"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Bezpieczeństwo systemów informacyjnych	Information systems security
Kod przedmiotu	WCYILWSM_.....	
Język wykładowy	polski	
Profil studiów	ogólnoakademicki	
Forma studiów	studia stacjonarne	
Poziom studiów	wojskowe studia jednolite magisterskie	
Rodzaj przedmiotu	obowiązkowy	
Obowiązuje od naboru	2021/2022	

Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS

semestr	(x egzamin, + zaliczenie, # projekt)						punkty ECTS
	razem	wykłady	ćwiczenia	laboratoria	projekt	seminarium	
VIII	30+	12	8+	10+			4.0
razem		12	8	10			4.0

Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających
Semestr/kierunek studiów	semestr 8 / Informatyka / Inżynieria systemów - systemy informatyczne
Autor	dr inż. Jerzy Stanik
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki/Instytut Systemów informatycznych/Zakład Informatycznych Systemów Zarządzania
Skrócony opis przedmiotu	• Wykład / metody dydaktyczne: Wykłady prowadzone są następującymi metodami: Metody oparte na słowie - wykład informacyjny - przekazywanie informacji i wiedzy w sposób usystematyzowany; wykład problemowy z wykorzystaniem prezentacji multimedialnych; Metody praktyczne - uczenie się przez działanie; pokaz z objaśnieniem, ćwiczenia przedmiotowe, ćwiczenia rachunkowe; Metody aktywizujące - burza mózgów (polega na zespołowym wytwarzaniu pomysłów rozwiązania jakiegoś zadania poprzez podanie jak największej ilości możliwości rozwiązań, po czym są one oceniane i weryfikowane), Metody pracy z normami i standardami - Zapoznanie się z podstawowymi zapisami w normach, Metody samodzielnego dochodzenia do wiedzy - samodzielne studiowanie materiałów dostępnych w literaturze, normach i/lub Internecie. • Ćwiczenia / metody dydaktyczne: Ćwiczenia realizowane są w formie kierowanej dyskusji poprzedzonej referatami, analizy przypadku i projektu, oraz ćwiczeń praktycznych.

Pełny opis przedmiotu (treści programowe)

lp.	Semestr VIII temat/tematyka zajęć	liczba godzin				
		wkł.	ćw.	lab.	prj.	sem.
1	Organizacja w ujęciu procesowym (procesy biznesowe, procesy informacyjne, procesy przetwarzania danych).Bezpieczeństwo procesów informacyjnych oraz bezpieczeństwo informacji.	1	1			
2	Wybrane modele bezpieczeństwa zasobów informacyjnych (Modele zorientowane na utratę atrybutów bezpieczeństwa, Modele zorientowane na zmiany wartości atrybutów bezpieczeństwa, Modele bazujące na praktykach i zasadach podejścia opartego na ryzyku, Modele oparte o kryteria oceny jakości funkcjonowania podmiotu działania lub jego systemów informatycznych, Modele bazujące na składowych/ charakterystykach w odniesieniu do wyróżnionych obszarów/ czynników ryzyka, inne modele np.: radarowy, wektorowy)	1	1			
3	Pojęcie ryzyka w świetle różnych standardów zgodności (ISO 31000, NIST, ISO 27001, inne standardy lub dyrektywy). Uogólniony model matematyczny ryzyka oraz jego odmiany z punktu widzenia charakterystyki kryterium (kryteria tabelaryczne, kryteria wzmacniacze, kryteria probabilistyczne)	2	1			
4	Modele cyklu zarządzania ryzykiem lub bezpieczeństwem informacji (NIST, ISO 27001, ISO 22301, RODO, NIST 2)	2	1			
5	Narzędzia o charakterze aplikacji/oprogramowania z komponentami sztucznej Inteligencji (AI) wspomagające prowadzenie projektów ISO 27001ISO 22301 lub NIST oraz usprawniające ścieżkę do certyfikacji ISO (CONFORMIO, EXSPERTA AI, CYBERCOMPLY, ISMS ONLINE, PROACTIVE QMS, VANTA, IT GOVERNANCE)	2	1	2		
6	Implementacja SZBI zgodnie z wybranym modelem zarzadzania bezpieczeństwem informacji lub standardem zgodności - wybrane elementy. Implementacja SZCD zgodnie z standardem zgodności	2	2	6		

