



KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-ID2C-04-s2, E-ID2C-04-s3
	studia niestacjonarne:	E-2IZ2C-1008-s3
Nazwa przedmiotu	Bezpieczeństwo systemów chmurowych	
Nazwa przedmiotu w języku angielskim	Cloud security	
Obowiązuje od roku akademickiego	2022/23	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	Informatyka
Poziom kształcenia	II stopień
Profil studiów	Ogólnoakademicki
Forma i tryb prowadzenia studiów	Studia stacjonarne i niestacjonarne
Zakres	Cyberbezpieczeństwo
Jednostka prowadząca przedmiot	Katedra Systemów Informatycznych
Koordynator przedmiotu	Dr inż. Mirosław Płaza, mgr inż. Marcin Kozłowski
Zatwierdził	Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki dr hab. inż. Roman Deniziak, prof. PŚk

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		Przedmiot specjalnościowy
Status przedmiotu		Wybieralny
Język prowadzenia zajęć		Polski
Usytuowanie w planie studiów - semestr	studia stacjonarne	Semestr II lub Semestr III
	studia niestacjonarne	Semestr II lub Semestr III
Wymagania wstępne		brak
Egzamin (TAK/NIE)		NIE
Liczba punktów ECTS		3

Forma prowadzenia zajęć		wykład	ćwiczenia	laboratorium	projekt	inne
Liczba godzin w semestrze	studia stacjonarne:	30		15	15	
	studia niestacjonarne:	18		9	9	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie zagrożenia związane z bezpieczeństwem rozwiązań chmurowych.	INF2_W02
	W02	Student zna i rozumie podstawowe technologie zabezpieczeń stosowane w rozwiązaniach chmurowych.	INF2_W06
	W03	Student zna i rozumie struktury rozwiązań bezpieczeństwa implementowanych w chmurze.	INF2_W06
Umiejętności	U01	Student potrafi konfigurować podstawowe zabezpieczenia w chmurze.	INF2_U01, INF2_U02, INF2_U05, INF2_U07, INF2_U09, INF2_U10
	U02	Student potrafi przewidywać ataki na infrastrukturę chmury i odpowiednio im zapobiegać.	INF2_U01, INF2_U05
	U03	Student potrafi weryfikować poziom bezpieczeństwa rozwiązań chmurowych.	INF2_U01, INF2_U02, INF2_U03, INF2_U05, INF2_U07, INF2_U11
Kompetencje społeczne	K01	Student jest gotów do poszerzania kompetencji w zakresie zagrożeń związanych z bezpieczeństwem rozwiązań chmurowych.	INF2_K03 INF2_K04
	K02	Student jest gotów do pracy i współdziałania w grupie w zakresie implementacji podstawowych technologii związanych z bezpieczeństwem rozwiązań chmurowych.	INF2_K03 INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	Podstawowe zasady i pojęcia (potencjalni atakujący, diagramy i granice zaufania). Model świadczenia usługi w chmurze (model współodpowiedzialności w chmurze, zarządzanie ryzykiem). Identyfikacja i klasyfikacja danych (wymaganie barażowe i prawne, oznaczanie zasobów w chmurze). Zarządzanie zasobami danych i ich ochrona (zasoby obliczeniowe, pamięciowe oraz sieciowe, ochrona danych w chmurze, tokenizacja, szyfrowanie). Zarządzanie tożsamością i dostępem (różnice w stosunku do tradycyjnych wymagań w branży IT, cykl życia dla tożsamości i metod dostępu). Uwierzytelnianie (hasła i klucze API, scentralizowana autoryzacja i autoryzacja wielopoziomowa). Podatności rozwiązań chmurowych (dostęp do danych i infrastruktury, monitorowanie incydentów w rozwiązaniach chmurowych) Procesy zarządzania ryzykiem (Kontrola konfiguracji usług chmurowych oraz zapewnienie zgodności z wewnętrznymi politykami bezpieczeństwa informacji, wykrywanie anomalii w zachowaniu użytkowników, szara strefa, ochrona danych) Bezpieczeństwo prywatnej chmury wirtualnej.

laboratorium	1. Operacje aplikacji wykorzystujących chmurę do udostępniania zasobów. 2. Szyfrowanie danych. 3. Zarządzanie zasobami w chmurze. 4. Operacje na kluczach API. 5. Autoryzacja użytkownika w infrastrukturze chmury. 6. Zapoznanie się z mechanizmami DAST, SAST, SCA, IAST, RASP 7. Monitorowanie incydentów w praktyce.
projekt	Tematyka zadań projektowych z zakresu Bezpieczeństwa systemów chmurowych obejmuje następujące zagadnienia: analizę literatury w zakresie dotychczas stosowanych rozwiązań dotyczących zadanego problemu inżynierskiego; analizę oraz dobranie odpowiednich technik umożliwiających skuteczną realizację zadanego problemu wraz z uzasadnieniem dokonanych wyborów; projekt opracowywanego systemu/zadania wraz z opisem zastosowanych technik oraz narzędzi; przygotowanie dokumentacji projektowej, która w sposób szczegółowy opisuje wykonany projekt wraz z założeniami projektowymi – dokumentacja przygotowywana jest samodzielnie przez zespół realizujący projekt; opis sposobu implementacji opracowanego rozwiązania wraz z instrukcją obsługi; analizę dalszych możliwości rozwoju przygotowanego rozwiązania, prezentacja opracowanego rozwiązania.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X			
W02			X			
W03			X			
U01			X	X		
U02			X	X		
U03			X	X		
K01				X		
K02				X		

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium zaliczeniowego.
laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium.
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z wykonanego projektu.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednos tka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30		15	15		18		9	9		
2.	Inne (konsultacje, egzamin)	2		2	2		2		2	2		h

3.	Razem przy bezpośrednim udziale nauczyciela akademickiego	66	42	h
4.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	2,64	1,68	ECTS
5.	Liczba godzin samodzielnej pracy studenta	9	33	h
6.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	0,36	1,32	ECTS
7.	Nakład pracy związany z zajęciami o charakterze praktycznym	30	18	h
8.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	1,2	0,72	ECTS
9.	Sumaryczne obciążenie pracą studenta	75	75	h
10.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	3		ECTS

LITERATURA

1. Chris Dotson, **Practical Cloud Security: A Guide for Secure Design and Deployment**, 2019
2. Eyal Estrin, **Cloud Security Handbook**, 2022.
3. Ronald L. Krutz, Russell Dean Vines, **Cloud Security: A Comprehensive Guide to Secure Cloud Computing**, 2010.