Politechnika Wrocławska

Program studiów

Wydział:	Wydział Informatyki i Telekomunikacji
Kierunek studiów:	cyberbezpieczeństwo
Poziom kształcenia:	studia drugiego stopnia 3 semestry (magister inżynier)
Forma kształcenia:	studia stacjonarne
Cykl kształcenia:	2025/2026

Spis treści

Charakterystyka kierunku studiów

Informacje podstawowe

Wydział:	Wydział Informatyki i Telekomunikacji
Kierunek studiów:	cyberbezpieczeństwo
Poziom kształcenia:	studia drugiego stopnia 3 semestry (magister inżynier)
Forma studiów:	studia stacjonarne
Profil studiów:	profil ogólnoakademicki
Język prowadzenia studiów:	polski
Obowiązuje od cyklu kształcenia:	2025/2026
Liczba semestrów:	3
Całkowita liczba godzin zajęć:	1035
Całkowita liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:	90
Tytuł zawodowy nadawany absolwentom:	magister inżynier

Dziedziny nauki i dyscypliny naukowe

Dziedziny nauki, do których przyporządkowany jest kierunek studiów:

Dziedzina nauk inżynieryjno-technicznych

Dyscypliny naukowe, do których przyporządkowany jest kierunek studiów:

Dyscyplina	Udział procentowy
informatyka techniczna i telekomunikacja	100%

Dyscyplina wiodąca: informatyka techniczna i telekomunikacja

Opis kierunku, sylwetka absolwenta i możliwości kontynuacji studiów

Absolwent jest przygotowany do pracy przy zabezpieczaniu systemów teleinformatycznych, obejmującej planowanie systemu zabezpieczeń, jego wdrażanie i utrzymywanie w gotowości podczas eksploatacji oraz wprowadzania niezbędnych modyfikacji dostosowujących system zabezpieczeń do występujących i nieustannie ewoluujących zagrożeń. Szczególny nacisk położono na monitorowanie i reakcję na zagrożenia, a także testowanie zabezpieczeń. Kształcenie obejmuje m.in. sposoby tworzenia bezpiecznych usług, przetwarzanie dużych zbiorów informacji (Big Data), w tym metodami sztucznej inteligencji, struktury i działanie centrów przetwarzania danych, bezpieczeństwo w systemach rozproszonych, bezpieczeństwo systemów i sieci, audytowanie sieci teleinformatycznych i bezpieczne usługi internetowe oraz informatykę śledczą. Po ukończeniu studiów istnieje możliwość ubiegania się o przyjęcie do szkoły doktorskiej, studia podyplomowe.

Aktualność programu studiów

Koncepcja i cele kształcenia

Realizując program nauczania, studenci uczęszczają na zajęcia zorganizowane na zasadach zgodnych z Regulaminem studiów wyższych na Politechnice Wrocławskiej. Zajęcia prowadzone są w formach określonych Regulaminem studiów, przy czym wykorzystywane są

zarówno tradycyjne metody i narzędzia dydaktyczne, jak i możliwości oferowane przez uczelnianą platformę e-learningową. Poza godzinami zajęć prowadzący są dostępni dla studentów w wyznaczonych i ogłoszonych na stronie Wydziału godzinach konsultacji. Ważnym elementem uczenia się jest praca własna studenta, polegająca na przygotowywaniu się do zajęć (na podstawie materiałów udostępnianych przez prowadzących, jak i zalecanej literatury), studiowaniu literatury, opracowywaniu raportów i sprawozdań, przygotowywaniu się do kolokwiów i egzaminów. Ma to na celu ugruntowanie świadomości potrzeby samokształcenia. Warto zaznaczyć, że na kierunku Cyberbezpieczeństwo położono nacisk na zajęcia praktyczne. Laboratoria i projekty, w ramach których studenci zdobywają praktyczne umiejętności stanowią większość zajęć zorganizowanych na kierunku.

Pracownicy prowadzący zajęcia dydaktyczne na kierunku często są zaangażowani również w pracę w tzw. biznesie, a także czynione są starania, aby na zajęcia dydaktyczne sprowadzać specjalistów z otoczenia społeczno-gospodarczego, stąd przekazywana wiedza jest bardzo aktualna i zgodna z obecnymi trendami, z którymi studenci spotkają się w przyszłej pracy zawodowej.

Studia na kierunku prowadzone są w oparciu o przedmioty obowiązkowe oraz bloki przedmiotów wybieralnych, które realizując, student może zdecydować o swojej ścieżce kształcenia. Student może wybrać zagadnienia związane z umiejętnościami ofensywnymi np. zaawansowane testy penetracyjne, zastosowanie AI w analizie zagrożeń czy audytowanie infrastruktury IT lub umiejętnościami defensywnymi ochrona systemów operacyjnych, centrów danych, aplikacji web czy informatyka śledcza.

Informacje dotyczące uwzględnienia w programie studiów potrzeb społeczno-gospodarczych oraz zgodności kierunkowych efektów uczenia się z tymi potrzebami

Zakładane efekty uczenia się są zgodne z potrzebami rynku pracy. Takie stanowisko znajduje potwierdzenie w wynikach analiz potrzeb rynku pracy, zawartych np. w Raporcie z II edycji badań: Branża IT w dobie pandemii – "Analiza sytuacji pracodawców, kluczowych trendów rozwojowych i zapotrzebowania na kompetencje" opracowanym w ramach Branżowego Bilansu Kapitału Ludzkiego z lat 2020-2021.

Wyniki analiz potwierdzają bardzo duże zapotrzebowanie na absolwentów kierunku cyberbezpieczeństwo. Jest to kierunek, który znajduje się na czele trendów, które w perspektywie 3-5 lat będą miały największy wpływ na zapotrzebowanie na specjalistów. Prognozy wskazują, że jednym z największych wyzwań będzie zapewnienie odpowiednio wykwalifikowanej kadry, m.in. w obszarze cyberbezpieczeństwa. Dodatkowo kompetencje związane z cyberbezpieczeństwem to kluczowy zasób z perspektywy rozwoju polskich firm IT. Zakładane efekty uczenia się pozwolą na nabycie kompetencji pożądanych przez pracodawców, takich jak np. umiejętność pracy zespołowej. Pozwolą również na uzyskanie preferowanych przez pracodawców umiejętności praktycznych, co zapewnia np. zaliczenie bloków kształcenia specjalistycznego.

Inne istotne czynniki warunkujące aktualność programu studiów

Program studiów został zaktualizowany w ramach realizacji projektu "Cyberbezpieczeństwo dla gospodarki przyszłości" realizowanego w latach 2019-2023.