	lp.	Semestr VIII temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
		ISO 22301 - wybrane elementy					
	7	Dokumentacja bezpieczeństwa informacji: dokumentacja obowiązkowa, dokumentacja uzupełniająca, zapisy i dowody z przeprowadzonych audytów	2	1	2		
		Razem	12	8	10		

Literatura

podstawowa:

- Andress J., Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie (ebook), Helion 2018
- Liderman K., (2017), Bezpieczeństwo informacyjne, Wydawnictwo Naukowe PWN Warszawa, 2017
- Rojszczak M. (2019), Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Wolters Kluwer Polska
- Standardy opracowane przez NIST • NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych - na podstawie FIPS 200. • NSC 800-30, Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne - na podstawie NIST SP 800-30. • NSC 800-37, Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu - na podstawie NIST SP 800-37 • NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego - na podstawie NIST SP 800-39.
- Normy serii ISO ISO/IEC 27001 - Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji - Wymagania ISO 22301:2019 Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania - Wymagania.
- Dyrektywa (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii"

uzupełniająca:

- Normy pomocnicze do ISO 27001 1. Norma ISO/IEC 27000 zawiera terminy i definicje stosowane w serii norm ISO 27k. 2. ISO/IEC 27002 zawiera wytyczne dotyczące wdrażania kontroli wymienionych w załączniku A do normy ISO 27001. 3. ISO/IEC 27004 zawiera wytyczne dotyczące pomiaru bezpieczeństwa informacji - dobrze pasuje do ISO 27001, ponieważ wyjaśnia, jak określić, czy SZBI osiągnął swoje cele. 4. ISO/IEC 27005 zawiera wytyczne dotyczące zarządzania ryzykiem związanym z bezpieczeństwem informacji. Jest to bardzo dobre uzupełnienie normy ISO 27001, ponieważ zawiera szczegółowe informacje na temat sposobu przeprowadzania oceny ryzyka i postępowania z ryzykiem, co jest prawdopodobnie najtrudniejszym etapem wdrażania. 5. ISO/IEC 27017 zawiera wytyczne dotyczące bezpieczeństwa informacji w środowiskach chmurowych. 6. ISO/IEC 27018 zawiera wytyczne dotyczące ochrony prywatności w środowiskach chmurowych. 7. Norma ISO/IEC 27031 zawiera wytyczne dotyczące tego, co należy wziąć pod uwagę przy opracowywaniu ciągłości działania w zakresie technologii informacyjno-komunikacyjnych (ICT). Norma ta stanowi doskonałe ogniwo łączące bezpieczeństwo informacji z praktykami ciągłości działania.
- Standardy pomocnicze opracowane przez NIST • NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji - na podstawie NIST SP 800-53. • NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny - na podstawie NIST SP 800-53A. • NSC 800-53B, Zabezpieczenia bazowe systemów informacyjnych oraz organizacji - na podstawie NIST SP 800-53B. • NSC 800-60, Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego - na podstawie NIST SP 800-60. • NSC 800-61, Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego - na podstawie NIST SP 800-61. • NSC 800-210, Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej - na podstawie NIST SP 800-210.
- UOODO, Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych - ISAP UOOIN, Ustawa o ochronie informacji niejawnych

