Politechnika Wrocławska

Program studiów

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

Spis treści

Charakterystyka kierunku studiów

Informacje podstawowe

Wydział:	Wydział Informatyki i Telekomunikacji
Kierunek studiów:	cyberbezpieczeństwo
Poziom kształcenia:	studia pierwszego stopnia (inżynier)
Forma studiów:	studia stacjonarne
Profil studiów:	profil ogólnoakademicki
Język prowadzenia studiów:	polski
Obowiązuje od cyklu kształcenia:	2025/2026
Liczba semestrów:	7
Całkowita liczba godzin zajęć:	kierunkowe: 2010 bezpieczeństwo infrastruktury krytycznej: 450 bezpieczeństwo systemów informatycznych: 450
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

Absolwent jest przygotowany 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. W ramach kierunku studenci będą przygotowani również do uzyskania certyfikatów, CCNA (Cisco Certified Network Associate), Network Security, CyberOps Associate. Absolwent może ubiegać się o przyjęcie na studia drugiego stopnia, studia podyplomowe.

Aktualność programu studiów

Koncepcja i cele kształcenia

Realizując program nauczania studenci uczęszczają na zajęcia zorganizowane na zasadach zgodnych z Regulaminem studiów wyższych na Politechnice Wrocławskiej. Zajęcia prowadzone są w formach określonych Regulaminem studiów, przy czym wykorzystywane są zarówno tradycyjne metody i narzędzia dydaktyczne jak i możliwości oferowane przez uczelnianą platformę e-learningową. Poza godzinami zajęć Prowadzący są dostępni dla studentów w wyznaczonych i ogłoszonych na stronie Wydziału godzinach konsultacji. Ważnym elementem uczenia się jest praca własna studenta, polegająca na przygotowywaniu się do zajęć (na podstawie materiałów udostępnianych przez Prowadzących, jak i zalecanej literatury), studiowaniu literatury, opracowywaniu raportów i sprawozdań, przygotowywaniu się do kolokwiów i egzaminów.

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 przez studenta efektów uczenia się, przypisanych do przedmiotu skutkuje brakiem zaliczenia przedmiotu i koniecznością powtórnej jego realizacji.

Studia na kierunu prowadzone są na dwóch specjalnościach: Bezpieczeństwo systemów informatycznych oraz Bezpieczeństwo infrastruktury krytycznej. Podział na specjalności przeprowadzany jest na czwartym semestrze, od piątego studenci realizują zarówno wspólne przedmioty kierunkowe, jak i specjalistyczne przedmioty dopasowane do każdej specjalności. W ramach studiów student realizuje praktykę zawodową w wybranej przez siebie instytucji w wymiarze nie mniejszym niż 4 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 student prezentuje zrealizowaną pracę inzynierską oraz omawia zagadnienia z przebiegu studiów.

Kształcenie na kierunku ukierunkowane jest na przekazanie studentom zarówno wszechstronnej wiedzy technicznej w ramach kierunku studiów, jak i umiejętności i kompetencji interpersonalnych. Niezwykle ważnym celem kształcenia jest wyposażenie absolwentów w kompetencje, które pozwolą im efektywnie funkcjonować na rynku pracy. Stąd na kierunku studenci zdobywają umiejętności między innymi z programowania głównie skrytpowego, zaawansowej konfiguracji i działania sieci komputerowych oraz ich bezpieczeństwa, konfiguracji i zabezpieczania systemów operacyjnych, chmur obliczeniowych czy stosowania sztucznej inteligencji do wykrywania zagrożeń. Studenci przygotowywani są również do przyszłej pracy poprzez wyposażenie ich w kompetencje miękkie, między innymi: praca w grupie i umiejętności komunikacyjne, potrzeba samorozwoju i samokształcenia czy w końcu zarządzanie projektami IT. W ten sposób absolwenci 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 kompentecji 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 wśród studentów i kandydatów, a także dąży do ciągłego udoskonalania oferty dydaktycznej. Na kierunku dominują nauki ścisłe, jednakże student nabywa również umiejętności miękkie co zwiększa jego atrakcyjność na rynku pracy, a to z kolei wzmacnia bezpieczeństwo oraz zwiększa potencjał gospodarczy kraju, co jest również jednym z założeń rozwoju uczelni. Cyberbezpieczeństwo i kryptografia zostały wpisane do strategii Politechniki Wrocławskiej na lata 2023-2030 jako priorytetowe obszary badawcze, ponadto w programie studiów zawarto przedmioty dotyczące między innymi informatyki, telekomunikacji, sieci komputerowych i mobilnych, Internetu Rzeczy, które rónwnież zawarto w priorytetowym obszarze badawczym Politechniki "Technologie informacyjne, nauka o danych i sztuczna inteligencja". Stąd kształcenie wysokiej klasy specjalistów w tych obszarach ma kluczowe znaczenie dla przyszłości Politechniki jako wiodącej uczelni technicznej w kraju. Program studiów umożliwia studentom 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	Zna podstawy metrologii, teorii i techniki pomiarów wielkości elektrycznych. Zna sprzęt pomiarowy stosowany w pomiarach wielkości elektrycznych. Jest w stanie scharakteryzować potrzeby pomiarowe, wskazać wielkości mierzone, dobrać metodykę pomiaru i oszacować niepewność. Zna rolę pomiarów i wpływ miarodajności i dokładności pomiarów w zapewnieniu niezawodności i bezpieczeństwa systemów teleinformatycznych i bieżącej ocenie jakości ich pracy.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W02	Ma wiedzę z zakresu programowania w środowisku UNIX, komunikacji między procesami i programowania współbieżnego.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W03	Zna podstawy technik informatycznych, usług sieciowych oraz technologii zapewnienia bezpieczeństwa związanych z pozyskiwaniem, przetwarzaniem i prezentowaniem informacji.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W04	Ma podstawową i podbudowaną teoretycznie wiedzę niezbędną do rozumienia społecznych, etycznych i filozoficznych uwarunkowań działalności inżynierskiej, zna i rozumie pojęcia z zakresu ochrony własności przemysłowej, prawa autorskiego, przedsiębiorczości i zarządzania jakością.	P6U_W, P6S_WG, P6S_WK	P6S_WK_INŻ
K1_CBE_W05	Ma podstawową wiedzę w zakresie wybranych działów matematyki i fizyki niezbędną do rozumienia zagadnień w zakresie cyberbezpieczeństwa.	P6U_W, P6S_WG	
K1_CBE_W06	Ma wiedzę o architekturze i zasadzie działania podstawowych komponentów SZBD. Potrafi omówić i porównać podstawowe metody organizacji danych, indeksowania danych oraz przetwarzania i optymalizacji transakcji i zapytań w SZBD. Zna kryptograficzne metody stosowane w ochronie SZBD oraz techniki projektowania bezpiecznych baz danych.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W07	Ma podstawową wiedzę o konstrukcji oraz funkcjonowaniu chmur obliczeniowych. Zna cechy charakterystyczne oraz modele dostarczania usług w chmurze obliczeniowej.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W08	Ma wiedzę z zakresu metod zarządzania ryzykiem oraz sposobu ich wyznaczania a także polityki bezpieczeństwa w różnych instytucjach.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W09	Zna zagadnienia i metody analizy i przetwarzania dowodów cyfrowych: rodzaje źródeł, sposoby pozyskiwania, rzetelność i zabezpieczanie dowodów, zna metody analizy artefaktów aktywności. Rozumie opisy dowodów w informatyce śledczej. Zna metody zapewniania rzetelności i niezaprzeczalności dowodów cyfrowych.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W10	Ma wiedzę na temat różnych metodyk zarządzania projektami. Zna procesy związane z zarządzaniem projektami.	P6U_W, P6S_WG	
K1_CBE_W11	Ma podstawową wiedzę oraz zna narzędzia i techniki z zakresu 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.	P6U_W, P6S_WG	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_W12	Ma ogólną wiedzę dotyczącą systemów zarządzania bezpieczeństwem informacji (SZBI) zgodnych z normami/regulacjami europejskimi (NIS) i krajowymi (ustawa KSC), budowy systemów ochrony: informacji niejawnych, danych osobowych i informacji objętych tajemnicą zawodową. Potrafi określić wymagania oraz obszary związane z projektowaniem i wdrażaniem Polityki Bezpieczeństwa Informacji w zależności od charakteru przedsiębiorstwa.Potrafi określić hierarchię i metody dostępu do informacji niejawnej. Potrafi określić ogólne ramy obowiązków osób odpowiedzialnych za ochronę informacji i systemów informatycznych w organizacji.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W13	Posiada podstawową wiedzę z zakresu budowy systemów operacyjnych, roli i zasad działania ich podsystemów, a także zna podstawowe algorytmy szeregowania zadań.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W14	Zna metody sztucznej inteligencji (AI) i metody uczenia maszynowego (ML) wykorzystywane w modelowaniu i wykrywaniu zagrożeń / ataków na systemy komputerowe a także metody wykrywania anomalii / nietypowych profili w oparciu o dane z monitoringu ruchu sieciowego, monitoringu zdarzeń i obciążenia urządzeń i z innych źródeł.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W15	Posiada wiedzę na temat systemów kryptograficznych w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W16	Ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie wybranych działów cyberbezpieczeństwa; zna i rozumie wybrane zagadnienia stanowiące wiedzę szczegółową, właściwe dla programu kształcenia w ramach określonej specjalności.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W17	Ma wiedzę dotyczącą funkcjonowania sieci komputerowych, modelem odniesienia, topologią, elementami sieci, protokołami komunikacyjnymi, w szczególności: potrafi wytłumaczyć działanie urządzeń sieciowych z protokołem TCP/IP, obejmującą planowanie adresacji IP, klasowe i bezklasowe mechanizmy wyboru trasy, rutowanie statyczne i dynamiczne oraz techniki przełączania w sieciach Ethernet.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W18	Zna podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych; Zna podstawowe pojęcia audytu technicznego i testów penetracyjnych; Zna podstawowe narzędzia monitorowania bezpieczeństwa systemów i ich cechy; Zna zastosowanie narzędzi: monitorowania bezpieczeństwa systemów, audytu technicznego i testów penetracyjnych.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W19	Posiada ogólną, przekrojową wiedzę z zakresu kompatybilności elektromagnetycznej (KEM) oraz powiązanymi aspektami bezpieczeństwa elektromagnetycznego i cyberbezpieczeństwa różnych urządzeń i systemów, obejmującą architekturę bezpieczeństwa i potencjalne źródła zagrożeń EM występujące w różnych środowiskach EM (w tym także terroryzm elektromagnetyczny), zjawiska fizyczne i drogi wnikania zaburzeń EM do wnętrza urządzeń oraz ich ulotu na zewnątrz, stosowane techniki oraz środki techniczne i organizacyjne zwiększające poziom bezpieczeństwa EM oraz niezawodność działania urządzeń i systemów, stosowane metody testowania i oceny bezpieczeństwa EM oraz klasyfikacji zabezpieczeń a także Identyfikacji krytycznych infrastruktur, elementów infrastruktury, urządzeń i ich części oraz oprogramowania istotnych dla życia i zdrowia ludzkiego oraz funkcjonowania państwa i gospodarki.	P6U_W, P6S_WG	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_W20	Ma wiedzę z zakresu działania sieci w topologii nadmiarowej z przełącznikami z użyciem VLAN. Zna metody działania i sposób zastosowania protokołów dynamicznego wyboru trasy. Zna typowe protokoły stosowane w sieciach rozległych WAN oraz metody dołączania LAN do ISP.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W21	Zna metody i mechanizmy zapewniające bezpieczeństwo w sieciach komputerowych, w tym: warunkowego dostępu, filtrowania ruchu oraz utajniania treści. Ma wiedzę o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom.	P6U_W, P6S_WG	P6S_WG_INŻ
K1_CBE_W22	Ma ogólną wiedzę na temat organizacji i usług bezpieczeństwa realizowanych w ramach Security Operation Center (SOC) oraz sposobów i metod monitorowania oraz detekcji zagrożeń w systemach informatycznych Ma ogólną wiedzę na temat struktury organizacji i architektury systemów wykrywania zagrożeń.	P6U_W, P6S_WG	P6S_WG_INŻ
Umiejętności			
K1_CBE_U01	Potrafi rozwiązywać zadania obliczeniowe z użyciem narzędzi komputerowych.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U02	Potrafi przygotować i skonfigurować środowisko uruchomieniowe oraz uruchamiać skrypty dla różnych języków programowania. Potrafi napisać skrypty przetwarzające dane z plików; pobierać i przetwarzać dane z internetu za pomocą interfejsów API. Potrafi automatyzować za pomocą skryptów zadania systemowe.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U03	Umie zapisać algorytm w postaci schematu blokowego, podać rozwiązanie prostych zadań w postaci algorytmów oraz podać sposób ich testowania. Umie korzystać ze środowiska informatycznego oraz programować z użyciem typów prostych, łańcuchów znakowych, pętli, procedur i funkcji.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U04	Umie posługiwać się edytorami tekstów, arkuszami kalkulacyjnymi, wykonać prezentację multimedialną, publikować informacje w sieci, przesyłać dane w sieci, kontrolować i konfigurować politykę bezpieczeństwa aplikacji.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U05	Potrafi posługiwać się metodami matematyki i fizyki do rozwiązywania szczegółowych problemów w obszarze cyberbezpieczeństwa.	P6U_U, P6S_UW	
K1_CBE_U06	Potrafi wybrać i dostosować odpowiednie do wymagań narzędzia tworzenia aplikacji baz danych oraz samodzielnie zaprojektować i zaimplementować bazę danych. Umie wykonać analizy oraz projektować i implementować mechanizmy bezpieczeństwa w bazach danych.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U07	Potrafi uruchamiać i konfigurować usługi serwerowe oraz komunikacyjne w środowisku wirtualnym oraz dobierać odpowiednie technologie dla usług świadczonych przez chmury obliczeniowe.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U08	Potrafi stosować mechanizmy synchronizacji procesów oraz programować komunikację sieciową w trybach klient-serwer i peer-to-peer.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U09	Potrafi stosować techniki pozyskiwania dowodów cyfrowych z różnych źródeł: obrazy dysków, logi, zrzuty, dane strumieniowe. Potrafi stosować zabezpieczenia dowodów cyfrowych (podpisy, skróty, kopie) oraz artefaktów aktywności. Potrafi przeprowadzić i udokumentować analizę powłamaniową incydentu teleinformatycznego.	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_U10	Potrafi wybrać i zastosować odpowiednią metodykę zarządzania projektami dla konkretnego zadania. Potrafi zdefiniować projekt i nim zarządzać.	P6U_U, P6S_UW, P6S_UO	
K1_CBE_U11	Umie dokonać wstępnego przeglądu standardów ochrony informacji, potrafi przedstawić założenia poszczególnych dokumentów normatywnych i prawnych. Umie omówić niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację. Potrafi określić założenia i zakres Polityki Bezpieczeństwa Informacji organizacji.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U12	Potrafi korzystać z systemu operacyjnego Linux w zakresie średnio zaawansowanego użytkownika, w tym pisać proste skrypty powłoki, stosując podstawowe konstrukcje pętli, instrukcje warunkowe oraz metody przekazywania parametrów.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U13	Potrafi zaplanować oraz przeprowadzić test penetracyjny.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U14	Potrafi dobrać i zastosować właściwe metod analizy danych w zadaniu analizy zagrożeń / wykrywania anomalii w zależności od specyfiki analizowanych danych.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U15	Potrafi konfigurować hosty i rutery do pracy w sieci lokalnej, stosować narzędzia diagnostyczne, obserwować i analizować zdarzenia sieciowe. Potrafi zaplanować adresację IP, podłączyć i skonfigurować rutery i przełączniki, użyć protokoły dynamicznego rutowania.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U16	Potrafi przeanalizować sposoby ochrony systemu operacyjnego (w tym konfiguruje komponenty bezpieczeństwa systemu) oraz rozpoznać podstawowe zagrożenia oraz ataki. Potrafi wdrożyć zalecenia norm i rekomendacji do systemu operacyjnego oraz mierzyć ich skuteczność - wykonać audyt bezpieczeństwa.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U17	Umie zaproponować i zestawić układ pomiarowy adekwatny do potrzeb oraz wykonać pomiary przyrządami wielkości elektrycznych, oszacować ich wiarygodność i ocenić niepewność.	P6U_U, P6S_UW	
K1_CBE_U18	Potrafi wytypować właściwe metody testowania EMC i oceny bezpieczeństwa, skonfigurować stanowiska i urządzenia, wykonać podstawowe testy oraz opracowywać i zinterpretować otrzymane wyniki badań. Potrafi zastosować dostępne techniki i materiały do rozwiązywania podstawowych problemów związanych z KEM i bezpieczeństwem elektromagnetycznym, wyznaczać ich parametry techniczne stosowanych zabezpieczeń, dokonywać ich klasyfikacji oraz ocenić skuteczność zastosowania.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U19	Potrafi opracować wybraną analizę ryzyka oraz politykę bezpieczeństwa różnych instytucji.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U20	Potrafi konfigurować i diagnozować sieci w topologii nadmiarowej z przełącznikami z użyciem VLAN oraz zastosować protokoły dynamicznego wyboru trasy. Potrafi konfigurować i diagnozować sieci z typowymi protokoły stosowane w sieciach rozległych WAN oraz podłączać LAN do ISP.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U21	Umie zaimplementować narzędzia monitorujące zdarzenia oraz bezpieczeństwo w systemie komputerowym. Potrafi przygotować system składający się z wielu komponentów do monitorowania zagrożeń. Potrafi dobrać sondy dla różnych kategorii zdarzeń w monitorowanym systemie. Umie korelować zdarzenia pochodzące z wielu źródeł danych i używać wskaźników jakościowych i ilościowych, np. ocenić skuteczność wdrożonego systemu monitorowania.	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_U22	Potrafi skonfigurować i uruchomić mechanizmy bezpieczeństwa na ruterach i urządzeniach firewall, tunele szyfrowane i mechanizmy IDS.	P6U_U, P6S_UW	P6S_UW_INŻ
K1_CBE_U23	Ma przygotowanie niezbędne do pracy w środowisku przemysłowym oraz znajomość zasad bezpieczeństwa związanych ze stanowiskiem pracy.	P6U_U, P6S_UO, P6S_UU	
K1_CBE_U24	Potrafi wykorzystywać posiadaną wiedzę specjalistyczną do formułowania i rozwiązywania złożonych i nietypowych problemów z wybranych zagadnień cyberbezpieczeństwa , pozyskiwać specjalistyczne informacje ze źródeł, dokonywać ich analizy, syntezy i oceny przydatności do realizowanych zadań.	P6U_U, P6S_UW, P6S_UO, P6S_UU	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	
K1_CBE_K02	Rozumie prawne aspekty i skutki działalności inżynierskiej.	P6U_K, P6S_KR	
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	
K1_CBE_K04	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	
K1_CBE_K05	Rozumie ideę normalizacji, certyfikacji i integracji systemów zarządzania jakością, ochroną środowiska, bezpieczeństwem pracy i bezpieczeństwem informacji. Rozumie koncepcję zarządzania przez jakość. Identyfikuje podstawowe problemy zarządzania jakością, w tym kosztów jakości oraz zasady ich rozwiązywania. Zna ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości.	P6U_K, P6S_KO	
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	2460	2460
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)	90	94
Liczba punktów ECTS, którą student uzyska realizując zajęcia wymagające bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów (BU)	106.9	106.7
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
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 w 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
Seminarium	Prezentacje multimedialne prowadzone i przygotowywane indywidualnie lub grupowo; analiza przypadków case study, aktywność na zajęciach, 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. Kursy niezaliczone student musi powtórzyć w kolejnych semestrach, osiągając w ten sposób pozostałe efekty uczenia się.