Związek programu z misją Uczelni i strategią jej rozwoju

Program studiów jest zgodny z misją i strategią uczelni, w szczególności z priorytetowym obszarem badawczym: Technologie informacyjne, nauka o danych i sztuczna inteligencja, określonym w Strategii Politechniki Wrocławskiej na lata 2023-30. Politechnika Wrocławska, jako uczelnia techniczna, prowadzi badania oraz kształci w zakresie nauk technicznych, w które wpisuje się kierunek Cyberbezpieczeństwo. Kierunek zwiększa potencjał uczelni, oferując prestiżowe kształcenie w bardzo aktualnej dziedzinie, podnosząc jej prestiż wśród studentów i kandydatów, a także dąży do ciągłego udoskonalania oferty dydaktycznej. Na kierunku dominują nauki ścisłe, jednakże student nabywa również umiejętności miękkie, co zwiększa jego atrakcyjność na rynku pracy, a to z kolei wzmacnia bezpieczeństwo oraz zwiększa potencjał gospodarczy kraju, co jest również jednym z założeń rozwoju uczelni. Cyberbezpieczeństwo i kryptografia zostały wpisane do strategii Politechniki Wrocławskiej na lata 2023-2030 jako priorytetowe obszary badawcze, ponadto w programie studiów zawarto przedmioty dotyczące między innymi informatyki, telekomunikacji, sieci komputerowych i mobilnych, Internetu Rzeczy, które również zawarto w priorytetowym obszarze badawczym Politechniki "Technologie informacyjne, nauka o danych i sztuczna inteligencja". Stąd kształcenie wysokiej klasy specjalistów w tych obszarach ma kluczowe znaczenie dla przyszłości Politechniki jako wiodącej uczelni technicznej w kraju. Program studiów umożliwia studentom wszechstronny rozwój obejmujący zdobywanie wiedzy i umiejętności związanych z potrzebami społecznymi i globalnymi wyzwaniami w obszarze dyscypliny informatyka techniczna i telekomunikacja.

Efekty uczenia się

Kod	Opis kierunkowego efektu uczenia się	Charakterystyki dla kwalifikacji na poziomie 6 lub 7 PRK	Charakterystyki dla kwalifikacji na poziomie 6 lub 7 PRK, umożliwiające uzyskanie kompetencji inżynierskich
Wiedza			
K2_CBE_W01	Zna typowe zagrożenia występujące w sieciach teleinformatycznych, ma wiedzę o metodach testowania, monitorowania sieci i reagowania na zagrożenia bezpieczeństwa cybernetycznego	P7U_W, P7S_WG	P7S_WG_INŻ
K2_CBE_W02	Ma poszerzoną i pogłębioną wiedzę w zakresie wybranych działów matematyki i fizyki niezbędną do rozumienia zagadnień w zakresie cyberbezpieczeństwa	P7U_W, P7S_WG	
K2_CBE_W03	Ma poszerzoną i pogłębioną wiedzę w zakresie ochrony i bezpieczeństwa infrastruktury oraz usług teleinformatycznych	P7U_W, P7S_WG	
K2_CBE_W04	Zna charakterystykę rynku teleinformatycznego i metodykę realizacji projektów teleinformatycznych	P7U_W, P7S_WK	P7S_WK_INŻ
K2_CBE_W05	Ma aktualną wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w obszarze cyberbezpieczeństwa	P7U_W, P7S_WG	P7S_WG_INŻ
Umiejętności			
K2_CBE_U01	Potrafi skonfigurować i uruchomić narzędzia do monitorowania i testowania ruchu sieciowego oraz identyfikować normalny i nietypowy ruch lub oznaki włamania. Potrafi przeprowadzić testy i audyt bezpieczeństwa sieci	P7U_U, P7S_UW, P7S_UO	P7S_UW_INŻ
K2_CBE_U02	Potrafi posługiwać się metodami matematyki i fizyki do rozwiązywania szczegółowych problemów z zakresu cyberbezpieczeństwa	P7U_U, P7S_UW	
K2_CBE_U03	Potrafi projektować i implementować mechanizmy bezpieczeństwa dla infrastruktury oraz usług teleinformatycznych	P7U_U, P7S_UW, P7S_UO	P7S_UW_INŻ
K2_CBE_U04	Potrafi przygotować biznes plan i elementy zarządzania projektem teleinformatycznym	P7U_U, P7S_UK, P7S_UO	
K2_CBE_U05	Potrafi referować poszczególne fazy realizacji pracy dyplomowej, przygotować prezentację zawierającą wyniki końcowe pracy, uzasadnić wnioski i konkluzje. Zna reguły kreatywnej dyskusji. Potrafi samodzielnie zrealizować dyplomową magisterską zawierającą aspekty badawcze	P7U_U, P7S_UW, P7S_UK, P7S_UU	P7S_UW_INŻ
Kompetencje społeczne			
K2_CBE_K01	Ma świadomość społecznych skutków działalności inżynierskiej i związanej z tym odpowiedzialności za podejmowane decyzje. Rozumie potrzebę przekazywania społeczeństwu informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności absolwenta uczelni technicznej. Rozumie rolę środków masowego przekazu	P7U_K, P7S_KO, P7S_KR	
K2_CBE_K02	Krytycznie ocenia odbierane treści, uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych. Potrafi odpowiednio określić priorytety służące realizacji określonego zadania	P7U_K, P7S_KK	
Efekty językowe			
SJO_S2_U01	Potrafi posługiwać się językiem obcym na poziomie B2+ ESOKJ oraz specjalistyczną terminologią	P7S_UK	

Szczegółowe informacje dotyczące punktów ECTS

cyberbezpieczeństwo

Nazwa	Wartość
Całkowita liczba punktów ECTS	90
Całkowita liczba godzin zajęć	1035
Liczba punktów ECTS przyporządkowana zajęciom związanym z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów (DN)	77/90 (85.56%)
Liczba punktów ECTS przyporządkowana zajęciom kształtującym umiejętności praktyczne (m.in. laboratorium, projekt) (P)	59.2
Liczba punktów ECTS, którą student uzyska realizując zajęcia wymagające bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów (BU)	45.6
Udział procentowy ECTS zajęć wybieralnych	53/90 (58.89%)
Liczba punktów ECTS, którą student uzyska realizując zajęcia z dziedziny nauk humanistycznych lub nauk społecznych właściwych dla danego kierunku studiów	5
Liczba punktów ECTS, którą student uzyska realizując zajęcia z zakresu nauk podstawowych (matematyka, fizyka/chemia)	4

Organizacja studiów

Realizacja programu studiów

Dopuszczalny deficyt ECTS

Semestr	Dopuszczalny deficyt punktów ECTS po semestrze
Semestr 1	8
Semestr 2	8
Semestr 3	0

Wymagania szczegółowe

Nie dotyczy.

Sposoby weryfikacji zakładanych efektów uczenia się

Forma zajęć	Sposoby weryfikacji zakładanych efektów uczenia się
Seminarium	Prezentacje multimedialne prowadzone i przygotowywane indywidualnie lub grupowo; analiza przypadków case study, aktywność na zajęciach, referat
Projekt	Przygotowanie projektu, realizacja projektu, dokumentacja projektowa, analiza przypadków case study, makieta
Praca dyplomowa	Ocena pracy przy przygotowywaniu pracy dyplomowej; egzamin dyplomowy
Wykład	Egzamin - ustny, pisemny, zaliczenie, kolokwium - ustne, pisemne
Ćwiczenia	Zaliczenie - ustne, pisemne; kartkówka, zadanie wejściowe, ocena zadań cząstkowych; egzamin praktyczny, makieta, esej, referat

Opis procesu prowadzącego do uzyskania efektów uczenia się

Zaliczenie każdego semestru studiów uwarunkowane jest zdobyciem określonej programem studiów liczby punktów ECTS, co jest jednoznaczne z osiągnięciem określonych efektów uczenia się przewidzianych w danym semestrze. Przedmioty niezaliczone student musi powtórzyć w kolejnych semestrach, osiągając w ten sposób pozostałe efekty uczenia się.

Pozytywne ukończenie studiów możliwe jest po osiągnięciu przez studenta wszystkich efektów uczenia się określonych programem studiów.

