



KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	Z-IZPJ1-U-522
	studia niestacjonarne:	Z-IZPJN1-U-522
Nazwa przedmiotu	Cyberbezpieczeństwo w sektorze przemysłowym	
Nazwa przedmiotu w języku angielskim	Cybersecurity in the Industrial Sector	
Obowiązuje od roku akademickiego	2026/2027	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	Inżynieria Zarządzania Produkcją i Jakością
Poziom kształcenia	I stopień
Profil studiów	Ogólnoakademicki
Forma i tryb prowadzenia studiów	Studia stacjonarne i niestacjonarne
Zakres	Inżynieria Jakości i Transformacji Cyfrowej
Jednostka prowadząca przedmiot	Katedra Technologii Informatycznych
Koordynator przedmiotu	dr inż. Damian Krzesimowski
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		Podstawy informatyki
Egzamin (TAK/NIE)		Nie
Liczba punktów ECTS		2

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

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student posiada zaawansowaną wiedzę o podstawowych metodach szyfrowania danych, podpisie cyfrowym, certyfikatach i aktualnie stosowanych algorytmach szyfrowania.	IZPJ1_W04
	W02	Student posiada zaawansowaną wiedzę o podstawowych rodzajach możliwych zagrożeń danych w systemach komputerowych przedsiębiorstw oraz podstawowych metodach zabezpieczeń danych.	IZPJ1_W04
	W03	Student posiada zaawansowaną wiedzę w zakresie bezpiecznych protokołów sieciowych oraz konfiguracji i diagnostyki sieci komputerowej pod kątem bezpieczeństwa.	IZPJ1_W04 IZPJ1_W06
Umiejętności	U01	Student potrafi zaprogramować podstawowe algorytmy szyfrowania danych oraz odszyfrować wiadomości na podstawie wskazówek ogólnych.	IZPJ1_U05
	U02	Student potrafi skonfigurować sieć komputerową oraz użyć narzędzi diagnostycznych do analizy zagrożeń w istniejącej sieci komputerowej.	IZPJ1_U02 IZPJ1_U05
	U03	Student potrafi wykonać wstępny audyt bezpieczeństwa danych w oparciu o istniejące przepisy prawne oraz dobre praktyki.	IZPJ1_U01 IZPJ1_U05
Kompetencje społeczne	K01	Student rozumie potrzebę uzupełniania i doskonalenia nabytej wiedzy i umiejętności z zakresu bezpieczeństwa danych.	IZPJ1_K01

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	Podstawowe pojęcia bezpieczeństwa danych w sektorze przemysłowym. Zarządzanie bezpieczeństwem i ryzykiem w systemach ICS. Etyka komputerowa i aspekty prawne bezpieczeństwa danych, transmisji i systemów informatycznych. Teoria informacji, metody łamania szyfrów, analiza szyfrogramów. Szyfrowanie przedstawieniowe i podstawieniowe – wybrane algorytmy. Metody uwierzytelniania, algorytm DES, algorytm AES, algorytm IDEA, podpis cyfrowy. Zapory sieciowe, usługi Proxy, usługi dostępu zdalnego. Detekcja intruzów, testy penetracyjne, techniki skanowania, podstawy audytu cyberbezpieczeństwa.
laboratorium	Klasyczne systemy kryptograficzne z narzędzia do szyfrowania, deszyfrowania oraz analizy kryptograficznej: szyfr Cezara, szyfr ROT-13, przesunięty szyfr rozrzedzony, szyfr cmentarny, szyfr Vigenere'a, szyfr homofoniczny, szyfr Beaufort'a, szyfrowanie XOR. Projektowanie sieci komputerowej z uwzględnieniem scenariuszy zagrożeń bezpieczeństwa i integracji danych oraz niezawodności komunikacji. Analiza istniejącej sieci komputerowej z wykorzystaniem narzędzi do skanowania i testów bezpieczeństwa. Przeprowadzenie elementarnego audytu bezpieczeństwa zgodnie z obowiązującymi przepisami i dobrymi praktykami.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

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

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie pozytywnej oceny z pracy pisemnej opisowej dotyczącej cyberbezpieczeństwa.
laboratorium	zaliczenie z oceną	Ocena końcowa będzie obliczona jako suma ocen częściowych uzyskanych z zadań i sprawozdań wykonywanych w ramach zajęć laboratoryjnych.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jed- nostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		15		15			9		9			
2.	Inne (konsultacje, egzamin)	2		2			2		2			h
3.	Razem przy bezpośrednim udziale nauczyciela akademickiego	34					22					h
4.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	1,4					0,9					ECTS
5.	Liczba godzin samodzielnej pracy studenta	16					28					h
6.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	0,6					1,1					ECTS
7.	Nakład pracy związany z zajęciami o charakterze praktycznym	25					25					h
8.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	1,0					1,0					ECTS
9.	Sumaryczne obciążenie pracą studenta	50					50					h
10.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	2										ECTS

LITERATURA

1. Wołowski F., Zawila-Niedźwiecki J., (2022), *Bezpieczeństwo systemów informacyjnych*, edu-Libri, Kraków
2. Kim P., (2015), *Podręcznik pentestera. Bezpieczeństwo systemów informatycznych*, Helion, Gliwice
3. Costa-Gazcón V., (2022), *Aktywne wykrywanie zagrożeń w systemach IT w praktyce*, Helion, Gliwice
4. Lidermann K., (2017), *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa
5. Stinson Douglas R., Paterson Maura B., (2021), *Kryptografia w teorii i praktyce*, PWN, Warszawa
6. Karbowski M., (2021), *Podstawy kryptografii*, Helion, Gliwice