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

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

Praktyki

Studenci realizują praktykę zawodową w wymiarze określonym w programie studiów. Praktyka powinna trwać co najmniej 4 tyg. Praktyki zawodowe odbywają się w trakcie wakacji letnich, po zakończeniu zajęć 6 semestru. Praktyka odbywa się zgodnie z zasadami określonymi na Wydziale Informatyki i Telekomunikacji opublikowanymi na stronie internetowej wydziału

Egzamin dyplomowy

Egzamin ustny przed komisją wyznaczoną przez Dziekana, składający się z prezentacji pracy dyplomowej oraz odpowiedzi na dwa wylosowane zagadnienia z uprzednio opublikowanej listy.

Zagadnienia dyplomowe zostaną podane do wiadomości studentów 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**	

Specjalność: 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**	

Specjalność: 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
Suma	**210**		**15**	

Specjalność: bezpieczeństwo systemów informatycznych

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Projekt zespołowy	Projekt: 45	Zaliczenie na ocenę	5	Obowiązkowy specjalnościowy
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	**165**		**15**	

Specjalność: bezpieczeństwo infrastruktury krytycznej

Przedmiot	Liczba godzin	Forma weryfikacji	Punkty ECTS	Obligatoryjność
Projekt zespołowy	Projekt: 45	Zaliczenie na ocenę	5	Obowiązkowy specjalnościowy
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	**165**		**15**	

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: 150	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	**255**		**27**	

Specjalność: 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**	

Specjalność: 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
2025/2026

Kod przedmiotu
W4NCBES.11PK.00010.25

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	zna 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	zna podstawy reprezentacji sygnałów w dziedzinie czasu i częstotliwości, w tym: zagadnienia związane konwersją analogowo-cyfrową, parametry opisujące sygnału telekom., 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	zna cel i rodzaje kodowania protekcyjnego informacji, jej modulacji oraz metod kryptograficznych. Zna podstawowe metody wielodostępu oraz zwielokrotniania kanału	K1_CBE_W03
PEU_W04	posiada wiedzę z zakresu modelowania nadajnika, odbiornika i anteny, zna podstawy notacji decybelowej oraz pojęcia szumu i zakłóceń	K1_CBE_W03
PEU_W05	posiada wiedzę z zakresu konstrukcji i właściwości mediów transmisyjnych miedzianych, światłowodowych (optycznych) oraz bezprzewodowych (radiowych). Zna 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	posiada ogólną wiedzę z zakresu sieci komputerowych (architektura, modele odniesienia, zasada działania, techniki kontroli dostępu i bezpieczeństwa transmisji). Zna najważniejsze cechy sieci dostępowych i szkieletowych	K1_CBE_W03
PEU_W07	posiada ogólną wiedzę z zakresu systemów komórkowych generacji 2G-5G, w tym metod zabezpieczania transmisji	K1_CBE_W03
PEU_W08	posiada ogólną wiedzę z zakresu sieci satelitarnych, z elementami aspektów bezpieczeństwa transmisji	K1_CBE_W03
PEU_W09	zna 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	posiada ogólną wiedzę o współczesnych systemach sieci bezprzewodowych 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). Zna główne źródła podatności na cyberataki tych systemów oraz techniki przeciwdziałania im	K1_CBE_W03

