

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

KARTA OPISU PRZEDMIOTU

Wydział		Informatyki	
Kierunek		Informatyka	
Specjalność		Bezpieczeństwo systemów komputerowych Cyberbezpieczeństwo	
Semestr	V	Program studiów, dla którego obowiązuje sylabus	2024/2025
Stopień studiów	I		

Nazwa przedmiotu	Zarządzanie i eksploatacja systemów informatycznych i sieci teleinformatycznych			
Kod przedmiotu	ZIESIIST			
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 koncentruje się na wykształceniu wiedzy i umiejętności z zakresu efektywnego zarządzania i utrzymania systemów informatycznych oraz sieci teleinformatycznych z wykorzystaniem systemów NMS, automatyzacji procesów, polityk bezpiecznej konfiguracji, zarządzania dostępem i tożsamości oraz planowania ciągłości działania. Studenci poznają narzędzia i metody zapewniające stabilną, bezpieczną i ciągłą pracę infrastruktury IT.
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	W01.Zasady działania i konfiguracji systemów		P6S_WG

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

– absolwent zna i rozumie:	<p>zarządzania siecią (NMS).</p> <p>W02. Narzędzia i metody automatyzacji zarządzania systemami (Ansible, Puppet, Chef).</p> <p>W03. Metody bezpiecznej kontroli wersji konfiguracji oraz polityki bezpieczeństwa związane z konfiguracją systemów.</p> <p>W04. Zasady zarządzania tożsamością i dostępem (IAM) oraz uwierzytelniania i autoryzacji użytkowników.</p> <p>W05. Zasady planowania ciągłości działania (BCP) i odzyskiwania po awarii (DRP), w tym znaczenie backupów i redundancji.</p>	K_W16	P6S_WG_INŻ
UMIEJĘTNOŚCI – absolwent potrafi:	<p>U01. Skonfigurować i wykorzystać system NMS do monitorowania i zarządzania infrastrukturą sieciową.</p> <p>U02. Wykorzystać narzędzia automatyzacji (Ansible, Puppet, Chef) do zarządzania konfiguracją i procesami eksploatacyjnymi.</p> <p>U03. Wdrażać polityki bezpieczeństwa konfiguracji oraz stosować systemy kontroli wersji w zarządzaniu ustawieniami urządzeń.</p> <p>U04. Zaimplementować systemy IAM w celu skutecznego zarządzania dostępem i tożsamością użytkowników.</p> <p>U05. Przygotować i wdrożyć plany BCP/DRP oraz zastosować rozwiązania backupowe i redundantne w celu zapewnienia ciągłości działania.</p>	<p>K_U01 K_U02 K_U03 K_U04 K_U18 K_U21</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	Systemy zarządzania siecią (NMS). Konfiguracja i wykorzystanie systemów NMS; monitorowanie infrastruktury.	6
2	Automatyzacja zarządzania systemami. Skrypty, narzędzia do automatyzacji (Ansible, Puppet, Chef).	6

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

3	Bezpieczne zarządzanie konfiguracją. Kontrola wersji, polityki bezpieczeństwa konfiguracji.	6
4	Zarządzanie dostępem i tożsamością. Implementacja systemów IAM; autoryzacja i uwierzytelnianie użytkowników.	6
5	Planowanie ciągłości działania i odzyskiwania po awarii. Tworzenie planów DRP/BCP, backupy, redundancja. Zaliczenie.	6

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. W. Stallings, <i>Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii</i>, Helion, Gliwice 2012. 5. 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