

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberbezpieczeństwo, PG_00156502						
Kierunek studiów	Informatyka i ekonometria (O)						
Data rozpoczęcia studiów	październik 2024 r.		Rok akademicki realizacji przedmiotu		2025/2026		
Poziom kształcenia	II stopnia		Grupa zajęć		Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	2		Język wykładowy		polski		
Semestr studiów	4		Liczba punktów ECTS		7.0		
Profil kształcenia	ogólnoakademicki		Forma zaliczenia		egzamin		
Jednostka prowadząca	Rektor -> Wydział Zarządzania -> Katedra Informatyki Ekonomicznej						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr inż. Przemysław Jatkiewicz				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	45.0	0.0	0.0	60
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach		Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	60		30.0		85.0	175
Cel przedmiotu	Zapoznanie studentów z procesami, dobrymi praktykami i rozwiązaniami technologicznymi, które ułatwiają ochronę krytycznych systemów i sieci przed atakami cyfrowymi.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[liEMU2_W07] Ma rozszerzoną i ugruntowaną wiedzę o normach etycznych obowiązujących w biznesie, dobrych praktykach jego prowadzenia oraz regulacjach prawnych w zakresie ochrony własności intelektualnej; ma rozszerzoną wiedzę dotyczącą ryzyka i odpowiedzialności związanej z informatyzacją procesów gospodarczych, zna zasady netykiety.	Zna prawne i etyczne uwarunkowania testowania systemów informatycznych.	[SW4] test/exam - oral or written
	[liEMU2_U04] Potrafi na poziomie zaawansowanym planować, projektować i programować systemy informatyczne, wspierające funkcjonowanie podmiotów gospodarczych.	Potrafi wdrożyć odpowiednie zabezpieczenia dla wskazanych podatności.	[SU5] implementation of a problem task
	[liEMU2_U08] Potrafi analizować potrzeby biznesowe i, stosownie do potrzeb, konfigurować i stosować nowoczesne technologie informacyjno-telekomunikacyjne w procesie zarządzania przedsiębiorstwem i komunikacji biznesowej.	Potrafi analizować potrzeby biznesowe i, stosownie do potrzeb, konfigurować i stosować nowoczesne technologie informacyjno-telekomunikacyjne w procesie zarządzania przedsiębiorstwem i komunikacji biznesowej. Potrafi dobrać odpowiednie zabezpieczenia dla wskazanych podatności.	[SU5] implementation of a problem task
	[liEMU2_K02] Potrafi swobodnie komunikować się z otoczeniem na specjalistyczne tematy z zakresu informatyki i ekonometrii w miejscu pracy i poza nim, przekazywać swoją wiedzę oraz dzielić się swoimi umiejętnościami za pomocą różnych środków przekazu. Kulturalnie uczestniczy w dyskusji, nie boi się zadawać pytań i umie wyrażać konstruktywną krytykę.	Zna i potrafi korzystać z kanałów komunikacyjnych dedykowanych zgłaszaniu incydentów cyberbezpieczeństwa.	[SK5] implementation of a problem task
	[liEMU2_W05] Ma pogłębioną wiedzę o źródłach danych społeczno-ekonomicznych, ich bazach oraz sposobie ich tworzenia.	Zna zagrożenia systemów informatycznych i ich wpływ na przedsiębiorstwo i społeczeństwo.	[SW4] test/exam - oral or written
	[liEMU2_K05] Potrafi myśleć i działać w sposób przedsiębiorczy oraz elastycznie dostosowywać się do zmieniających się warunków otoczenia. Myśli kreatywnie i potrafi wyjść poza utarte schematy.	Jest świadomy zagrożeń związanych z poruszaniem się w cyberprzestrzeni	[SK5] implementation of a problem task

Treści przedmiotu	Przepisy, normy, dobre praktyki związane z cyberbezpieczeństwem.		
	Ochrona danych osobowych		
	Zagrożenia i podatności systemów informatycznych		
	Bezpieczeństwo fizyczne serwerów		
	Szkodliwe oprogramowanie		
	Audyt, kontrola, testy, sprawdzenia		
	Metodyki analizy ryzyka		
	Kryptografia		
	Zapoznanie studentów z zasadami ochrony serwerów typu LAMP (Linux, Apache, Mysql, PHP).		
	Identyfikacja. uwierzytelnianie, autoryzacja.		
	Ochrona serwera przed złośliwym oprogramowanie		
	Planowanie i przygotowanie audytu, przeprowadzenie audytu, czynności poaudytowe		
	Narzędzia wspomagające audyt		
	Prowadzenie analizy ryzyka		
	Wymagania wstępne i dodatkowe	Brak	
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	test/egzamin - ustny lub pisemny	51.0%	50.0%
	realizacja zadania problemowego	51.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	Jatkiewicz ,Security of information systems of companies and institutions UG 2020 R.R. Moeller, IT audit, control, and security John Wiley & Sons 2010	
	Uzupełniająca lista lektur	E. Nemeth, G. Snyder, T. Hein, B. Whaley, UNIX and Linux System Administration Handbook, Pearson Education 2017	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Zabezpiecz wskazaną aplikację przed atakiem sqlinjection		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.