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zdobedą więdzię z zakresu podstaw telekomunikacji w kontekście aspektów cyberbezpieczeństwa

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
2025/2026

Kod przedmiotu
W4NCBES.11PF.00002.25

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	Zna podstawowe zasady pomiarów, teorię niepewności pomiarów i techniki pomiarów wybranych sygnałów elektrycznych	K1_CBE_W01
PEU_W02	Zna 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

Poznanie i zrozumienie istoty 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
Nabycie wiedzy dotyczącej parametrów sygnałów elektrycznych, metod pomiarów i przyrządów pomiarowych

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
2025/2026

Kod przedmiotu
W4NCBES.11HS.00003.25

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	Student zna podstawowe metody interpretacji przepisów prawnych związanych z prawem własności intelektualnej	K1_CBE_W04
PEU_W02	Student posiada wiedzę o podstawowych instytucjach prawnych związanych z prawem własności intelektualnej	K1_CBE_W04
PEU_W03	Student potrafi odnaleźć potrzebny przepis w systemie obowiązującego prawa	K1_CBE_W04
Z zakresu kompetencji społecznych		
PEU_K01	Student rozumie 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

Prawo własności intelektualnej to dziedziny prawa, które regulują zasady ochrony twórczości intelektualnej oraz jej użytkowania. Obejmuje sowim zakresem przepisy chroniące m.in. wynalazki, wzory przemysłowe, znaki towarowe i inne formy innowacji oraz twórczości. Natomiast prawo autorskie odnosi się do ochrony utworu zapewniając twórcom prawo do kontrolowania sposobu wykorzystywania ich dzieł. Te dziedziny prawa mają na celu zachowanie równowagi między interesem twórców a dostępem społeczeństwa do innowacji i kultury. Jednoczesnie studen pozna podstawowe metody interpretacji przepisów prawnych związanych z prawem własności intelektualnej i będzie mial świadomośc konieczności dalszego dokształcania i kontrolowania zmianprawa.

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
2025/2026

Kod przedmiotu
W4NCBES.11HS.00004.25

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	Po zakończeniu przedmiotu student prawidłowo określa filozoficzno-etyczne uwarunkowania działalności inżynierskiej	K1_CBE_W04
PEU_W02	Po zakończeniu przedmiotu student prawidłowo identyfikuje uwarunkowanie działalności inżynierskiej w postaci filozoficznego namysłu nad istotą technologii.	K1_CBE_W04
Z zakresu kompetencji społecznych		
PEU_K01	Student prawidłowo rozstrzyga dylematy moralne związane z wykonywaniem zawodu.	K1_CBE_K01
PEU_K02	Po zakończeniu przedmiotu student postępuje zgodnie z zasadami kodeksów etyki inżynierskiej.	K1_CBE_K01

Treści programowe zapewniające uzyskanie efektów uczenia się

Treści programowe zapewniające uzyskanie efektów uczenia się
1. Przedstawienie etyki jako dziedziny wiedzy oraz filozofii praktycznej.
2. Rozwijanie umiejętności krytycznego myślenia.
3. Objaśnienie struktury dylematy moralnego i zapoznanie z dylematami wynikającymi z wykonywania działalności inżynierskiej
4. Przedstawienie problematyki etyki zawodowej, kodeksowej i pozakodeksowej.
5. Przedstawienie społecznych i humanistycznych uwarunkowań działalności inżynierskiej.
6. 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	2
Przygotowanie do egzaminu/zaliczenia	6
Zaliczenie/Egzamin	2
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
2025/2026

Kod przedmiotu
W4NCBES.11HS.00005.25

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	Ma podstawową wiedzę niezbędną do zrozumienia prawnych, etyczno-społecznych, filozoficznych uwarunkowań działalności inżynierskiej. Zna i rozumie fundamentalne dylematy współczesnej cywilizacji.	K1_CBE_W04
Z zakresu kompetencji społecznych		
PEU_K01	Prawidłowo 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 opinie w sposób zrozumiały, z uzasadnieniem różnych punktów widzenia.	K1_CBE_K03

Treści programowe zapewniające uzyskanie efektów uczenia się

Kurs wprowadza studentów w podstawowe zagadnienia filozoficzne, kładąc nacisk na te z nich, których poznanie pozwala lepiej zrozumieć fundamentalne wyzwania współczesności. Po przedstawieniu specyfiki filozofii jako rodzaju ludzkiej wiedzy o świecie, omawiane są zagadnienia związane z podstawowymi problemami z zakresu etyki, filozofii społecznej, epistemologii, metafizyki, teorii argumentacji oraz filozofii nauki i techniki. Sposób prowadzenia kursu oraz dobór zagadnień zamierzone są na wsparcie rozwoju umiejętności krytycznego myślenia słuchaczy oraz zwiększenia ich świadomości w zakresie społecznej odpowiedzialności nauki i techniki.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Przygotowanie do zajęć	20
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
2025/2026

Kod przedmiotu
W4NCBES.11PK.00069.25

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	Potrafi napisać prosty skrypt w języku Python	K1_CBE_U03
PEU_U02	Potrafi przygotować skrypty do automatyzacji zadań systemowych	K1_CBE_U03
PEU_U03	Potrafi stworzyć skrypty do obsługi plików i przetwarzania danych	K1_CBE_U03
PEU_U04	Potrafi zaprojektować interfejs graficzny w języku Python	K1_CBE_U03

Treści programowe zapewniające uzyskanie efektów uczenia się

Podstawy – typy danych, wprowadzanie wyrażeń, podstawowe funkcje, pierwszy program
Instrukcje warunkowe, pętle, operacje logiczne i bitowe
Definiowanie własnych funkcji, zakresy, listy, krotki, słowniki, operacje na łańcuchach znaków
Moduły, metody list i łańcuchów znaków, wyjątki
Programowanie obiektowe: klasy, metody, obiekty
Obsługa plików w skryptach oraz organizacja plików

Czas, harmonogram zadań, wielowątkowość, uruchamianie programów
Praca z obrazami, arkuszami kalkulacyjnymi i dokumentami tekstowymi
Analiza danych z wykorzystaniem modułów języka Python
Kontrolowanie myszy i klawiatury za pomocą skryptów
Projektowanie interfejsu graficznego w języku Python

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
2025/2026

Kod przedmiotu
W4NCBES.11PM.00070.25

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	zna podstawowe metody rozwiązywania równań liniowych	K1_CBE_W05
PEU_W02	zna podstawowe własności liczb zespolonych	K1_CBE_W05
PEU_W03	zna podstawowe własności algebraiczne wielomianów	K1_CBE_W05
PEU_W04	zna metody opisu prostych i płaszczyzn.	K1_CBE_W05
Z zakresu umiejętności		
PEU_U01	potrafi dodawać i mnożyć macierze, obliczać wyznaczniki	K1_CBE_U05
PEU_U02	potrafi rozwiązywać układy równań liniowych	K1_CBE_U05

PEU_U03	potrafi wyznaczać wektory i wartości własne macierzy	K1_CBE_U05
PEU_U04	potrafi przeprowadzać obliczenia z wykorzystaniem liczb zespolonych	K1_CBE_U05
PEU_U05	potrafi wyznaczać równania płaszczyzn i prostych w przestrzeni.	K1_CBE_U05

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Elementy logiki matematycznej. Indukcja matematyczna.
2. Wzór dwumianowy Newtona. Struktury algebraiczne: grupa. ciało.
3. Ciało liczb zespolonych. Postać algebraiczna liczby zespolonej. Liczba sprzężona.
4. Działania na liczbach zespolonych. Interpretacja geometryczna liczby zespolonej.
5. Moduł i argument liczby zespolonej. Postać trygonometryczna i wykładnicza liczby zespolonej. Wzór de Moivre'a. Pierwiastek n-tego stopnia z liczby zespolonej.

4. Pojęcie wielomianu. Pierwiastki wielomianów. Twierdzenie Bezout. Zasadnicze twierdzenie algebry.
5. Dzielnik liniowy i kwadratowy wielomianu rzeczywistego. Rozkład wielomianu na czynniki stopnia co najwyżej drugiego. Pojęcie funkcji wymiernej. Rozkład funkcji wymiernej na rzeczywiste ułamki proste. Przestrzenie wektorowe.
6. Podprzestrzenie. Liniowa niezależność wektorów. Baza przestrzeni wektorowej. Przestrzeń Euklidesa.
7. Pojęcie macierzy. Działania na macierzach. Macierz transponowana. Macierze: trójkątna, symetryczna, diagonalna.
8. Obliczanie wyznacznika macierzy z zastosowaniem wzoru Sarrusa, rozwinięcia Laplace'a. Własności wyznaczników.Macierz nieosobliwa. Operacjie elementarne na macierzach. Twierdzenie Cauchy'ego.

9. Pojęcie macierzy odwrotnej. Metody wyznaczania macierzy odwrotnych: metoda dopełnień algebraicznych, metoda bezwyznacznikowa. Własności macierzy odwrotnych. Równania macierzowe. Rząd macierzy. Wybrane zastosowania wyznaczników, związki z rzędem i odwracalnością macierzy
10. Układ równań liniowych i ich związek z równaniami macierzowymi.Twierdzenie Kroneckera-Capellego. Wzory Cramera. Metoda eliminacji Gaussa.
11. Funkcje i odwzorowania liniowe. Wektory i wartości własne. Diagonalizacja macierzy.
12. Geometria analityczna w przestrzeni R^3. Działania na wektorach. Długość wektora. Iloczyny: skalarny, wektorowy, mieszany i ich zastosowania.

13. Niekartezjańskie układy współrzędnych. Współrzędne sferyczne i cylindryczne (walcowe).
14. Płaszczyzna. Wektor normalny. Równanie płaszczyzny: ogólne, parametryczne, wyznacznikowe. Prosta. Równanie prostej: parametryczne, kierunkowe, krawędziowe.
15. Wzajemne położenie płaszczyzn i prostych. Odległość punktu od prostej i od płaszczyzny. Rzut punktu na prostą i na płaszczyznę.

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
2025/2026

Kod przedmiotu
W4NCBES.11PM.00111.25

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	zna podstawowe pojęcia i twierdzenia rachunku różniczkowego funkcji jednej zmiennej	K1_CBE_W05
PEU_W02	W03 zna podstawowe pojęcia i twierdzenia rachunku różniczkowego funkcji wielu zmiennych	K1_CBE_W05
PEU_W03	zna pojęcie całki podwójnej i potrójnej, jej własności i podstawowe zastosowania. Z zakresu umiejętności student	K1_CBE_W05
Z zakresu umiejętności		
PEU_U01	umie stosować elementy badania przebiegu zmienności funkcji do rozwiązywania typowych zadań	K1_CBE_U05

PEU_U02	U04 umie stosować pochodne cząstkowe, wyznaczać gradient i pochodną kierunkową oraz wyznaczać ekstrema lokalne i warunkowe funkcji dwóch zmiennych	K1_CBE_U05

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.