Jakość prowadzonych zajęć i osiąganie efektów uczenia się kontrolowane są przez Wydziałowy System Zapewnienia Jakości Kształcenia, obejmujący między innymi procedury tworzenia i modyfikowania programów kształcenia, indywidualizowania programów studiów, realizowania procesu dydaktycznego oraz dyplomowania. Kontrola jakości procesu kształcenia obejmuje ewaluację osiąganych przez studentów efektów uczenia się. Kontrola jakości prowadzonych zajęć wspomagana jest przez hospitacje oraz ankietyzacje, przeprowadzane według ściśle zdefiniowanych wydziałowych procedur.

Praktyki

Nie dotyczy.

Egzamin dyplomowy

Egzamin dyplomowy składa się z dwóch etapów: prezentacji pracy dyplomowej oraz odpowiedzi na dwa wylosowane pytania: jedno dotyczące przedmiotów obowiązkowych, jedno dotyczące przedmiotów wybieralnych.

Zagadnienia dyplomowe zostaną podane do wiadomości studentów do końca drugiego semestru studiów.

Plan studiów

cyberbezpieczeństwo

Semestr 1

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Monitorowanie i detekcja zagrożeń	Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Projekt: 45, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 45 Seminarium: 15, w tym zajęcia zdalne: • Seminarium synchroniczne: 15	Egzamin	6	Obowiązkowy
Testy penetracyjne	Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Projekt: 45, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 45 Seminarium: 15, w tym zajęcia zdalne: • Seminarium synchroniczne: 15	Egzamin	6	Obowiązkowy
Analiza ryzyka i reakcja na incydenty	Wykład: 30 Projekt: 60	Egzamin	7	Obowiązkowy
Matematyka	Wykład: 15 Ćwiczenia: 15	Zaliczenie na ocenę	3	Obowiązkowy
Autoprezentacja i wystąpienia publiczne	Seminarium: 15	Zaliczenie na ocenę	2	Obowiązkowy
Fizyka	Wykład: 15	Zaliczenie na ocenę	1	Obowiązkowy
Lektorat 2.1	Ćwiczenia: 30	Zaliczenie na ocenę	2	Obowiązkowa grupa
Student/ka wybiera jeden przedmiot językowy z oferty Studium Języków Obcych				
Język obcy 2.1	Ćwiczenia: 30	Zaliczenie na ocenę	2	Wybieralny

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Lektorat 2.2	Ćwiczenia: 60	Zaliczenie na ocenę	3	Obowiązkowa grupa
Student/ka wybiera jeden przedmiot językowy z oferty Studium Języków Obcych				
Język obcy 2.2	Ćwiczenia: 60	Zaliczenie na ocenę	3	Wybieralny
Suma	**420**		**30**	

Semestr 2

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Zarządzanie bezpieczeństwem informacji	Wykład: 15, w tym zajęcia zdalne: • Wykład synchroniczny: 15 Projekt: 45, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 45 Seminarium: 15, w tym zajęcia zdalne: • Seminarium synchroniczne: 15	Egzamin	6	Obowiązkowy
Seminarium kierunkowe	Seminarium: 30	Zaliczenie na ocenę	3	Obowiązkowy
Blok A	Wykład: 90 Projekt: 135 Seminarium: 45	Zaliczenie na ocenę	21	Obowiązkowa grupa
Student/ka wybiera trzy przedmioty wybieralne z bloku A				
Ochrona systemów operacyjnych	Wykład: 30 Projekt: 45 Seminarium: 15	Zaliczenie na ocenę	7	Wybieralny
Metody AI w badaniu zagrożeń w systemach komputerowych	Wykład: 30 Projekt: 45 Seminarium: 15	Zaliczenie na ocenę	7	Wybieralny

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Zaawansowane testy penetracyjne sieci i aplikacji Web	Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Projekt: 45, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 45 Seminarium: 15, w tym zajęcia zdalne: • Seminarium synchroniczne: 15	Zaliczenie na ocenę	7	Wybieralny
Informatyka śledcza	Wykład: 30 Projekt: 45 Seminarium: 15	Zaliczenie na ocenę	7	Wybieralny
Suma	**375**		**30**	

Semestr 3

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Przedsiębiorczość w ICT	Wykład: 30 Projekt: 15	Zaliczenie na ocenę	3	Obowiązkowy
Seminarium dyplomowe	Seminarium: 30	Zaliczenie na ocenę	3	Obowiązkowy do wyboru
Praca dyplomowa	Praca dyplomowa: 75	Zaliczenie na ocenę	16	Obowiązkowy do wyboru
Blok B	Wykład: 30 Projekt: 60	Zaliczenie na ocenę	8	Obowiązkowa grupa
Student/ka wybiera dwa przedmioty wybieralne z bloku B				
Ochrona centrów danych	Wykład: 15 Projekt: 30	Zaliczenie na ocenę	4	Wybieralny
Audytowanie infrastruktury IT	Wykład: 15, w tym zajęcia zdalne: • Wykład synchroniczny: 15 Projekt: 30, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 30	Zaliczenie na ocenę	4	Wybieralny
Bezpieczeństwo aplikacji webowych	Wykład: 15 Projekt: 30	Zaliczenie na ocenę	4	Wybieralny
Suma	**240**		**30**	

Sylabusy

Politechnika Wrocławska

Monitorowanie i detekcja zagrożeń

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2025/2026
Specjalność -	**Kod przedmiotu**
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Grupa zajęć** Tak
Poziom kształcenia studia drugiego stopnia 3 semestry (magister inżynier)	**Języki wykładowe** polski
Forma studiów studia stacjonarne	**Obligatoryjność** Obowiązkowy
Profil studiów profil ogólnoakademicki	**Blok zajęciowy** Przedmioty kierunkowe
	Przedmiot powiązany z badaniami naukowymi Tak

Semestr Semestr 1	**Forma zaliczenia** Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Projekt: 45, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 45 Seminarium: 15, w tym zajęcia zdalne: • Seminarium synchroniczne: 15	**Liczba punktów ECTS** 6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Przedstawia koncepcję oraz cele monitorowania i detekcji zagrożeń.	K2_CBE_W01
PEU_W02	Wskazuje sposoby i dobiera narzędzia do prowadzania monitorowania i detekcji zagrożeń.	K2_CBE_W01
Z zakresu umiejętności		

PEU_U01	Planuje i przygotowuje narzędzia do monitorowania i detekcji zagrożeń.	K2_CBE_U01
PEU_U02	Analizuje dane pozyskane dzięki monitorowaniu i ocenia wykryte zagrożenia.	K2_CBE_U01
PEU_U03	Przygotowuje prezentację i przedstawia w sposób logiczny i zrozumiały opracowane koncepcje oraz dokumentację techniczną.	K2_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Przedmiot ma za zadanie zapoznać studentów z zagadnieniami dotyczącymi monitorowania infrastruktury IT oraz narzędziami wspomagającymi realizację monitorowania i detekcji zagrożeń. Uczestnicy poznają podstawowe cele i potrzeby prowadzenia monitorowania infrastruktury IT. Przedmiot obejmuje zarówno teorię, jak i praktyczne ćwiczenia projektowe, które pomogą w utrwaleniu zdobytej wiedzy. W ramach przedmiotu studenci zdobędą umiejętności wdrażania, monitorowania i detekcji zagrożeń w sieciach teleinformatycznych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	45
Seminarium	15
Przygotowanie do zajęć	10
Przygotowanie do egzaminu/zaliczenia	6
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Samodzielne doskonalenie umiejętności praktycznych	10
Przygotowanie projektu	20
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Testy penetracyjne