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
W1	zna i rozumie w zaawansowanym stopniu modele, metody, metodyki oraz narzędzia do wytwarzania (analizy, projektowania i implementacji) systemów informatycznych (początkowe etapy cyklu życia systemów)	K_W08, K_W03
W2	zna i rozumie pojęcia, opisy, wybrane fakty i zjawiska w zakresie bezpieczeństwa informacyjnego oraz metody badań i przykłady implementacji w obszarze bezpieczeństwa systemów teleinformatycznych	K_W04, K_W10
W3	zna i rozumie w zaawansowanym stopniu informatyczne metody i narzędzia służące do modelowania i wspomagania procesów zarządzania organizacją oraz ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości	K_W05
U1	potrafi wykorzystywać informatyczne metody i narzędzia do modelowania i wspomagania procesów zarządzania	K_U10
U2	potrafi samodzielnie planować i realizować własne permanentne uczenie się, pozyskiwać informacje z literatury, baz danych i innych źródeł, dokonywać syntezy i analizy tych informacji	K_U10
K1	jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz do krytycznej oceny posiadanej wiedzy	K_K01

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
	K2	jest gotów do odpowiedzialnego pełnienia ról zawodowych, w tym: – przestrzegania zasad etyki zawodowej i wymagania tego od innych, – dbałości o dorobek i tradycje zawodu	K_K01

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)

- Przedmiot zaliczany jest na podstawie zaliczenia na ocenę; Zaliczenie przedmiotu przeprowadzane jest: w formie pisemnej; Warunkiem dopuszczenia do zaliczenia przedmiotu jest :zaliczenie ćwiczeń; Ćwiczenia zaliczane są na podstawie: oceny dwóch zapowiedzianych kolokwiów pisemnych (jedno z procesu analizy ryzyka w bezpieczeństwie informacji, drugie ze znajomości ustaw, norm i standardów bezpieczeństwa informacji) oraz oceny pracy studenta na zajęciach efekt W1, W2 - sprawdzane są podczas zaliczania przedmiotu; efekty U1-U5 oraz K1 sprawdzane są na ćwiczeniach poprzez: niezapowiedziane kartkówki sprawdzające stopień przygotowania studentów do zajęć, jak również na podstawie ustnych odpowiedzi studentów; analizę i ocenę bieżących wyników z realizacji postawionych zadań rachunkowych; analizę prezentacji oraz efektów prac projektowych realizowanych w grupie, w tym skutków z nich płynących.
- Ocenę bardzo dobrą otrzymuje student, który zaliczył ćwiczenia i laboratoria co najmniej na ocenę dobry plus. Ocenę dobrą plus otrzymuje student, który zaliczył ćwiczenia i laboratoria co najmniej na ocenę dobry.
- Ocenę dobrą otrzymuje student, który zaliczył ćwiczenia i laboratoria co najmniej na dostateczny plus. Ocenę dostateczną plus otrzymuje student, który zaliczył ćwiczenia i laboratoria co najmniej na dostateczny.
- Ocenę dostateczną otrzymuje student, który zaliczył ćwiczenia i laboratoria na dostateczny. Ocenę niedostateczną otrzymuje student, który nie zaliczył ćwiczenia lub laboratoria co najmniej na dostateczny.

Bilans ECTS (nakład pracy studenta)

SEMESTR 8		
Aktywność	**Obciążenie studenta**	
	Liczba godzin	**Liczba ECTS**
Udział w wykładach	12	1
Udział w laboratoriach	10	1
Udział w ćwiczeniach	8	0.5
Udział w projektach	0	0
Udział w seminariach	0	0
Samodzielne studiowanie tematyki wykładów		
Samodzielne przygotowanie do laboratoriów	30	0.5
Samodzielne przygotowanie do ćwiczeń	30	0.5
Samodzielna realizacja projektu		
Samodzielne przygotowanie do seminariów		
Udział w konsultacjach		
Przygotowanie do egzaminu		
Przygotowanie do zaliczenia	20	0.5
Udział w egzaminie / kolokwium		
Sumaryczne obciążenie pracą studenta	110	4
Zajęcia z udziałem nauczycieli	30	2.5
Zajęcia powiązane z działalnością naukową	90	3.5
Zajęcia o charakterze praktycznym	78	2.5

autor

dr inż. Jerzy Stanik
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

dr hab. inż. Nowicki Tadeusz
tytuł, stopień naukowy, imię, NAZWISKO, podpis