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
2025/2026

Kod przedmiotu
W4NCBES.11PK.00071.25

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	Student opisuje podstawowe zagadnienia cyberbezpieczeństwa	K1_CBE_W12
PEU_W02	Student rozpoznaje zagrożenia w infrastrukturze teleinformatycznej	K1_CBE_W12
PEU_W03	Student charakteryzuje bezpieczeństwo sieci i systemów teleinformatycznych	K1_CBE_W12
PEU_W04	Student identyfikuje bezpieczeństwo systemów operacyjnych	K1_CBE_W12

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zapoznają się z podstawowymi pojęciami z zakresu cyberbezpieczeństwa (poufność, integralność, dostępność) i sposobami ich zapewnienia oraz zdobędą wiedzę z zakresu bezpieczeństwa systemów operacyjnych (Widows, Linux, Android, IoS), sieci komputerowych przewodowych i bezprzewodowych (zapory ogniowe, systemy IDS, system IPS), testów penetracyjnych a także zagrożeń występujących 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	18
Samodzielne studiowanie tematyki zajęć	50
Zaliczenie/Egzamin	2
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
2025/2026

Kod przedmiotu
W4NCBES.12PF.00011.25

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	Potrafi wykorzystywać i obsługiwać podstawowe analogowe i cyfrowe przyrządy do pomiarów wielkości elektrycznych oraz zestawić stanowisko pomiarowe, dokonać pomiarów i przeanalizować wyniki tych pomiarów	K1_CBE_U21
PEU_U02	Potrafi dobrać i uzasadnić metodę pomiaru podstawowych wielkości elektrycznych i oszacować niepewność wybranej metody	K1_CBE_U21
PEU_U03	Potrafi zastosować oscyloskop do obrazowania i podstawowych pomiarów sygnałów elektrycznych.	K1_CBE_U21

Treści programowe zapewniające uzyskanie efektów uczenia się

Nabycie umiejętności planowania i wykonywania pomiarów
Nabycie umiejętności doboru metody i sprzętu pomiarowego w pomiarach wielkości elektrycznych
Nabycie umiejętności zestawienia stanowiska pomiarowego, pomiarów i analizy wyników

Nabycie umiejętności pomiarów napięć i prądów w obwodach prądu stałego i przemiennego
Nabycie umiejętności 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	**Cykl kształcenia** 2025/2026
Specjalność -	**Kod przedmiotu** W4NCBES.12PK.00072.25
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Grupa zajęć** Tak
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Języki wykładowe** polski
Forma studiów studia stacjonarne	**Obligatoryjność** Obowiązkowy
Profil studiów profil ogólnoakademicki	**Blok zajęciowy** Przedmioty kierunkowe
	Przedmiot powiązany z badaniami naukowymi Tak

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

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Student ma ogólną, spójną wiedzę teoretyczną na temat dostępu do informacji oraz konstrukcji ochrony informacji niejawnych, danych osobowych i informacji objętych tajemnicą przedsiębiorstwa	K1_CBE_W12
PEU_W02	Umie określić hierarchię i metody dostępu do informacji niejawnej	K1_CBE_W12
PEU_W03	Ma ogólną wiedzę dotyczącą systemów zarządzania bezpieczeństwem informacji (SZBI) zgodnych z normami/regulacjami europejskimi (NIS) i krajowymi (ustawa KSC), budowy systemów ochrony: informacji niejawnych, danych osobowych i informacji objętych tajemnicą zawodową	K1_CBE_W12

PEU_W04	Umie określić 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_W12
PEU_W05	Umie określić ogólne ramy obowiązków osób odpowiedzialnych za ochronę informacji i systemów informatycznych w organizacji.	K1_CBE_W12
PEU_W06	Rozumie mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację	K1_CBE_W12
Z zakresu umiejętności		
PEU_U01	Potrafi dokonać wstępnego przeglądu standardów ochrony informacji, potrafi przedstawić założenia poszczególnych dokumentów normatywnych i prawnych	K1_CBE_U11
PEU_U02	Umie omówić niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację.	K1_CBE_U11
PEU_U03	Umie dokonać wstępnego przeglądu standardów ochrony informacji	K1_CBE_U11
PEU_U04	Potrafi określić założenia i zakres Polityki Bezpieczeństwa Informacji organizacji	K1_CBE_U11

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci uzyskają wiedzę z zakresu ochrony informacji, przeprowadzania analizy procesów biznesowych
i zasobów teleinformatycznych oraz wdrażania Systemów Zarządzania Bezpieczeństwem 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
2025/2026

Kod przedmiotu
W4NCBES.12PK.00073.25

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	Student charakteryzuje rolę i zastosowanie sieci komputerowej. Zna modele odniesienia ISO/OSI i TCP/IP	K1_CBE_W17
PEU_W02	Student nazywa funkcje warstwy fizycznej i łącza danych na przykładzie sieci Ethernet	K1_CBE_W17
PEU_W03	Student nazywa funkcje warstwy sieciowej, sposób adresacji IP i podział na podsieci	K1_CBE_W17
PEU_W04	Student dobiera odpowiednią adresację IP dla sieci, topologię oraz rodzaj okablowania	K1_CBE_W17

PEU_W05	Student nazywa funkcje warstwy transportowej i aplikacji	K1_CBE_W17
Z zakresu umiejętności		
PEU_U01	Student dobiera i wdraża parametry urządzeń z Sieciowym Systemem Operacyjnym	K1_CBE_U15
PEU_U02	Student testuje sieci przy użyciu narzędzi diagnostycznych i analizatorów protokołów	K1_CBE_U15
PEU_U03	Student weryfikuje działanie rutera, funkcje wyboru trasy i sprawdza zawartość tablicy rutowania	K1_CBE_U15
PEU_U04	Student weryfikuje działanie przełącznika i sprawdza zawartość tablicy MAC	K1_CBE_U15
PEU_U05	Student przygotowuje konfigurację rutera, podstawowe parametry i rutowanie statyczne	K1_CBE_U15
PEU_U06	Student potrafi zaplanować, podłączyć i uruchomić niewielką sieć zawierającą hosty, ruter i przełącznik	K1_CBE_U15

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przediotu studenci zdobędą podstawową wiedzę dotyczącą sieci komputerowych związaną z ich funkcjonowaniem, modelem odniesienia, topologią, elementami sieci i protokołami komunikacyjnymi oraz wiedzę z zakresu działania urządzeń sieciowych, konfigurowania hostów i ruterów do pracy w sieci lokalnej, stosowania narzędzi diagnostycznych, obserwacji i analizy zdarzeń sieciowych.

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	18
Przygotowanie do zajęć	20
Realizacja praktyki zawodowej	2
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
2025/2026

Kod przedmiotu
W4NCBES.12PK.00074.25

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	Potrafi napisać skrypty automatyzujące zadania systemowe za pomocą Basha albo PowerShella	K1_CBE_U02
PEU_U02	Potrafi napisać skrypty w języku Python, które pobierają i przetwarzają dane pobrane z Internetu	K1_CBE_U02
PEU_U03	Potrafi testować podatności serwerów i aplikacji na ataki sieciowe za pomocą skryptów w języku Python	K1_CBE_U02

Treści programowe zapewniające uzyskanie efektów uczenia się

Bash – wprowadzenie, skrypty, automatyzacja zadań
Powershell – wprowadzenie, skrypty, automatyzacja zadań
Pobieranie i przetwarzanie danych pobranych z Internetu
Usługi FTP i SSH realizowane za pomocą skryptów

Uzyskiwanie informacji geolokalizacyjnych i wyodrębnianie metadanych z dokumentów z wykorzystaniem skryptów
Techniki kryptograficzne w modułach języka Python
Język Python do testowania podatności serwerów i aplikacji na ataki sieciowe

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
2025/2026

Kod przedmiotu
W4NCBES.12TI.00075.25

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	Posiada podstawową wiedzę z zakresu budowy systemów operacyjnych.	K1_CBE_W03
PEU_W02	Posiada wiedzę w zakresie zasad działania podsystemów systemu operacyjnego	K1_CBE_W03
PEU_W03	Zna podstawowe algorytmy szeregowania zadań.	K1_CBE_W03
PEU_W04	Posiada wiedzę w zakresie działania typów systemów rozproszonych i rozproszonych systemów plików.	K1_CBE_W03
Z zakresu umiejętności		

PEU_U01	Potrafi korzystać z systemu operacyjnego Linux w zakresie średnio zaawansowanego użytkownika.	K1_CBE_U04
PEU_U02	Potrafi pisać proste skrypty powłoki stosując podstawowe konstrukcje pętli, instrukcji warunkowych oraz metod przekazywania parametrów.	K1_CBE_U04
PEU_U03	Potrafi zaplanować i przeprowadzić ocenę eksperymentalną prostych algorytmów szeregowania.	K1_CBE_U04
PEU_U04	Potrafi zaplanować i przeprowadzić ocenę eksperymentalną prostych algorytmów zastępowania stron.	K1_CBE_U04

Treści programowe zapewniające uzyskanie efektów uczenia się

Kurs umożliwia studentom zapoznanie się z podstawami działania i budowy systemów operacyjnych.
Kurs umożliwia studentom zapoznanie się z systemem operacyjnym Linux i powłoką bash.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	45
Przygotowanie do zajęć	35
Przygotowanie do egzaminu/zaliczenia	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
2025/2026

Kod przedmiotu
W4NCBES.12PM.00076.25

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	posiada wiedzę w zakresie podstawowych i zaawansowanych obiektów kombinatorycznych	K1_CBE_W05
PEU_W02	posiada wiedzę dotyczącą narzędzi kombinatoryki, w szczególności grup modulo, grup permutacji, oraz ich własności	K1_CBE_W05
Z zakresu umiejętności		
PEU_U01	potrafi stosować narzędzia kombinatoryki do rozwiązywania problemów definiowanych na zbiorach przeliczalnych	K1_CBE_U05
PEU_U02	potrafi poprawnie i efektywnie zastosować wiedzę z kombinatoryki do konstrukcji efektywnych algorytmów szyfrowania	K1_CBE_U05

Treści programowe zapewniające uzyskanie efektów uczenia się

Elementy logiki matematcznej, 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	55
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
2025/2026

Kod przedmiotu
W4NCBES.12PF.00016.25

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

PEU_U01	Potrafi ilościowo i jakościowo opisywać zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się podstawowymi prawami również dotyczącymi ruchu obiektów oraz ruchu drgającego i falowego.	K1_CBE_U05
PEU_U02	Potrafi ilościowo i jakościowo opisywać zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się podstawowymi prawami związanymi z przepływem prądu.	K1_CBE_U05
PEU_U03	Potrafi ilościowo i jakościowo opisywać zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się podstawowymi prawami optyki geometrycznej i falowej.	K1_CBE_U05

Treści programowe zapewniające uzyskanie efektów uczenia się

- Wprowadzenie: zakres i metodologia fizyki; metoda naukowa. Podstawowe prawa i zasady fizyki.
- Podstawowe prawa i zasady fizyki – siły, praca i energia mechaniczna. Zasada zachowania energii mechanicznej. Zasada zachowania pędu.
- Oscylator harmoniczny, drgania harmoniczne i swobodne, Drgania tłumione i wymuszone (rezonans) oraz składanie drgań, analiza Fouriera.
- Fale mechaniczne, równanie falowe, fala stojąca, energia fal, nakładanie fal, paczka falowa, prędkości w ruchu falowym, fale akustyczne, efekt Dopplera.
- Podstawy elektrostatyki i elektromagnetyzmu
- Pole grawitacyjne. Prędkości kosmiczne.
- Podstawowe prawa i definicje dla przepływu prądu stałego.
- Kondensator – ładowanie i rozładowanie oraz magazynowanie energii, obwody prądu sinusoidalnego, moc prądu zmiennego.
- Zjawiska i prawa optyki geometrycznej, metamateriały.
- Elementy i przyrządy optyczne, wady odwzorowań w ujęciu inżynierskim.
- Podstawy modelu falowego w ujęciu skalarnym, interferencja, interferometry.
- Dyfrakcja – podstawowe prawa i podstawy przetwarzania sygnału optycznego. Dyfrakcja w ujęciu bliskiego i dalekiego pola.
- Elementy zapisu i odtwarzania informacji falowej w ujęciu przestrzennym, holografia.
- Polaryzacja – podstawy modelu, stany polaryzacji, metody polaryzacji, anizotropia i dwójłomność.

