

# 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>Bezpieczeństwo systemów komputerowych Cyberbezpieczeństwo</b>	
<b>Semestr</b>	<b>V</b>	<b>Program studiów, dla którego obowiązuje sylabus</b>	<b>2024/2025</b>
<b>Stopień studiów</b>	<b>I</b>		

Nazwa przedmiotu	Skuteczna ochrona sieci i systemów informatycznych przed atakami			
Kod przedmiotu	SOSISIPA			
Łączna liczba godzin	30	Tryb	stacjonarny	niestacjonarny
Profil kształcenia	Ogólnoakademicki (A)		Praktyczny (P)	
Forma zajęć	laboratorium			
Język przedmiotu	polski			
Liczba punktów ECTS	2			

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

<b>Wymagania wstępne</b>	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.
<b>Założenia i cele przedmiotu</b>	Celem przedmiotu jest kształtowanie umiejętności rozpoznawania i przeciwdziałania najczęstszym atakom, konfigurowania zapór sieciowych i systemów IDS/IPS, ochrony przed atakami DDoS, zabezpieczania aplikacji (np. webowych) oraz efektywnego reagowania na incydenty bezpieczeństwa.
<b>Metody dydaktyczne</b>	<ol style="list-style-type: none"> <li>1. Prezentacje multimedialne.</li> <li>2. Pokazy przykładowych rozwiązań problemów.</li> <li>3. Rozwiązywanie zadań praktycznych.</li> </ol>

<b>Efekty uczenia się (odniesienie do charakterystyk poziomów Polskiej Ramy Kwalifikacji)</b>		<b>Odniesienie do efektów dla kierunku</b>	<b>Odniesienie do efektów uczenia się wg Polskiej Ramy Kwalifikacji</b>
WIEDZA – absolwent zna i rozumie:	W01. Najczęstsze rodzaje ataków na sieci i systemy oraz typowe techniki stosowane przez atakujących.  W02. Zasady implementacji i konfiguracji zapór	K_W04 K_W05 K_W16	P6S_WG P6S_WG_INŻ

## AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

	<p>sieciowych oraz systemów IDS/IPS.</p> <p>W03. Metody ochrony przed atakami DDoS, w tym techniki detekcji i neutralizacji.</p> <p>W04. Zasady bezpieczeństwa aplikacji sieciowych, testy penetracyjne oraz standardy OWASP Top 10.</p> <p>W05. Procedury reagowania na incydenty bezpieczeństwa oraz narzędzia służące ich analizie.</p>		
UMIEJĘTNOŚCI – absolwent potrafi:	<p>U01. Wykrywać i analizować próby ataków na sieci i systemy.</p> <p>U02. Konfigurować i utrzymywać zapory sieciowe oraz systemy IDS/IPS celem ochrony zasobów.</p> <p>U03. Wdrożyć środki ochrony przed atakami DDoS, analizować ruch i podejmować działania zapobiegawcze.</p> <p>U04. Przeprowadzić podstawowe testy penetracyjne aplikacji webowych i wdrożyć zabezpieczenia zgodne z OWASP Top 10.</p> <p>U05. Opracować procedury reagowania na incydenty, korzystać z narzędzi analizy oraz koordynować działania zespołu w sytuacjach kryzysowych.</p>	<p>K_U01 K_U02 K_U03 K_U04 K_U07 K_U12 K_U13 K_U14 K_U18</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
<b>Forma zajęć – laboratorium</b>		
1	Systemy zarządzania siecią (NMS). Konfiguracja i wykorzystanie systemów NMS; monitorowanie infrastruktury.	6
2	Automatyzacja zarządzania systemami. Skrypty, narzędzia do automatyzacji (Ansible, Puppet, Chef).	6
3	Bezpieczne zarządzanie konfiguracją. Kontrola wersji, polityki bezpieczeństwa konfiguracji.	6
4	Zarządzanie dostępem i tożsamością. Implementacja systemów IAM; autoryzacja i uwierzytelnianie użytkowników.	6

## AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

5	Planowanie ciągłości działania i odzyskiwania po awarii. Tworzenie planów DRP/BCP, backupy, redundancja. Zaliczenie.	6
---	--	---

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

<b>Literatura podstawowa</b>	<ol style="list-style-type: none"> <li>1. R. Kurose, <i>Sieci komputerowe. Ujęcie całościowe</i>, Helion, Gliwice 2017.</li> <li>2. W. Kabaciński, M. Żal, <i>Sieci telekomunikacyjne</i>, Warszawa 2008.</li> <li>3. D. E. Comer, <i>Sieci komputerowe i intersieci</i>, Helion, Gliwice 2012.</li> <li>4. W. Stallings, <i>Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii</i>, Helion, Gliwice 2012.</li> <li>5. E. Cole, R. Krutz, J. Conle, <i>Bezpieczeństwo sieci: biblia</i>, Helion, Gliwice 2005.</li> </ol>
<b>Literatura uzupełniająca</b>	<ol style="list-style-type: none"> <li>1. S. A. Tanenbaum, M. Steen, <i>Systemy rozproszone Zasady i paradygmaty</i>, WNT, Warszawa 2006.</li> <li>2. B. Dunsmore, T. Skandier, <i>Cisco, technologie telekomunikacyjne</i>, MIKOM, Warszawa 2008.</li> </ol>

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	-
<b>ŁĄCZNY nakład pracy studenta w godz.</b>	<b>60</b>
<b>Liczba punktów ECTS</b>	<b>2</b>