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Projekt: 45, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 45 Seminarium: 15, w tym zajęcia zdalne: • Seminarium synchroniczne: 15	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Formułuje koncepcję oraz cele testowania penetracyjnego.	K2_CBE_W01
PEU_W02	Klasyfikuje sposoby i narzędzia do prowadzania testów penetracyjnych.	K2_CBE_W01
Z zakresu umiejętności		
PEU_U01	Planuje i przygotowuje procedury testowania penetracyjnego.	K2_CBE_U01

PEU_U02	Przygotowuje i stosuje podstawowe testy penetracyjne w obszarze infrastruktury teleinformatycznej oraz na poziomie aplikacji internetowych.	K2_CBE_U01
PEU_U03	Opracowuje w sposób logiczny i zrozumiały koncepcje oraz dokumentację techniczną.	K2_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Przedmiot ma za zadanie zaznajomienie z podstawową wiedzą, narzędziami i technikami wykonywania testów penetracyjnych w celu odnalezienia i wyeliminowania słabych punktów - elementów podatnych na ataki, zarówno w obszarze infrastruktury teleinformatycznej jak i na poziomie aplikacji internetowych. Nabycie umiejętności planowania i przeprowadzania testów penetracyjnych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	45
Seminarium	15
Przygotowanie do zajęć	15
Przygotowanie projektu	30
Zaliczenie/Egzamin	4
Przygotowanie do egzaminu/zaliczenia	11
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Analiza ryzyka i reakcja na incydenty

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Projekt: 60	7.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje podstawowe parametry bezpieczeństwa informacji w aspekcie ryzyka	K2_CBE_W01
PEU_W02	Określa i opisuje wymagane parametry pod względem dostępności informacji w aspekcie ryzyka	K2_CBE_W01
PEU_W03	Określa i opisuje wymagane parametry pod kątem spójności / integralności informacji w aspekcie ryzyka	K2_CBE_W01
PEU_W04	Określa i opisuje wymagane parametry pod kątem poufności informacji w aspekcie ryzyka	K2_CBE_W01

PEU_W05	Charakteryzuje oraz określa ryzyka związane z parametrami bezpieczeństwa informacji pod kątem prawdopodobieństwa oraz wpływu	K2_CBE_W01
Z zakresu umiejętności		
PEU_U01	Analizuje ryzyka występujące w strukturach informatycznych określając parametry dostępności, spójności i poufności	K2_CBE_U01
PEU_U02	Dokonuje klasyfikacji oraz wycenia ryzyka w oparciu o matryce ryzyk dla poszczególnych procesów	K2_CBE_U01
PEU_U03	Opracowuje plan obsługi incydentu informatycznego w oparciu o przeprowadzone analizy ryzyka	K2_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zapoznają się z podstawowymi parametrami bezpieczeństwa informacji takimi jak: dostępność, spójność, poufność, poznają tabele oraz matryce ryzyka: prawdopodobieństwo, wpływ i skutki. Omówione zostaną incydenty informatyczne i sposób ich obsługi, a także role grup SOC (Security operation Center), CERT, CSIRT (Computer Security Incident Response Team), blue team, red team

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	60
Przygotowanie do zajęć	10
Przygotowanie projektu	60
Zaliczenie/Egzamin	4
Przygotowanie do egzaminu/zaliczenia	11
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 175

Politechnika Wrocławska

Matematyka

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kształcenia podstawowego - matematyka

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Ćwiczenia: 15	3.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Przytacza podstawowe pojęcia i własności przestrzeni liniowych i przekształceń liniowych.	K2_CBE_W02
PEU_W02	Definiuje pojęcie funkcji zespolonej, holomorficznej oraz całki zespolonej.	K2_CBE_W02
PEU_W03	Objaśnia podstawowe własności iloczynu skalarnego, przestrzeni Banacha i Hilberta.	K2_CBE_W02
PEU_W04	Definiuje pojęcie transformaty Laplace’a oraz uzasadnia jej zastosowanie przy rozwiązywaniu równań różniczkowych i liczeniu splotów.	K2_CBE_W02
PEU_W05	Formułuje działanie transformaty Fouriera oraz jej zastosowania.	K2_CBE_W02

Z zakresu umiejętności		
PEU_U01	Oblicza bazę i wymiar przestrzeni liniowej o skończonym wymiarze oraz współrzędne wektora w zadanej bazie.	K2_CBE_U02
PEU_U02	Konstruuje macierz przekształcenia liniowego w zadanych bazach, potrafi wykorzystać własności przekształceń liniowych do wyznaczania potęg macierzy.	K2_CBE_U02
PEU_U03	Konstruuje układ ortogonalny w przestrzeni Hilberta oraz rozwija w szereg ortogonalny wektor z przestrzeni Hilberta z zadanym układem ortogonalnym.	K2_CBE_U02
PEU_U04	Rozwiązuje problemy z użyciem transformaty Laplace'a.	K2_CBE_U02
PEU_U05	Rozwiązuje problemy z użyciem transformaty Fouriera.	K2_CBE_U02

Treści programowe zapewniające uzyskanie efektów uczenia się

Przedmiot ma za zadanie zapoznać studentów z zagadnieniami dotyczącymi matematyki wyższej. Uczestnicy poznają podstawowe koncepcje matematyki wyższej takie jak przekształcenia liniowe, funkcje zespolone, przestrzenie Banacha oraz transformaty Fouriera i Laplace'a. Omówione zostaną pojęcia bazy i wymiaru przestrzeni liniowej o skończonym wymiarze oraz współrzędne wektora w zadanej bazie. Studenci nauczą się wyznaczać macierz przekształcenia liniowego w zadanych bazach oraz wykorzystać własności przekształceń liniowych do wyznaczania potęg macierzy. Przedmiot obejmuje zarówno teorię, jak i praktyczne ćwiczenia, które pomogą w utrwaleniu zdobytej wiedzy. Uczestnicy będą pracować nad rzeczywistymi problemami np. aby skonstruować układ ortogonalny w przestrzeni Hilberta oraz rozwinąć w szereg ortogonalny wektor z przestrzeni Hilberta z zadanym układem ortogonalnym. W ramach przedmiotu studenci zdobędą umiejętności posługiwania się transformatami Fouriera i Laplace'a w celu rozwiązywania równań różniczkowych lub liczenia splotów miar probabilistycznych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Ćwiczenia	15
Przygotowanie do zajęć	11
Przeprowadzenie badań literaturowych	10
Przygotowanie do egzaminu/zaliczenia	12
Samodzielne studiowanie tematyki zajęć	10
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Autoprezentacja i wystąpienia publiczne

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty z dziedziny nauk humanistycznych lub społecznych

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 1	• Seminarium: 15 godz., 2 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Świadomie i racjonalnie tworzy swój wizerunek publiczny na potrzeby relacji biznesowych.	K2_CBE_U04
PEU_U02	Racjonalnie argumentuje na rzecz swoich racji i przejmuje pozycję lidera w grupie.	K2_CBE_U04
Z zakresu kompetencji społecznych		
PEU_K01	Jest wrażliwy na dobrostan relacyjny swój i swojego otoczenia społecznego.	K2_CBE_K01
PEU_K02	Respektuje ogólne zasady życia społecznego.	K2_CBE_K01