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
2025/2026

Kod przedmiotu
PWRSWFS.82WF.04466.25

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Zajęcia z wychowania fizycznego

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 2	• 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
2025/2026

Kod przedmiotu
W4NCBES.14PK.00077.25

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	Student poprawnie identyfikuje i uzasadnia miejsca zastosowania elementów kryptograficznych w kanale telekomunikacyjnym.	K1_CBE_W15
PEU_W02	Student wyjaśnia sposób wyznaczania odwrotności liczb w ciałach skończonych, znaczenie liczb pierwszych w kryptografii niesymetrycznej oraz wylicza entropię informacji.	K1_CBE_W15
PEU_W03	Student rozpoznaje podstawowe pojęcia stosowane w kryptografii i potrafi je wyjaśnić.	K1_CBE_W15
PEU_W04	Student charakteryzuje klasyczne systemy kryptograficzne stosowane przed erą systemów cyfrowych.	K1_CBE_W15

PEU_W05	Student identyfikuje metody służące do kryptoanalizy algorytmów kryptograficznych	K1_CBE_W15
PEU_W06	Student objaśnia współczesne symetryczne algorytmy kryptograficzne oraz charakteryzuje standardy kryptograficzne wykorzystywane w świecie.	K1_CBE_W15
PEU_W07	Student objaśnia współczesne niesymetryczne algorytmy kryptograficzne oraz charakteryzuje standardy kryptograficzne wykorzystywane w świecie.	K1_CBE_W15
PEU_W08	Student objaśnia sposoby realizacji podpisów cyfrowych oraz charakteryzuje ich właściwości.	K1_CBE_W15
PEU_W09	Student charakteryzuje progowe i bezprogowe systemy dzielenia tajemnicy pomiędzy większą ilość osób.	K1_CBE_W15
PEU_W10	Student objaśnia podstawy kryptografii kwantowej oraz przytacza jej wykorzystanie w praktyce.	K1_CBE_W15
PEU_W11	Student definiuje pojęcie protokołu kryptograficznego i potrafi go analizować.	K1_CBE_W15
PEU_W12	Student wymienia implementacje protokołów kryptograficznych we współczesnych systemach telekomunikacyjnych.	K1_CBE_W15
PEU_W13	Student objaśnia sposoby generowania i wykorzystania liczb pierwszych.	K1_CBE_W15
PEU_W14	Student wymienia metody zabezpieczenia informacji oraz charakteryzuje protokoły we współczesnych systemach sieciowych, komputerowych oraz systemach ochronny.	K1_CBE_W15
Z zakresu umiejętności		
PEU_U01	Student konstruuje szyfrogramy wiadomości za pomocą metod klasycznych.	K1_CBE_U01
PEU_U02	Student analizuje szyfrogram pod kątem statystycznym.	K1_CBE_U01
PEU_U03	Student tworzy programy do łamania szyfrów utworzonych przy pomocy klasycznych metod kryptograficznych	K1_CBE_U01

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu omówiona jest rola kryptografii w zapewnieniu poufności i integralności danych. Celem łatwiejszego zrozumienia zagadnień związanych z kryptografią, na wstępie omawiane są klasyczne algorytmy kryptograficzne, a następnie współczesne algorytmy kryptograficzne. Zasadniczy akcent przedmiotu położony jest na zapoznanie studentów z obowiązującymi standardami w zakresie szyfrowania danych, podpisów cyfrowych i dzielenia tajemnicy. Scharakteryzowana jest również rola kryptografii w tworzeniu kryptowalut. Omówione są 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
2025/2026

Kod przedmiotu
W4NCBES.14PK.00078.25

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	zna model OSI: potrafi zidentyfikować poszczególne warstwy i przynależność do nich odpowiednich części oprogramowania systemowego i programów użytkownika.	K1_CBE_W02
PEU_W02	wie na czym polega kontrola procesów, sposoby uruchamiania procesów w systemie UNIX oraz metody komunikacji między nimi	K1_CBE_W02
PEU_W03	zna i potrafi opisać metody synchronizacji wątków za pomocą moniotorów i zmiennych warunkowych.	K1_CBE_W02

PEU_W04	zna i kojarzy 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	zna model działania klient-serwer oraz peer-to-peer	K1_CBE_W02
Z zakresu umiejętności		
PEU_U01	posiada praktyczną znajomość systemów i narzędzi służących uruchamianiu procesów, komunikacji między nimi, a także mechanizmów synchronizacji zadań, monitorów, semaforów i zmiennych warunkowych.	K1_CBE_U08
PEU_U02	potrafi pisać i testować aplikacje sieciowe działające w architekturze klient-serwer i peer-to-peer z użyciem TCP i UDP.	K1_CBE_U08
PEU_U03	potrafi kompilować programy w języku C na platformie UNIX oraz korzystać edytora vim i plików projektowych Makefile	K1_CBE_U08

Treści programowe zapewniające uzyskanie efektów uczenia się

Nabycie praktycznej wiedzy z zakresu programowania w środowisku UNIX
Nabycie wiedzy dotyczącej komunikacji między procesami i programowania współbieżnego
Nabycie wiedzy i umiejętności praktycznych dotyczących stosowania mechanizmów synchronizacji procesów
Nabycie wiedzy i umiejętności praktycznych dotyczących gniazdek sieciowych BSD i programowania komunikacji sieciowej w trybach klient-serwer i peer-to-peer
Nabycie 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
2025/2026

Kod przedmiotu
W4NCBES.14PK.00079.25

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	Student: posiada podstawową wiedzę dotyczącą budowania sieci z przełącznikami i sieciami VLAN.	K1_CBE_W17
PEU_W02	Student: posiada podstawową wiedzę dotyczącą zagrożeń i bezpieczeństwa urządzeń	K1_CBE_W17
PEU_W03	Student: posiada podstawową wiedzę na temat mechanizmów nadmiarowości w sieciach lokalnych i działania usługi DHCP	K1_CBE_W17
PEU_W04	Student: posiada podstawową wiedzę dotyczącą routingu statycznego i dynamicznego w sieciach IPv4 i IPv6	K1_CBE_W17

Z zakresu umiejętności		
PEU_U01	Student: potrafi konfigurować przełączniki Ethernet z użyciem techniki VLAN oraz rozwiązywać problemy w sieciach przełączanych.	K1_CBE_U15
PEU_U02	Student: potrafi konfigurować proste sieci z użyciem statycznego routingu w sieciach IPv4 i IPv6 oraz rozwiązywać problemy związane z działaniem sieci	K1_CBE_U15
PEU_U03	Student: potrafi skonfigurować podstawowe funkcje bezpieczeństwa, mechanizmy nadmiarowości oraz usługi serwera i klienta protokołu DHCP	K1_CBE_U15

Treści programowe zapewniające uzyskanie efektów uczenia się

Zdobycie podstawowej wiedzy dotyczącej sieci komputerowych związanej z jej funkcjonowaniem, modelem odniesienia, topologią, elementami sieci i protokołami komunikacyjnymi.
Zdobycie podstawowej wiedzy o działaniu urządzeń sieciowych.
Zdobycie umiejętności konfigurowania hostów ruterów i przełączników do pracy w sieci lokalnej, stosowania narzędzi diagnostycznych, obserwacji i analizy zdarzeń sieciowych.
Zdobycie umiejętności konfigurowania podstawowych funkcji bezpieczeństwa na urządzeniach sieciowych

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	15
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Przeprowadzenie badań empirycznych	15
Samodzielne studiowanie tematyki zajęć	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Systemy operacyjne

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
2025/2026

Kod przedmiotu
W4NCBES.14PK.00021.25

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: 45	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Posiada zaawansowaną wiedzę z zakresu posługiwania się systemem Linux	K1_CBE_W13
PEU_W02	Posiada wiedzę z zakresu administrowania systemem Linux	K1_CBE_W13
PEU_W03	Posiada podstawową wiedzę z zakresu bezpieczeństwa systemów z rodziny Linux	K1_CBE_W13
PEU_W04	Posiada wiedzę na temat zagadnień związanych z wirtualizacją systemów operacyjnych	K1_CBE_W13
Z zakresu umiejętności		

PEU_U01	Potrafi korzystać z systemu operacyjnego Linux w zakresie zaawansowanego użytkownika	K1_CBE_U12
PEU_U02	Potrafi administrować systemem operacyjnym Linux	K1_CBE_U12
PEU_U03	Potrafi w podstawowym stopniu zabezpieczyć system operacyjny Linux	K1_CBE_U12
PEU_U04	Potrafi obsługiwać system wirtualizacji	K1_CBE_U12

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zdobędą wiedzę z zakresu użytkowania 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
2025/2026

Kod przedmiotu
W4NCBES.14PM.00025.25

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	Zna prawdopodobieństwo dyskretne. Prawdopodobieństwo ciągłe. Wartości oczekiwane. Procesy stochastyczne. Próbkowanie. Estymacja. Testowanie hipotez statystycznych.	K1_CBE_W05
Z zakresu umiejętności		
PEU_U01	Potrafi dobrać i zastosować podstawowe testy statystyczne oraz stosować i dobierać metod estymacji dla prostych modeli statystycznych	K1_CBE_U05

Treści programowe zapewniające uzyskanie efektów uczenia się

Nabycie wiedzy na temat zadań testowania hipotez statystycznych i podstawowych testów o parametrach rozkładów oraz wybranych testów nieparametrycznych.
Nabycie podstawowej wiedzy na temat wymagań nakładanych na estymatory parametrów rozkładów i klasycznych metod ich konstruowania oraz stosowania.
Nabycie wiedzy w zakresie zastosowań estymacji i testowania hipotez w systemach przetwarzania informacji i telekomunikacji
Zdobycie umiejętności doboru i stosowania podstawowych testów statystycznych
Nabycie umiejętności 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
2025/2026

Kod przedmiotu
PWRSJOS.81EJO.04091.25

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
2025/2026

Kod przedmiotu
PWRSWFS.84WF.04467.25

Języki wykładowe
polski

Obligatoryjność
Wybieralny

Blok zajęciowy
Zajęcia z wychowania fizycznego

Semestr	Forma dydaktyczna, godziny zajęć, liczba punktów ECTS i forma zaliczenia
Semestr 3	• 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
2025/2026

Kod przedmiotu
W4NCBES.18PK.00052.25

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	Zna koncepcję wirtualizacji oraz kluczowe zagadnienia związane z platformą sprzętową oraz oprogramowaniem, modelem warstwowym, a także cechy charakterystycznych chmur obliczeniowych.	K1_CBE_W07
PEU_W02	Posiada podstawową koncepcję kontenerów oraz wiedzę o ich środowiskach uruchomieniowych.	K1_CBE_W07
PEU_W03	Zna modele dostarczania usług chmury oraz zakresy odpowiedzialności dostawcy i klienta.	K1_CBE_W07

