Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Cybersecurity, PG_00156476						
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		angielski		
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
	[IiEMU2_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
	[IiEMU2_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 uwarunbkowania testowania systemów informatycznych.	[SW4] test/exam - oral or written
	[IiEMU2_U08] 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 zabezpiecenia dla wskazanych podatności.	[SU5] implementation of a problem task
	[IiEMU2_K03] Potrafi swobodnie komunikować się z otoczeniem w miejscu pracy i poza nim, przekazywać swoją wiedzę oraz dzielić się swoimi umiejętnościami za pomocą różnych środków przekazu.	Zna i potrafi korzystać z kanałów komunikacyjnych dedykowanych zgłaszaniu incydentów cyberbezpieczeństwa.	[SK5] implementation of a problem task
	[IiEMU2_U04] Potrafi na poziomie zaawansowanym planować, projektować i programować systemy informatyczne, wspierające funkcjonowanie podmiotów gospodarczych.	Potrafi wdrożyć odpowiednie zabezpiecenia dla wskazanych podatności	[SU5] implementation of a problem task
	[IiEMU2_K06] Ma świadomość konieczności etycznego, zrównoważonego i społecznie odpowiedzialnego zachowywania się w życiu zawodowym i społecznym. Inicjuje i organizuje działalność na rzecz środowiska społecznego i interesu publicznego.	Jest świadomy zagrożeń związanych z poruszaniem się w cyberprzestrzeni.	[SK5] implementation of a problem task

<table>
<tr><td>Treści przedmiotu</td><td>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</td></tr>
<tr><td>Wymagania wstępne i dodatkowe</td><td>Brak</td></tr>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td>
<table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>realizacja zadania problemowego</td><td>51.0%</td><td>50.0%</td></tr>
<tr><td>test/egzamin - ustny lub pisemny</td><td>51.0%</td><td>50.0%</td></tr>
</table>
</td></tr>
<tr><td>Zalecana lista lektur</td><td>
<table>
<tr><td>Podstawowa lista lektur</td><td>P. Jatkiewicz ,Security of information systems of companies and institutions UG 2020

R.R. Moeller, IT audit, control, and security John Wiley & Sons 2010</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>E. Nemeth, G. Snyder, T. Hein, B. Whaley, UNIX and Linux System Administration Handbook, Pearson Education 2017</td></tr>
<tr><td>Adresy eZasobów</td><td></td></tr>
</table>
</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td>Zabezpiecz wskazaną aplikację przed atakiem sqlinjection</td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td>Nie dotyczy</td></tr>
</table>

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.