Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberbezpieczeństwo, PG_00178740		
Kierunek studiów	Informatyka i ekonometria (O)		
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu	2027/2028
Poziom kształcenia	II stopnia	Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki
Forma studiów	niestacjonarne	Sposób realizacji	na uczelni
Rok studiów	2	Język wykładowy	polski
Semestr studiów	4	Liczba punktów ECTS	6.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	egzamin
Jednostka prowadząca			
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	8.0	0.0	24.0	0.0	0.0	32
	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	32	2.0	116.0	150

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_K02] Student jest gotów do odpowiedzialnego pełnienia ról zawodowych, przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz ich przestrzegania, a także do dbałości o rozwój dorobku oraz podtrzymywanie etosu i tradycji zawodów związanych z ekonometrią, informatyką lub statystyką.	Student jest gotów do pełnienia ról Inspektora Ochrony Danych Osobowych, Specjalisty ds cyberbezpieczeństwa, audytora cyberbezpieczeństwa	[SK4] test/egzamin - ustny lub pisemny
	[IiEMU2_U05] Student potrafi identyfikować oraz poprawnie stosować normy prawne, zawodowe i etyczne w kontekście obszaru nauk o zarządzaniu i jakości oraz ekonomii i finansów.	Student potrafi przeprowadzić analizę ryzyka, zaplanować audyt, opracować Politykę bezpieczeństwa informacji.	[SU6] demonstracja umiejętności praktycznych
	[IiEMU2_U12] Student potrafi przystosowywać, projektować lub tworzyć oraz eksploatować systemy informatyczne, wspierające funkcjonowanie podmiotów gospodarczych.	Student potrafi zabezpieczzać systemy operacyjne i usługi sieciowe.	[SU5] realizacja zadania problemowego
	[IiEMU2_W07] Student w pogłębionym stopniu zna i rozumie regulacje oraz normy prawne, organizacyjne i etyczne, w tym dotyczące ochrony własności intelektualnej, istotne w kontekście wykorzystania narzędzi informatycznych.	Student zna normy serii 27000, Dyrektywa NIS, RODO.	[SW4] test/egzamin - ustny lub pisemny

<table>
<tr><td>Treści przedmiotu</td><td>Wykład

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

Ćwiczenia

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>Egzamin pisemny</td><td>51.0%</td><td>50.0%</td></tr>
<tr><td>Zadania problemowe</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, Bezpieczeństwo systemów informatycznych firm, Wydawnictwo UG 2020</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>Molski M., Łacheta M., Przewodnik audytora systemów informatycznych, Helion 2006

E. Nemeth, G. Snyder, T. Hein, B. Whaley, Unix i Linux Przewodnik administratora systemów, Helion 2023</td></tr>
<tr><td>Adresy eZasobów</td><td></td></tr>
</table>
</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td>Podaj różnice pomiędzy szyfrowaniem symetrycznym, asymetrycznym i funkcją skrótu.

Zaimplementuj uwierzytelnianie dwuskładnikowe z wykorzystaniem Google Authenticator.</td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td>Nie dotyczy</td></tr>
</table>

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.