Politechnika Wrocławska

Program studiów

Wydział:	Wydział Informatyki i Telekomunikacji
Kierunek studiów:	cyberbezpieczeństwo
Poziom kształcenia:	studia pierwszego stopnia (inżynier)
Forma kształcenia:	studia stacjonarne
Cykl kształcenia:	2026/2027

Spis treści

Charakterystyka kierunku studiów

Informacje podstawowe

Wydział:	Wydział Informatyki i Telekomunikacji
Kierunek studiów:	cyberbezpieczeństwo
Poziom kształcenia:	studia pierwszego stopnia (inżynier)
Forma studiów:	studia stacjonarne
Profil studiów:	profil ogólnoakademicki
Język prowadzenia studiów:	polski
Obowiązuje od cyklu kształcenia:	2026/2027
Liczba semestrów:	7
Całkowita liczba godzin zajęć:	kierunkowe: 1980 bezpieczeństwo infrastruktury krytycznej: 405 bezpieczeństwo systemów informatycznych: 405
Całkowita liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:	210
Tytuł zawodowy nadawany absolwentom:	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

Osoby kończące studia na kierunku Cyberbezpieczenstwo są przygotowane do pracy przy zabezpieczaniu informacji na wszystkich etapach jej życia, obejmujących planowanie systemu zabezpieczeń, jego wdrażanie i utrzymywanie w gotowości podczas eksploatacji oraz wprowadzania niezbędnych modyfikacji dostosowujących system zabezpieczeń do występujących i ciągle ewoluujących zagrożeń. Szczególny nacisk położono na bezpieczeństwo przechowywanych informacji i dostęp do niej przy użyciu nowoczesnych systemów transmisyjnych. Kształcenie obejmuje m.in. sposoby tworzenia bezpiecznych usług multimedialnych, przetwarzanie dużych zbiorów informacji (Big Data), struktury i działanie centrów przetwarzania danych, bazy danych, biometryczne zabezpieczanie dostępu, bezpieczeństwo w systemach rozproszonych, kryptografię, elektromagnetyczne bezpieczeństwo systemów i sieci, audytowanie sieci teleinformatycznych i bezpieczne usługi internetowe oraz informatykę śledczą. Studia przygotowują również do uzyskania certyfikatów, CCNA (Cisco Certified Network Associate), Network Security, CyberOps Associate. Podczas studiów na kierunku Cyberbezpieczeństwo nabywane są również między innymi umiejętności pracy grupowej, czy prezentacji uzyskanych wyników i zrealizowanych zadań, świadomość konieczności samokształcenia, odpowiedzialności zawodowej czy prawnych i etycznych skutków działalności inżynierskiej, a także gotowość do odpowiedzialnego podejmowania decyzji. Osoby, które ukończyły studia mogą ubiegać się o przyjęcie na studia drugiego stopnia lub studia podyplomowe.

Aktualność programu studiów

Koncepcja i cele kształcenia

Realizując program nauczania studenci i studentki 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. Ważnym elementem uczenia się jest praca własna, 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. Poza godzinami zajęć prowadzący są dostępni w wyznaczonych i ogłoszonych na stronie Wydziału godzinach konsultacji.

Do każdego efektu uczenia się PRK przyporządkowane są kody przedmiotów obecnych w programie studiów. Zaliczenie tych przedmiotów (tego przedmiotu) oznacza uzyskanie danego efektu. Przedmioty zaliczane są zgodnie z zasadami zdefiniowanymi w kartach przedmiotów. Brak osiągnięcia efektów uczenia się, przypisanych do przedmiotu skutkuje brakiem zaliczenia przedmiotu i koniecznością powtórnej jego realizacji.

Studia na kierunku prowadzone są na dwóch specjalnościach: Bezpieczeństwo systemów informatycznych oraz Bezpieczeństwo infrastruktury krytycznej. Podział na specjalności przeprowadzany jest na czwartym semestrze, od piątego semestru realizowane są zarówno wspólne przedmioty kierunkowe, jak i specjalistyczne przedmioty dopasowane do każdej specjalności. Osoby studiujące realizują praktykę zawodową w wybranej przez siebie instytucji w wymiarze nie mniejszym niż cztery tygodnie, praktyka realizowana jest w okresie wakacyjnym. Do ukończenia studiów wymagane jest zrealizowanie pracy inżynierskiej oraz zdanie egzaminu dyplomowego (po pomyślnym zaliczeniu wszystkich przedmiotów z programu studiów), na którym prezentowana jest zrealizowana praca inżynierska oraz omawiane są zagadnienia z przebiegu studiów.

Kształcenie ukierunkowane jest na przekazanie zarówno wszechstronnej wiedzy technicznej w ramach kierunku studiów, jak i umiejętności i kompetencji interpersonalnych. Niezwykle ważnym celem kształcenia jest wyposażenie absolwentów i absolwentki w kompetencje, które pozwolą im efektywnie funkcjonować na rynku pracy. Stąd zdobywają oni umiejętności między innymi z programowania głównie skryptowego, zaawansowanej konfiguracji i działania sieci komputerowych oraz ich bezpieczeństwa, konfiguracji i zabezpieczania systemów operacyjnych, chmur obliczeniowych, czy stosowania sztucznej inteligencji do wykrywania zagrożeń. Studia te przygotowują do przyszłej pracy, wyposażając ich w kompetencje miękkie, takie jak: praca w grupie i umiejętności komunikacyjne, potrzeba samorozwoju i samokształcenia, czy w końcu zarządzanie projektami IT. W ten sposób absolwenci i absolwentki stają się nie tylko cennymi pracownikami na rynku pracy, ale mogą również zakładać swoje firmy i odpowiednio nimi kierować i zarządzać.

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 jest uprawomocnione wynikami 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. Prognozuje się, że z największymi wyzwaniami będzie się wiązało zapewnienie odpowiednich kadr między innymi 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. pracy grupowej. Pozwolą również na uzyskanie preferowanych przez pracodawców umiejętności praktycznych, co zapewnia np. odbycie praktyki zawodowej.

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, rozwija 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 w środowisku, a także dąży do ciągłego udoskonalania oferty dydaktycznej. Na kierunku dominują nauki ścisłe, jednakże nabywane są również umiejętności miękkie, co zwiększa atrakcyjność absolwentów i absolwentek 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 równnież 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 szeroki 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			
K1_CBE_W01	Wyjaśnia zasady metrologii i technik pomiarowych oraz charakteryzuje zjawiska kompatybilności elektromagnetycznej i ich wpływ na bezpieczeństwo urządzeń i systemów.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W02	Opisuje architekturę systemów UNIX i wyjaśnia zasady działania oraz zabezpieczania różnych typów baz danych.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W03	Charakteryzuje techniki informatyczne, usługi sieciowe oraz technologie zapewnienia bezpieczeństwa związanych z pozyskiwaniem, przetwarzaniem i prezentowaniem informacji.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W04	Wyjaśnia społeczne, etyczne i prawne uwarunkowania działalności inżynierskiej oraz interpretuje zasady ochrony własności przemysłowej, prawa autorskiego, przedsiębiorczości i zarządzania jakością.	P6U_W, P6S_WG, P6S_WK	
K1_CBE_W05	Stosuje wybrane, zaawansowane pojęcia matematyki i fizyki do analizy zagadnień istotnych dla cyberbezpieczeństwa.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W06	Opisuje architekturę oraz funkcjonowanie chmur obliczeniowych i porównuje modele dostarczania usług w chmurze obliczeniowej.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W07	Charakteryzuje zagadnienia i metody analizy oraz przetwarzania dowodów cyfrowych: rodzaje źródeł, sposoby pozyskiwania, rzetelność i zabezpieczanie dowodów, wyjaśnia metody analizy artefaktów aktywności, a także metody zapewniania rzetelności i niezaprzeczalności dowodów cyfrowych.	P6U_W, P6S_WG, P6S_WK	P6S_WG_INŻ
K1_CBE_W08	Opisuje metodyki zarządzania projektami i wyjaśnia przebieg procesów związanych z zarządzaniem projektami.	P6U_W, P6S_WG	
K1_CBE_W09	Wyjaśnia zasady wykonywania testów penetracyjnych w celu znalezienia i wyeliminowania słabych punktów - elementów podatnych na ataki, zarówno w obszarze infrastruktury teleinformatycznej jak i na poziomie aplikacji internetowych oraz charakteryzuje narzędzia i techniki wykrywania podatności.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W10	Analizuje filary cyberbezpieczeństwa (poufność, integralność, dostępność) oraz opisuje systemy zarządzania bezpieczeństwem informacji a także metody zarządzania ryzykiem i opracowywania polityk bezpieczeństwa w różnych instytucjach.	P6U_W, P6S_WG, P6S_WK	P6S_WG_INŻ
K1_CBE_W11	Charakteryzuje budowę systemów operacyjnych i wyjaśnia mechanizmy zwiększania ich bezpieczeństwa.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W12	Opisuje metody sztucznej inteligencji (AI) i uczenia maszynowego (ML) wykorzystywane w modelowaniu i wykrywaniu zagrożeń/ataków na systemy komputerowe, a także metody wykrywania anomalii, nietypowych profili na podstawie danych pochodzących z monitorowania ruchu sieciowego, monitorowania zdarzeń i obciążenia urządzeń oraz innych źródeł.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W13	Rozróżnia zaawansowane metody szyfrowania informacji i wyjaśnia zasady działania systemów kryptograficznych.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W14	Charakteryzuje wybrane, zaawansowane zagadnienia specjalistyczne z zakresu cyberbezpieczeństwa właściwe dla programu kształcenia w ramach określonej specjalności.	P6U_W, P6S_WG, P6S_WK	P6S_WG_INŻ

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
K1_CBE_W15	Opisuje architekturę i funkcjonowanie sieci komputerowych, wyjaśnia działanie protokołów komunikacyjnych i urządzeń sieciowych z protokołem TCP/IP, analizuje metody zabezpieczania sieci.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W16	Wyjaśnia organizację i usługi bezpieczeństwa realizowane w ramach Security Operation Center (SOC) oraz sposoby i metody monitorowania oraz detekcji zagrożeń w systemach informatycznych. Charakteryzuje struktury organizacji i architektury systemów wykrywania zagrożeń.	P6U_W, P6S_WG	P6S_WG_INŻ
Umiejętności			
K1_CBE_U01	Rozwiązuje zadania obliczeniowe i analityczne z zakresu kryptografii z użyciem narzędzi komputerowych.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U02	Zapisuje algorytm w postaci schematu blokowego, korzysta ze środowiska informatycznego, pisze skrypty dla różnych języków programowania, w tym automatyzujące zadania systemowe, a także stosuje mechanizmy synchronizacji procesów oraz programuje komunikację sieciową. Dobiera narzędzia tworzenia aplikacji oraz projektuje i implementuje bazę danych.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U03	Posługuje się edytorami tekstów, arkuszami kalkulacyjnymi, wykonuje prezentację multimedialną, publikuje informacje w sieci, przesyła dane w sieci, kontroluje i konfiguruje politykę bezpieczeństwa aplikacji.	P6U_U, P6S_UW	
K1_CBE_U04	Stosuje metody matematyki i fizyki do rozwiązywania szczegółowych problemów w obszarze cyberbezpieczeństwa.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U05	Uruchamia i konfiguruje usługi serwerowe oraz komunikacyjne w środowisku wirtualnym oraz dobiera odpowiednie technologie dla usług świadczonych przez chmury obliczeniowe.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U06	Stosuje techniki pozyskiwania dowodów cyfrowych z różnych źródeł: obrazy dysków, logi, zrzuty, dane strumieniowe oraz zabezpieczenia dowodów cyfrowych (podpisy, skróty, kopie) i artefaktów aktywności. Przeprowadza i dokumentuje analizę powłamaniową incydentu teleinformatycznego.	P6U_U, P6S_UW, P6S_UK, P6S_UU	P6S_UW_INŻ
K1_CBE_U07	Wybiera i stosuje odpowiednią metodykę zarządzania projektami dla konkretnego zadania. Definiuje projekt i nim zarządza.	P6U_U, P6S_UW, P6S_UO	
K1_CBE_U08	Opracowuje wybraną analizę ryzyka oraz politykę bezpieczeństwa różnych instytucji, a także omówia niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U09	Wykorzystuje system operacyjny Linux w zakresie zaawansowanym, w tym pisze skrypty powłoki, a także analizuje sposoby ochrony systemu operacyjnego oraz rozpoznaje zagrożenia, ataki i wdraża zalecenia norm i rekomendacji do systemu operacyjnego.	P6U_U, P6S_UW, P6S_UU	P6S_UW_INŻ
K1_CBE_U10	Planuje i przeprowadza test penetracyjny.	P6U_U, P6S_UW, P6S_UU	P6S_UW_INŻ
K1_CBE_U11	Dobiera i stosuje właściwe metody analizy danych w zadaniu analizy zagrożeń / wykrywania anomalii w zależności od specyfiki analizowanych danych.	P6U_U, P6S_UW, P6S_UU	P6S_UW_INŻ
K1_CBE_U12	Konfiguruje urządzenia sieciowe do pracy w sieci lokalnej, stosuje protokoły dynamicznego routowania, konfiguruje i diagnozuje sieci w topologii nadmiarowej, a także wdraża mechanizmy zabezpieczenia (zapory, listy dostępu, tunele).	P6U_U, P6S_UW	P6S_UW_INŻ

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
K1_CBE_U13	Dobiera i zestawia układ pomiarowy adekwatny do potrzeb oraz przeprowadza odpowiednio pomiary, a także dobiera właściwe metody testowania EMC oraz oceny bezpieczeństwa elektromagnetycznego.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U14	Stosuje narzędzia monitorujące zdarzenia oraz bezpieczeństwo w systemie komputerowym. Dobiera sondy dla różnych kategorii zdarzeń w monitorowanym systemie. Analizuje zdarzenia pochodzące z wielu źródeł danych i używa wskaźników jakościowych i ilościowych, np. do oceny skuteczności wdrożonego systemu monitorowania.	P6U_U, P6S_UW, P6S_UK	P6S_UW_INŻ
K1_CBE_U15	Stosuje zasady bezpieczeństwa związane ze stanowiskiem pracy w środowisku biznesowym.	P6U_U, P6S_UO, P6S_UU	
K1_CBE_U16	Wykorzystuje posiadaną wiedzę specjalistyczną do formułowania i rozwiązywania złożonych i nietypowych problemów z wybranych zagadnień cyberbezpieczeństwa, pozyskuje specjalistyczne informacje ze źródeł, analizuje ich przydatności do realizowanych zadań.	P6U_U, P6S_UW, P6S_UO, P6S_UU, P6S_UK	P6S_UW_INŻ
Kompetencje społeczne			
K1_CBE_K01	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu inżyniera. Ma świadomość roli społecznej absolwenta uczelni technicznej. Rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności inżyniera. Potrafi przekazać taką informację i opinie w sposób zrozumiały, z uzasadnieniem różnych punktów widzenia.	P6U_K, P6S_KR, P6S_KO	
K1_CBE_K02	Rozumie prawne aspekty i skutki działalności inżynierskiej.	P6U_K, P6S_KR, P6S_KO	
K1_CBE_K03	Ma świadomość ważności i zrozumienie humanistycznych aspektów i skutków działalności inżynierskiej. Poznaje skutki wpływu działalności technicznej na środowisko, i związaną z tym odpowiedzialność społeczną nauki i techniki.	P6U_K, P6S_KK, P6S_KO, P6S_KR	
K1_CBE_K04	Rozumie ideę normalizacji, certyfikacji i integracji systemów zarządzania jakością, ochroną środowiska, bezpieczeństwem pracy i bezpieczeństwem informacji. Rozumie koncepcję zarządzania przez jakość. Identyfikuje problemy zarządzania jakością, w tym kosztów jakości oraz zasady ich rozwiązywania. Zna ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości.	P6U_K, P6S_KO	
K1_CBE_K05	Potrafi współpracować z zespołem przy realizacji złożonego zadania inżynierskiego. Potrafi przedstawić efekty swojej pracy w zrozumiałej formie. Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.	P6U_K, P6S_KK	
Efekty językowe i z wychowania fizycznego			
SJO_S1_U01	Potrafi posługiwać się językiem obcym na poziomie B2 ESOKJ	P6S_UK	
SWF_S1_U01	Ma świadomość ważności systematycznej aktywności fizycznej dla zdrowia fizycznego i psychicznego		

Szczegółowe informacje dotyczące punktów ECTS

cyberbezpieczeństwo

Nazwa	bezpieczeństwo infrastruktury krytycznej	bezpieczeństwo systemów informatycznych
Całkowita liczba punktów ECTS	210	210
Całkowita liczba godzin zajęć	2385	2385
Liczba punktów ECTS przyporządkowana zajęciom związanym z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów (DN)	168/210 (80%)	170/210 (80.95%)
Liczba punktów ECTS przyporządkowana zajęciom kształtującym umiejętności praktyczne (m.in. laboratorium, projekt) (P)	88.8	93.1
Liczba punktów ECTS, którą student uzyska realizując zajęcia wymagające bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów (BU)	107.4	107.4
Udział procentowy ECTS zajęć wybieralnych	64/210 (30.48%)	64/210 (30.48%)
Liczba punktów ECTS, którą student uzyska realizując zajęcia z dziedziny nauk humanistycznych lub nauk społecznych właściwych dla danego kierunku studiów	6	6
Liczba godzin kontaktowych, którą student uzyska realizując zajęcia z wychowania fizycznego	60	60
Liczba punktów ECTS, którą student uzyska realizując zajęcia z zakresu nauk podstawowych (matematyka, fizyka/chemia)	31	31

Organizacja studiów

Realizacja programu studiów

Dopuszczalny deficyt ECTS

Semestr	Dopuszczalny deficyt punktów ECTS po semestrze
Semestr 1	11
Semestr 2	11
Semestr 3	11
Semestr 4	11
Semestr 5	11
Semestr 6	11
Semestr 7	0

Wymagania szczegółowe

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;
Praktyka	Sprawozdanie z odbycia praktyki, dziennik praktyk, potwierdzenie realizacji programu praktyki
Laboratorium	Wykonanie sprawozdań laboratoryjnych; wypowiedzi ustne, aktywność na zajęciach; kartkówka, zadanie wejściowe, ocena zadań cząstkowych
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 muszą zostać powtórzone w kolejnych semestrach, osiągając w ten sposób pozostałe efekty uczenia się.