Treści programowe zapewniające uzyskanie efektów uczenia się

Przedmiot zapewnia nabycie wiedzy i umiejętności niezbędnych w zakresie podstawowych kompetencji komunikacyjnych,

szczególnie w wymiarze komunikacji bezpośredniej. Zajęcia obejmują takie zagadnienia, jak: podstawy psychologii, komunikacji, rozwój osobisty, umiejętności interpersonalne, odporność komunikacyjna, skuteczność i zdolności organizacyjne czy kształtowanie kariery zgodnie z profilem osobowościowym.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Seminarium	15
Przygotowanie do zajęć	5
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Przeprowadzenie badań literaturowych	5
Samodzielne studiowanie tematyki zajęć	10
Przygotowanie projektu	5
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

Politechnika Wrocławska

Fizyka

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kształcenia podstawowego - fizyka

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 1	• Wykład: 15 godz., 1 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Charakteryzuje podstawowe prawa związane z podstawami mechaniki kwantowej.	K2_CBE_W02
PEU_W02	Charakteryzuje podstawowe prawa teorii względności.	K2_CBE_W02
PEU_W03	Charakteryzuje podstawowe zagadnienia fizyki współczesnej i przytacza przykłady ich zastosowań.	K2_CBE_W02
PEU_W04	objaśnia zjawiska fizyczne wykorzystywane do przesyłania informacji, jej kodowania i przetwarzania.	K2_CBE_W02

Treści programowe zapewniające uzyskanie efektów uczenia się

Treści programowe zapewniają uzyskanie efektów uczenia się poprzez poszerzenie wiedzy z zakresu podstaw mechaniki kwantowej i teorii względności. Uczestnicy poznają teorie fizyczne, na bazie których odbywa się kwantowe kodowanie informacji oraz jej przetwarzanie. Omówione jest również nowe podejście fizyczne do zagadnień czasu i jego roli w

przesyłaniu informacji. Efektem kształcenia jest pogłębiona wiedza z zakresu fizyki stosowanej do przesyłania informacji, jej kodowania i przetwarzania na przykładzie komputerów kwantowych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Samodzielne studiowanie tematyki zajęć	2
Przygotowanie do egzaminu/zaliczenia	4
Zaliczenie/Egzamin	2
Przygotowanie do zajęć	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 25

Politechnika Wrocławska

Język obcy 2.1

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
lektoraty

Specjalność
-

Jednostka organizacyjna
Politechnika Wrocławska

Poziom kształcenia
studia drugiego stopnia

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu
SJO000-25SM04094C

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Języki obce

Semestry	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 1, Semestr 2, Semestr 3, Semestr 4	• Ćwiczenia: 30 godz., 2 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Ma wiedzę, umiejętności i kompetencje zgodne z wymaganiami określonymi dla poziomu minimum B2 wg Europejskiego Systemu Opisu Kształcenia Językowego; zna, rozumie i stosuje środki językowe (gramatyczne, leksykalne i stylistyczne) z języka akademickiego, specjalistycznego i technicznego stosowane w dziedzinie studiowanego kierunku oraz w środowisku akademickim i zawodowym; porozumiewa się w środowisku interkulturowym i zawodowym; rozumie i posiada umiejętność analizy obcojęzycznych tekstów specjalistycznych; doskonali swoje umiejętności w obszarze języka specjalistycznego i akademickiego.	SJO_S2_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

B2 plus język angielski, francuski, hiszpański, niemiecki

C1 plus język angielski
Ogólne treści kształcenia
Kształcenie oraz pogłębianie kompetencji komunikacyjnych w środowisku akademickim i zawodowym.
Interakcja adekwatna dla właściwego poziomu kompetencji językowych, np. własny profil studenta dla celów akademickich i zawodowych. Pogłębianie kompetencji twórczych, odbiorczych i interaktywnych w zespole.
Język w komunikacji na polu specjalistycznym i zawodowym we współczesnym świecie. Komunikacja werbalna i niewerbalna – swobodne funkcjonowanie w środowisku interkulturowym, prowadzenie dyskursu, polemiki, analiza tekstów specjalistycznych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Ćwiczenia	30
Przygotowanie do zajęć	30
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 60

Politechnika Wrocławska

Język obcy 2.2

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
lektoraty

Specjalność
-

Jednostka organizacyjna
Politechnika Wrocławska

Poziom kształcenia
studia drugiego stopnia

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu
SJO000-25SM04095C

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Języki obce

Semestry	**Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia**
Semestr 1, Semestr 2, Semestr 3, Semestr 4	• Ćwiczenia: 60 godz., 3 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Ma wiedzę, umiejętności i kompetencje zgodne z wymaganiami określonymi dla właściwego poziomu językowego; zna, rozumie i stosuje określone poziomem środki językowe (gramatyczne, leksykalne i stylistyczne) z życia codziennego z wybranymi elementami języka akademickiego, specjalistycznego i technicznego stosowane w dziedzinie studiowanego kierunku oraz w środowisku akademickim i zawodowym; porozumiewa się w środowisku rodzinnym, towarzyskim i interkulturowym ćwicząc umiejętność komunikacji; docenia potrzebę doskonalenia swoich umiejętności w zakresie efektywnej komunikacji, rozwija kompetencje w obszarze języka komunikacji, podstaw języka specjalistycznego i akademickiego.	SJO_S2_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

A1; A2; B1 język francuski, hiszpański, japoński, niemiecki, polski jako obcy, rosyjski
Ogólne treści kształcenia
Kształcenie oraz pogłębianie kompetencji komunikacyjnych w środowisku rodzinnym, towarzyskim oraz interkulturowym oraz dla określonego poziomu dla potrzeb akademickich i zawodowych.
Interakcja adekwatna dla właściwego poziomu kompetencji językowych, np. własny profil studenta oraz zainteresowań; prezentowanie siebie, swoich zainteresowań i pomysłów w kontekstach środowiskowych, akademickich i zawodowych.
Rozwijanie kompetencji twórczych, odbiorczych i interaktywnych w grupie.
Język w komunikacji we współczesnym świecie. Komunikacja werbalna i niewerbalna – wrażliwość na różnice kulturowe, nawiązywanie rozmowy, włączanie się do dyskusji, przechodzenie do kolejnych punktów, podsumowywanie wypowiedzi, stosowanie charakterystycznych zwrotów i wyrażeń dla określonego poziomu językowego; branie udziału w różnych formach interakcji.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Ćwiczenia	60
Przygotowanie do zajęć	30
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 90

Politechnika Wrocławska

Zarządzanie bezpieczeństwem informacji

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 15, w tym zajęcia zdalne: • Wykład synchroniczny: 15 Projekt: 45, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 45 Seminarium: 15, w tym zajęcia zdalne: • Seminarium synchroniczne: 15	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Identyfikuje, klasyfikuje i umiejętnie wykorzystuje pozyskaną wiedzę na temat norm i regulacji w zakresie bezpieczeństwa informacji.	K2_CBE_W01
PEU_W02	Wskazuje, przytacza i wyjaśnia wiedzę teoretyczną i kwestie techniczne z zakresu zarządzania, bezpieczeństwa i ochrony informacji.	K2_CBE_W01

