b>	<b>Laboratorium</b>
<b>Wymiar zajęć</b>	<b>18 h</b>
<b>Stopień (tytuł) naukowy</b>	
<b>Imię</b>	
<b>Nazwisko</b>	

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

## 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 P7S_WG_INŻ
UMIEJĘTNOŚCI – absolwent potrafi:	U01. Podjąć środki sprzętowe i programowe w celu zapewnienia ciągłości działania oraz bezpieczeństwa sieci informatycznych. U02. Ocenić 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
<b>Forma zajęć – wykład</b>		
1	Wprowadzenie, podstawowe pojęcia i definicje, atrybuty bezpieczeństwa.	2
2	Zagrożenia i podatności systemów informatycznych.	2
3	Kryptografia: algorytmy symetryczne i asymetryczne, funkcje skrótu, podpis cyfrowy.	3
4	Dystrybucja kluczy, infrastruktura klucza publicznego.	3
5	Bezpieczne usługi sieciowe, wirtualne sieci prywatne.	2
6	Niezawodność systemów informatycznych.	2
7	Filtrowanie ruchu sieciowego, zapory ogniowe.	2
8	Aspekty organizacyjne i prawne bezpieczeństwa i niezawodności.	2
<b>Forma zajęć – laboratorium</b>		
1	Analiza bezpieczeństwa usług internetowych.	2
2	Bezpieczeństwo i niezawodność infrastruktury sieciowej.	2
3	Zagrożenia i podatności sieci komputerowych.	2
4	Bezpieczeństwo systemów operacyjnych.	2

## AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

5	Narzędzia kryptograficzne: szyfrowanie i deszyfrowanie, podpisywanie i weryfikacja podpisów cyfrowych.	2
6	Konfiguracja bezpiecznych usług sieciowych.	4
7	Filtrowanie ruchu sieciowego. Zaliczenie.	4

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

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

Nakład pracy studenta	
	Liczba godzin
Zajęcia dydaktyczne	36
Przygotowanie się do zajęć	21
Studiowanie literatury	16
Udział w konsultacjach	5
Przygotowanie projektu / eseju / prezentacji itp.	21
Przygotowanie się do egzaminu / zaliczenia	26
Inne	-
<b>ŁĄCZNY nakład pracy studenta w godz.</b>	<b>125</b>
<b>Liczba punktów ECTS</b>	<b>5</b>