Pozytywne ukończenie studiów możliwe jest po osiągnięciu 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 efektów uczenia się. Kontrola jakości prowadzonych zajęć wspomagana jest przez hospitacje oraz ankietyzacje, przeprowadzane według ściśle zdefiniowanych wydziałowych procedur.

Praktyki

Praktyka zawodowa jest realizowana w wymiarze określonym w programie studiów. Praktyka powinna trwać co najmniej 4 tygodnie. Praktyki zawodowe odbywają się w trakcie wakacji letnich, po zakończeniu zajęć szóstego semestru. Praktyka odbywa się zgodnie z zasadami określonymi na Wydziale Informatyki i Telekomunikacji opublikowanymi na stronie internetowej wydziału

Egzamin dyplomowy

Egzamin dyplomowy składa się ze sprawdzianu wiedzy i umiejętności w drodze weryfikacji stopnia opanowania treści kształcenia przekazywanych w czasie studiów. Komisja Programowa Kierunku przygotowuje listę zagadnień egzaminu dyplomowego w konsultacji z nauczycielami akademickimi prowadzącymi zajęcia z poszczególnych przedmiotów. Egzamin odbywa się w formie ustnej przed komisją wyznaczoną przez Dziekana, składa się z prezentacji pracy dyplomowej oraz odpowiedzi na dwa wylosowane zagadnienia z uprzednio opublikowanej listy.

Zagadnienia dyplomowe zostaną opublikowane na stronie Wydziału do końca szóstego semestru.

Plan studiów

cyberbezpieczeństwo

Semestr 1

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Podstawy telekomunikacji	Wykład: 30	Zaliczenie na ocenę	2	Obowiązkowy
Miernictwo 1	Wykład: 30	Zaliczenie na ocenę	3	Obowiązkowy
Własność intelektualna i prawa autorskie	Wykład: 15	Zaliczenie na ocenę	1	Obowiązkowy
Etyka inżynierska	Wykład: 15	Zaliczenie na ocenę	1	Obowiązkowy
Filozofia	Wykład: 30	Zaliczenie na ocenę	2	Obowiązkowy
Podstawy programowania	Laboratorium: 45	Zaliczenie na ocenę	5	Obowiązkowy
Algebra liniowa z geometrią analityczną	Wykład: 30 Ćwiczenia: 30	Egzamin	6	Obowiązkowy
Analiza matematyczna 1	Wykład: 30 Ćwiczenia: 30	Egzamin	6	Obowiązkowy
Podstawy cyberbezpieczeństwa	Wykład: 30	Zaliczenie na ocenę	4	Obowiązkowy
Suma	**315**		**30**	

Semestr 2

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Miernictwo 2	Laboratorium: 15	Zaliczenie na ocenę	2	Obowiązkowy
Ochrona informacji	Wykład: 30 Seminarium: 15	Zaliczenie na ocenę	4	Obowiązkowy
Sieci komputerowe 1	Wykład: 15 Laboratorium: 30	Zaliczenie na ocenę	5	Obowiązkowy

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Programowanie skryptowe	Laboratorium: 45	Zaliczenie na ocenę	5	Obowiązkowy
Wprowadzenie do systemów komputerowych	Wykład: 30 Laboratorium: 45	Zaliczenie na ocenę	5	Obowiązkowy
Zaawansowana kombinatoryka	Wykład: 30 Ćwiczenia: 15	Zaliczenie na ocenę	4	Obowiązkowy
Fizyka 1.1A	Wykład: 30 Ćwiczenia: 15	Egzamin	5	Obowiązkowy
Wychowanie fizyczne	Ćwiczenia: 30	Zaliczenie na ocenę	-	Obowiązkowa grupa
Student/ka wybiera jeden przedmiot z oferty Studium Wychowania Fizycznego i Sportu				
Wychowanie fizyczne 1	Ćwiczenia: 30	Zaliczenie na ocenę	-	Wybieralny
Suma	**345**		**30**	

Semestr 3

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Kryptografia stosowana	Wykład: 30 Laboratorium: 30	Egzamin	6	Obowiązkowy
Programowanie systemowe	Wykład: 30 Laboratorium: 30	Zaliczenie na ocenę	5	Obowiązkowy
Sieci komputerowe 2	Wykład: 15 Laboratorium: 45	Zaliczenie na ocenę	5	Obowiązkowy
Systemy operacyjne	Wykład: 30 Laboratorium: 45	Zaliczenie na ocenę	6	Obowiązkowy
Inżynierskie zastosowania statystyki	Wykład: 30 Ćwiczenia: 15	Zaliczenie na ocenę	5	Obowiązkowy
Lektorat 1.1	Ćwiczenia: 60	Zaliczenie na ocenę	3	Obowiązkowa grupa
Student/ka wybiera jeden przedmiot językowy z oferty Studium Języków Obcych				
Język obcy 1.1	Ćwiczenia: 60	Zaliczenie na ocenę	3	Wybieralny

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Wychowanie fizyczne	Ćwiczenia: 30	Zaliczenie na ocenę	-	Obowiązkowa grupa
Student/ka wybiera jeden przedmiot z oferty Studium Wychowania Fizycznego i Sportu				
Wychowanie fizyczne 2	Ćwiczenia: 30	Zaliczenie na ocenę	-	Wybieralny
Suma	**390**		**30**	

Semestr 4

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Chmury obliczeniowe	Wykład: 15 Laboratorium: 45	Zaliczenie na ocenę	5	Obowiązkowy
Bazy danych	Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Laboratorium: 30	Zaliczenie na ocenę	6	Obowiązkowy
Sieci komputerowe 3	Wykład: 15 Laboratorium: 45	Zaliczenie na ocenę	5	Obowiązkowy
Informatyka śledcza	Wykład: 15 Laboratorium: 30, w tym zajęcia zdalne: • Laboratorium synchroniczne: 30	Zaliczenie na ocenę	5	Obowiązkowy
Ochrona systemów operacyjnych	Wykład: 30 Laboratorium: 45, w tym zajęcia zdalne: • Laboratorium synchroniczne: 45	Egzamin	6	Obowiązkowy
Lektorat 1.2	Ćwiczenia: 60	Zaliczenie na ocenę	3	Obowiązkowa grupa
Student/ka wybiera jeden przedmiot językowy z oferty Studium Języków Obcych				
Język obcy 1.2	Ćwiczenia: 60	Zaliczenie na ocenę	3	Wybieralny
Suma	**360**		**30**	

Semestr 5

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Bezpieczeństwo sieci komputerowych	Wykład: 30 Laboratorium: 60	Egzamin	6	Obowiązkowy
Bezpieczeństwo elektromagnetyczne	Wykład: 15 Laboratorium: 30	Zaliczenie na ocenę	5	Obowiązkowy
Suma	**135**		**11**	

bezpieczeństwo systemów informatycznych

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Bezpieczeństwo w sieciach bezprzewodowych	Wykład: 30 Laboratorium: 30	Zaliczenie na ocenę	4	Obowiązkowy specjalnościowy
Biometria	Wykład: 30 Laboratorium: 15 Seminarium: 15	Zaliczenie na ocenę	4	Obowiązkowy specjalnościowy
Bezpieczeństwo serwerów i aplikacji Web	Wykład: 15 Laboratorium: 45	Zaliczenie na ocenę	6	Obowiązkowy specjalnościowy
Bezpieczeństwo chmur obliczeniowych	Wykład: 15 Laboratorium: 45	Zaliczenie na ocenę	5	Obowiązkowy specjalnościowy
Suma	**240**		**19**	

bezpieczeństwo infrastruktury krytycznej

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Bezpieczeństwo w wytwarzaniu i przesyle energii elektrycznej	Wykład: 30	Zaliczenie na ocenę	3	Obowiązkowy specjalnościowy
Elektroenergetyczna automatyka zabezpieczeniowa	Wykład: 30 Laboratorium: 15	Egzamin	4	Obowiązkowy specjalnościowy

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Zagrożenia w funkcjonowaniu infrastruktury elektroenergetycznej	Wykład: 30 Laboratorium: 15	Zaliczenie na ocenę	3	Obowiązkowy specjalnościowy
Komunikacja w inteligentnych systemach pomiarowych	Wykład: 30 Laboratorium: 15	Zaliczenie na ocenę	3	Obowiązkowy specjalnościowy
Zaburzenia jakości energii elektrycznej	Wykład: 30 Laboratorium: 15	Zaliczenie na ocenę	4	Obowiązkowy specjalnościowy
Podstawy elektrotechniki	Wykład: 30	Zaliczenie na ocenę	2	Obowiązkowy specjalnościowy
Suma	**240**		**19**	

Semestr 6

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Zarządzanie projektami IT	Wykład: 15 Projekt: 15	Zaliczenie na ocenę	2	Obowiązkowy
Testy penetracyjne	Wykład: 15 Laboratorium: 45	Zaliczenie na ocenę	4	Obowiązkowy
Metody AI w badaniu zagrożeń w systemach komputerowych	Wykład: 30 Laboratorium: 30	Egzamin	5	Obowiązkowy
Wykrywanie zagrożeń i reakcja na incydenty	Wykład: 30 Laboratorium: 30	Zaliczenie na ocenę	4	Obowiązkowy
Projekt zespołowy	Projekt: 45	Zaliczenie na ocenę	5	Obowiązkowy do wyboru
Suma	**255**		**20**	

bezpieczeństwo systemów informatycznych

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Przetwarzanie dużych zbiorów danych	Wykład: 30 Projekt: 15	Zaliczenie na ocenę	4	Obowiązkowy specjalnościowy

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Cyberbezpieczeństwo w Internecie Rzeczy	Wykład: 15 Laboratorium: 30	Zaliczenie na ocenę	4	Obowiązkowy specjalnościowy
Aplikacje mobilne	Wykład: 15 Projekt: 15	Zaliczenie na ocenę	2	Obowiązkowy specjalnościowy
Suma	**120**		**10**	

bezpieczeństwo infrastruktury krytycznej

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Bezpieczeństwo systemów sterowania i nadzoru w elektroenergetyce	Wykład: 15 Laboratorium: 30	Zaliczenie na ocenę	4	Obowiązkowy specjalnościowy
Cyberbezpieczeństwo inteligentnych sieci elektroenergetycznych	Wykład: 15 Projekt: 15	Zaliczenie na ocenę	3	Obowiązkowy specjalnościowy
Systemy zasilania gwarantowanego	Wykład: 30 Laboratorium: 15	Zaliczenie na ocenę	3	Obowiązkowy specjalnościowy
Suma	**120**		**10**	

Semestr 7

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Metody monitorowania jakości produkcji	Wykład: 30	Zaliczenie na ocenę	2	Obowiązkowy
Zarządzanie ryzykiem i polityki bezpieczeństwa	Wykład: 30 Seminarium: 15	Zaliczenie na ocenę	4	Obowiązkowy
Praca dyplomowa	Praca dyplomowa: 75	Zaliczenie na ocenę	12	Obowiązkowy do wyboru
Praktyka zawodowa	-	Zaliczenie na ocenę	7	Obowiązkowy do wyboru
Seminarium dyplomowe	Seminarium: 30	Zaliczenie na ocenę	2	Obowiązkowy do wyboru
Suma	**180**		**27**	

bezpieczeństwo systemów informatycznych

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Audytowanie sieci teleinformatycznych	Wykład: 15 Laboratorium: 30	Zaliczenie na ocenę	3	Obowiązkowy specjalnościowy
Suma	**45**		**3**	

bezpieczeństwo infrastruktury krytycznej

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Rozproszone systemy automatyki	Wykład: 15 Laboratorium: 30	Zaliczenie na ocenę	3	Obowiązkowy specjalnościowy
Suma	**45**		**3**	

Sylabusy

Politechnika Wrocławska

Podstawy telekomunikacji

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 1	• Wykład: 30 godz., 2 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
	Z zakresu wiedzy	
PEU_W01	Wyjaśnia główne elementy, pojęcia, etapy oraz procesy zachodzące w kolejnych etapach nadawania i odbioru sygnału, z uwzględnieniem kontekstu cyberbezpieczeństwa, czyli podstawowych schematów uwierzytelniania i autoryzacji. Posiada wiedzę dot. organizacji standaryzacyjnych właściwych branży telekomunikacyjnej	K1_CBE_W03
PEU_W02	Objaśnia podstawy reprezentacji sygnałów w dziedzinie czasu i częstotliwości, w tym: zagadnienia związane z konwersją analogowo-cyfrową, parametry opisujące sygnał telekomunikacyjny, przestrzeń widmową. Zna i rozumie definicję metryk oceny transmisji, takich jak: pojemność, przepustowość, opóźnienie, jitter. Wartości tych metryk umie interpretować w kontekście detekcji potencjalnych cyberataków	K1_CBE_W03

PEU_W03	Definiuje cel i rodzaje kodowania protekcyjnego informacji, jej modulacji oraz metod kryptograficznych. Zna podstawowe metody wielodostępu oraz zwielokrotniania kanału	K1_CBE_W03
PEU_W04	Opisuje modelowanie nadajnika, odbiornika i anteny oraz podstawy notacji decybelowej i pojęcia szumu i zakłóceń	K1_CBE_W03
PEU_W05	Objaśnia konstrukcję i właściwości mediów transmisyjnych miedzianych, światłowodowych (optycznych) oraz bezprzewodowych (radiowych), najważniejsze zagadnienia związane z propagacją sygnału fizycznego w tych mediach, w tym dotyczące podatności tych mediów na cyberataki i próby zakłócenia/blokady transmisji w warstwie fizycznej	K1_CBE_W03
PEU_W06	Opisuje sieci komputerowe (architektura, modele odniesienia, zasada działania, techniki kontroli dostępu i bezpieczeństwa transmisji) oraz najważniejsze cechy sieci dostępowych i szkieletowych	K1_CBE_W03
PEU_W07	Opisuje systemy komórkowe generacji 2G-5G, w tym metody zabezpieczania transmisji	K1_CBE_W03
PEU_W08	Opisuje sieci satelitarne z elementami bezpieczeństwa transmisji	K1_CBE_W03
PEU_W09	Definiuje problematykę komunikacji rozsiewczej, w tym: właściwości nadawania analogowego i cyfrowego, główne standardy radiofonii cyfrowej oraz telewizji cyfrowej, stan obecny wdrożenia i trendy	K1_CBE_W03
PEU_W10	Opisuje współczesne systemy sieci bezprzewodowej transmisji danych na różnych zasięgach docelowych, w tym: sieci nanośne (WBAN), osobiste (WPAN), lokalne (WLAN), metropolitalne (WMAN/WRAN), sensorowe (WSN), systemy RFID, Internetu Rzeczy (IoT) oraz główne źródła podatności na cyberataki tych systemów oraz techniki przeciwdziałania im	K1_CBE_W03

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu omówione zostaną podstawe zagadnienia telekomunikacji w kontekście aspektów cyberbezpieczeństwa w tym: budowa i działanie systemu telekomunikacyjnego, charakterystyka przewodowych i bezprzewodowych mediów transmisyjnych, metody kodowonia, kryptografii i modulacji. Omówione zostaną również podstawy sieci koomputerowych oraz różnych systemów telekomunikacyjnych: komórkowych, satelitarych, rozsiewczych czy systemów IoT

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Przygotowanie do egzaminu/zaliczenia	10
Samodzielne studiowanie tematyki zajęć	10
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

Politechnika Wrocławska

Miernictwo 1

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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: 30 godz., 3 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia zasady pomiarów, teorię niepewności pomiarów i techniki pomiarów wybranych sygnałów elektrycznych	K1_CBE_W01
PEU_W02	Charakteryzuje metody pomiarowe i sprzęt stosowany w pomiarach sygnałów elektrycznych. Jest w stanie scharakteryzować potrzeby pomiarowe pod kątem oceny parametrów sygnałów elektrycznych, wskazać wielkości mierzone, dobrać metodę pomiaru i określić miarodajność wyników	K1_CBE_W01

Treści programowe zapewniające uzyskanie efektów uczenia się

Istota pomiarów ze szczególnym uwzględnieniem roli pomiarów, ich niepewności i rzetelności na koszty jakości w jednostkach gospodarczych. Poznanie zasad pomiarów i nabycie wiedzy dotyczącej niepewności pomiarów i umiejętności jej szacowania. Parametry sygnałów elektrycznych, metody pomiarów, przyrządy pomiarowe.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Wykład	30
Samodzielne studiowanie tematyki zajęć	25
Przeprowadzenie badań literaturowych	10
Przygotowanie do egzaminu/zaliczenia	10
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Własność intelektualna i prawa autorskie