PEU_W03	Wyjaśnia wiedzę z zakresu metod kryptograficznych stosowanych w ochronie informacji.	K2_CBE_W01
Z zakresu umiejętności		
PEU_U01	Analizuje oraz dobiera właściwe normy bezpieczeństwa do chronionych systemów.	K2_CBE_U01
PEU_U02	Projektuje, implementuje i właściwie stosuje System Zarządzania Bezpieczeństwem Informacji.	K2_CBE_U01
PEU_U03	Projektuje i stosuje adekwatne rozwiązania kryptograficzne do ochrony informacji.	K2_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci nabywają wiedzę z zakresu projektowania systemu ochrony informacj i wdrażania zaawansowanych systemów zarządzania bezpieczeństwem informacji (SZBI) oraz poszerzają umiejętności z zakresu przeprowadzania analizy procesów biznesowych i zasobów teleinformatycznych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	45
Seminarium	15
Przygotowanie do zajęć	10
Samodzielne studiowanie tematyki zajęć	10
Samodzielne doskonalenie umiejętności praktycznych	13
Przygotowanie projektu	20
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Przygotowanie do egzaminu/zaliczenia	3
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Seminarium kierunkowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 2	• Seminarium: 30 godz., 3 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Identyfikuje i dobiera aktualną wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w obszarze cyberbezpieczeństwa.	K2_CBE_W05
Z zakresu kompetencji społecznych		
PEU_K01	Poprawnie wykorzystuje, cytuje i opisuje źródła bibliograficzne.	K2_CBE_K02
PEU_K02	Decyduje o wyborze dostępnych narzędziach multimedialnych pomocnych podczas przygotowywania prezentacji multimedialnych.	K2_CBE_K02
PEU_K03	Odpowiada za prezentowanie wyników wykonanych prac z uwzględnieniem: rygorów czasowych, poziomu wiedzy odbiorców oraz przyjętych standardów z zakresu umiejętności komunikacji.	K2_CBE_K02

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci wykształcą umiejętności poprawnego wykorzystywania dostępnych źródeł bibliograficznych, wnioskowania oraz prezentacji wyników, a także umiejętności poprawnej prezentacji wyników studiów własnych nad opracowywanym zagadnieniem z zakresu cyberbezpieczeństwa.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Seminarium	30
Przygotowanie do zajęć	5
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Przeprowadzenie badań literaturowych	20
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Ochrona systemów operacyjnych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Projekt: 45 Seminarium: 15	7.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje zbiór zagadnień składających się na bezpieczeństwo popularnych systemów operacyjnych	K2_CBE_W01
PEU_W02	Wskazuje metody ataków i zagrożeń oraz metody wykrywania zagrożeń.	K2_CBE_W01
PEU_W03	Wybiera metody i narzędzia służące weryfikacji poziomu bezpieczeństwa systemów Microsoft i Unix i poprawy ich bezpieczeństwa.	K2_CBE_W01
Z zakresu umiejętności		

PEU_U01	Dobiera narzędzia służące weryfikacji bezpieczeństwa systemów operacyjnych.	K2_CBE_U01
PEU_U02	Ocenia metody poprawy ochrony systemów operacyjnych.	K2_CBE_U01
PEU_U03	Bada i testuje bezpieczeństwo systemów operacyjnych.	K2_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci poznają zbiór zagadnień związanych z aktywną ochroną systemów operacyjnych oraz narzędzi i metod weryfikacji bezpieczeństwa i ochrony systemów operacyjnych. Zapoznają się z powłoką PowerShell oraz platformą Metasploit i wykorzystaniem eksploitów do ataków na systemy operacyjne. Poznają architekturę oraz podatności systemów operacyjnych, a także działania zwiększające ich bezpieczeństwo: analiza szkodliwego oprogramowania, ochrona sieci bezprzewodowych, narzędzia i metody łamania haseł, zbieranie dowodów ataków, czy reagowanie na incydenty.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	45
Seminarium	15
Przygotowanie projektu	40
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Zaliczenie/Egzamin	2
Przygotowanie do egzaminu/zaliczenia	13
Samodzielne studiowanie tematyki zajęć	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 175

Politechnika Wrocławska

Metody AI w badaniu zagrożeń w systemach komputerowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2025/2026
Specjalność -	**Kod przedmiotu**
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Grupa zajęć** Tak
Poziom kształcenia studia drugiego stopnia 3 semestry (magister inżynier)	**Języki wykładowe** polski
Forma studiów studia stacjonarne	**Obligatoryjność** Wybieralny
Profil studiów profil ogólnoakademicki	**Blok zajęciowy** Przedmioty kierunkowe
	Przedmiot powiązany z badaniami naukowymi Tak

Semestr Semestr 2	**Forma zaliczenia** Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Projekt: 45 Seminarium: 15	**Liczba punktów ECTS** 7.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Kategoryzuje i wyjaśnia najważniejsze metody sztucznej inteligencji (AI) i uczenia maszynowego (ML) stosowane w modelowaniu i wykrywaniu zagrożeń / ataków w systemach komputerowych.	K2_CBE_W01
PEU_W02	Dobiera odpowiednie metody uczenia maszynowego do zadania modelowania zagrożeń oraz wykrywania anomalii w zależności od specyfiki danych z systemu komputerowego.	K2_CBE_W01
Z zakresu umiejętności		

PEU_U01	Dobiera właściwe metody analizy danych w zadaniu modelowania i badania zagrożeń lub wykrywania anomalii w zależności od specyfiki ataku i specyfiki źródła danych obrazujących stan systemu komputerowego.	K2_CBE_U01
PEU_U02	Prawidłowo posługuje się metodami i algorytmami uczenia maszynowego/AI - dobiera i konstruuje modele, weryfikuje ich skuteczność i interpretuje wyniki w zadaniach modelowania zagrożeń lub wykrywania anomalii w oparciu o dane z różnych źródeł. .	K2_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Przedmiot ma za zadanie zapoznać studentów z zagadnieniami i metodami uczenia maszynowego i sztucznej inteligencji, które można wykorzystać do wykrywania i analizowania zagrożeń w systemach komputerowych. Studenci poznają metody i algorytmy uczenia nadzorowanego i nienadzorowanego i metody użycia tych narzędzi w zadaniach modelowania zagrożeń i ataków oraz w zadaniach wykrywania anomalii. Omówione zostaną techniki analizy i modelowania na podstawie różnego typu danych - w tym wysokowymiarowych, niezbalansowanych, szeregów czasowych jedno- i wielowymiarowych, danych grafowych. Poruszone zostaną również zagadnienia wyjaśnialności modeli uczenia maszynowego/AI oraz kwestie wiarogodności i bezpieczeństwa samych modeli AI. Przedmiot obejmuje zarówno teorię jak i praktyczne zadania projektowe. W ich ramach studenci poznają zarówno narzędzia komputerowe - biblioteki narzędzi programistycznych i analitycznych do budowy systemów wykrywania i analizy zagrożeń metodami ML/AI oraz specyfikę danych ilustrujących rzeczywiste zadania wykrywania i analizy zagrożeń w systemach komputerowych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	45
Seminarium	15
Przeprowadzenie badań literaturowych	6
Przygotowanie projektu	50
Przygotowanie do egzaminu/zaliczenia	6
Zaliczenie/Egzamin	2
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Samodzielne doskonalenie umiejętności praktycznych	11
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 175

Politechnika Wrocławska

Zaawansowane testy penetracyjne sieci i aplikacji Web

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2025/2026
Specjalność -	**Kod przedmiotu**
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Grupa zajęć** Tak
Poziom kształcenia studia drugiego stopnia 3 semestry (magister inżynier)	**Języki wykładowe** polski
Forma studiów studia stacjonarne	**Obligatoryjność** Wybieralny
Profil studiów profil ogólnoakademicki	**Blok zajęciowy** Przedmioty kierunkowe
	Przedmiot powiązany z badaniami naukowymi Tak

