

**Karta przedmiotu**

Nazwa i kod przedmiotu	Cybersecurity, PG_00177468						
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	stacjonarne	Sposób realizacji			na uczelni		
Rok studiów	2	Język wykładowy			angielski		
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 Jatkiwicz				
	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		4.0		86.0	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_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
	[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 zabezpieczać systemy operacyjne i usługi sieciowe.	[SU5] realizacja zadania problemowego

Treści przedmiotu	<p><b>Wykład</b></p> <p>Przepisy, normy, dobre praktyki związane z cyberbezpieczeństwem.</p> <p>Ochrona danych osobowych</p> <p>Zagrożenia i podatności systemów informatycznych</p> <p>Bezpieczeństwo fizyczne serwerów</p> <p>Szkodliwe oprogramowanie</p> <p>Audyt, kontrola, testy, sprawdzenia</p> <p>Metodyki analizy ryzyka</p> <p>Kryptografia</p> <p><b>Ćwiczenia</b></p> <p>Zapoznanie studentów z zasadami ochrony serwerów typu LAMP (Linux, Apache, Mysql, PHP).</p> <p>Identyfikacja. uwierzytelnianie, autoryzacja.</p> <p>Ochrona serwera przed złośliwym oprogramowanie</p> <p>Planowanie i przygotowanie audytu, przeprowadzenie audytu, czynności poaudytowe</p> <p>Narzędzia wspomagające audyt</p> <p>Prowadzenie analizy ryzyka</p>											
Wymagania wstępne i dodatkowe	Brak											
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	<table border="1"> <thead> <tr> <th data-bbox="456 1429 794 1458">Sposób oceniania (składowe)</th> <th data-bbox="799 1429 1137 1458">Próg zaliczeniowy</th> <th data-bbox="1142 1429 1481 1458">Składowa oceny końcowej</th> </tr> </thead> <tbody> <tr> <td data-bbox="456 1464 794 1494">Zadania problemowe</td> <td data-bbox="799 1464 1137 1494">51.0%</td> <td data-bbox="1142 1464 1481 1494">50.0%</td> </tr> <tr> <td data-bbox="456 1500 794 1529">Egzamin pisemny</td> <td data-bbox="799 1500 1137 1529">51.0%</td> <td data-bbox="1142 1500 1481 1529">50.0%</td> </tr> </tbody> </table>			Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej	Zadania problemowe	51.0%	50.0%	Egzamin pisemny	51.0%	50.0%
Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej										
Zadania problemowe	51.0%	50.0%										
Egzamin pisemny	51.0%	50.0%										
Zalecana lista lektur	<table border="1"> <tr> <td data-bbox="456 1541 794 1585">Podstawowa lista lektur</td> <td colspan="2" data-bbox="799 1541 1481 1585"><b>P. Jatkiewicz, Bezpieczeństwo systemów informatycznych firm, Wydawnictwo UG 2020</b></td> </tr> <tr> <td data-bbox="456 1592 794 1827">Uzupełniająca lista lektur</td> <td colspan="2" data-bbox="799 1592 1481 1827"> <b>Molski M., Łacheta M., Przewodnik audytora systemów informatycznych, Helion 2006</b>   <b>E. Nemeth, G. Snyder, T. Hein, B. Whaley, Unix i Linux Przewodnik administratora systemów, Helion 2023</b> </td> </tr> <tr> <td data-bbox="456 1834 794 1832">Adresy eZasobów</td> <td colspan="2" data-bbox="799 1834 1481 1832"></td> </tr> </table>			Podstawowa lista lektur	<b>P. Jatkiewicz, Bezpieczeństwo systemów informatycznych firm, Wydawnictwo UG 2020</b>		Uzupełniająca lista lektur	<b>Molski M., Łacheta M., Przewodnik audytora systemów informatycznych, Helion 2006</b>  <b>E. Nemeth, G. Snyder, T. Hein, B. Whaley, Unix i Linux Przewodnik administratora systemów, Helion 2023</b>		Adresy eZasobów		
Podstawowa lista lektur	<b>P. Jatkiewicz, Bezpieczeństwo systemów informatycznych firm, Wydawnictwo UG 2020</b>											
Uzupełniająca lista lektur	<b>Molski M., Łacheta M., Przewodnik audytora systemów informatycznych, Helion 2006</b>  <b>E. Nemeth, G. Snyder, T. Hein, B. Whaley, Unix i Linux Przewodnik administratora systemów, Helion 2023</b>											
Adresy eZasobów												
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<p>Podaj różnice pomiędzy szyfrowaniem symetrycznym, asymetrycznym i funkcją skrótu.</p> <p>Zaimplementuj uwierzytelnianie dwuskładnikowe z wykorzystaniem Google Authenticator.</p>											
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy											

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.