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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	• Wykład: 15 godz., 1 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje podstawowe metody interpretacji przepisów prawnych związanych z prawem własności intelektualnej	K1_CBE_W04
PEU_W02	Opisuje podstawowe instytucje prawne związane z prawem własności intelektualnej	K1_CBE_W04
PEU_W03	Wybiera właściwy przepis w systemie obowiązującego prawa	K1_CBE_W04
Z zakresu kompetencji społecznych		
PEU_K01	Docenia potrzebę i zna możliwości ciągłego dokształcania się w zakresie prawniczych aspektów pracy inżyniera w celu podnoszenia kompetencji zawodowych, osobistych i społecznych.	K1_CBE_K02

Treści programowe zapewniające uzyskanie efektów uczenia się

Ochrona twórczości intelektualnej, regulacje prawne dotyczące innowacji i utworów, wynalazków, znaków towarowych, interpretacja przepisów prawnych związanych z prawem własności intelektualnej, równowaga między interesem twórców a dostępem do wiedzy i kultury, świadomość konieczności aktualizacji wiedzy prawnej, etyka i odpowiedzialność w zakresie własności intelektualnej, prawo autorskie.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Przygotowanie do zajęć	10
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 25

Politechnika Wrocławska

Etyka inżynierska

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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	• Wykład: 15 godz., 1 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje filozoficzno-etyczne uwarunkowania działalności inżynierskiej	K1_CBE_W04
PEU_W02	Identyfikuje uwarunkowania działalności inżynierskiej w postaci filozoficznego namysłu nad istotą technologii.	K1_CBE_W04
Z zakresu kompetencji społecznych		
PEU_K01	Rozstrzyga dylematy moralne związane z wykonywaniem zawodu.	K1_CBE_K01
PEU_K02	Postępuje zgodnie z zasadami kodeksów etyki inżynierskiej.	K1_CBE_K01

Treści programowe zapewniające uzyskanie efektów uczenia się

Etyka jako dziedzina wiedzy oraz filozofii praktycznej. Umiejętności krytycznego myślenia. Struktury dylematu moralnego i zapoznanie z dylematami wynikającymi z wykonywania działalności inżynierskiej. Problematyka etyki zawodowej,

kodeksowej i pozakodeksowej. Przedstawienie społecznych i humanistycznych uwarunkowań działalności inżynierskiej. Przybliżenie problemu społecznej odpowiedzialności nauki i techniki.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Samodzielne studiowanie tematyki zajęć	4
Przygotowanie do egzaminu/zaliczenia	6
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 25

Politechnika Wrocławska

Filozofia

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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	• Wykład: 30 godz., 2 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Identyfikuje prawne, etyczno-społeczne, filozoficzne uwarunkowania działalności inżynierskiej. Zna i rozumie fundamentalne dylematy współczesnej cywilizacji.	K1_CBE_W04
Z zakresu kompetencji społecznych		
PEU_K01	Identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu; ma świadomość roli społecznej absolwenta uczelni technicznej; rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności inżyniera; potrafi przekazać taką informację i opinię w sposób zrozumiały, z uzasadnieniem różnych punktów widzenia.	K1_CBE_K03

Treści programowe zapewniające uzyskanie efektów uczenia się

Podstawowe zagadnienia filozoficzne, etyka, filozofia społeczna, epistemologia, metafizyka, teoria argumentacji, filozofia nauki i techniki. Krytyczne myślenie, świadomość społecznej odpowiedzialności, refleksja nad wyzwaniami współczesności, interpretacja pojęć i koncepcji filozoficznych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Przygotowanie do zajęć	10
Przygotowanie do egzaminu/zaliczenia	10
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

Politechnika Wrocławska

Podstawy programowania

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 1	• Laboratorium: 45 godz., 5 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Tworzy prosty skrypt w języku Python	K1_CBE_U02
PEU_U02	Sporządza skrypty do automatyzacji zadań systemowych	K1_CBE_U02
PEU_U03	Tworzy skrypty do obsługi plików i przetwarzania danych	K1_CBE_U02
PEU_U04	Projektuje interfejs graficzny w języku Python	K1_CBE_U02

Treści programowe zapewniające uzyskanie efektów uczenia się

Typy danych, wyrażenia, funkcje, struktury sterujące, własne funkcje, struktury danych, operacje na tekstach, obsługa wyjątków, programowanie obiektowe, organizacja i obsługa plików, zarządzanie czasem i zadaniami, wielowątkowość, przetwarzanie dokumentów i obrazów, analiza danych, interakcja z urządzeniami wejścia, projektowanie interfejsów użytkownika, automatyzacja i testowanie zadań.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Laboratorium	45
Samodzielne studiowanie tematyki zajęć	45
Przygotowanie do egzaminu/zaliczenia	35
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Algebra liniowa z geometrią analityczną

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kształcenia podstawowego - matematyka

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Ćwiczenia: 30	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia podstawowe metody rozwiązywania równań liniowych	K1_CBE_W05
PEU_W02	Przedstawia podstawowe własności liczb zespolonych	K1_CBE_W05
PEU_W03	Opisuje podstawowe własności algebraiczne wielomianów	K1_CBE_W05
PEU_W04	Przedstawia metody opisu prostych i płaszczyzn.	K1_CBE_W05
Z zakresu umiejętności		
PEU_U01	Oblicza wyznaczniki, dodaje i mnoży macierze	K1_CBE_U04
PEU_U02	Rozwiązuje układy równań liniowych	K1_CBE_U04

PEU_U03	Wyznacza wektory i wartości własne macierzy	K1_CBE_U04
PEU_U04	Przeprowadza obliczenia z wykorzystaniem liczb zespolonych	K1_CBE_U04
PEU_U05	Wyznacza równania płaszczyzn i prostych w przestrzeni.	K1_CBE_U04

Treści programowe zapewniające uzyskanie efektów uczenia się

Logika matematyczna, indukcja, struktury algebraiczne, liczby zespolone, działania i interpretacje geometryczne, postacie liczby zespolonej, pierwiastki zespolone. Wielomiany, pierwiastki, rozkład na czynniki, funkcje wymierne, przestrzenie wektorowe, podprzestrzenie, baza przestrzeni wektorowej, przestrzeń euklidesowa. Macierze, działania na macierzach, wyznaczniki, macierze odwrotne, równania macierzowe, układy równań liniowych, funkcje i odwzorowanie liniowe, wektory i wartości własne, diagonalizacja macierzy. Geometria analityczna w przestrzeni, działania na wektorach, układy współrzędnych, równania płaszczyzn i prostych, wzajemne położenie płaszczyzn i prostych, odległości, rzuty.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Ćwiczenia	30
Przygotowanie do zajęć	86
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Analiza matematyczna 1

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kształcenia podstawowego - matematyka

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 1	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Ćwiczenia: 30	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Wyjaśnia podstawowe pojęcia i twierdzenia rachunku różniczkowego funkcji jednej zmiennej	K1_CBE_W05
PEU_W02	Wyjaśnia podstawowe pojęcia i twierdzenia rachunku różniczkowego funkcji wielu zmiennych	K1_CBE_W05
PEU_W03	Objaśnia pojęcie całki podwójnej i potrójnej, jej własności i podstawowe zastosowania	K1_CBE_W05
Z zakresu umiejętności		
PEU_U01	Stosuje elementy badania przebiegu zmienności funkcji do rozwiązywania typowych zadań	K1_CBE_U04

PEU_U02	Stosuje pochodne cząstkowe, wyznaczać gradient i pochodną kierunkową oraz wyznaczać ekstrema lokalne i warunkowe funkcji dwóch zmiennych	K1_CBE_U04

Treści programowe zapewniające uzyskanie efektów uczenia się

Funkcje jednej zmiennej, granica funkcji, ciągłość, pochodne, badanie przebiegu. Funkcje 2 i 3 zmiennych, pochodne cząstkowe, ekstrema. Całka oznaczona i nieoznaczona, ich własności i zastosowania. Rachunek różniczkowy i jego twierdzenia. Ciągi, granice ciągów, przebieg zmienności funkcji, szeregi liczbowe.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Ćwiczenia	30
Przygotowanie do zajęć	86
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Podstawy cyberbezpieczeństwa

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 1	• Wykład: 30 godz., 4 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje podstawowe zagadnienia cyberbezpieczeństwa: poufność, integralność, dostępność	K1_CBE_W10
PEU_W02	Rozpoznaje zagrożenia w infrastrukturze teleinformatycznej	K1_CBE_W10
PEU_W03	Charakteryzuje bezpieczeństwo sieci i systemów teleinformatycznych	K1_CBE_W10
PEU_W04	Identyfikuje bezpieczeństwo systemów operacyjnych Linux, Windows, Android, iOS	K1_CBE_W10

Treści programowe zapewniające uzyskanie efektów uczenia się

Pojęcia z zakresu cyberbezpieczeństwa (poufność, integralność, dostępność) i sposoby ich zapewnienia (szyfrowanie, kontrola dostępu, funkcje skrótu, koncepcja AAA (Authentication, Authorization, Accounting)), bezpieczeństwo systemów operacyjnych (Windows, Linux, Android, iOS), bezpieczeństwo sieci komputerowych przewodowych i bezprzewodowych

(zapory ogniowe, system IDS, system IPS), testy penetracyjne, zagrożenia i ataki występujące w sieciach teleinformatycznych (złośliwe oprogramowanie, sniffing, spoofing, socjotechnika).

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Przygotowanie do egzaminu/zaliczenia	20
Samodzielne studiowanie tematyki zajęć	50
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Miernictwo 2

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 2	• Laboratorium: 15 godz., 2 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Wykorzystuje i obsługuje podstawowe analogowe i cyfrowe przyrządy do pomiarów wielkości elektrycznych oraz zestawia stanowisko pomiarowe, dokonuje pomiarów i analizuje wyniki tych pomiarów	K1_CBE_U13
PEU_U02	Dobiera i uzasadnia metodę pomiaru podstawowych wielkości elektrycznych i szacuje niepewność wybranej metody	K1_CBE_U13
PEU_U03	Stosuje oscyloskop do obrazowania oraz wykonywania podstawowych pomiarów sygnałów elektrycznych.	K1_CBE_U13

Treści programowe zapewniające uzyskanie efektów uczenia się

Planowanie i wykonywanie pomiarów, dobór metod i sprzętu pomiarowego w pomiarach wielkości elektrycznych, umiejętności zestawienia stanowiska pomiarowego, pomiarów i analizy wyników, pomiarów napięć i prądów w obwodach prądu stałego i przemiennego, wykorzystania oscyloskopu w pomiarach wielkości elektrycznych.

Nakład pracy studenta

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

Politechnika Wrocławska

Ochrona informacji

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Seminarium: 15	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia dostęp do informacji oraz konstrukcję ochrony informacji niejawnych, danych osobowych i informacji objętych tajemnicą przedsiębiorstwa	K1_CBE_W10
PEU_W02	Definiuje hierarchię i metody dostępu do informacji niejawnej	K1_CBE_W10
PEU_W03	Charakteryzuje systemy zarządzania bezpieczeństwem informacji (SZBI) zgodne z normami/regulacjami europejskimi (NIS) i krajowymi (ustawa KSC), budowy systemów ochrony: informacji niejawnych, danych osobowych i informacji objętych tajemnicą zawodową	K1_CBE_W10

PEU_W04	Definiuje wymagania ogólne dotyczące wdrażania systemów zarządzania bezpieczeństwem informacji zgodnych z odpowiednimi normami oraz potrafi określić wymagania oraz obszary związane z projektowaniem i wdrażaniem Polityki Bezpieczeństwa Informacji w zależności od charakteru przedsiębiorstwa	K1_CBE_W10
PEU_W05	Wyjaśnia ogólne ramy obowiązków osób odpowiedzialnych za ochronę informacji i systemów informatycznych w organizacji.	K1_CBE_W10
PEU_W06	Przedstawia mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację	K1_CBE_W10
Z zakresu umiejętności		
PEU_U01	Przygotowuje wstępny przegląd standardów ochrony informacji, przedstawia założenia poszczególnych dokumentów normatywnych i prawnych	K1_CBE_U08
PEU_U02	Stosuje niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację.	K1_CBE_U08
PEU_U03	Przygotowuje wstępny przegląd standardów ochrony informacji	K1_CBE_U08
PEU_U04	Planuje założenia i zakres Polityki Bezpieczeństwa Informacji organizacji	K1_CBE_U08

Treści programowe zapewniające uzyskanie efektów uczenia się

Ochrona informacji, przeprowadzanie analizy procesów biznesowych i zasobów teleinformatycznych oraz wdrażanie Systemów Zarządzania Bezpieczeństwem Informacji. Prawne aspekty ochrony informacji, pojęcie informacji chronionej i klasyfikacja rodzajów chronionych informacji, systemowe zarządzanie bezpieczeństwem informacji, polityka bezpieczeństwa informacji, norma ISO 27001,
szacowanie ryzyka bezpieczeństwa informacji, modele bezpieczeństwa i ochrony informacji w przedsiębiorstwie, audyt bezpieczeństwa informacji.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Seminarium	15
Samodzielne studiowanie tematyki zajęć	15
Przygotowanie do egzaminu/zaliczenia	20
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Sieci komputerowe 1

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 30	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Charakteryzuje rolę i zastosowanie sieci komputerowej. Zna modele odniesienia ISO/OSI i TCP/IP	K1_CBE_W15
PEU_W02	Nazywa funkcje warstwy fizycznej i łącza danych na przykładzie sieci Ethernet	K1_CBE_W15
PEU_W03	Wyjaśnia funkcje warstwy sieciowej, sposób adresacji IPv4 oraz IPv6 i podział na podsieci	K1_CBE_W15
PEU_W04	Dobiera odpowiednią adresację IP dla sieci, topologię oraz rodzaj okablowania	K1_CBE_W15
PEU_W05	Wyjaśnia funkcje warstwy transportowej i aplikacji oraz opisuje protokoły sieciowe w nich stosowane	K1_CBE_W15

Z zakresu umiejętności		
PEU_U01	Dobiera i wdraża parametry urządzeń z sieciowym systemem operacyjnym	K1_CBE_U12
PEU_U02	Testuje sieci przy użyciu narzędzi diagnostycznych i analizatorów protokołów	K1_CBE_U12
PEU_U03	Weryfikuje działanie routera, funkcje wyboru trasy i sprawdza zawartość tablicy routowania	K1_CBE_U12
PEU_U04	Weryfikuje działanie przełącznika i sprawdza zawartość tablicy MAC	K1_CBE_U12
PEU_U05	Przygotowuje konfigurację routera, podstawowe parametry i routowanie statyczne	K1_CBE_U12
PEU_U06	Planuje i uruchamia niewielką sieć zawierającą hosty, router i przełącznik	K1_CBE_U12

Treści programowe zapewniające uzyskanie efektów uczenia się

Sieci komputerowe związane z ich funkcjonowaniem, modelem odniesienia, topologią, elementami sieci i protokołami komunikacyjnymi, działanie urządzeń sieciowych, konfigurowanie hostów i ruterów do pracy w sieci lokalnej, stosowanie narzędzi diagnostycznych, obserwacja i analiza zdarzeń sieciowych. Model ISO/OSI: jakie funkcje realizują, jakie protokoły są do nich przypisane i jaki sprzęt sieciowy pracuje w odpowiednich warstwach.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	30
Samodzielne studiowanie tematyki zajęć	40
Przygotowanie do egzaminu/zaliczenia	20
Przygotowanie do zajęć	20
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Programowanie skryptowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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	• Laboratorium: 45 godz., 5 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Tworzy skrypty automatyzujące zadania systemowe za pomocą Basha albo PowerShella	K1_CBE_U02
PEU_U02	Tworzy skrypty w języku Python, które pobierają i przetwarzają dane pobrane z Internetu	K1_CBE_U02
PEU_U03	Testuje podatności serwerów i aplikacji na ataki sieciowe za pomocą skryptów w języku Python	K1_CBE_U02

Treści programowe zapewniające uzyskanie efektów uczenia się

Automatyzacja zadań w środowiskach systemowych Bash, Powershell, przetwarzanie danych z sieci, obsługa usług komunikacyjnych za pomocą skryptów, pozyskiwanie i analiza danych, geolokalizacja, metadane, zabezpieczanie danych - techniki kryptograficzne, testowanie odporności systemów na zagrożenia sieciowe. Treści dostosowywane do poziomu grupy i bieżących potrzeb.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Laboratorium	45
Samodzielne studiowanie tematyki zajęć	45
Przygotowanie do egzaminu/zaliczenia	35
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Wprowadzenie do systemów komputerowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Technologie informacyjne

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 45	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje budowę systemów operacyjnych.	K1_CBE_W03
PEU_W02	Objaśnia zasady działania podsystemów systemu operacyjnego	K1_CBE_W03
PEU_W03	Wyjaśnia podstawowe algorytmy szeregowania zadań.	K1_CBE_W03
PEU_W04	Charakteryzuje działanie typów systemów rozproszonych i rozproszonych systemów plików.	K1_CBE_W03
Z zakresu umiejętności		
PEU_U01	Eksploatuje system operacyjnego Linux w zakresie średnio zaawansowanego użytkownika.	K1_CBE_U03

PEU_U02	Tworzy proste skrypty powłoki stosując podstawowe konstrukcje pętli, instrukcji warunkowych oraz metod przekazywania parametrów.	K1_CBE_U03
PEU_U03	Planuje i przeprowadza ocenę eksperymentalną prostych algorytmów szeregowania.	K1_CBE_U03
PEU_U04	Planuje i przeprowadza ocenę eksperymentalną prostych algorytmów zastępowania stron.	K1_CBE_U03

Treści programowe zapewniające uzyskanie efektów uczenia się

Podstawy działania i budowy systemów operacyjnych, systemy operacyjne Linux i powłoka bash, struktura systemów operacyjnych, procesy - pojęcie i koordynacja, komunikacja międzyprocesowa, zarządzanie pamięcią operacyjną, model dyskretny pamięci operacyjnej, pamięć wirtualna, systemy plików, organizacja struktury katalogowej, ochrona plików, funkcje systemu wejścia-wyjścia.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	45
Przygotowanie do zajęć	20
Przygotowanie do egzaminu/zaliczenia	15
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Zaawansowana kombinatoryka

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kształcenia podstawowego - matematyka

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Ćwiczenia: 15	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje podstawowe i zaawansowane obiekty kombinatoryczne	K1_CBE_W05
PEU_W02	Objaśnia narzędzia kombinatoryki, w szczególności grupy modulo, grupy permutacji, oraz ich własności	K1_CBE_W05
Z zakresu umiejętności		
PEU_U01	Stosuje narzędzia kombinatoryki do rozwiązywania problemów definiowanych na zbiorach przeliczalnych	K1_CBE_U04
PEU_U02	Stosuje wiedzę z kombinatoryki do konstrukcji efektywnych algorytmów szyfrowania	K1_CBE_U04

Treści programowe zapewniające uzyskanie efektów uczenia się

Elementy logiki matematycznej, Elementy teorii liczb. Relacje, klasy abstrakcji. Zasada Dirichleta, włączania - wyłączania. Równania rekurencyjne, funkcje tworzące. Elementy kombinatoryki. Elementy teorii grafów (drzewa spinające, cykle, drogi). Kolorowanie oraz płaskość grafów. Problem komiwojażera.

