

KARTA KURSU

Nazwa	Standaryzacja systemów cyberbezpieczeństwa
Nazwa w j. ang.	Standardization of security systems

Koordinator	mgr Wojciech Baran	Zespół dydaktyczny
		mgr Wojciech Baran
Punktacja ECTS*	st. stacjonarne: 2 st. niestacjonarne: 2	

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów ze standardami i normami obowiązującymi przy wdrażaniu, utrzymaniu i rozwijaniu zintegrowanych systemów bezpieczeństwa.

Warunki wstępneWiedza	<p>Student powinien posiadać podstawową wiedzę z zakresu cyberbezpieczeństwa, w tym dotyczącą:</p> <ul style="list-style-type: none"> • Podstawowych norm i standardów bezpieczeństwa informacyjnego (np. ISO 27001), • Procesów zarządzania ryzykiem w organizacjach, • Zasad wdrażania i monitorowania polityk bezpieczeństwa, • Aktualnych zagrożeń cybernetycznych oraz metod ich przeciwdziałania.
Umiejętności	<p>Student powinien być zdolny do:</p> <ul style="list-style-type: none"> • Identyfikowania zagrożeń i analizowania ryzyka w zakresie bezpieczeństwa systemów informacyjnych, • Posługiwania się narzędziami do zarządzania bezpieczeństwem informacji, • Opracowywania i wdrażania procedur oraz polityk bezpieczeństwa w organizacji, • Pracy zespołowej w zakresie standaryzacji i audytów bezpieczeństwa, • Korzystania z dokumentacji normatywnej oraz stosowania dobrych praktyk branżowych.
Kursy	<p>Zalecane wcześniejsze kursy lub kompetencje:</p> <ul style="list-style-type: none"> • Podstawy zarządzania bezpieczeństwem informacji, • Podstawy kryptografii i ochrony danych, • Audyt i analiza ryzyka w cyberbezpieczeństwie, • Podstawy sieci komputerowych i ich zabezpieczeń.

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów (określonych w karcie programu studiów)
Wiedza	Po zakończeniu kursu student:	
	W01: Zna kluczowe standardy i normy dotyczące cyberbezpieczeństwa, w tym PN-EN ISO/IEC 27001 oraz inne międzynarodowe regulacje dotyczące ochrony informacji.	K_W07, K_W10, K_W12
	W02: Rozumie procesy i struktury związane z wdrażaniem systemów bezpieczeństwa w organizacjach oraz ich znaczenie dla funkcjonowania instytucji publicznych i prywatnych.	K_W07, K_W10, K_W12
	W03: Posiada wiedzę na temat metod zarządzania ryzykiem, w tym analizy zagrożeń i oceny skuteczności mechanizmów ochrony.	K_W07, K_W10, K_W12
	W04: Zna podstawowe narzędzia wykorzystywane w audytach bezpieczeństwa oraz sposoby monitorowania zgodności z obowiązującymi normami.	K_W07, K_W10, K_W12

	Efekt uczenia się dla kursu	Odniesienie do efektów (określonych w karcie programu studiów)
Umiejętności	Po zakończeniu kursu student:	
	U01: Potrafi analizować i interpretować normy bezpieczeństwa w kontekście praktycznego zastosowania w organizacjach.	K_U05, K_U14
	U02: Umie przeprowadzać ocenę ryzyka oraz proponować adekwatne środki zabezpieczające w systemach informacyjnych.	K_U05, K_U14
	U03: Potrafi opracować politykę bezpieczeństwa zgodną z obowiązującymi standardami oraz wdrażać ją w praktyce.	K_U05, K_U14
	U04: Umie pracować w zespołach projektowych zajmujących się cyberbezpieczeństwem, przygotowując raporty i rekomendacje zgodnie z wymaganiami branżowymi.	K_U05
	U05: Potrafi efektywnie komunikować się w kontekście zagadnień cyberbezpieczeństwa, także w języku obcym, stosując terminologię fachową.	K_U05, K_U14

	Efekt uczenia się dla kursu	Odniesienie do efektów (określonych w karcie programu studiów)
Kompetencje społeczne	Po zakończeniu kursu student:	
	K01: Rozumie znaczenie ciągłego doskonalenia wiedzy w obszarze cyberbezpieczeństwa oraz śledzenia nowych zagrożeń i technologii.	K_K02
	K02: Potrafi krytycznie ocenić poziom własnych kompetencji i podejmować działania w celu ich rozwoju.	K_K02
	K03: Ma świadomość odpowiedzialności związanej z zarządzaniem bezpieczeństwem informacji oraz konsekwencji naruszenia zasad ochrony danych.	K_K02

Studia stacjonarne

Organizacja												
Forma zajęć	Wykład (W)	Ćwiczenia w grupach										
		A		K		L		S		P		E
Liczba godzin		25										

Studia niestacjonarne

Organizacja													
Forma zajęć	Wykład (W)	Ćwiczenia w grupach											
		A		K		L		S		P		E	
Liczba godzin		15											

Opis metod prowadzenia zajęć

Zajęcia audytoryjne

Zadaniem studenta jest zapoznanie się z normą PN-EN ISO/IEC 27001 dotyczącą Systemu Zarządzania Bezpieczeństwem Informacji oraz przykładowym jej zastosowaniem w wybranym podmiocie.

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01						X		X					
W02						X		X					
W03						X		X					
W04						X		X					
W05						X		X					
U01						X		X					
U02						X		X					
U03						X		X					
U04						X		X					
U05						X		X					
K01						X		X					
K02						X		X					
K03						X		X					

Kryteria oceny

Na ocenę 5: Zaliczenie projektu na 90% + kolokwium zaliczeniowe na 90%
 Na ocenę 4,5: Zaliczenie projektu na 80% + kolokwium zaliczeniowe na 80%
 Na ocenę 4: Zaliczenie projektu na 70% + kolokwium zaliczeniowe na 70%
 Na ocenę 3,5: Zaliczenie projektu na 60% + kolokwium zaliczeniowe na 60%
 Na ocenę 3: Zaliczenie projektu na 50% + kolokwium zaliczeniowe na 50%

Uwagi

Treści merytoryczne (wykaz tematów)

1. Wprowadzenie do metodologii związanej ze standaryzacją.
2. Instytucje, organizacje, certyfikaty – lista, zasady działania, zakresy.
3. Wprowadzenie do normy ISO 27001.
4. Szacowanie ryzyka.
5. Metody ciągłego udoskonalania.

Wykaz literatury podstawowej

1. Norma ISO 27001 wersja polska
2. *ISO 27001 Controls*, Bridget Kenyon, IT Governance Publishing Ltd 2019
3. *Systemy i usługi informatyczne. Cykl życia, procesy i zarządzanie w normach ISO*, Bilski E., Kosmulska-Bochenek E., Oficyna Wydawnicza Politechniki Wrocławskiej 2009

Wykaz literatury uzupełniającej

1. *Zakładowa kontrola produkcji a norma ISO 9001 - wydanie II*, Artur Preus; Wiedza i Praktyka 2015
2. *Zarządzanie jakością podstawy, systemy i narzędzia*; Wawak St; One Press 2011

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) - studia stacjonarne

Liczba godzin w kontakcie z prowadzącymi	Wykład	
	Konwersatorium (ćwiczenia, laboratorium itd.)	25
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	5
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) - studia niestacjonarne

Liczba godzin w kontakcie z prowadzącymi	Wykład	
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	20
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	5
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2