



KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	Z-ZB-506b
	studia niestacjonarne:	Z-ZBN-506b
Nazwa przedmiotu	Bezpieczeństwo cyfrowe	
Nazwa przedmiotu w języku angielskim	Digital security	
Obowiązuje od roku akademickiego	2026/2027	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	ZARZĄDZANIE BIZNESOWE
Poziom kształcenia	I stopień
Profil studiów	Ogólnoakademicki
Forma i tryb prowadzenia studiów	Studia stacjonarne i niestacjonarne
Zakres	E-commerce
Jednostka prowadząca przedmiot	Katedra Zarządzania i Organizacji
Koordinator przedmiotu	mgr inż. Artur Tusień
Zatwierdził	dr hab. inż. Dariusz Bojczuk, prof. PŚK

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		Przedmiot specjalnościowy
Status przedmiotu		Obowiązkowy
Język prowadzenia zajęć		Polski
Usytuowanie w planie studiów - semestr	studia stacjonarne	Semestr V
	studia niestacjonarne	Semestr V
Wymagania wstępne		Wiedza z zakresu technologii informacyjnych
Egzamin (TAK/NIE)		NIE
Liczba punktów ECTS		1

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

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Ma wiedzę z zakresu bezpiecznego przechowywania, przetwarzania informacji i danych, kontroli danych oraz ich prywatności.	ZB1_W03 ZB1_W08
	W02	Ma wiedzę z zakresu rozpoznawania zagrożeń ze strony złośliwego oprogramowania i skutecznej ochrony przed nim.	ZB1_W03 ZB1_W08
	W03	Ma wiedzę na temat sposobów ochrony sieci komputerowych, ochrony komputera i urządzeń pracujących w sieci.	ZB1_W03 ZB1_W08
	W04	Ma wiedzę na temat zagadnień bezpieczeństwa przy korzystaniu z hasła, poczty elektronicznej, sieci społecznościowych, telefonii VoIP, komunikatorów i urządzeń mobilnych.	ZB1_W03 ZB1_W08
Umiejętności	U01	Posiada umiejętności w zakresie rozpoznawania zagrożeń bezpieczeństwa w zakresie kradzieży tożsamości, zagrożeń dla danych wynikających z użycia ich w sieci, w tym przetwarzania w chmurze.	ZB1_U05 ZB1_U10
	U02	Posiada umiejętności identyfikacji ataków złośliwego oprogramowania.	ZB1_U05 ZB1_U10
	U03	Posiada umiejętność bezpiecznego używania przeglądarek internetowych i ich ustawień, potwierdzania tożsamości stron internetowych i bezpiecznego korzystania z internetowych serwisów sieciowych.	ZB1_U05 ZB1_U10
	U04	Posiada umiejętności dotyczące archiwizowania i przywracania plików lokalnie i w chmurze oraz trwałego usuwania danych.	ZB1_U05 ZB1_U10
Kompetencje społeczne	K01	Ma świadomość działań dotyczących ochrony środowiska w aspekcie zarządzania i oszczędzania energii oraz wpływu technologii informacyjnych na środowisko naturalne.	ZB1_K05
	K02	Rozumie zasady netykiety i poprawnych zachowań w trakcie używania serwisów społecznościowych i pracy grupowej w sieci.	ZB1_K03

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	Bezpieczeństwo: zagrożenia dla danych, wartość informacji, bezpieczeństwo osobiste, bezpieczeństwo plików. Złośliwe oprogramowanie: typy złośliwego oprogramowania i metody jego działania, ochrona przed złośliwym oprogramowaniem, rozwiązywanie problemów wynikających z działania złośliwego oprogramowania oraz metody jego usuwania. Bezpieczeństwo w sieci i połączenia sieciowe, sieci bezprzewodowe. Kontrola dostępu: metody kontroli dostępu, zarządzanie hasłami. Bezpieczeństwo użycia technologii WWW: ustawienia przeglądarki internetowej, bezpieczeństwo przeglądania zasobów internetowych, Komunikacja: używanie poczty elektronicznej (w tym szyfrowanie), sieci społecznościowe, technologia VoIP, komunikatory internetowe, tele- i videokonferencje, urządzenia mobilne. Bezpieczne zarządzanie danymi: zabezpieczenie i archiwizacja danych, bezpieczne usuwanie i niszczenie danych. Ochrona środowiska: oszczędzanie energii, świadomość wpływu technologii komputerowych na środowisko naturalne. Treści programowe są zgodne z międzynarodowym certyfikatem ECDL – IT Security. Po zakończeniu kształcenia student jest przygotowany do uzyskania w/w certyfikatu.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne (obserwacja)
W01			X			
W02			X			
W03			X			
W04			X			
U01			X			
U02			X			
U03			X			
U04			X			
K01						X
K02						X

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Zaliczenie na poziomie co najmniej 50 % kolokwium semestralnego.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		15					9					
2.	Inne (konsultacje, egzamin)	2					2					h
3.	Razem przy bezpośrednim udziale nauczyciela akademickiego	17					11					h
4.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	0,7					0,4					ECTS
5.	Liczba godzin samodzielnej pracy studenta	8					14					h
6.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	0,3					0,6					ECTS
7.	Nakład pracy związany z zajęciami o charakterze praktycznym	0					0					h
8.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	0,0					0,0					ECTS
9.	Sumaryczne obciążenie pracą studenta	25					25					h
10.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	1										ECTS

LITERATURA

1. Mazur D., Żarnowska – Mazur, A., (2014), *ECDL IT Security*, wyd. PWN, Warszawa.
2. Skórka J., Skórka J., Kaim M., (2020), *Bezpieczeństwo w sieci. Jak skutecznie chronić się przed atakami*, wyd. iTstart, Piekary Śląskie.