Nakład pracy studenta

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

Politechnika Wrocławska

Fizyka 1.1A

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kształcenia podstawowego - fizyka

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 2	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Ćwiczenia: 15	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Charakteryzuje modele fizyczne, wskazuje ich ograniczenia.	K1_CBE_W05
PEU_W02	Charakteryzuje prawa związane z ruchem drgającym i zjawiskami falowymi, także w ujęciu optycznym.	K1_CBE_W05
PEU_W03	Wyjaśnia zagadnienia elektryczności oraz prawa elektrostatyki, elektromagnetyzmu.	K1_CBE_W05
PEU_W04	Wyjaśnia prawa optyki geometrycznej i falowej.	K1_CBE_W05
Z zakresu umiejętności		

PEU_U01	Ilościowo i jakościowo opisuje zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się prawami również dotyczącymi ruchu obiektów oraz ruchu drgającego i falowego.	K1_CBE_U04
PEU_U02	Ilościowo i jakościowo opisuje zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się prawami związanymi z przepływem prądu.	K1_CBE_U04
PEU_U03	Ilościowo i jakościowo kategoryzuje zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się prawami optyki geometrycznej i falowej.	K1_CBE_U04

Treści programowe zapewniające uzyskanie efektów uczenia się

Zagadnienia fizyki obejmujące: podstawowe prawa i zasady fizyki - siły, praca i energia mechaniczna. Zasada zachowania energii mechanicznej, zasada zachowania pędu. Oscylator harmoniczny, drgania harmoniczne i swobodne, podstawy elektrostatyki i elektromagnetyzmu. Pole grawitacyjne. Prędkości kosmiczne. Podstawowe prawa i definicje dla przepływu prądu stałego i przemiennego. Zjawiska i prawa optyki geometrycznej, metamateriały. Podstawy modelu falowego w ujęciu skalarnym, interferencja, interferometry. Dyfrakcja, polaryzacja.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Ćwiczenia	15
Samodzielne studiowanie tematyki zajęć	30
Przygotowanie do zajęć	15
Przygotowanie do egzaminu/zaliczenia	31
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Wychowanie fizyczne 1

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
wychowanie fizyczne

Specjalność
-

Jednostka organizacyjna
Politechnika Wrocławska

Poziom kształcenia
studia pierwszego stopnia

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Zajęcia z wychowania fizycznego

Semestry	**Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia**
Semestr 1, Semestr 2, Semestr 3, Semestr 4, Semestr 5	• Ćwiczenia: 30 godz., 0 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Uczestnik zajęć wie, jak zorganizować zgodnie ze swoimi zainteresowaniami trening prozdrowotny z wykorzystaniem zasad wybranej dyscypliny sportowej lub formy rekreacji.	SWF_S1_U01
PEU_U02	Student zna metody treningowe kształtujące cechy motoryczne z wykorzystaniem masy własnego ciała i różnych przyborów.	SWF_S1_U01
PEU_U03	Student zna podstawową technikę ćwiczeń kształtujących potrzebną w przygotowaniu organizmu do wysiłku fizycznego.	SWF_S1_U01
PEU_U04	Student zna podstawowe zasady bezpiecznego zachowania się podczas aktywności ruchowej.	SWF_S1_U01
PEU_U05	Student potrafi opracować plan treningowy krótko- i długoterminowy adekwatny do swoich możliwości.	SWF_S1_U01

PEU_U06	Student zna zasady wzmacniania aparatu stabilizacyjnego głębokiego i obwodowego oraz technikę podstawowych ćwiczeń kształtujących wydolność aerobową i siłową.	SWF_S1_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Zajęcia sportowe – ABT, aikido, badminton, bodyART, body ball, brazylijskie Jiu Jitsu, Callanetics, cuban salsa fit, futsal, joga, jogging, judo, karate, koszykówka, kulturystyka, lekkoatletyka, modelowanie ciała, narciarstwo, Nordic walking, pilates, piłka nożna, piłka ręczna, piłka siatkowa, pływanie, pump, rugby, samoobrona, shape, squash, stretch-one, taniec towarzyski, tenis stołowy, tenis ziemny, trening funkcjonalny, trening prozdrowotny, turystyka górska, turystyka rowerowa, unihokej, wioślarstwo, wspinaczka, zajęcia korekcyjne, zumba, zajęcia korekcyjne dla studentów z niepełnosprawnością.
Sekcje sportowe – aerobik sportowy, badminton, judo, karate, koszykówka, lekkoatletyka, narciarstwo, piłka nożna, piłka ręczna, piłka siatkowa, pływanie, sporty siłowe, szachy, tenis stołowy, tenis ziemny, unihokej , wioślarstwo, wspinaczka.

Nakład pracy studenta

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

Politechnika Wrocławska

Kryptografia stosowana

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 3	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 30	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Identyfikuje i uzasadnia miejsca zastosowania elementów kryptograficznych w kanale telekomunikacyjnym.	K1_CBE_W13
PEU_W02	Wyjaśnia sposób wyznaczania odwrotności liczb w ciałach skończonych, znaczenie liczb pierwszych w kryptografii niesymetrycznej oraz wylicza entropię informacji.	K1_CBE_W13
PEU_W03	Rozpoznaje podstawowe pojęcia stosowane w kryptografii i potrafi je wyjaśnić.	K1_CBE_W13
PEU_W04	Charakteryzuje klasyczne systemy kryptograficzne stosowane przed erą systemów cyfrowych.	K1_CBE_W13

PEU_W05	Identyfikuje metody służące do kryptoanalizy algorytmów kryptograficznych	K1_CBE_W13
PEU_W06	Objaśnia współczesne symetryczne algorytmy kryptograficzne oraz charakteryzuje standardy kryptograficzne wykorzystywane w świecie.	K1_CBE_W13
PEU_W07	Objaśnia współczesne niesymetryczne algorytmy kryptograficzne oraz charakteryzuje standardy kryptograficzne wykorzystywane w świecie.	K1_CBE_W13
PEU_W08	Objaśnia sposoby realizacji podpisów cyfrowych oraz charakteryzuje ich właściwości.	K1_CBE_W13
PEU_W09	Charakteryzuje progowe i bezprogowe systemy dzielenia tajemnicy pomiędzy większą ilość osób.	K1_CBE_W13
PEU_W10	Objaśnia podstawy kryptografii kwantowej oraz przytacza jej wykorzystanie w praktyce.	K1_CBE_W13
PEU_W11	Definiuje pojęcie protokołu kryptograficznego i potrafi go analizować.	K1_CBE_W13
PEU_W12	Wymienia implementacje protokołów kryptograficznych we współczesnych systemach telekomunikacyjnych.	K1_CBE_W13
PEU_W13	Objaśnia sposoby generowania i wykorzystania liczb pierwszych.	K1_CBE_W13
PEU_W14	Wymienia metody zabezpieczenia informacji oraz charakteryzuje protokoły we współczesnych systemach sieciowych, komputerowych oraz systemach ochronny.	K1_CBE_W13
Z zakresu umiejętności		
PEU_U01	Konstruuje szyfrogramy wiadomości za pomocą metod klasycznych.	K1_CBE_U01
PEU_U02	Analizuje szyfrogram pod kątem statystycznym.	K1_CBE_U01
PEU_U03	Tworzy programy do łamania szyfrów utworzonych przy pomocy klasycznych metod kryptograficznych	K1_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Rola kryptografii w zapewnieniu poufności i integralności danych, klasyczne algorytmy kryptograficzne, współczesne algorytmy kryptograficzne. Obowiązujące standardy w zakresie szyfrowania danych, podpisów cyfrowych i dzielenia tajemnicy, rola kryptografii w tworzeniu kryptowalut, metody wymiany kluczy kryptograficznych, w tym również w wykorzystaniem kryptografii kwantowej.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	30
Zaliczenie/Egzamin	4
Przygotowanie do zajęć	30

Samodzielne studiowanie tematyki zajęć	26
Samodzielne doskonalenie umiejętności praktycznych	30
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Programowanie systemowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 3	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 30	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Wyjaśnia model OSI: poszczególne warstwy i przynależność do nich odpowiednich części oprogramowania systemowego i programów użytkownika.	K1_CBE_W02
PEU_W02	Charakteryzuje kontrolę procesów, sposoby uruchamiania procesów w systemie UNIX oraz metody komunikacji między nimi	K1_CBE_W02
PEU_W03	Opisuje metody synchronizacji wątków za pomocą moniotorów i zmiennych warunkowych.	K1_CBE_W02

PEU_W04	Objaśnia podstawowe protokoły sieciowe TCP/IP, potrafi scharakteryzować sposób komunikacji przy użyciu TCP i UDP, zna funkcje systemowe dotyczące gniazdek sieciowych pozwalające na pisanie programów sieciowych	K1_CBE_W02
PEU_W05	Opisuje model działania klient-serwer oraz peer-to-peer	K1_CBE_W02
Z zakresu umiejętności		
PEU_U01	Dobiera systemy i narzędzia służące uruchamianiu procesów, komunikacji między nimi, a także mechanizmy synchronizacji zadań, monitorów, semaforów i zmiennych warunkowych.	K1_CBE_U02
PEU_U02	Tworzy i testuje aplikacje sieciowe działające w architekturze klient-serwer i peer-to-peer z użyciem TCP i UDP.	K1_CBE_U02
PEU_U03	Kompiluje programy w języku C na platformie UNIX oraz korzysta z edytora vim i plików projektowych Makefile	K1_CBE_U02

Treści programowe zapewniające uzyskanie efektów uczenia się

Praktyczna wiedza z zakresu programowania w środowisku UNIX. Komunikacja między procesami i programowania współbieżnego. Wiedza i umiejętności praktyczne dotyczące stosowania mechanizmów synchronizacji procesów, gniazdek sieciowych BSD i programowania komunikacji sieciowej w trybach klient-serwer i peer-to-peer. Umiejętności wyszukiwania i korzystania z dokumentacji technicznej.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	30
Przygotowanie do zajęć	10
Przygotowanie projektu	10
Samodzielne studiowanie tematyki zajęć	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Przygotowanie do egzaminu/zaliczenia	5
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Sieci komputerowe 2

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 3	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 45	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje budowę sieci z przełącznikami i sieciami VLAN.	K1_CBE_W15
PEU_W02	Definiuje zagrożenia i bezpieczeństwo urządzeń	K1_CBE_W15
PEU_W03	Objaśnia mechanizmy nadmiarowości w sieciach lokalnych i działania usługi DHCP	K1_CBE_W15
PEU_W04	Objaśnia routing statyczny i dynamiczny w sieciach IPv4 i IPv6	K1_CBE_W15
Z zakresu umiejętności		
PEU_U01	Przygotowuje konfigurację przełączników Ethernet z użyciem techniki VLAN oraz rozwiązuje problemy w sieciach przełączanych.	K1_CBE_U12

PEU_U02	Przygotowuje konfigurację prostych sieci z użyciem statycznego routingu w sieciach IPv4 i IPv6 oraz rozwiązuje problemy związane z działaniem sieci	K1_CBE_U12
PEU_U03	Przygotowuje konfigurację podstawowych funkcji bezpieczeństwa, mechanizmów nadmiarowości oraz usług serwera i klienta protokołu DHCP	K1_CBE_U12

Treści programowe zapewniające uzyskanie efektów uczenia się

Sieci komputerowe związane z jej funkcjonowaniem, modelem odniesienia, topologią, elementami sieci i protokołami komunikacyjnymi.
Działanie urządzeń sieciowych. Konfigurowanie hostów ruterów i przełączników do pracy w sieci lokalnej, stosowanie narzędzi diagnostycznych, obserwacja i analiza zdarzeń sieciowych. Konfigurowanie podstawowych funkcji bezpieczeństwa na urządzeniach sieciowych, sieci wirtualne VLAN, działanie i konfiguracja protokołu DHCP, ruting statyczny.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	45
Przygotowanie do zajęć	10
Przygotowanie do egzaminu/zaliczenia	13
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Przeprowadzenie badań empirycznych	15
Samodzielne studiowanie tematyki zajęć	15
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Systemy operacyjne

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność -	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty kierunkowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr Semestr 3	**Forma zaliczenia** Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 45	**Liczba punktów ECTS** 6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje posługiwanie się systemem Linux	K1_CBE_W11
PEU_W02	Charakteryzuje administrowanie systemem Linux	K1_CBE_W11
PEU_W03	Definiuje bezpieczeństwo systemów z rodziny Linux	K1_CBE_W11
PEU_W04	Opisuje wirtualizację systemów operacyjnych	K1_CBE_W11
Z zakresu umiejętności		
PEU_U01	Obsługuje system operacyjny Linux w zakresie zaawansowanego użytkownika	K1_CBE_U09
PEU_U02	Administruje systemem operacyjnym Linux	K1_CBE_U09

PEU_U03	Wdraża podstawowe zabezpieczenia systemu operacyjnego Linux	K1_CBE_U09
PEU_U04	Stosuje system wirtualizacji	K1_CBE_U09

Treści programowe zapewniające uzyskanie efektów uczenia się

Użytkowanie systemu z rodziny Linux, lokalnego administrowania systemem z rodziny Linux, sieciowego administrowania systemem z rodziny Linux, bezpieczeństwa systemu z rodziny Linux, wirtualizacji systemów operacyjnych, umiejętności pracy w systemie operacyjnym z rodziny Linux, administrowania systemem operacyjnym z rodziny Linux oraz posługiwania się najbardziej popularnym darmowym systemem

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	45
Samodzielne studiowanie tematyki zajęć	25
Przygotowanie do egzaminu/zaliczenia	20
Przygotowanie raportu/sprawozdania/prezentacji/referatu	30
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Inżynierskie zastosowania statystyki

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kształcenia podstawowego - matematyka

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 3	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Ćwiczenia: 15	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Określa prawdopodobieństwo dyskretne i ciągłe. Wartości oczekiwane. Procesy stochastyczne. Próbkowanie. Estymacja. Testowanie hipotez statystycznych.	K1_CBE_W05
Z zakresu umiejętności		
PEU_U01	Dobiera i stosuje podstawowe testy statystyczne oraz stosować i dobierać metod estymacji dla prostych modeli statystycznych	K1_CBE_U04

Treści programowe zapewniające uzyskanie efektów uczenia się

Zadania testowania hipotez statystycznych i podstawowych testów o parametrach rozkładów oraz

wybranych testów nieparametrycznych.
Wymagania nakładane na estymatory parametrów rozkładów i klasycznych metod ich konstruowania oraz stosowania.
Zastosowania estymacji i testowania hipotez w systemach przetwarzania informacji i telekomunikacji
Umiejętność doboru i stosowania podstawowych testów statystycznych
Umiejętność stosowania i doboru metody estymacji dla prostych modeli statystycznych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Ćwiczenia	15
Przygotowanie do zajęć	70
Samodzielne studiowanie tematyki zajęć	10
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Język obcy 1.1

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
lektoraty

Specjalność
-

Jednostka organizacyjna
Politechnika Wrocławska

Poziom kształcenia
studia pierwszego stopnia

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Języki obce

Semestry	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 2, Semestr 3, Semestr 4, Semestr 5	• 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 określone dla właściwego poziomu językowego: zna i stosuje określone poziomem środki językowe (gramatyczne, leksykalne) oraz ze środowiska akademickiego; posługuje się umiejętnością ogólnego i selektywnego czytania ze zrozumieniem; tworzy pisemne formy wypowiedzi; porozumiewa się w środowisku rodzinnym, towarzyskim, akademickim i zawodowym; rozwija kompetencje społeczne współpracując w grupie i dostrzegając kontekst interkulturowości.	SJO_S1_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Forma zajęć - ćwiczenia. Zagadnienia tematyczne i gramatyczne.
a. A1, A2, B1 język francuski, hiszpański, japoński, niemiecki, polski jako obcy, rosyjski

b. B2.1, C1.1 język angielski, niemiecki; C2.1 angielski
Ogólne treści kształcenia
a. Podstawowe informacje personalne w kontekście uczelni i miejsca pracy, moje najbliższe otoczenie, przebieg dnia, poruszanie się po kampusie i mieście, życie kulturalne, czas wolny, praktyka, wyjazdy zagraniczne, uczelnia, plany zawodowe, miniprojekty
b. autoprezentacja i budowanie zespołu; praca z tekstami specjalistycznymi (w celu zrozumienia ogólnego przekazu tekstu, informacji szczegółowych, kluczowych słów oraz zwrotów; parafrazowanie informacji; streszczanie tekstów); przygotowanie do pracy indywidualnej i projektowej z wybranymi zagadnieniami z języka specjalistycznego związanego ze studiowaną dziedziną; skuteczna komunikacja na tematy związane ze środowiskiem akademickim, naukami technicznymi oraz współczesnym światem.