Semestr Semestr 2	**Forma zaliczenia** Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Projekt: 45, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 45 Seminarium: 15, w tym zajęcia zdalne: • Seminarium synchroniczne: 15	**Liczba punktów ECTS** 7.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Wskazuje koncepcję oraz cele zaawansowanego testowania penetracyjnego.	K2_CBE_W01
PEU_W02	Wymienia sposoby i narzędzia do prowadzania zaawansowanych testów penetracyjnych.	K2_CBE_W01
Z zakresu umiejętności		

PEU_U01	Planuje i przygotowuje procedury zaawansowanego testowania penetracyjnego.	K2_CBE_U01
PEU_U02	Stosuje zaawansowane testy penetracyjne w obszarze infrastruktury teleinformatycznej oraz na poziomie aplikacji internetowych.	K2_CBE_U01
PEU_U03	Opracowuje w sposób logiczny i zrozumiały koncepcje oraz dokumentację techniczną.	K2_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Celem przedmiotu jest rozwinięcie wiedzy i umiejętności studentów w zakresie zaawansowanych technik testów penetracyjnych. Przedmiot obejmuje identyfikację oraz analizę podatności w infrastrukturze teleinformatycznej i aplikacjach webowych, a także planowanie i realizację pełnych kampanii testowych w zgodzie z najlepszymi praktykami branżowymi i obowiązującymi standardami bezpieczeństwa.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	45
Seminarium	15
Przygotowanie do zajęć	20
Przygotowanie projektu	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	25
Zaliczenie/Egzamin	2
Przygotowanie do egzaminu/zaliczenia	8
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 175

Politechnika Wrocławska

Informatyka śledcza

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Projekt: 45 Seminarium: 15	7.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Identyfikuje i charakteryzuje rodzaje informacji w procesach analitycznych, określa sposób akwizycji tych danych z zachowaniem wymaganych parametrów procesu.	K2_CBE_W01
PEU_W02	Określa bazowe parametry różnych systemów zapisu informacji. Rozróżnia systemy operacyjne, systemy plików, systemy transmisji informacji oraz umie wskazać ich cechy i parametry wymagane w procesach analitycznych	K2_CBE_W01
PEU_W03	Formułuje i objaśnia procesy analityczne zgodnie z wymaganiami prawnymi, zapewniając wymagane parametry dostępności, spójności, poufności, niezaprzeczalności oraz rzetelności informacji.	K2_CBE_W01

PEU_W04	Określa i przedstawia różne procesy kryptograficzne, zna i opisuje różne sposoby kompresji, kodowania oraz szyfrowania danych, zna ich zalety oraz wady w aspekcie analiz danych.	K2_CBE_W01
Z zakresu umiejętności		
PEU_U01	Identyfikuje oraz analizuje różne rodzaje informacji zawarte w postaci cyfrowej (plików). Potrafi skorzystać z różnych narzędzi do analiz plików, zna ich możliwości oraz ograniczenia.	K2_CBE_U01
PEU_U02	Potrafi zaplanować i zrealizować proces obsługi incydentów informatycznych, korzystając z dostępnych narzędzi oraz współpracując z innymi.	K2_CBE_U01
PEU_U03	Weryfikuje wiarygodność materiałów dowodowych w postaci cyfrowej, stosuje różne metody analityczne, właściwie dobiera i korzysta z dostępnych narzędzi.	K2_CBE_U01
PEU_U04	Określa i stosuje metodyki białego wywiadu (OSINT) w zakresie akwizycji danych i wyszukiwania informacji w otwartych źródłach (internet)	K2_CBE_U01
PEU_U05	Przygotowuje spójny i rzetelny raport z prowadzonych czynności oraz ich rezultatów, właściwie zabezpieczony, przeznaczony do dalszych postępowań	K2_CBE_U01
PEU_U06	Stosuje różne metody i sposoby zabezpieczania informacji pod kątem dostępności, spójności, poufności, wiarygodności i niezaprzeczalności.	K2_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zdobędą wiedzę z zakresu cech i właściwości danych w zakresie analiz śledczych, źródeł danych, nośników, akwizycji danych, metadanych, odzyskiwania i ekstracji danych, cech i parametrów dowodów cyfrowych w analizach danych, aspektów prawnych w zakresie analiz danych, wymagania procesowe, zabezpieczania dowodów cyfrowych oraz procesów przetwarzania informacji, inżynierii odwrotnej, detekcji i analizy złośliwych kodów (malware), charakterystyki incydentów informatycznych, technik kryptograficznych w analizach danych oraz procesów raportowania, zabezpieczania i prezentacji wyników.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	45
Seminarium	15
Przygotowanie projektu	45
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Przygotowanie do zajęć	10
Przygotowanie do egzaminu/zaliczenia	13
Zaliczenie/Egzamin	2

Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 175

Politechnika Wrocławska

Przedsiębiorczość w ICT

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty z dziedziny nauk humanistycznych lub społecznych

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Projekt: 15	3.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Charakteryzuje rynek teleinformatyczny.	K2_CBE_W04
PEU_W02	Wybiera metodykę realizacji projektów teleinformatycznych.	K2_CBE_W04
PEU_W03	Przedstawia ekonomiczne zasady działalności.	K2_CBE_W04
Z zakresu umiejętności		
PEU_U01	Analizuje raporty o stanie rynku teleinformatycznego.	K2_CBE_U04
PEU_U02	Przygotowuje projekcje finansowe.	K2_CBE_U04
PEU_U03	Przygotowuje biznes plan.	K2_CBE_U04

PEU_U04	Przygotowuje elementy zarządzania projektem.	K2_CBE_U04

Treści programowe zapewniające uzyskanie efektów uczenia się

Przedmiot ma za zadanie zapoznanie studentów z podstawami prawnymi prowadzenia działalności w cyberbezpieczeństwie. Uczestnicy poznają ekonomiczne podstawy działalności. Studenci nauczą się przygotowywać elementy biznes planu. Przedstawiane są zasady projekcji finansowych, w tym sprawozdania finansowe i mierniki opłacalności inwestycji. Omawiane są metodyki zarządzania projektami informatycznymi.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	15
Przygotowanie do zajęć	8
Przygotowanie projektu	20
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Seminarium dyplomowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy do wyboru

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 3	• Seminarium: 30 godz., 3 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Przygotowuje prezentację zawierającą wyniki własnych oryginalnych badań.	K2_CBE_U05
PEU_U02	Rzeczowo uzasadnia swoje oryginalne pomysły i rozwiązania.	K2_CBE_U05
PEU_U03	Ocenia rozwiązania naukowo-techniczne innych osób.	K2_CBE_U05

Treści programowe zapewniające uzyskanie efektów uczenia się

Przedmiot ma za zadanie nauczanie poszukiwania selektywnej wiedzy niezbędnej do tworzenia własnych oryginalnych rozwiązań. Uczestnicy nauczą się przygotowania prezentacji pozwalającej w sposób komunikatywny przekazanie swoich oryginalnych pomysłów, koncepcji i rozwiązań. Studenci zdobędą umiejętności pisania dzieła prezentującego własne osiągnięcia, w tym prezentacji własnych osiągnięć na tle rozwoju myśli światowej.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Seminarium	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	45
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Praca dyplomowa