PEU_W04	Identyfikuje chmury prywatne, publiczne oraz hybrydowe, zna typowe zastosowania oraz zalety i wady poszczególnych rozwiązań.	K1_CBE_W07
PEU_W05	Zna charakterystykę usług z obszaru Compute, Storage i Network - na przykładzie dostawcy usług chmury publicznej Amazon AWS	K1_CBE_W07
Z zakresu umiejętności		
PEU_U01	Potrafi zarządzać zasobami hipervisorów, tworzyć maszyny wirtualne oraz instalować systemy operacyjne.	K1_CBE_U07
PEU_U02	Potrafi instalować środowiska uruchomieniowe kontenerów oraz uruchamiać przykładowe aplikacje wielo-kontenerowe, takze w środowisku klastra serwerów	K1_CBE_U07
PEU_U03	Potrafi zarządzać zasobami publicznej chmury obliczeniowej z pozycji klienta chmury, tworzyć projekty oraz zamawiać maszyny wirtualne i usługi	K1_CBE_U07

Treści programowe zapewniające uzyskanie efektów uczenia się

Zdobycie podstawowej wiedzy dotyczącej infrastruktury chmur obliczeniowych oraz aplikacji i usług w chmurach.
Zdobycie umiejętności uruchamiania usług teleinformatycznych w oparciu o infrastrukturę chmury, a także formułowania charakterystyk chmury obliczeniowej.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	45
Przygotowanie do egzaminu/zaliczenia	15
Samodzielne studiowanie tematyki zajęć	50
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
2025/2026

Kod przedmiotu
W4NCBES.18PK.00128.25

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	Ma wiedzę o architekturze i zasadzie działania podstawowych komponentów SZBD	K1_CBE_W06
PEU_W02	Jest w stanie omówić i porównać podstawowe metody organizacji danych, indeksowania danych oraz przetwarzania i optymalizacji transakcji i zapytań w SZBD	K1_CBE_W06
Z zakresu umiejętności		
PEU_U01	Potrafi wybrać i dostosować odpowiednie do wymagań narzędzia tworzenia aplikacji baz danych	K1_CBE_U06

PEU_U02	Potrafi samodzielnie zaprojektować i zaimplementować bazę danych	K1_CBE_U06

Treści programowe zapewniające uzyskanie efektów uczenia się

Wprowadzenie do historii i kluczowych pojęć związanych z bazami danych, takich jak modele hierarchiczne, relacyjne oraz nowoczesne rozwiązania NoSQL. Program kładzie nacisk na modelowanie danych, ucząc studentów, jak tworzyć modele koncepcyjne oraz diagramy ER, a także przeprowadzać normalizację danych w celu optymalizacji struktur bazodanowych. Studenci poznają relacyjny model danych, w tym zasady tworzenia i zarządzania tabelami oraz relacjami między nimi. Ważnym elementem kursu jest także 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
2025/2026

Kod przedmiotu
W4NCBES.18PK.00080.25

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	Posiada wiedze z zakresu skalowania sieci oraz działania sieci w topologii nadmiarowej z przełącznikami z użyciem VLAN.	K1_CBE_W20
PEU_W02	Posiada wiedze z zakresu ograniczania zagrożeń i zwiększania bezpieczeństwa sieci, korzystając z list kontroli dostępu IPv4 do filtrowania ruchu i bezpiecznego dostępu administracyjnego oraz najlepszych praktyk w zakresie zabezpieczeń.	K1_CBE_W20
PEU_W03	Rozumie i potrafi planować ruting statyczny i dynamiczny oraz zna zasady działania protokołów routingu dynamicznego, stanu łącza OSPF w sieciach IPv4 i IPv6.	K1_CBE_W20

PEU_W04	Posiada wiedzę dotyczącą projektowania sieci hierarchicznych i architektury sieci biznesowych oraz technik zapewniających skalowalność adresów i bezpieczny dostęp zdalny dla sieci WAN.	K1_CBE_W20
PEU_W05	Posiada wiedzę dotyczącą metod dołączania sieci LAN do ISP oraz typowych protokołów stosowanych w publicznych i prywatnych sieciach WAN (protokoły PPP, sieci VPN, usługa translacji adresów NAT).	K1_CBE_W20
PEU_W06	Posiada wiedzę dotyczącą zarządzania siecią (monitorowania i diagnostyki sieci), wie jak urządzenia sieciowe implementują QoS oraz w jaki sposób technologie takie jak wirtualizacja, sieci programowalne i automatyzacja wpływają na rozwijające się sieci.	K1_CBE_W20
Z zakresu umiejętności		
PEU_U01	Potrafi posługiwać się narzędziami diagnostycznymi i analizatorem protokołów.	K1_CBE_U20
PEU_U02	Potrafi konfigurować i diagnozować przełączniki i rutery.	K1_CBE_U20
PEU_U03	Potrafi konfigurować i diagnozować sieci VLAN, agregację łączy w technologii EtherChannel, protokół STP oraz porty brzegowe przy użyciu PortFast i BPDU Guard.	K1_CBE_U20
PEU_U04	Potrafi konfigurować proste sieci z użyciem statycznego wyboru trasy i protokołów dynamicznego wyboru tras, stanu łącza OSPF w sieciach IPv4 i IPv6 oraz rozwiązywać problemy związane z działaniem sieci	K1_CBE_U20
PEU_U05	Potrafi konfigurować podłączenia do sieci WAN na ruterach i ograniczać zagrożenia i zwiększać bezpieczeństwo sieci, korzystając z list kontroli dostępu ACL.	K1_CBE_U20
PEU_U06	Potrafi skonfigurować usługę Network Address Translation na ruterach oraz zabezpieczenia na połączeniach site-to-site (łacza VPN).	K1_CBE_U20

Treści programowe zapewniające uzyskanie efektów uczenia się

C1 Zdobycie wiedzy dotyczącej sieci przełączanych i ich skalowania oraz działania protokołów routingu dynamicznego, stanu łącza i wektora odległości.
C2. Zdobycie wiedzy dotyczącej metod dołączania sieci LAN do ISP oraz typowych protokołów stosowanych w publicznych i prywatnych sieciach WAN.
C3. Zdobycie umiejętności konfigurowania nadmiarowości i agregacji łączy w przełączanych sieciach LAN, rutingu dynamicznego oraz stosowania narzędzi diagnostycznych, obserwacji i analizy zdarzeń sieciowych.
C4. Zdobycie 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	35
Przygotowanie do egzaminu/zaliczenia	30

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
2025/2026

Kod przedmiotu
W4NCBES.18PK.00081.25

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	Zna zasady prowadzenia analizy powłamaniowej.	K1_CBE_W09
PEU_W02	Zna zagadnienia i procedury obsługi incydentu teleinformatycznego.	K1_CBE_W09
PEU_W03	Zna zagadnienia i metody analizy i przetwarzania dowodów cyfrowych.	K1_CBE_W09
PEU_W04	Rozumie i określa parametry dowodów cyfrowych.	K1_CBE_W09

PEU_W05	Zna metody zapewniania rzetelności i niezaprzeczalności dowodów cyfrowych.	K1_CBE_W09
Z zakresu umiejętności		
PEU_U01	Potrafi przeprowadzić i udokumentować analizę powłamaniową incydentu teleinformatycznego.	K1_CBE_U09
PEU_U02	Potrafi stosować techniki pozyskiwania dowodów cyfrowych z różnych źródeł.	K1_CBE_U09
PEU_U03	Potrafi rozróżnić różne typy zapisu i formatów źródeł dowodów cyfrowych.	K1_CBE_U09
PEU_U04	Potrafi stosować zabezpieczenia dowodów cyfrowych.	K1_CBE_U09
PEU_U05	Potrafi określić potrzebne źródła i uzyskać określone informacje na zadane kwestie.	K1_CBE_U09

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Nabycie wiedzy z zakresu prowadzenia analizy powłamaniowej.
2. Nabycie wiedzy z zakresu obsługi incydentu teleinformatycznego.
3. Nabycie wiedzy z zakresu pozyskiwania i zabezpieczania dowodów cyfrowych w celach własnej analizy oraz przedstawienia tych dowodów innym podmiotom.

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	15
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
2025/2026

Kod przedmiotu
W4NCBES.18PK.00082.25

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	Zna podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych.	K1_CBE_W18
PEU_W02	Zna i rozróżnia podstawowe metody uwierzytelniania i autoryzacji, rozumie działanie mechanizmów kontroli dostępu w systemach komputerowych	K1_CBE_W18
PEU_W03	Zna podstawowe pojęcia audytu technicznego i testów penetracyjnych.	K1_CBE_W18

PEU_W04	Zna zastosowanie narzędzi: monitorowania bezpieczeństwa systemów, audytutechnicznego i testów penetracyjnych.	K1_CBE_W18
Z zakresu umiejętności		
PEU_U01	Potrafi przeanalizować działanie systemu operacyjnego pod kątem bezpieczeństwa (na podstawie dzienników systemowych i innych plików) oraz rozpoznać podstawowe zagrożenia oraz ataki.	K1_CBE_U16
PEU_U02	Potrafi konfigurować komponenty bezpieczeństwa systemu	K1_CBE_U16
PEU_U03	Potrafi wdrożyć zalecenia norm i rekomendacji do systemu operacyjnego oraz mierzyć ich skuteczność	K1_CBE_U16

Treści programowe zapewniające uzyskanie efektów uczenia się

Poznanie metod ochrony systemów operacyjnych przed atakami naruszającymi bezpieczeństwo tych systemów.
Poznanie ataków komputerowych na systemy operacyjne oraz metod wykrywania ataków z tych źródeł.
Poznanie metod zapobiegania atakom oraz minimalizowania zagrożeń z nich wynikających.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	45
Przygotowanie do zajęć	12
Samodzielne studiowanie tematyki zajęć	40
Przygotowanie raportu/sprawozdania/prezentacji/referatu	15
Przygotowanie do egzaminu/zaliczenia	6
Zaliczenie/Egzamin	2
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
2025/2026

Kod przedmiotu
PWRSJOS.83CJO.04092.25

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 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
2025/2026

Kod przedmiotu
W4NCBECSIS.110PS.00091.25

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_W16
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_W16
PEU_W03	Charakteryzuje metryki jakościowe pomocne w detekcji cyberataków oraz wskazuje metody ich prewencji.	K1_CBE_W16

Z zakresu umiejętności		
PEU_U01	Potrafi skonfigurować sieć WLAN, przeprowadzać podstawową diagnostykę i nią zarządzać.	K1_CBE_U24
PEU_U02	Potrafi skonfigurować pikosieć Bluetooth, przeprowadzać podstawową diagnostykę i nią zarządzać.	K1_CBE_U24
PEU_U03	Potrafi stosować narzędzia do testów wydajnościowych sieci WLAN oraz Bluetooth.	K1_CBE_U24
PEU_U04	Obsługuje analizator widma.	K1_CBE_U24
PEU_U05	Konfiguruje nastawy zapewniające wymagany poziom bezpieczeństwa urządzeń dostępowych systemów bezprzewodowych oraz założone parametry bezpieczeństwa transmisji.	K1_CBE_U24
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_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach realizacji kursu poruszane są aspekty z zakresu współczesnych sieci radiowych o różnym zasięgu i charakterze. Prezentowane są metody szacowania pojemności, przewidywania zagrożeń z zakresu kompatybilności elektromagnetycznej oraz szacowania osiągów interfejsu bezprzewodowego. Studenci zdobywają również wiedzę z zakresu konfiguracji urządzeń ze szczególnym uwzględnieniem zasad cyberbezpieczeństwa (metodyk detekcji ataków i ich prewencji).