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

Wychowanie fizyczne 2

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
wychowanie fizyczne

Specjalność
-

Jednostka organizacyjna
Politechnika Wrocławska

Poziom kształcenia
studia pierwszego stopnia

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Zajęcia z wychowania fizycznego

Semestry	**Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia**
Semestr 2, Semestr 3, Semestr 4, Semestr 5, Semestr 6, Semestr 7, Semestr 8	• Ćwiczenia: 30 godz., 0 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Uczestnik zajęć wie, jak zorganizować zgodnie ze swoimi zainteresowaniami trening prozdrowotny z wykorzystaniem zasad wybranej dyscypliny sportowej lub formy rekreacji.	SWF_S1_U01
PEU_U02	Student zna metody treningowe kształtujące cechy motoryczne z wykorzystaniem masy własnego ciała i różnych przyborów.	SWF_S1_U01
PEU_U03	Student zna podstawową technikę ćwiczeń kształtujących potrzebną w przygotowaniu organizmu do wysiłku fizycznego.	SWF_S1_U01
PEU_U04	Student zna podstawowe zasady bezpiecznego zachowania się podczas aktywności ruchowej.	SWF_S1_U01
PEU_U05	Student potrafi opracować plan treningowy krótko- i długoterminowy adekwatny do swoich możliwości.	SWF_S1_U01

PEU_U06	Student zna zasady wzmacniania aparatu stabilizacyjnego głębokiego i obwodowego oraz technikę podstawowych ćwiczeń kształtujących wydolność aerobową i siłową.	SWF_S1_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Zajęcia sportowe – ABT, aikido, badminton, bodyART, body ball, brazylijskie Jiu Jitsu, Callanetics, cuban salsa fit, futsal, joga, jogging, judo, karate, koszykówka, kulturystyka, lekkoatletyka, modelowanie ciała, narciarstwo, Nordic walking, pilates, piłka nożna, piłka ręczna, piłka siatkowa, pływanie, pump, rugby, samoobrona, shape, squash, stretch-one, taniec towarzyski, tenis stołowy, tenis ziemny, trening funkcjonalny, trening prozdrowotny, turystyka górska, turystyka rowerowa, unihokej, wioślarstwo, wspinaczka, zajęcia korekcyjne, zumba, zajęcia korekcyjne dla studentów z niepełnosprawnością.
Sekcje sportowe – aerobik sportowy, badminton, judo, karate, koszykówka, lekkoatletyka, narciarstwo, piłka nożna, piłka ręczna, piłka siatkowa, pływanie, sporty siłowe, szachy, tenis stołowy, tenis ziemny, unihokej , wioślarstwo, wspinaczka.

Nakład pracy studenta

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

Politechnika Wrocławska

Chmury obliczeniowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 4	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 45	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
	Z zakresu wiedzy	
PEU_W01	Objaśnia koncepcję wirtualizacji oraz kluczowe zagadnienia związane z platformą sprzętową oraz oprogramowaniem, modelem warstwowym, a także cechy charakterystycznych chmur obliczeniowych.	K1_CBE_W06
PEU_W02	Definiuje koncepcję kontenerów oraz wiedzę o ich środowiskach uruchomieniowych.	K1_CBE_W06
PEU_W03	Charakteryzuje modele dostarczania usług chmury oraz zakresy odpowiedzialności dostawcy i klienta.	K1_CBE_W06
PEU_W04	Identyfikuje chmury prywatne, publiczne oraz hybrydowe, zna typowe zastosowania oraz zalety i wady poszczególnych rozwiązań.	K1_CBE_W06

PEU_W05	Charakteryzuje usługi z obszaru Compute, Storage i Network - na przykładzie dostawcy usług chmury publicznej Amazon AWS	K1_CBE_W06
Z zakresu umiejętności		
PEU_U01	Zarządza zasobami hipervisorów, tworzyć maszyny wirtualne oraz instalować systemy operacyjne.	K1_CBE_U05
PEU_U02	Instaluje środowiska uruchomieniowe kontenerów oraz uruchamiać przykładowe aplikacje wielo-kontenerowe, takze w środowisku klastra serwerów	K1_CBE_U05
PEU_U03	Zarządza zasobami publicznej chmury obliczeniowej z pozycji klienta chmury, tworzyć projekty oraz zamawiać maszyny wirtualne i usługi	K1_CBE_U05

Treści programowe zapewniające uzyskanie efektów uczenia się

Infrastruktura chmur obliczeniowych oraz aplikacji i usług w chmurach. Uruchamianie usług teleinformatycznych w oparciu o infrastrukturę chmury, a także formułowania charakterystyk chmury obliczeniowej. Wirtualizacja w chmurach obliczeniowych. Charakterystyka chmur obliczeniowych. Model warstwowy chmur obliczeniowych. Koncepcja kontenerów oraz środowisko uruchomieniowe Docker. Usług XaaS w chmurach obliczeniowych. Chmury prywatne, publiczne i hybrydowe. Charakterystyka usług AWS Compute, Storage i VPC.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	45
Przygotowanie do egzaminu/zaliczenia	13
Samodzielne studiowanie tematyki zajęć	50
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Bazy danych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 4	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Laboratorium: 30	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Przedstawia architekturę i zasadę działania podstawowych komponentów SZBD	K1_CBE_W02
PEU_W02	Objaśnia i porównuje podstawowe metody organizacji danych, indeksowania danych oraz przetwarzania i optymalizacji transakcji i zapytań w SZBD	K1_CBE_W02
Z zakresu umiejętności		
PEU_U01	Dobiera i dostosowuje odpowiednie do wymagań narzędzia tworzenia aplikacji baz danych	K1_CBE_U02
PEU_U02	Projektuje i implementuje bazę danych	K1_CBE_U02

Treści programowe zapewniające uzyskanie efektów uczenia się

Historia i podstawowe pojęcia związane z bazami danych,takich jak modele hierarchiczne, relacyjne oraz nowoczesne rozwiązania NoSQL. modelowanie danych- tworzenie modeli koncepcyjnych oraz diagramów ER, przeprowadzanie normalizacji danych w celu optymalizacji struktur bazodanowych, relacyjny model danych- zasady tworzenia i zarządzania tabelami oraz relacjami między nim, nauka języka SQL, obejmująca tworzenie zapytań, modyfikację danych oraz definiowanie struktury bazy.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	30
Przygotowanie do egzaminu/zaliczenia	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	30
Przygotowanie do zajęć	30
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Sieci komputerowe 3

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 4	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 45	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje skalowanie sieci oraz działanie sieci w topologii nadmiarowej z przełącznikami z użyciem VLAN.	K1_CBE_W15
PEU_W02	Opisuje ograniczanie zagrożeń i zwiększanie bezpieczeństwa sieci, korzystając z list kontroli dostępu IPv4 do filtrowania ruchu i bezpiecznego dostępu administracyjnego oraz najlepszych praktyk w zakresie zabezpieczeń.	K1_CBE_W15
PEU_W03	Objaśnia ruting statyczny i dynamiczny oraz działanie protokołów routingu dynamicznego, stanu łącza OSPF w sieciach IPv4 i IPv6.	K1_CBE_W15

PEU_W04	Opisuje projektowanie sieci hierarchicznych i architektury sieci biznesowych oraz technik zapewniających skalowalność adresów i bezpieczny dostęp zdalny dla sieci WAN.	K1_CBE_W15
PEU_W05	Wyjaśnia metody dołączania sieci LAN do ISP oraz typowe protokoły stosowane w publicznych i prywatnych sieciach WAN (protokoły PPP, sieci VPN, usługa translacji adresów NAT).	K1_CBE_W15
PEU_W06	Opisuje zarządzanie siecią (monitorowanie i diagnostykę sieci), wie w jaki sposób urządzenia sieciowe implementują QoS oraz w jaki sposób technologie takie jak wirtualizacja, sieci programowalne i automatyzacja wpływają na rozwijające się sieci.	K1_CBE_W15
Z zakresu umiejętności		
PEU_U01	Stosuje narzędzia diagnostyczne i analizatory protokołów.	K1_CBE_U12
PEU_U02	Konfiguruje i diagnozuje przełączniki i rutery.	K1_CBE_U12
PEU_U03	Przygotowuje konfigurację i diagnozuje sieci VLAN, agregację łączy w technologii EtherChannel, protokół STP oraz porty brzegowe przy użyciu PortFast i BPDU Guard.	K1_CBE_U12
PEU_U04	Przygotowuje konfigurację prostych sieci z użyciem statycznego wyboru trasy i protokołów dynamicznego wyboru tras, stanu łącza OSPF w sieciach IPv4 i IPv6 oraz rozwiązuje problemy związane z działaniem sieci	K1_CBE_U12
PEU_U05	Konfiguruje podłączenia do sieci WAN na routerach i ogranicza zagrożenia oraz zwiększa bezpieczeństwo sieci, korzystając z list kontroli dostępu ACL.	K1_CBE_U12
PEU_U06	Stosuje usługę Network Address Translation na routerach oraz zabezpieczenia na połączeniach site-to-site (łącza VPN).	K1_CBE_U12

Treści programowe zapewniające uzyskanie efektów uczenia się

Sieci przełączane i ich skalowanie, działanie protokołów routingu dynamicznego, stanu łącza i wektora odległości. Metody dołączania sieci LAN do ISP, typowe protokoły stosowane w publicznych i prywatnych sieciach WAN. Umiejętności konfigurowania nadmiarowości i agregacji łączy w przełączanych sieciach LAN, rutingu dynamicznego oraz stosowania narzędzi diagnostycznych, obserwacji i analizy zdarzeń sieciowych. Umiejętności konfigurowania połączeń do i w sieciach WAN, stosowania narzędzi diagnostycznych, obserwacji i analizy zdarzeń sieciowych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	45
Przygotowanie do zajęć	33
Przygotowanie do egzaminu/zaliczenia	30
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Informatyka śledcza

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 4	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 30, w tym zajęcia zdalne: • Laboratorium synchroniczne: 30	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia zasady prowadzenia analizy powłamaniowej.	K1_CBE_W07
PEU_W02	Charakteryzuje zagadnienia i procedury obsługi incydentu teleinformatycznego.	K1_CBE_W07
PEU_W03	Definiuje zagadnienia i metody analizy i przetwarzania dowodów cyfrowych.	K1_CBE_W07
PEU_W04	Rozróżnia i określa parametry dowodów cyfrowych.	K1_CBE_W07
PEU_W05	Objaśnia metody zapewniania rzetelności i niezaprzeczalności dowodów cyfrowych.	K1_CBE_W07

Z zakresu umiejętności		
PEU_U01	Przeprowadza i dokumentuje analizę powłamaniową incydentu teleinformatycznego.	K1_CBE_U06
PEU_U02	Stosuje techniki pozyskiwania dowodów cyfrowych z różnych źródeł.	K1_CBE_U06
PEU_U03	Rozróżnia różne typy zapisu i formatów źródeł dowodów cyfrowych.	K1_CBE_U06
PEU_U04	Stosuje zabezpieczenia dowodów cyfrowych.	K1_CBE_U06
PEU_U05	Określa potrzebne źródła i uzyskuje określone informacje na zadane kwestie.	K1_CBE_U06

Treści programowe zapewniające uzyskanie efektów uczenia się

Analiza powłamaniowa, obsługa incydentu teleinformatycznego, pozyskiwanie i zabezpieczanie dowodów cyfrowych w celach własnej analizy oraz przedstawienia tych dowodów innym podmiotom w tym: prawne aspekty IT pod kątem przygotowania materiałów do postępowań, zasady pozyskiwania danych, nienaruszalność dowodów, rozpoznawanie, pozyskiwanie istotnych informacji, przedstawienie funkcjonalności narzędzi OSS / komercyjnych, metodyka obejścia zabezpieczeń dostępu oraz analizy zdarzeń, metody i procedury obsługi incydentu teleinformatycznego, raportowanie, analiza danych potokowych, śledzenie danych w sieciach.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	30
Przygotowanie do zajęć	15
Przygotowanie raportu/sprawozdania/prezentacji/referatu	30
Samodzielne studiowanie tematyki zajęć	20
Przygotowanie do egzaminu/zaliczenia	13
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Ochrona systemów operacyjnych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 4	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 45, w tym zajęcia zdalne: • Laboratorium synchroniczne: 45	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych.	K1_CBE_W11
PEU_W02	Rozróżnia podstawowe metody uwierzytelniania i autoryzacji, rozumie działanie mechanizmów kontroli dostępu w systemach komputerowych	K1_CBE_W11
PEU_W03	Objaśnia podstawowe pojęcia audytu technicznego i testów penetracyjnych.	K1_CBE_W11
PEU_W04	Uzasadnia zastosowanie narzędzi: monitorowania bezpieczeństwa systemów, audytu technicznego i testów penetracyjnych.	K1_CBE_W11

Z zakresu umiejętności		
PEU_U01	Analizuje działanie systemu operacyjnego pod kątem bezpieczeństwa (na podstawie dzienników systemowych i innych plików) oraz rozpoznaje zagrożenia oraz ataki.	K1_CBE_U09
PEU_U02	Konfiguruje komponenty bezpieczeństwa systemu	K1_CBE_U09
PEU_U03	Wdraża zalecenia norm i rekomendacji do systemu operacyjnego oraz mierzy ich skuteczność	K1_CBE_U09

Treści programowe zapewniające uzyskanie efektów uczenia się

Metody ochrony systemów operacyjnych przed atakami naruszającymi bezpieczeństwo tych systemów, ataki komputerowe na systemy operacyjne oraz metody wykrywania ataków z tych źródeł, metody zapobiegania atakom oraz minimalizowanie zagrożeń z nich wynikających, a także architektura systemu operacyjnego: jądro, pliki, użytkownicy, procesy, komunikacja sieciowa, mechanizmy uwierzytelniania, użytkownicy w systemie operacyjnym, ochrona pamięci w systemie operacyjnym, ochrona plików, kontrola procesów i dostęp do zasobów, modele dotępu do zasobów, utwardzanie systemu operacyjnego, zagrożenia i ataki na system operacyjny, bezpieczeństwo systemu Linux/Unix, środowisk zwirtualizowanych i aplikacji, narzędzia ochrony sieciowej.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	45
Przygotowanie do zajęć	10
Samodzielne studiowanie tematyki zajęć	40
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Przygotowanie do egzaminu/zaliczenia	6
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Język obcy 1.2

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
lektoraty

Specjalność
-

Jednostka organizacyjna
Politechnika Wrocławska

Poziom kształcenia
studia pierwszego stopnia

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Języki obce

Semestry	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 3, Semestr 4, Semestr 5, Semestr 6	• 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 poziomu minimum B2 ESOKJ; zna, rozumie i stosuje środki językowe (gramatyczne, leksykalne i stylistyczne) typowe dla języka akademickiego, specjalistycznego i technicznego stosowane w dziedzinie studiowanego kierunku stosowane w środowisku akademickim i zawodowym; skutecznie porozumiewa się w zespołach interdyscyplinarnych ćwicząc umiejętność komunikacji, kreatywności i krytycznego myślenia; docenia potrzebę doskonalenia swoich umiejętności w zakresie języka specjalistycznego.	SJO_S1_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

Forma zajęć - ćwiczenia. Zagadnienia tematyczne i gramatyczne.

B2.2 język angielski, francuski, hiszpański, niemiecki
C1.2 język angielski, niemiecki
Ogólne treści kształcenia
Autoprezentacja i budowanie zespołu, np. własny profil studenta w kontekście uczelni technicznej oraz zainteresowań w obszarze nauk ścisłych; efektywne prezentowanie siebie, swoich zainteresowań i pomysłów w kontekstach akademickich i zawodowych, interaktywne zadania budujące zespół.
Prezentacja na temat związany z kierunkiem studiów oraz zainteresowaniami naukowymi studentów – struktura prezentacji, opracowanie oraz omówienie materiałów wizualnych – wykresy, tabele, ilustracje; stosowanie charakterystycznych zwrotów i wyrażeń, przedstawienie prezentacji oraz przeprowadzenie dyskusji odnoszącej się do przedstawionej prezentacji.
Przygotowanie do pracy indywidualnej i projektowej z wybranymi zagadnieniami z języka specjalistycznego związanego ze studiowaną dziedziną – materiały wyselekcjonowane przez studentów i prowadzącego.
Język w komunikacji na tematy akademickie z wykorzystaniem języka specjalistycznego – np. formułowanie oraz wymiana poglądów popartych argumentami, włączanie się do dyskusji, parafrazowanie przedstawionych treści, przechodzenie do kolejnych punktów, podsumowywanie wypowiedzi, stosowanie charakterystycznych zwrotów i wyrażeń; branie udziału w różnych formach interakcji, używanie różnorodnych strategii dyskursu.