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy do wyboru

Blok zajęciowy
Praca dyplomowa

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 3	• Praca dyplomowa: 75 godz., 16 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Wyszukuje informacje z różnych źródeł, umie dokonać ich krytycznej analizy, syntezy, twórczej interpretacji oraz potrafi je zaprezentować	K2_CBE_U05
PEU_U02	Dobiera i testuje hipotezy dotyczące zaawansowanych problemów badawczych	K2_CBE_U05
PEU_U03	Zgodnie z zadaną specyfikacją projektuje i tworzy (przynajmniej w części) złożony system informatyczny mający na celu ekstrakcję wiedzy z danych używając właściwych metod, technik i narzędzi.	K2_CBE_U05
Z zakresu kompetencji społecznych		
PEU_K01	Docenia krytyczną ocene odbieranych treści, docenia znaczenie wiedzy w rozwiązywaniu problemów.	K2_CBE_K02

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zapoznają się z wytycznymi formalnymi odnośnie przygotowania pracy pisemnej, opisu literatury i struktury pracy dyplomowej, nabędą poszerzoną wiedzę z zakresu tematyki pracy dyplomowej oraz nabędą umiejętności przygotowania eksperymentów, weryfikacji i opracowania wyników przeprowadzonych badań

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Praca dyplomowa	75
Przeprowadzenie badań literaturowych	40
Przygotowanie pracy dyplomowej	170
Przygotowanie raportu/sprawozdania/prezentacji/referatu	40
Praca z opiekunem nad częścią merytoryczną pracy	75
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 400

Politechnika Wrocławska

Ochrona centrów danych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Projekt: 30	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Identyfikuje typowe zagrożenia dla środowisk wirtualnych oraz chmur obliczeniowych w centrach danych oraz metody zabezpieczania infrastruktury i przetwarzanych danych.	K2_CBE_W03
PEU_W02	Charakteryzuje strategie w podejściu do cyberbezpieczeństwa, w kontekście modelu Zero Trust i sztucznej inteligencji.	K2_CBE_W03
PEU_W03	Wyjaśnia działanie mechanizmów Zarządzania Tożsamością i Dostępem (IAM) na styku pomiędzy organizacją a dostawcami chmury lub między samymi dostawcami chmurowymi i usługami.	K2_CBE_W03

PEU_W04	Identyfikuje i opisuje najlepsze praktyki w zakresie reagowania na incydenty w chmurze i budowania odporności, które mogą być wykorzystywane przez specjalistów ds. bezpieczeństwa przy opracowywaniu własnych planów i procesów reagowania.	K2_CBE_W03
Z zakresu umiejętności		
PEU_U01	Ocenia podatności w środowisku chmur obliczeniowych oraz dokonuje klasyfikacji danych pod kątem ich ważności i wrażliwości.	K2_CBE_U03
PEU_U02	Planuje i projektuje zabezpieczenia dla centrów danych oraz dostosowuje je do kontekstu i przedmiotu ochrony.	K2_CBE_U03

Treści programowe zapewniające uzyskanie efektów uczenia się

Przedmiot ma za zadanie zapoznać studentów z zagadnieniami dotyczącymi zabezpieczania centrów danych - polityki, metody i podział odpowiedzialności. Koncentruje się na zarządzaniu ogólną infrastrukturą oraz bezpieczeństwem sieci, w tym na odpowiedzialności dostawcy usług chmurowych (CSP) za bezpieczeństwo infrastruktury. Omówione zostaną złożone koncepcje ochrony danych w chmurze, obejmujące kluczowe strategie, narzędzia i praktyki związane z zabezpieczaniem danych w tranzycie i w stanie spoczynku. Zostanie również przedstawione Zarządzanie Tożsamością i Dostępem (IAM), które koncentruje się na styku pomiędzy organizacją a dostawcami chmury lub między samymi dostawcami chmurowymi i usługami. W dalszej części przedmiot skupia się na identyfikacji i opisie najlepszych praktyk w zakresie reagowania na incydenty w chmurze i budowania odporności, które mogą być wykorzystywane przez specjalistów ds. bezpieczeństwa przy opracowywaniu własnych planów i procesów reagowania. Ponadto, uczestnicy poznają strategie w podejściu do cyberbezpieczeństwa, w kontekście modelu Zero Trust.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	30
Samodzielne studiowanie tematyki zajęć	15
Przygotowanie projektu	20
Przygotowanie raportu/sprawozdania/prezentacji/referatu	5
Przygotowanie do egzaminu/zaliczenia	5
Przeprowadzenie badań literaturowych	8
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Audytowanie infrastruktury IT

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	**Forma zaliczenia**	**Liczba punktów ECTS**
Semestr 3	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15, w tym zajęcia zdalne: • Wykład synchroniczny: 15 Projekt: 30, w tym zajęcia zdalne: • Zajęcia projektowe synchroniczne: 30	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia koncepcję oraz cele prowadzenie audytu.	K2_CBE_W03
PEU_W02	Opisuje sposoby i narzędzia do prowadzania monitorowania i audytu.	K2_CBE_W03
Z zakresu umiejętności		
PEU_U01	Planuje i przygotowuje narzędzia do audytu.	K2_CBE_U03
PEU_U02	Analizuje dane pozyskane dzięki przeprowadzonemu audytowi i reaguje na wykryte zagrożenia.	K2_CBE_U03

PEU_U03	Opracowuje sposób logiczny i zrozumiały koncepcje oraz dokumentację techniczną.	K2_CBE_U03

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zdobędą wiedzę z zakresu celów i potrzeb prowadzenia audytu infrastruktury IT, narzędzi wspomagających realizację audytu sieci i systemów, różnych rodzajów audytu (infrastruktury, aplikacji, systemów operacyjnych, usług chmurowych), analizy ryzyka na potrzeby audytu, a także zdobędą umiejętność przeprowadzenia różnych rodzajów audytów.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	30
Przygotowanie do zajęć	15
Przygotowanie do egzaminu/zaliczenia	8
Zaliczenie/Egzamin	2
Przygotowanie projektu	30
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Bezpieczeństwo aplikacji webowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia drugiego stopnia 3 semestry (magister inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2025/2026

Kod przedmiotu

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Przedmioty kierunkowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Projekt: 30	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych	K2_CBE_W03
PEU_W02	Objaśnia certyfikaty SSL i działanie protokołów SSL/TLS	K2_CBE_W03
PEU_W03	Identyfikuje metody ataków typu XSS i CSRF	K2_CBE_W03
PEU_W04	Opisuje metody ataków typu ,,code injection'', w szczególności SQL-Injection oraz problemy z przekazywaniem parametrów pomiędzy programami	K2_CBE_W03
Z zakresu umiejętności		

PEU_U01	Analizuje typowe błędy związane z bezpieczeństwem w konfiguracji serwerów sieciowych	K2_CBE_U03
PEU_U02	Testuje integralność danych w systemie komputerowym i stosuje techniki kryptograficzne do zwiększenia bezpieczeństwa systemu (m.in. SSL)	K2_CBE_U03
PEU_U03	Przygotowuje konfigurację serwera WWW	K2_CBE_U03
PEU_U04	Wyszukuje informacje o bieżących problemach związanych z bezpieczeństwem serwerów WWW i aplikacji webowych	K2_CBE_U03

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zdobędą wiedzę i podniosą kompetencje z zakresu bezpiecznego programowania w różnych środowiskach, ze szczególnym uwzględnieniem programowania web (skrypty, middleware, clientapps), a także poznają metodologie wspomagające tworzenie bezpiecznych programów, takie jak programowanie defensywne i programowanie sterowane testowaniem. Studenci zapoznają się z typowymi atakami i metodami ich przeciwdziałania, jak również poznają narzędzia wspomagające tworzenie bezpiecznych rozwiązań webowych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	30
Przygotowanie projektu	40
Przygotowanie do egzaminu/zaliczenia	13
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100