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	13
Przygotowanie do zajęć	5
Przygotowanie raportu/sprawozdania/prezentacji/referatu	10
Zaliczenie/Egzamin	2
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

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
2025/2026

Kod przedmiotu
W4NCBECIKS.110PS.00098.25

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_W16
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_W16

Treści programowe zapewniające uzyskanie efektów uczenia się

Celem przedmiotu jest zapoznanie studentów z zagrożeniami 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

Biometria

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
2025/2026

Kod przedmiotu
W4NCBECSIS.110PS.00092.25

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 Seminarium: 15	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Student posiada podstawową wiedzę dotyczącą modalności biometrycznych, metod weryfikacji i identyfikacji oraz metryk stosowanych w systemach biometrycznych	K1_CBE_W16
PEU_W02	Student posiada wiedzę dotyczącą budowy i zasad działania urządzeń wykorzystywanych w systemach biometrycznych (sond, skanerów itp.) oraz architektury systemów biometrycznych, w tym jej zasadniczych elementów.	K1_CBE_W16

PEU_W03	Student zna algorytmy, koncepcje oraz techniki pozwalające przetwarzać dane biometryczne oraz uzyskiwać z nich profile użytkowników.	K1_CBE_W16
PEU_W04	Student zna kontekst prawny i etyczny związany z biometrią, w tym problemy stronniczości sytemów biomerycznych (ang. bias) oraz ochrony danych osobowych	K1_CBE_W16
PEU_W05	Student posiada wiedzę dotyczącą procesów standaryzacyjnych oraz certyfikacyjnych rozwiązań w biometrii	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Student potrafi dobrać odpowiednią modalność biometryczną do konkretnych potrzeb scenariusza weryfikacji i identyfikacji tożsamości oraz określić warunki brzegowe dla opracowywanego rozwiązania.	K1_CBE_U24
PEU_U02	Student potrafi wyspecyfikować parametry niezbędne do dokonania poprawnej identyfikacji biometrycznej oraz wskazać odpowiednią metodę, aparaturę i oprogramowanie	K1_CBE_U24
PEU_U03	Student potrafi opracować 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_U24
PEU_U04	Student analizuje krytycznie zaprezentowany materiał o systemach biometrycznych i argumentuje swoje wątpliwości	K1_CBE_U24
PEU_U05	Student posługuje się bazami wiedzy naukowej i dobiera źródła literaturowe, w tym artykuły naukowe, do zadanego tematu biometrycznego oraz przygotowuje podsumowanie wybranego zagadnienia.	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Kurs Biometria jest interdyscyplinarnym przedmiotem czerpiącym z wielu obszarów kształcenia, w tym przetwarzania sygnałów, bezpieczeństwa komputerowego, programowania, wizji komputerowej i projektowania systemów informatycznych, jak również obszaru regulacji prawnych i standaryzacji.
Wprowadza słuchacza do zawiłego świata biometrii i wyjaśnia stosowaną nomenklaturę, używane wskaźniki mówiące o jakości klasyfikatorów biometrycznych, deskryptory dla poszczególnych modalności biometrycznych, prezentuje szereg algorytmów, koncepcji i technik związanych z przetwarzaniem danych biometrycznych i uzyskiwania z nich modeli użytkownika, jak również porusza kwestie etyczne i prawne związane z danymi biometrycznymi.
Na kursie studenci uczą się podejścia do projektowania systemów biometrycznych, zapoznają się z ich problematyką na wielu płaszczyznach, począwszy od technicznej, poprzez scenariusze użycia, a kończąc na wdrożeniu i eksploatacji systemu. Nieodzowny element kursy stanowią 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	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Elektroenergetyczna automatyka zabezpieczeniowa

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
2025/2026

Kod przedmiotu
W4NCBECIKS.110PS.00099.25

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	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	Zna budowę i zasadę działania przekładników prądowych, napięciowych i filtrów składowych symetrycznych oraz analogowych i cyfrowych przekaźników elektroenergetycznych.	K1_CBE_W16
PEU_W02	Rozumie i potrafi opisać podstawowe kryteria działania zabezpieczeń elektroenergetycznych oraz przedstawić podstawowe charakterystyki jednowejściowych i wielowejściowych przekaźników elektroenergetycznych.	K1_CBE_W16
PEU_W03	Zna zasady wyposażania elementów systemu elektroenergetycznego w automatykę zabezpieczeniową i rozumie zasady doboru nastaw tej automatyki.	K1_CBE_W16

Z zakresu umiejętności		
PEU_U01	Potrafi zaprojektować układ pomiarowy, dobrać przyrządy pomiarowe oraz połączyć układ do badania przetworników i przekaźników pomiarowych jedno i wielowejściowych.	K1_CBE_U24
PEU_U02	Potrafi wykonać pomiary charakterystyk, opracować wyniki i sformułować wnioski.	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Treści programowe obejmują:
1. Zapoznanie studenta z rodzajami elektroenergetycznej automatyki zabezpieczeniowej w powiązaniu z rodzajem zakłócenia w pracy systemu elektroenergetycznego.
2. Zapoznanie studenta z budową i zasadą działania przetworników wielkości pomiarowych zabezpieczeń.
3. Zapoznanie studenta z budową i zasadami działania elektroenergetycznych przekaźników pomiarowych jedno i wielowejściowych.
4. Zapoznanie studenta z zasadami i technikami realizacji zabezpieczeń elementów systemu elektroenergetycznego.
5. Nabycie praktycznej umiejętności wykonywania badań elementów elektroenergetycznej automatyki zabezpieczeniowej – przetworników i przekaźników pomiarowych oraz zabezpieczeń elektroenergetycznych.
6. Nabycie praktycznej umiejętności doboru rodzaju i obliczania nastaw zabezpieczeń elektroenergetycznych
7. Nabycie umiejętności 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

Bezpieczeństwo serwerów i aplikacji Web

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
2025/2026

Kod przedmiotu
W4NCBECSIS.110PS.00093.25

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	6.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Zna podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych	K1_CBE_W16
PEU_W02	Zna metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych	K1_CBE_W16
PEU_W03	Wie co to są certyfikaty SSL i jak działają protokoły SSL/TLS	K1_CBE_W16
PEU_W04	Zna metody ataków typu XSS, CSRF, ,,code injection'', w szczególności SQLinjection i problemy z przekazywaniem parametrów pomiędzy programami	K1_CBE_W16

Z zakresu umiejętności		
PEU_U01	Potrafi wskazać typowe błędy związane z bezpieczeństwem w konfiguracji serwerów sieciowych, potrafi skonfigurować serwer WWW	K1_CBE_U24
PEU_U02	Potrafi sprawdzić integralność danych w systemie komputerowym i wykorzystać techniki kryptograficzne do do zwiększenia bezpieczeństwa systemu.	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zdobędą wiedzę z zakresu bezpiecznego programowania w różnych środowiskach, ze szczególnym uwzględnieniem programowania web (skrypty, muddleware, aplikacje klienckie), metodologii wspomagających tworzenie bezpiecznych programów, takich jak programowanie defensywne i programowanie sterowane testowaniem, typowych ataków na serwery WWW i aplikacje webowe oraz metod zapobiegania atakom na aplikacje webowe oraz minimalizowania 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	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	50
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Zagrożenia w funkcjonowaniu infrastruktury elektroenergetycznej

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
2025/2026

Kod przedmiotu
W4NCBECIKS.110PS.00100.25

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	Ma wiedzę z zakresu roli, funkcjonowania i wyposażenia stacji elektroenergetycznych.	K1_CBE_W16
PEU_W02	Zna narażenia klimatyczne, środowiskowe i eksploatacyjne występujące w stacjach elektroenergetycznych.	K1_CBE_W16
PEU_W03	Zna urządzenia prowadzenia ruchu stacji oraz rozwiązania automatyki stacyjnej i systemy sterowania i nadzoru (SSiN) w kontekście bezpieczeństwa pracy i jego zagrożeń.	K1_CBE_W16
Z zakresu umiejętności		

PEU_U01	Potrafi określić narażenia klimatyczne, środowiskowe i eksploatacyjne występujące w stacjach elektroenergetycznych i im przeciwdziałać.	K1_CBE_U24
PEU_U02	Potrafi określić poziom bezpieczeństwa pracy dla urządzeń prowadzenia ruchu stacji, automatyki stacyjnej i systemów sterowania i nadzoru (SSiN).	K1_CBE_U24
PEU_U03	Potrafi zidentyfikować zagrożenia bezpieczeństwa pracy stacji elektroenergetycznej i zastosować adekwatne środki w celu jego ograniczenia.	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Funkcjonowanie, rola i znaczenie stacji elektroenergetycznych w Krajowym Systemie Elektroenergetycznym (KSE).
Rozwiązania i wyposażenie stacji elektroenergetycznych.
Narażenia klimatyczne i środowiskowe występujące w stacjach elektroenergetycznych.
Eksploatacja stacji elektroenergetycznych.
Identyfikacja narażeń klimatycznych, środowiskowych i eksploatacyjnych występujących w stacjach elektroenergetycznych.
Sposoby i środki przeciwdziałania lub ograniczania narażeń.
Urządzenia prowadzenia ruchu stacji i automatyka stacyjna.
Systemy sterowania i nadzoru (SSiN) stacji elektroenergetycznych.
Komputerowe systemy wspomagania, nadzorowania i kierowania pracą stacji stosowane w stacjach energetyki zawodowej.
Zawansowane systemy sterowania i nadzoru stacji elektroenergetycznych (Smart Operations) w ramach Smart Grid.
Ocena poziomu bezpieczeństwa pracy stacji elektroenergetycznych.
Identyfikacja zagrożeń bezpieczeństwa pracy stacji elektroenergetycznej.
Sposoby i środki przeciwdziałania lub ograniczania zagrożeń bezpieczeństwa pracy stacji elektroenergetycznej.
Uwarunkowania prawne, techniczne, ekonomiczne i społeczne związane z bezpieczeństwem pracy infrastruktury elektroenergetycznej.

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

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
2025/2026

Kod przedmiotu
W4NCBECSIS.110PS.00094.25

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	Zna typowe zagrożenia dla środowisk wirtualnych oraz chmur obliczeniowych w centrach danych, w tym sposoby wykrywania włamań sieciowych i kontroli dostępu.	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Potrafi planować oraz implementować mechanizmy zabezpieczające w środowisku chmur obliczeniowych.	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Nabycie wiedzy z zakresu zabezpieczania chmur obliczeniowych - polityki, kontrakty i zarządzanie na wszystkich warstwach. Poszerzenie umiejętności z zakresu zabezpieczania chmur obliczeniowych.