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

Bezpieczeństwo sieci komputerowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 5	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 60	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Rozróżnia zagrożenia i zabezpieczanie urządzeń teleinformatycznych. Zna koncepcję uwierzytelniania, kontroli dostępu i rozliczalności (AAA).	K1_CBE_W15
PEU_W02	Charakteryzuje systemy zapór sieciowych oraz implementacje systemów ochrony przed włamaniami sieciowymi (IPS).	K1_CBE_W15
PEU_W03	Objaśnia metody zabezpieczania sieci LAN oraz techniki szyfrowania używane w połączeniach VPN.	K1_CBE_W15
PEU_W04	Wyjaśnia koncepcję zarządzania bezpieczną siecią oraz funkcjonalność dedykowanych zapór sieciowych (ASA).	K1_CBE_W15
Z zakresu umiejętności		

PEU_U01	Zabezpiecza dostęp administracyjny na routerach.	K1_CBE_U12
PEU_U02	Konfiguruje zapory sieciowe.	K1_CBE_U12
PEU_U03	Konfiguruje systemy ochrony przed włamaniami sieciowymi (IPS).	K1_CBE_U12
PEU_U04	Konfiguruje funkcje bezpieczeństwa na urządzeniach warstwy drugiej	K1_CBE_U12
PEU_U05	Tworzy konfiguracje sieci VPN i tunelowanie ruchu na routerach i dedykowanych zaporach sieciowych	K1_CBE_U12

Treści programowe zapewniające uzyskanie efektów uczenia się

Metody i mechanizmy bezpieczeństwa w sieciach komputerowych, ochrony dostępu, filtrowania ruchu oraz utajniania treści. Metody uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom. Umiejętności konfigurowania i uruchamiania mechanizmów bezpieczeństwa na routerach, tuneli szyfrowanych i mechanizmów zapobiegania atakom z sieci

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	60
Przygotowanie do zajęć	26
Przygotowanie do egzaminu/zaliczenia	5
Samodzielne studiowanie tematyki zajęć	25
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Bezpieczeństwo w wytwarzaniu i przesyle energii elektrycznej

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo infrastruktury krytycznej

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 5	• Wykład: 30 godz., 3 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Charakteryzuje podstawowe zagrożenia dla systemów elektroenergetycznych, w tym zagrożenia fizyczne, cybernetyczne i techniczne, oraz wskazuje metody ochrony przed tymi zagrożeniami.	K1_CBE_W14
PEU_W02	Opisuje elementy infrastruktury systemu elektroenergetycznego, w tym elektrownie, transformatory, linie przesyłowe, oraz rozróżnia ich funkcje w zapewnianiu stabilności i bezpieczeństwa systemu.	K1_CBE_W14

Treści programowe zapewniające uzyskanie efektów uczenia się

Zagrożenia dla bezpieczeństwa w systemach wytwarzania i przesyłu energii elektrycznej, z uwzględnieniem specyfiki systemów energetycznych, oraz przedstawienie metod i narzędzi służących ochronie infrastruktury krytycznej przed cyberatakami i innymi zagrożeniami.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Wykład	30
Samodzielne studiowanie tematyki zajęć	30
Przygotowanie do egzaminu/zaliczenia	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Bezpieczeństwo w sieciach bezprzewodowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo systemów informatycznych

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 5	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 30	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
	Z zakresu wiedzy	
PEU_W01	Charakteryzuje podstawowe parametry systemów telekomunikacyjnych. Posiada podstawową wiedzę o metodach szacowania pojemności oraz wynikowej sprawności radiowych systemów bezprzewodowych w określonej technice wielodostępu.	K1_CBE_W14
PEU_W02	Charakteryzuje systemy pracujące w pasmach nielicencjonowanych (WLAN, Bluetooth, UWB) oraz pracujące w pasmach licencjonowanych, takie jak UMTS, (DC-)HSPA(+), LTE(-Advanced), 5G.	K1_CBE_W14
PEU_W03	Charakteryzuje metryki jakościowe pomocne w detekcji cyberataków oraz wskazuje metody ich prewencji.	K1_CBE_W14

Z zakresu umiejętności		
PEU_U01	Konfiguruje sieć WLAN, przeprowadza podstawową diagnostykę i nią zarządzać.	K1_CBE_U16
PEU_U02	Konfiguruje pikosieć Bluetooth, przeprowadza podstawową diagnostykę i nią zarządzać.	K1_CBE_U16
PEU_U03	Stosuje narzędzia do testów wydajnościowych sieci WLAN oraz Bluetooth.	K1_CBE_U16
PEU_U04	Obsługuje analizator widma.	K1_CBE_U16
PEU_U05	Konfiguruje ustawienia zapewniające wymagany poziom bezpieczeństwa urządzeń dostępowych systemów bezprzewodowych oraz założone parametry bezpieczeństwa transmisji.	K1_CBE_U16
PEU_U06	Wykonuje szacunkowe wyliczenia spodziewanych zakłóceń w segmencie dostępowym na podstawie znajomości charakterystyk toru odbiorczego systemu zakłócanego i charakterystyk torów nadawczych systemów zakłócających.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Aspekty z zakresu współczesnych sieci radiowych o różnym zasięgu i charakterze, metody szacowania pojemności, przewidywania zagrożeń z zakresu kompatybilności elektromagnetycznej oraz szacowania osiągów interfejsu bezprzewodowego, konfiguracja urządzeń ze szczególnym uwzględnieniem zasad cyberbezpieczeństwa (metodyk detekcji ataków i ich prewencji). Zagrożenia oraz sposoby zapewnienia bezpieczeństwa sieci WLAN, Bluetooth, RFiD, NFC

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	30
Samodzielne studiowanie tematyki zajęć	10
Przygotowanie do egzaminu/zaliczenia	15
Przygotowanie do zajęć	5
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Bezpieczeństwo elektromagnetyczne

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność -	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty kierunkowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr Semestr 5	**Forma zaliczenia** Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 30	**Liczba punktów ECTS** 5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje zagrożenia oraz skutki wynikające z elektromagnetycznego ulotu informacji jak i oddziaływania zaburzeń elektromagnetycznych wytwarzanych celowo i w sposób niezamierzony w środowisku użytkowania urządzeń, systemów i sieci, w tym możliwych ataków elektromagnetycznych.	K1_CBE_W01
PEU_W02	Nazywa rozwiązania techniczne i organizacyjne, które poprawiają bezpieczeństwo elektromagnetyczne i niezawodność działania urządzeń, systemów, sieci.	K1_CBE_W01
PEU_W03	Charakteryzuje wymagania w zakresie bezpieczeństwa elektromagnetycznego, stosowanych zabezpieczeń i środków ochrony.	K1_CBE_W01

PEU_W04	Charakteryzuje rodzaje i charakterystyki zaburzeń elektromagnetycznych oraz zna mechanizmy i drogi ich rozprzestrzeniania.	K1_CBE_W01
PEU_W05	Wylicza pojęcia odporność i podatność na zaburzenia elektromagnetyczne oraz emisję elektromagnetyczną i kanały ulotu informacji.	K1_CBE_W01
PEU_W06	Rozróżnia architekturę bezpieczeństwa sieci oraz systemów oraz identyfikuje elementy architektury (infrastruktury, urządzeń końcowych i aplikacji).	K1_CBE_W01
PEU_W07	Klasyfikuje metody szacowania ryzyka czasowego lub całkowitego uszkodzenia lub zaburzenia pracy infrastruktury, jej elementów, w tym urządzeń końcowych i aplikacji.	K1_CBE_W01
PEU_W08	Identyfikuje metody ochrony organizacyjnej i technicznej stosowane m.in. dla osób, w budynkach i pomieszczeniach oraz urządzeniach, systemach, sieciach i instalacjach, które ograniczają poziomy narażeń elektromagnetycznych i skutki ich oddziaływania, także pozwalają skutecznie chronić przed elektromagnetycznym ulotem informacji.	K1_CBE_W01
Z zakresu umiejętności		
PEU_U01	Potrafi wytypować odpowiednią metodę pomiarową, przygotować stanowiska pomiarowe, wykonywać podstawowe pomiary emisji ujawniających i badania podatności urządzeń na zaburzenia elektromagnetyczne, sprzężenia elektromagnetyczne oraz wyznaczać parametry techniczne stosowanych zabezpieczeń	K1_CBE_U13
PEU_U02	Potrafi opracować i zinterpretować otrzymane wyniki badań, w tym dokonać klasyfikacji zagrożeń i efektywności stosowanych zabezpieczeń	K1_CBE_U13
PEU_U03	Potrafi rozwiązywać problemy związane z bezpieczeństwem elektromagnetycznym, w tym zastosować w praktyce podstawowe techniki ograniczające poziomy zaburzeń elektromagnetycznych i poprawiające niezawodność działania i bezpieczeństwo w obecności narażeń elektromagnetycznych	K1_CBE_U13
PEU_U04	Potrafi posługiwać się: podstawowymi przyrządami pomiarowymi (m.in., analizatorem widma, oscyloskopem) oraz metodami pomiarowymi w celu lokalizacji i identyfikacji źródła „wycieków” elektromagnetycznych, wykonania podstawowych pomiarów z zakresu ulotu elektromagnetycznego oraz określania skuteczności zastosowanych technik ograniczania ulotu informacji	K1_CBE_U13
PEU_U05	Potrafi krytycznie ocenić rozwiązania naukowo-techniczne stosowane dla oceny i zapewnienia bezpieczeństwa elektromagnetycznego	K1_CBE_U13

Treści programowe zapewniające uzyskanie efektów uczenia się

Bezpieczeństwo elektromagnetyczne, identyfikacja zagrożeń, ataki elektromagnetyczne na urządzenia i systemy, rozwiązania techniczne i organizacyjne zwiększające niezawodność oraz bezpieczeństwo elektromagnetyczne. Techniki badawcze, konfiguracja stanowisk, pomiary parametrów technicznych, klasyfikacja zabezpieczeń, badania emisyjności i podatności, interpretacja wyników.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**

Wykład	15
Laboratorium	30
Przygotowanie do zajęć	28
Przygotowanie raportu/sprawozdania/prezentacji/referatu	30
Przeprowadzenie badań literaturowych	15
Przygotowanie do egzaminu/zaliczenia	5
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Elektroenergetyczna automatyka zabezpieczeniowa

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność bezpieczeństwo infrastruktury krytycznej	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy specjalnościowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty specjalnościowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr	**Forma zaliczenia**	**Liczba punktów ECTS**
Semestr 5	Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 15	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Obajśnia budowę i zasadę działania przekładników prądowych, napięciowych i filtrów składowych symetrycznych oraz analogowych i cyfrowych przekaźników elektroenergetycznych.	K1_CBE_W14
PEU_W02	Opisuje podstawowe kryteria działania zabezpieczeń elektroenergetycznych oraz przedstawić podstawowe charakterystyki jednowejściowych i wielowejściowych przekaźników elektroenergetycznych.	K1_CBE_W14
PEU_W03	Charakteryzuje zasady wyposażania elementów systemu elektroenergetycznego w automatykę zabezpieczeniową i rozumie zasady doboru nastaw tej automatyki.	K1_CBE_W14

Z zakresu umiejętności		
PEU_U01	Projektuje układ pomiarowy, dobrać przyrządy pomiarowe oraz połączyć układ do badania przetworników i przekaźników pomiarowych jedno i wielowejściowych.	K1_CBE_U16
PEU_U02	Wykonuje pomiary charakterystyk, opracowuje wyniki i formułuje wnioski.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Rodzaje elektroenergetycznej automatyki zabezpieczeniowej w powiązaniu z rodzajem zakłócenia w pracy systemu elektroenergetycznego.
Budowa i zasada działania przetworników wielkości pomiarowych zabezpieczeń.
Budowa i zasada działania elektroenergetycznych przekaźników pomiarowych jedno i wielowejściowych.
Zasady i techniki realizacji zabezpieczeń elementów systemu elektroenergetycznego.
Praktyczna umiejętność wykonywania badań elementów elektroenergetycznej automatyki zabezpieczeniowej – przetworników i przekaźników pomiarowych oraz zabezpieczeń elektroenergetycznych.
Praktyczna umiejętność doboru rodzaju i obliczania nastaw zabezpieczeń elektroenergetycznych
Umiejętność pracy w zespole

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	15
Zaliczenie/Egzamin	4
Przygotowanie do zajęć	16
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Przygotowanie do egzaminu/zaliczenia	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Biometria

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność bezpieczeństwo systemów informatycznych	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy specjalnościowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty specjalnościowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr Semestr 5	**Forma zaliczenia** Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 15 Seminarium: 15	**Liczba punktów ECTS** 4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia modalność biometryczną, metody weryfikacji i identyfikacji oraz metryk stosowanych w systemach biometrycznych	K1_CBE_W14
PEU_W02	Objaśnia budowę i zasady działania urządzeń wykorzystywanych w systemach biometrycznych (sond, skanerów itp.) oraz architektury systemów biometrycznych, w tym jej zasadniczych elementów.	K1_CBE_W14
PEU_W03	Wymienia algorytmy, koncepcje oraz techniki pozwalające przetwarzać dane biometryczne oraz uzyskiwać z nich profile użytkowników.	K1_CBE_W14

PEU_W04	Objaśnia kontekst prawny i etyczny związany z biometrią, w tym problemy stronniczości sytemów biomerycznych (ang. bias) oraz ochrony danych osobowych	K1_CBE_W14
PEU_W05	Definiuje procesy standaryzacyjne oraz certyfikacyjne rozwiązań w biometrii	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	Dobiera odpowiednią modalność biometryczną do konkretnych potrzeb scenariusza weryfikacji i identyfikacji tożsamości oraz określić warunki brzegowe dla opracowywanego rozwiązania.	K1_CBE_U16
PEU_U02	Specyfikuje parametry niezbędne do dokonania poprawnej identyfikacji biometrycznej oraz wskazać odpowiednią metodę, aparaturę i oprogramowanie	K1_CBE_U16
PEU_U03	Opracowuje praktyczne rozwiązanie identyfikacyjne bądź weryfikacyjne w oparciu o wybraną platformę (np. mikroprocesorową typu Arduino) dysponując dostępnymi czytnikami (np. linii papilarnych) lub gotowymi danymi cyfrowymi	K1_CBE_U16
PEU_U04	Analizuje krytycznie zaprezentowany materiał o systemach biometrycznych i argumentuje swoje wątpliwości	K1_CBE_U16
PEU_U05	Posługuje się bazami wiedzy naukowej i dobiera źródła literaturowe, w tym artykuły naukowe, do zadanego tematu biometrycznego oraz przygotowuje podsumowanie wybranego zagadnienia.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Zagadnienia interdyscyplinarne związane z przetwarzaniem danych biometrycznych, klasyfikacją, projektowaniem systemów, oceną jakości, scenariuszami wdrożeniowymi, aspektami technicznymi, prawnymi i etycznymi. Projektowanie i analiza systemów, przeciwdziałanie atakom, bezpieczeństwo danych, standaryzacja, interpretacja wskaźników jakości klasyfikatorów biometrycznych, deskryptory dla poszczególnych modalności biometrycznych, wrogie działania wobec systemów biometrycznych i ataki impersonacyjne oraz przeciwdziałanie im.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	15
Seminarium	15
Przygotowanie do zajęć	5
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Samodzielne studiowanie tematyki zajęć	13
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Zagrożenia w funkcjonowaniu infrastruktury elektroenergetycznej

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność bezpieczeństwo infrastruktury krytycznej	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy specjalnościowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty specjalnościowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr	**Forma zaliczenia**	**Liczba punktów ECTS**
Semestr 5	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 15	3.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Przedstawia rolę, funkcjonowanie i wyposażenie stacji elektroenergetycznych.	K1_CBE_W14
PEU_W02	Opisuje narażenia klimatyczne, środowiskowe i eksploatacyjne występujące w stacjach elektroenergetycznych.	K1_CBE_W14
PEU_W03	Opisuje urządzenia prowadzenia ruchu stacji oraz rozwiązania automatyki stacyjnej i systemy sterowania i nadzoru (SSiN) w kontekście bezpieczeństwa pracy i jego zagrożeń.	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	Ocenia narażenia klimatyczne, środowiskowe i eksploatacyjne występujące w stacjach elektroenergetycznych i im przeciwdziałać.	K1_CBE_U16

PEU_U02	Szacuje poziom bezpieczeństwa pracy dla urządzeń prowadzenia ruchu stacji, automatyki stacyjnej i systemów sterowania i nadzoru (SSiN).	K1_CBE_U16
PEU_U03	Ocenia zagrożenia bezpieczeństwa pracy stacji elektroenergetycznej i stosuje adekwatne środki w celu jego ograniczenia.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Funkcje i znaczenie stacji elektroenergetycznych, wyposażenie techniczne, narażenia klimatyczne i środowiskowe, eksploatacja, identyfikacja narażeń i im przeciwdziałanie. Urządzenia prowadzenia ruchu, automatyka, komputerowe systemy sterowania i nadzoru, wspomaganie pracy stacji, zaawansowane rozwiązania w ramach inteligentnych sieci. Bezpieczeństwo pracy stacji elektroenergetycznej, identyfikacja zagrożeń, środki ochrony, uwarunkowania prawne, techniczne, ekonomiczne i społeczne.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	15
Przygotowanie do zajęć	13
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Bezpieczeństwo serwerów i aplikacji Web

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność bezpieczeństwo systemów informatycznych	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy specjalnościowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty specjalnościowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr Semestr 5	**Forma zaliczenia** Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 45	**Liczba punktów ECTS** 6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Wyjaśnia podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych	K1_CBE_W14
PEU_W02	Wymienia metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych	K1_CBE_W14
PEU_W03	Objaśnia działanie certyfikatów SSL i protokołów SSL/TLS	K1_CBE_W14
PEU_W04	Opisuje metody ataków typu XSS, CSRF, ,,code injection'', w szczególności SQLinjection i problemy z przekazywaniem parametrów pomiędzy programami	K1_CBE_W14
Z zakresu umiejętności		

PEU_U01	Ocenia typowe błędy związane z bezpieczeństwem w konfiguracji serwerów sieciowych, konfiguruje serwer WWW	K1_CBE_U16
PEU_U02	Sprawdza integralność danych w systemie komputerowym i wykorzystać techniki kryptograficzne do do zwiększenia bezpieczeństwa systemu.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Bezpieczne programowanie w różnych środowiskach, ze szczególnym uwzględnieniem programowania web (skrypty, muddleware, aplikacje klienckie), metodologie wspomagające tworzenie bezpiecznych programów, takich jak programowanie defensywne i programowanie sterowane testowaniem, typowe ataki na serwery WWW i aplikacje webowe oraz metody zapobiegania atakom na aplikacje webowe oraz minimalizowanie zagrożeń z nich wynikających.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	45
Przygotowanie do zajęć	10
Przygotowanie do egzaminu/zaliczenia	28
Przygotowanie raportu/sprawozdania/prezentacji/referatu	50
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Komunikacja w inteligentnych systemach pomiarowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo infrastruktury krytycznej

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 5	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 15	3.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje podstawy działania oraz zastosowania urządzeń pomiarowych w inteligentnych systemach pomiarowych.	K1_CBE_W14
PEU_W02	Identyfikuje i przedstawia techniki sterowania i technologie komunikacji wykorzystywanych w układach automatyki elektroenergetycznej	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	Dobiera, projektuje i testuje układy inteligentnych systemów pomiarowych i układy automatyki elektroenergetycznej	K1_CBE_U16
PEU_U02	Opracowuje wyniki przeprowadzonych pomiarów i testów. Formułuje wnioski.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Zadania przewodowej oraz bezprzewodowej komunikacji, normalizacja komunikacji przewodowej, architektura sieci elektrycznej, modelowanie urządzeń elektrycznych, architektura warstwowa OSI, funkcjonalność kanału transmisyjnego, przegląd sposobów zabezpieczania sieci PLC, funkcjonalność trybów transmisji w sieci: klient – serwer, p2p, centralizowana, sposoby sprzęgania, problemy aplikacji wybranych czujników/urządzeń pomiarowych, monitorowanie wielkości elektrycznych i nieelektrycznych oraz zdalny pomiar, architektura bezprzewodowych i przewodowych sieci HAN, LAN, komunikacja GOOSE oraz komunikacja MMS, jako część komunikacji zgodnej ze standardem IEC61850, komunikacja między urządzeniami po protokole MODBUS (RS485), komunikacja po protokole DNP3 ze zdalnym Centrum Nadzoru, lokalne stanowisko Systemu Sterowania i Nadzoru (SCADA).

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	15
Przygotowanie do zajęć	10
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Bezpieczeństwo chmur obliczeniowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo systemów informatycznych

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 5	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 45	5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	objaśnia typowe zagrożenia dla środowisk wirtualnych oraz chmur obliczeniowych w centrach danych, w tym sposoby wykrywania włamań sieciowych i kontroli dostępu.	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	planuje oraz implementuje mechanizmy zabezpieczające w środowisku chmur obliczeniowych.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Wiedza z zakresu zabezpieczania chmur obliczeniowych - polityki, kontrakty i zarządzanie na wszystkich warstwach.

Poszerzenie umiejętności z zakresu zabezpieczania chmur obliczeniowych w tym: zagrożenia, standardy bezpieczeństwa dla środowisk chmur obliczeniowych, bezpieczeństwo infrastruktury, koncepcja Software Defined Networks (SDN), ochrona w chmurach publicznych na przykładzie Amazon AWS IAM i AWS VPC, bezpieczeństwo danych w chmurach obliczeniowych, metody kryptograficzne, zarządzanie kluczami i certyfikatami, zarządzanie dostępem uprzywilejowanym.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	45
Przygotowanie do egzaminu/zaliczenia	13
Samodzielne studiowanie tematyki zajęć	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Zaburzenia jakości energii elektrycznej

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo infrastruktury krytycznej

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 5	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 15	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje zagadnienia związane z zaburzeniami jakości energii elektrycznej, zna dokumenty legislacyjne i regulacje dotyczące wymogów w tym zakresie	K1_CBE_W14
PEU_W02	Przedstawia obecny stan rozwoju urządzeń i systemów monitorowania jakości energii elektrycznej oraz zasady tworzenia raportów oceny jakości energii elektrycznej	K1_CBE_W14
PEU_W03	Opisuje potencjalne źródła zaburzeń jakości energii oraz ich wpływu na pracę urządzeń elektrycznych	K1_CBE_W14
Z zakresu umiejętności		

PEU_U01	Oblicza i ocenia parametry charakteryzujące jakość energii elektrycznej	K1_CBE_U16
PEU_U02	Łączy podstawowe źródła zaburzeń z ich potencjalnym wpływem na pracę elementów sieci elektroenergetycznych, stosuje procedury przeprowadzania badań odporności odbiorników energii elektrycznej na zaburzenia jakości energii	K1_CBE_U16
PEU_U03	Dobiera i ocenia wybrane rozwiązania poprawy jakości napięcia zasilającego	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Parametry definiujące jakość energii oraz norm i przepisów dedykowanych poziomom dopuszczalnym i metodom oceny jakości energii, zjawiska dotyczące zaburzeń jakości energii, źródeł i skutków tych zaburzeń, zastosowanie analizatorów jakości energii oraz metodyki oceny i wykonywania raportów.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	15
Przygotowanie do zajęć	15
Samodzielne studiowanie tematyki zajęć	20
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Podstawy elektrotechniki

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność bezpieczeństwo infrastruktury krytycznej	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy specjalnościowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty specjalnościowe
Profil studiów profil ogólnoakademicki	

Semestr Semestr 5	**Forma zaliczenia** Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30	**Liczba punktów ECTS** 2.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia prawa elektrotechniki, pola elektrycznego i magnetycznego prądu elektrycznego wraz ze zjawiskami związanymi z indukcyjnością elektromagnetyczną i polem magnetycznym w urządzeniach i maszynach elektrycznych.	K1_CBE_W14
PEU_W02	Objaśnia budowę i zasadę działania transformatorów i silników elektrycznych prądu przemiennego i stałego oraz bezpieczną obsługę urządzeń elektrycznych niskiego napięcia i zna odpowiednie środki i metody ochrony przeciwporażeniowej.	K1_CBE_W14

Treści programowe zapewniające uzyskanie efektów uczenia się

Elektrotechnika, pojęcia związane z pracą i eksploatacją elementów elektrycznych, z wiedzą na temat np. elektrostatyki, prądu elektrycznego, napięcia, indukcji elektromagnetycznej oraz fal elektromagnetycznych pozwolą na wykonywanie badań obwodów elektrycznych prądu stałego i przemiennego, realizowanych na innych przedmiotach.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Przygotowanie do zajęć	10
Przeprowadzenie badań literaturowych	5
Przygotowanie do egzaminu/zaliczenia	5
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

Politechnika Wrocławska

Zarządzanie projektami IT

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy

Blok zajęciowy
Przedmioty kierunkowe

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 6	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Projekt: 15	2.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje metody zarządzania projektami	K1_CBE_W08
PEU_W02	Przedstawia monitorowanie postępu projektu	K1_CBE_W08
Z zakresu umiejętności		
PEU_U01	Dobiera i stosuje metodykę zarządzania projektami	K1_CBE_U07
PEU_U02	Przygotowuje harmonogramy i alokować zasoby.	K1_CBE_U07
PEU_U03	Kontroluje realizację projektu	K1_CBE_U07

Treści programowe zapewniające uzyskanie efektów uczenia się

Podstawowe zasady zarządania projektami IT. Przegląd różnych metodologii. Umiejętność wyboru metodologii do konkretnego projektu. Fazy zarzadzania projektem, planowanie projektu: harmonogram, zasoby, monitorowanie postępów i zarzadzanie zmianą, wybrane metodyki zarzadzania projektami.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	15
Przygotowanie projektu	10
Przygotowanie do egzaminu/zaliczenia	10
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

Politechnika Wrocławska

Testy penetracyjne

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 6	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 45	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje koncepcję oraz cele testowania penetracyjnego.	K1_CBE_W09
PEU_W02	Objaśnia sposoby i narzędzia do prowadzania testów penetracyjnych.	K1_CBE_W09
Z zakresu umiejętności		
PEU_U01	Planuje i przygotowuje procedury testowania penetracyjnego.	K1_CBE_U10
PEU_U02	Stosuje podstawowe testy penetracyjne w obszarze infrastruktury teleinformatycznej oraz na poziomie aplikacji internetowych.	K1_CBE_U10
PEU_U03	Prezentuje i omawia w sposób logiczny i zrozumiały opracowane koncepcje oraz dokumentację techniczną.	K1_CBE_U10

Treści programowe zapewniające uzyskanie efektów uczenia się

Narzędzia i techniki 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. Planowanie i przeprowadzanie testów penetracyjnych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	45
Przygotowanie raportu/sprawozdania/prezentacji/referatu	30
Przygotowanie do egzaminu/zaliczenia	8
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Przetwarzanie dużych zbiorów danych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo systemów informatycznych

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 6	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Projekt: 15	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
	Z zakresu wiedzy	
PEU_W01	Określa potrzeby oraz wyzwania związane z rozwojem systemów baz danych i przetwarzaniem dużych wolumenów danych, uwzględniając wymagania analityki biznesowej oraz tworzenia hurtowni danych.	K1_CBE_W14
PEU_W02	Wyjaśnia procesy związane z ekstrakcją, transformacją i ładowaniem danych (ETL), a także rozpoznaje modele logiczne oraz warstwy hurtowni danych wykorzystywane w analizie dużych zbiorów danych.	K1_CBE_W14

PEU_W03	Formułuje podstawowe pojęcia związane z rozproszonym uczeniem maszynowym, dobiera odpowiednie techniki inżynierii cech i trenowania modeli, oraz wskazuje wzorce wdrażania modeli uczenia maszynowego w środowisku produkcyjnym.	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	Projektuje modele logiczne systemów do przetwarzania dużych wolumenów danych, opracowuje strukturę systemów analityki biznesowej oraz wdraża procesy przetwarzania danych, uwzględniając potrzeby firm w zakresie analizy danych.	K1_CBE_U16
PEU_U02	Tworzy procesy ekstrakcji, transformacji i ładowania danych (ETL), stosuje odpowiednie techniki raportowania analitycznego oraz dostosowuje narzędzia do specyficznych wymagań środowiska analitycznego.	K1_CBE_U16
PEU_U03	Tworzy rozwiązania z zakresu rozproszonego uczenia maszynowego, testuje modele za pomocą Spark MLlib, wdraża odpowiednie wzorce implementacji modeli oraz kontroluje cykl życia eksperymentów przy użyciu MLflow.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Przetwarzanie i analiza danych, pozyskiwanie wiedzy z dużych zbiorów, modele logiczne systemów danych, analityka biznesowa i hurtownie danych, procesy ekstrakcji, transformacji i ładowania danych, raportowanie analityczne, uczenie maszynowe, wprowadzenie do Spark i PySpark, cykl życia eksperymentów, pobieranie danych i wstępne przetwarzanie danych, statystyki opisowe, inżynieria cech, trenowanie modeli, wdrażanie rozwiązań uczenia maszynowego dla dużych zbiorów danych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	15
Przygotowanie do egzaminu/zaliczenia	10
Samodzielne studiowanie tematyki zajęć	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Bezpieczeństwo systemów sterowania i nadzoru w elektroenergetyce

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo infrastruktury krytycznej

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 6	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 30	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia sposoby realizacji łączności pomiędzy zabezpieczeniami elektroenergetycznymi, układami sterowania i regulacji oraz stanowiskiem dyspozytorskim.	K1_CBE_W14
PEU_W02	Charakteryzuje środki stosowane w systemach elektroenergetycznych w celu zapewnienia bezpieczeństwa ich pracy.	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	Dobiera i dokonuje nastaw wartości rozruchowych wielkości kryterialnych zabezpieczeń oraz wyznaczyć charakterystyki podstawowych kryteriów zabezpieczeń elektroenergetycznych	K1_CBE_U16

PEU_U02	Wdraża metody nawiązywania komunikacji cyfrowej między zabezpieczeniem elektroenergetycznym a sterownikiem polowym (koncentratorem), jako elementem Systemu Sterowania i Nadzoru.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Zabezpieczenia sieci elektroenergetycznych, konfiguracja urządzeń i stanowisk, nastawianie parametrów rozruchowych, metody badania zabezpieczeń elektroenergetycznych, techniki i narzędzia pomiarowe, aplikacje systemów nadzoru i sterowania, komunikacja, koncentratory, stanowiska operatorskie.

Nakład pracy studenta

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

Politechnika Wrocławska

Metody AI w badaniu zagrożeń w systemach komputerowych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność -	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty kierunkowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr Semestr 6	**Forma zaliczenia** Egzamin **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 30	**Liczba punktów ECTS** 5.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje najważniejsze metody sztucznej inteligencji (AI) i uczenia maszynowego (ML) stosowane w modelowaniu i wykrywaniu zagrożeń / ataków na systemy komputerowe	K1_CBE_W12
PEU_W02	Objaśnia najważniejsze metody wykrywania anomalii / nietypowych profili w danych z monitoringu ruchu sieciowego, monitoringu zdarzeń i obciążenia urządzeń i z innych źródeł	K1_CBE_W12
PEU_W03	Charakteryzuje strukturę i specyfikę zbiorów i źródeł danych wykorzystywanych w modelowaniu i wykrywaniu zagrożeń w systemach komputerowych	K1_CBE_W12
Z zakresu umiejętności		

PEU_U01	Dobiera i stosuje właściwe metody analizy danych w zadaniu analizy zagrożeń lub wykrywania anomalii w zależności od specyfiki ataku i specyfiki źródła danych	K1_CBE_U11

Treści programowe zapewniające uzyskanie efektów uczenia się

Metody AI i uczenia maszynowego w zadaniach związanych z modelowaniem i wykrywaniem zagrożeń w systemach komputerowych, metody analizy danych i uczenia maszynowego, uczenie nadzorowane i nienadzorowane, uczenie w oparciu o dane niezbalansowane, uczenie głębokie, metody wykrywania anomalii, wizualizacja danych wielowymiarowych, bezpieczeństwo systemów AI.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	30
Przygotowanie do zajęć	46
Przygotowanie do egzaminu/zaliczenia	15
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Cyberbezpieczeństwo w Internecie Rzeczy

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo systemów informatycznych

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 6	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 30	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia genezę, zastosowania, stan badań i perspektyw rozwoju, architektury oraz warstwy fizycznej i protokołów wielodostępu stosowanych w systemach IoT	K1_CBE_W14
PEU_W02	Charakteryzuje podstawowe systemy telekomunikacyjne IoT: z grupy 3GPP (NB-IoT, LTE-M/TC), rozwiązań firmowych (LoRa, Weightless, SigFox itp.)	K1_CBE_W14
PEU_W03	Definiuje zagrożenia wynikające ze stosowania systemów i podejścia IoT, zarówno pod kątem sprzętowym jak i programowym, oraz metody przeciwdziałania zagrożeniom w tych zakresach	K1_CBE_W14

Z zakresu umiejętności		
PEU_U01	Konifguruje układ mikroprocesorowy (np. Arduino, Raspberry Pi) do rejestracji odczytów rozmaitych czujników analogowych i cyfrowych	K1_CBE_U16
PEU_U02	Dobiera oraz konstruuje sieć sensorową w segmencie lokalnym z wykorzystaniem jednej z dostępnych technik transmisyjnych (tj. ZigBee, WLAN, Bluetooth, UWB, NRF24L01, 315/433/434 MHz) uwzględniając określone wymagania pomiarowe oraz implementując techniki zapewniające założony poziom cyberbezpieczeństwa	K1_CBE_U16
PEU_U03	Dobiera oraz konstruuje sieć IoT w segmencie dostępowym bądź dalekosiężnym (LPWAN) z zastosowaniem jednej z dostępnych technik transmisyjnych (np. LoRa, NB-IoT) oraz implementując techniki zapewniające założony poziom cyberbezpieczeństwa	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Istota i rola Internetu Rzeczy (IoT) we współczesnych realiach gospodarczych i technologicznych, zastosowania, specyfika i zasady działania systemów stosowanych w Internecie Rzeczy, wiodące standardy transmisyjnych IoT, zagrożenia dla prywatności, urządzeń i sieci IoT, metody przeciwdziałania im, instalowanie i zarządzanie bezpieczną siecią sensorową dostosowaną do określonych potrzeb, z zastosowaniem dostępnych i optymalnych technik transmisyjnych Internetu Rzeczy

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	30
Samodzielne studiowanie tematyki zajęć	15
Przygotowanie do egzaminu/zaliczenia	13
Przygotowanie raportu/sprawozdania/prezentacji/referatu	25
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Cyberbezpieczeństwo inteligentnych sieci elektroenergetycznych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo infrastruktury krytycznej

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 6	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Projekt: 15	3.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje przyczyny i skutki zagrożeń informatycznych dla infrastruktury inteligentnych sieci elektroenergetycznych	K1_CBE_W14
PEU_W02	Identyfikuje i reaguje na incydenty cybernetyczne w systemach IIoT [Industrial Internet of Things]	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	Opracowuje procedury wspierające bezpieczeństwo informatyczne systemów IIoT [Industrial Internet of Things]	K1_CBE_U16
PEU_U02	Podejmuje działania związane z naruszeniem poufności informacji przetwarzanych w inteligentnych sieciach elektroenergetycznych	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Inteligentne sieci elektroenergetyczne jako element infrastruktury krytycznej, bezpieczeństwo informacji, klasyfikacja systemów informacyjnych, strategie ochrony danych w systemach IIoT oraz w sieciach HAN, zarządzanie bezpieczeństwem w systemach zdalnego odczytu, teoria bezpieczeństwa w systemach przemysłowych, zarządzanie rozproszonymi źródłami energii, utrzymanie ciągłości działania systemów IIoT, procedury wznowienia pracy po zakłóceniach.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	15
Przygotowanie do zajęć	15
Przygotowanie projektu	28
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Wykrywanie zagrożeń i reakcja na incydenty

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność -	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty kierunkowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr Semestr 6	**Forma zaliczenia** Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 30	**Liczba punktów ECTS** 4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje organizację i usługi bezpieczeństwa realizowane w ramach Security Operation Center (SOC) oraz sposoby i metody monitorowania oraz detekcji zagrożeń w systemach informatycznych	K1_CBE_W16
PEU_W02	Objaśnia strukturę organizacji i architektury systemów wykrywania zagrożeń.	K1_CBE_W16
PEU_W03	Opisuje systemy wykrywające zagrożenia oraz systemy prewencyjne, rozumie analizę korelacji zdarzeń w systemach komputerowych, wie jak dobrać oraz skonfigurować narzędzia monitorujące zagrożenia.	K1_CBE_W16

Z zakresu umiejętności		
PEU_U01	Posługuje się narzędziami monitorującymi zdarzenia oraz bezpieczeństwo w systemie komputerowym.	K1_CBE_U14
PEU_U02	Przygotowuje system składający się z wielu komponentów do monitorowania zagrożeń.	K1_CBE_U14
PEU_U03	Koreluje zdarzenia pochodzące z wielu źródeł danych i używa wskaźników jakościowych i ilościowych, np. ocenić skuteczność wdrożonego systemu monitorowania.	K1_CBE_U14
PEU_U04	Projektuje rozwiązania mające na celu monitorowanie oraz wykrywanie zagrożeń w systemach informatycznych.	K1_CBE_U14

Treści programowe zapewniające uzyskanie efektów uczenia się

Sposoby monitorowania oraz detekcji zagrożeń w systemach informatycznych.
Systemy wykrywające zagrożenia oraz systemów prewencyjnych, zrozumienie korelacji zdarzeń w systemach komputerowych.
Metodologia doboru oraz parametryzacji narzędzi monitorujących zagrożenia.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	25
Przygotowanie do egzaminu/zaliczenia	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Aplikacje mobilne

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo systemów informatycznych

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 6	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Projekt: 15	2.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	klasyfikuje elementy usługi internetowej	K1_CBE_W14
PEU_W02	definiuje architektoniczny wzorzec projektowy REST	K1_CBE_W14
PEU_W03	rozpoznaje krytyczne ryzyka dla bezpieczeństwa sieciowych interfejsów programistycznych	K1_CBE_W14
PEU_W04	odtwarza dobre praktyki projektowania sieciowych interfejsów programistycznych	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	konstruuje bazę danych dla usługi internetowej	K1_CBE_U16

PEU_U02	kwestionuje zasadność poszczególnych elementów interfejsu programistycznego	K1_CBE_U16
PEU_U03	dokumentuje wykonany samodzielnie sieciowy interfejs programistyczny	K1_CBE_U16
PEU_U04	współpracuje w grupie	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Projektowanie usług internetowych opartych o architektoniczny wzorzec projektowy REST, komunikacja sieciowa, architektura interfejsów, reprezentacja danych, dokumentacja kodu, planowanie struktury systemu, wdrażanie i eksploatacja aplikacji, analiza scenariuszy użycia, działania wrogie wobec systemów, przeciwdziałanie atakom, samodzielna realizacja złożonych zadań projektowych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	15
Przygotowanie projektu	18
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

Politechnika Wrocławska

Systemy zasilania gwarantowanego

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo infrastruktury krytycznej

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 6	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Laboratorium: 15	3.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje mechanizm rozwoju wyładowań piorunowych oraz rodzajów wyładowań doziemnych.	K1_CBE_W14
PEU_W02	Objaśnia zasady ochrony przepięciowej w instalacjach elektroenergetycznych i sygnałowych.	K1_CBE_W14
PEU_W03	Opisuje ekranowanie pola elektromagnetycznego	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	Organizuje próby i badania urządzeń wysokimi napięciami udarowymi, symulującymi przepięcia piorunowe i łączeniowe	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Zasady i technikami realizacji zabezpieczeń instalacji elektrycznych zasilających urządzenia lokalnych sieci komputerowych, praktyczne umiejętności wykonywania badań elementów zabezpieczeniowych. Przedmiot obejmuje również zagadnienia: pole elektromagnetyczne, zakłócenia impulsowe, wyładowania piorunowe, urządzenia i zasady ochrony przeciwprzepięciowej, wyładowania elektrostatyczne, problematyka ekranowania pola elektromagnetycznego, skuteczność ekranowania, materiały na ekrany elektromagnetyczne, systemy zasilania dodatkowego.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	15
Przygotowanie do zajęć	15
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Projekt zespołowy

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 6	• Projekt: 45 godz., 5 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Przygotowuje zadania w ramach realizacji złożonego projektu informatycznego.	K1_CBE_U16
PEU_U02	Stosuje zasady zarządzania projektem do realizacji złożonego projektu informatycznego.	K1_CBE_U16
PEU_U03	Opracowuje dokumentację projektu.	K1_CBE_U16
Z zakresu kompetencji społecznych		
PEU_K01	Podejmuje wyzwanie konieczności należytej współpracy z zespołem, wykazuje się świadomością swojej roli w projekcie oraz dbałością o terminową realizację powierzonych zadań.	K1_CBE_K05

Treści programowe zapewniające uzyskanie efektów uczenia się

Realizacja zadań inżynierskich, praca zespołowa, planowanie, harmonogramowanie, komunikacja w zespole, pełnienie ról, kreatywność, innowacyjność, orientacja na cel zespołowy. Organizacja pracy, zarządzanie czasem, odpowiedzialność za zadania, profesjonalizacja zachowań, etyka zawodowa, otwartość na technologie, świadomość środowiskowa.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Projekt	45
Przygotowanie do zajęć	10
Przygotowanie projektu	50
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Audytowanie sieci teleinformatycznych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
bezpieczeństwo systemów informatycznych

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma zaliczenia	Liczba punktów ECTS
Semestr 7	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 30	3.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Identyfikuje stosowane metody audytu formalnego oraz technicznego a w szczególności podstawowe założenia norm ISO rodziny 27000.	K1_CBE_W14
PEU_W02	Objaśnia strukturę organizacji i architektury systemów wykrywania zagrożeń	K1_CBE_W14
PEU_W03	Wybiera narzędzia i metody audytu technicznego oraz zna wybrane metody audytu technicznego oraz zastosowanie wybranych narzędzi do audytu technicznego i testów penetracyjnych.	K1_CBE_W14
PEU_W04	Objaśnia metodyki zarządzania ryzykiem	K1_CBE_W14
Z zakresu umiejętności		

PEU_U01	Stosuje narzędzia audytu technicznego do przetestowania bezpieczeństwo aplikacji sieciowej	K1_CBE_U16
PEU_U02	Planuje poszczególne etapy testu penetracyjnego i określić ich kryteria	K1_CBE_U16
PEU_U03	Stosuje poszczególne etapy testu penetracyjnego i przygotować raport	K1_CBE_U16
PEU_U04	Opracowuje mapowanie potrzeb (formalnych i związanych z cechami organizacji) oraz niezbędnego poziomu organizacji usług bezpieczeństwa	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Audyt bezpieczeństwa sieci komputerowych, metodologia audytów i testów penetracyjnych, organizacja i prowadzenie audytów i testów penetracyjnych, a także: modele audytu, standardy dotyczące audytowania systemów informatycznych ISACA, COBIT, GTAG, GAIT, normy ISO, metodologie audytu technicznego i testów penetracyjnych, klasyfikacja, przegląd i zastosowanie narzędzi audytorskich, normy bezpieczeństwa ISO/IEC 27000.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	30
Przygotowanie do egzaminu/zaliczenia	8
Samodzielne studiowanie tematyki zajęć	5
Przygotowanie do zajęć	5
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Rozproszone systemy automatyki

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2026/2027
Specjalność bezpieczeństwo infrastruktury krytycznej	**Grupa zajęć** Tak
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Języki wykładowe** polski
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Obligatoryjność** Obowiązkowy specjalnościowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty specjalnościowe
Profil studiów profil ogólnoakademicki	**Przedmiot powiązany z badaniami naukowymi** Tak

Semestr	**Forma zaliczenia**	**Liczba punktów ECTS**
Semestr 7	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 15 Laboratorium: 30	3.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Opisuje stosowanie sterowników PLC oraz sieci komunikacyjnych w rozproszonych systemach automatyki	K1_CBE_W14
PEU_W02	Wyjaśnia charakterystyczne cechy rozproszonego systemu automatyki	K1_CBE_W14
Z zakresu umiejętności		
PEU_U01	Stosuje sterowniki PLC w rozproszonych systemach automatyki	K1_CBE_U16
PEU_U02	Formułuje algorytm sterowania w rozproszonym systemie automatyki oraz napisać program sterujący na wybrany sterownik	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Rozproszone systemów automatyki, wybrane rodzaje przemysłowych sieci komunikacyjnych wykorzystywanych w rozproszonych systemach automatyki, praktyczne zapoznanie z urządzeniami wykorzystywanymi w rozproszonych systemach automatyki. Przedmiot obejmuje również zagdnienia: budowa i programowanie sterowników PLC, systemy czasu rzeczywistego w rozproszonych systemach automatyki, komunikacja w rozproszonych systemach automatyki, systemy SCADA i DCS w rozproszonych systemach automatyki, wymiana danych za pomocą protokołów DDE i OPC.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	30
Przygotowanie do zajęć	5
Przygotowanie raportu/sprawozdania/prezentacji/referatu	2
Przygotowanie projektu	10
Samodzielne studiowanie tematyki zajęć	6
Przygotowanie do egzaminu/zaliczenia	5
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

Politechnika Wrocławska

Metody monitorowania jakości produkcji

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 7	• Wykład: 30 godz., 2 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Objaśnia podstawowe metody monitorowania jakości produkcji	K1_CBE_W04
Z zakresu kompetencji społecznych		
PEU_K01	Identyfikuje problemy w zakresie kontroli jakości.	K1_CBE_K04

Treści programowe zapewniające uzyskanie efektów uczenia się

Podstawowe metody monitorowania jakości produkcji w tym: metody statystyczne wykorzystywane do monitorowania jakości produkcji, wykrywanie zmian jakości – pojęcie karty kontrolnej i kryteria oceny kart kontrolnych, rodzaje błędów, karty do oceny zmian wartości średniej procesu, karty do oceny liczby i prawdopodobieństwa liczby wadliwych produktów, normy kontroli jakości, kamery przemysłowe i na podczerwień w monitorowaniu jakości produkcji.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Wykład	30
Przygotowanie do zajęć	10
Przygotowanie do egzaminu/zaliczenia	10
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

Politechnika Wrocławska

Zarządzanie ryzykiem i polityki bezpieczeństwa

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 7	Zaliczenie na ocenę **Forma dydaktyczna i godziny zajęć** Wykład: 30 Seminarium: 15	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Definiuje ryzyka w systemach informatycznych.	K1_CBE_W10
PEU_W02	Opisuje zasady określania oraz definiowania obszarów ryzyka w systemach.	K1_CBE_W10
PEU_W03	Objaśnia zasady tworzenia matryc ryzyka w oparciu o prawdopodobieństwo oraz wpływ.	K1_CBE_W10
PEU_W04	Określa parametry ryzyka: istotność, wpływ, prawdopodobieństwo.	K1_CBE_W10
PEU_W05	Objaśnia metodykę i zasady tworzenia i analiz polityk bezpieczeństwa.	K1_CBE_W10
Z zakresu umiejętności		

PEU_U01	Analizuje ryzyka związane z procesami przetwarzania informacji.	K1_CBE_U08
PEU_U02	Tworzy stosowne matryce ryzyka dla procesów przetwarzania danych.	K1_CBE_U08
PEU_U03	Dokonuje klasyfikacji różnych typów ryzyk oraz odnosi je do warstwy technologicznej.	K1_CBE_U08
PEU_U04	Ocenia ryzyka związane z użytkowaniem systemów informatycznych.	K1_CBE_U08
PEU_U05	Rozdziela ryzyka procesowe oraz technologiczne.	K1_CBE_U08

Treści programowe zapewniające uzyskanie efektów uczenia się

Zarządzanie ryzykiem w systemach informatycznych.
Analiza i wycena ryzyk.
Określenie i tworzenie zasad bezpieczeństwa oraz tworzenia i analizy polityk bezpieczeństwa.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Seminarium	15
Przygotowanie do zajęć	15
Samodzielne studiowanie tematyki zajęć	15
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Przygotowanie do egzaminu/zaliczenia	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Praca dyplomowa

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

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 7	• Praca dyplomowa: 75 godz., 12 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Wyszukuje informacje z różnych źródeł, dokonuje ich krytycznej analizy, syntezy oraz twórczej interpretacji.	K1_CBE_U16
PEU_U02	Konstruuje i testuje hipotezy dotyczące prostych problemów badawczych.	K1_CBE_U16
PEU_U03	Planuje, analizuje lub wdraża (przynajmniej w części) złożony i bezpieczny system teleinformatyczny mający na celu realizację szeroko rozumianych usług transmisyjnych i przetwarzania danych, używając właściwych metod, technik i narzędzi.	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Formalne wytyczne odnośnie przygotowania pracy pisemnej, opisu literatury i struktury pracy dyplomowej. Wiedzę dotyczącą pracy dyplomowej oraz umiejętności przygotowania badań, weryfikacji, opracowania i prezentacji wyników a także terminowej i systematycznej pracy.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Praca dyplomowa	75
Przygotowanie pracy dyplomowej	120
Przeprowadzenie badań literaturowych	30
Praca z opiekunem nad częścią merytoryczną pracy	75
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 300

Politechnika Wrocławska

Praktyka zawodowa

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy do wyboru

Blok zajęciowy
Praktyka zawodowa

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Liczba punktów ECTS i forma zaliczenia
Semestr 7	• 7 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Organizuje pracę indywidualną i zespołową.	K1_CBE_U15
PEU_U02	Korzysta ze zdobytej wiedzy do twórczego analizowania i rozwiązywania różnych problemów inżynierskich.	K1_CBE_U15
PEU_U03	Prowadzi dyskusję na temat odpowiedzialności za pracę własną, jest otwarty na wymianę myśli i nowe wyzwania.	K1_CBE_U15

Treści programowe zapewniające uzyskanie efektów uczenia się

Weryfikacja wiedzy w kontekście wymagań środowiska zawodowego, zdobycie doświadczenia praktycznego, poznanie wyposażenia technicznego i organizacji pracy. Specyfika pracy dozoru technicznego, rozwijanie umiejętności zawodowych związanych z miejscem praktyki. Organizacja pracy własnej i zespołowej, zarządzanie czasem, odpowiedzialność za zadania. Kształtowanie postaw zawodowych, etyka pracy, otwartość na nowe technologie, świadomość ekologiczna.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Realizacja praktyki zawodowej	175
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 175

Politechnika Wrocławska

Seminarium dyplomowe

Karta przedmiotu

Informacje podstawowe

Kierunek studiów
cyberbezpieczeństwo

Specjalność
-

Jednostka organizacyjna
Wydział Informatyki i Telekomunikacji

Poziom kształcenia
studia pierwszego stopnia (inżynier)

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl kształcenia
2026/2027

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy do wyboru

Blok zajęciowy
Przedmioty specjalnościowe

Przedmiot powiązany z badaniami naukowymi
Tak

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 7	• Seminarium: 30 godz., 2 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Opracowuje prezentację zawierającą wyniki rozwiązań	K1_CBE_U16
PEU_U02	Prowadzi rzeczową dyskusję uzasadniającą swoje oryginalne pomysły i rozwiązania	K1_CBE_U16
PEU_U03	Krytycznie ocenia rozwiązania naukowo-techniczne innych osób	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Pozyskiwanie wiedzy niezbędnej do tworzenia oryginalnych rozwiązań, przygotowanie prezentacji pozwalającej w sposób komunikatywny przekazać słuchaczom swoje oryginalne pomysły, koncpecje i rozwiązania, uzasadnianie stanowiska w dyskusji, opracowanie tekstu prezentującego własne osiągnięcia, odniesienie do kontekstu globalnego, rozwijanie umiejętności argumentacji i prezentacji.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Seminarium	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50