Nakład pracy studenta

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

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
2025/2026

Kod przedmiotu
W4NCBECIKS.110PS.00102.25

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_W16
PEU_W02	Identyfikuje i przedstawia techniki sterowania i technologie komunikacji wykorzystywanych w układach automatyki elektroenergetycznej	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Dobiera, projektuje i testuje układy inteligentnych systemów pomiarowych i układy automatyki elektroenergetycznej	K1_CBE_U24

PEU_U02	Opracowuje wyniki przeprowadzonych pomiarów i testów. Formułuje wnioski.	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Zadania przewodowej w tym PLC oraz bezprzewodowej komunikacji, podstawowe definicje.
2. Normalizacja komunikacji przewodowej w tym PLC, wady i zalety
3. Architektura sieci elektrycznej, modelowanie urządzeń elektrycznych, architektura warstwowa OSI.
4. Funkcjonalność kanału transmisyjnego, synchronizacja, sterowanie ramkami, priorytety zarządzania ramką.
5. Przegląd sposobów zabezpieczania sieci PLC. Funkcjonalność trybów transmisji w sieci: klient – serwer, p2p, centralizowana.
6. Główny obszar zastosowań: telefonia, przesyłanie obrazu, multimedia, urządzenia dla różnych trybów transmisji.
7. Wybór kabla transmisyjnego, sposoby sprzęgania, transformatory i mierniki.
8. Problemy aplikacji wybranych czujników/urządzeń pomiarowych.
9. Monitorowanie wielkości elektrycznych i nieelektrycznych oraz zdalny pomiar.
10. Architektura bezprzewodowych sieci HAN, LAN, zalety i wady .
11. Architektura przewodowych sieci HAN, LAN, zalety i wady.
12. Komunikacja GOOSE, jako część komunikacji zgodnej ze standardem IEC61850.
13. Komunikacja MMS, jako część komunikacji zgodnej ze standardem IEC61850, Komunikacja między urządzeniami po protokole MODBUS (RS485).
14. 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
Przygotowanie do zajęć	10
Przygotowanie raportu/sprawozdania/prezentacji/referatu	20
Laboratorium	15
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 75

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
2025/2026

Kod przedmiotu
W4NCBECIKS.110PS.00103.25

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	Ma ogólną wiedzę na temat zagadnień związanych z zaburzeniami jakości energii elektrycznej, zna dokumenty legislacyjne i regulacje dotyczące wymogów w tym zakresie	K1_CBE_W16
PEU_W02	Orientuje się w obecnym stanie rozwoju urządzeń i systemów monitorowania jakości energii elektrycznej, zna zasady tworzenia raportów oceny jakości energii elektrycznej	K1_CBE_W16
PEU_W03	Posiada wiedzę w zakresie potencjalnych źródeł zaburzeń jakości energii oraz ich wpływu na pracę urządzeń elektrycznych	K1_CBE_W16
Z zakresu umiejętności		

PEU_U01	Potrafi wyznaczyć i ocenić parametry charakteryzujące jakość energii elektrycznej	K1_CBE_U24
PEU_U02	Potrafi powiązać podstawowe źródła zaburzeń z ich potencjalnym wpływem na pracę elementów sieci elektroenergetycznych, zna procedury przeprowadzania badań odporności odbiorników energii elektrycznej na zaburzenia jakości energii	K1_CBE_U24
PEU_U03	Posiada umiejętności pozwalające na dobór i ocenę wybranych rozwiązań poprawy jakości napięcia zasilającego	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Treści programowe obejmują:

- zdobycie wiedzy na temat parametrów definiujących jakość energii oraz norm i przepisów dedykowanych poziomom dopuszczalnym i metodom oceny jakości energii,
- poznanie zjawisk dotyczących zaburzeń jakości energii, źródeł i skutków tych zaburzeń,
- nabycie umiejętności zastosowania 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

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
2025/2026

Kod przedmiotu
W4NCBECIKS.110PS.00858.25

Grupa zajęć
Tak

Języki wykładowe
polski

Obligatoryjność
Obowiązkowy specjalnościowy

Blok zajęciowy
Przedmioty specjalnościowe

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

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Ma podstawową wiedzę dotyczącą praw elektrotechniki, pola elektrycznego i magnetycznego prądu elektrycznego wraz ze zjawiskami związanymi z indukcyjnością elektromagnetyczną i polem magnetycznym w urządzeniach i maszynach elektrycznych.	K1_CBE_W16
PEU_W02	Posiada uporządkowaną wiedzę z budowy i zasady działania transformatorów i silników elektrycznych prądu przemiennego i stałego oraz wiedzę w zakresie bezpiecznej obsługi urządzeń elektrycznych niskiego napięcia i zna odpowiednie środki i metody ochrony przeciwporażeniowej.	K1_CBE_W16

Treści programowe zapewniające uzyskanie efektów uczenia się

Treści programowe obejmują wiedzę z zakresu elektrotechniki. Przyswojenie pojęć związanych 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 kursach.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Przygotowanie do zajęć	8
Przeprowadzenie badań literaturowych	5
Przygotowanie do egzaminu/zaliczenia	7
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

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
2025/2026

Kod przedmiotu
W4NCBES.110PK.00083.25

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	Posiada podstawową wiedze o zagrożeniach i zabezpieczaniu urządzeń teleinformatycznych. Zna koncepcję uwierzytelniania, kontroli dostępu i rozliczalności (AAA).	K1_CBE_W21
PEU_W02	Zna systemy zapór sieciowych oraz implementacje systemów ochrony przed włamaniami sieciowymi (IPS).	K1_CBE_W21
PEU_W03	Zna metody zabezpieczania sieci LAN oraz techniki szyfrowania używane w połączeniach VPN.	K1_CBE_W21
PEU_W04	Zna koncepcję zarządzania bezpieczną siecią oraz funkcjonalność dedykowanych zapór sieciowych (ASA).	K1_CBE_W21

Z zakresu umiejętności		
PEU_U01	Potrafi zabezpieczać dostęp administracyjny na routerach.	K1_CBE_U17
PEU_U02	Potrafi konfigurować zapory sieciowe.	K1_CBE_U17
PEU_U03	Potrafi konfigurować systemy ochrony przed włamaniami sieciowymi (IPS).	K1_CBE_U17
PEU_U04	Potrafi konfigurować funkcje bezpieczeństwa na urządzeniach warstwy 2	K1_CBE_U17
PEU_U05	Potrafi konfigurować sieci VPN i tunelowanie ruchu na routerach i dedykowanych zaporach sieciowych	K1_CBE_U17

Treści programowe zapewniające uzyskanie efektów uczenia się

Zdobycie podstawowej wiedzy o metodach i mechanizmach bezpieczeństwa w sieciach komputerowych, ochrony dostępu, filtrowania ruchu oraz utajniania treści.
Zdobycie podstawowej wiedzy o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom.
Zdobycie 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	30
Przygotowanie do egzaminu/zaliczenia	5
Samodzielne studiowanie tematyki zajęć	25
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 150

Politechnika Wrocławska

Bezpieczeństwo elektromagnetyczne

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
2025/2026

Kod przedmiotu
W4NCBES.110PK.00084.25

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	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	Ma podstawową wiedzę z zakresu bezpieczeństwa elektromagnetycznego, obejmującą identyfikację zagrożeń oraz skutków wynikających 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_W19
PEU_W02	Ma podstawową wiedzę o stosowanych rozwiązaniach technicznych i organizacyjnych, które poprawiają bezpieczeństwo elektromagnetyczne i niezawodność działania urządzeń, systemów, sieci.	K1_CBE_W19

PEU_W03	Wie, jak scharakteryzować wymagania w zakresie bezpieczeństwa elektromagnetycznego, stosowanych zabezpieczeń i środków ochrony, jak i określić zagrożenia elektromagnetyczne występujące w różnych środowiskach elektromagnetycznych.	K1_CBE_W19
PEU_W04	Zna rodzaje i charakterystyki zaburzeń elektromagnetycznych oraz zna mechanizmy i drogi ich rozprzestrzeniania.	K1_CBE_W19
PEU_W05	Zna pojęcia odporność i podatność na zaburzenia elektromagnetyczne oraz emisję elektromagnetyczną i kanały ulotu informacji. Wie, jak wskazać właściwe metody ich pomiaru i testowania oraz wyjaśnić kryteria ich wyboru.	K1_CBE_W19
PEU_W06	Zna architekturę bezpieczeństwa sieci oraz systemów oraz potrafi zidentyfikować elementy architektury (infrastruktury, urządzeń końcowych i aplikacji)	K1_CBE_W19
PEU_W07	Zna metody szacowania ryzyka czasowego lub całkowitego uszkodzenia lub zaburzenia pracy infrastruktury, jej elementów, w tym urządzeń końcowych i aplikacji.	K1_CBE_W19
PEU_W08	Wie jakie metody ochrony organizacyjnej i technicznej są stosowane m.in. dla osób, w budynkach i pomieszczeniach oraz urządzeniach, systemach, sieciach i instalacjach, aby ograniczyć poziomy narażeń elektromagnetycznych i skutki ich oddziaływania, a także skutecznie chronić się przez elektromagnetycznym ulotem informacji	K1_CBE_W19
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_U18
PEU_U02	Potrafi opracować i zinterpretować otrzymane wyniki badań, w tym dokonać klasyfikacji zagrożeń i efektywności stosowanych zabezpieczeń	K1_CBE_U18
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_U18
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_U18
PEU_U05	Potrafi krytycznie ocenić rozwiązania naukowo-techniczne stosowane dla oceny i zapewnienia bezpieczeństwa elektromagnetycznego	K1_CBE_U18

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Zdobycie podstawowej wiedzy z zakresu bezpieczeństwa elektromagnetycznego, obejmujące identyfikację zagrożeń wynikających z elektromagnetycznego ulotu informacji jak i możliwych zagrożeń i ataków elektromagnetycznych na urządzenia, systemy, sieci oraz ich części oraz zaznajomienie się z typowymi rozwiązaniami technicznymi i organizacyjnymi, które poprawiają bezpieczeństwo elektromagnetyczne i niezawodność działania urządzeń, systemów, sieci i instalacji.
2. Zdobycie umiejętności: wyboru technik badawczych, konfigurowania stanowisk testowych, wyznaczania parametrów technicznych i skuteczności stosowanych zabezpieczeń i ich klasyfikacji, wykonywania podstawowych badań emisyjności i

podatności na zaburzenia elektromagnetyczne oraz opracowywania i interpretacji otrzymanych wyników badań. Zdobycie umiejętności pomiaru rozwiązań technicznych ograniczających ulot informacji.
3. Nabywanie i utrwalanie kompetencji społecznych obejmujących inteligencję emocjonalną polegającą na umiejętności współpracy w grupie studenckiej, których celem jest efektywne rozwiązywanie problemów i wyzwań. Odpowiedzialność, uczciwość i rzetelność w postępowaniu; przestrzeganie obyczajów obowiązujących w środowisku akademickim i społeczeństwie.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	30
Przygotowanie do zajęć	30
Przygotowanie raportu/sprawozdania/prezentacji/referatu	30
Przeprowadzenie badań literaturowych	15
Przygotowanie do egzaminu/zaliczenia	5
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Projekt zespołowy

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
2025/2026

Kod przedmiotu
W4NCBECSIS.120PS.00051.25

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

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Potrafi wykonać zadania w ramach realizacji złożonego projektu informatycznego.	K1_CBE_U24
PEU_U02	Umie zastosować zasady zarządzania projektem do realizacji złożonego projektu informatycznego.	K1_CBE_U24
PEU_U03	Umie opracować dokumentację projektu.	K1_CBE_U24
Z zakresu kompetencji społecznych		
PEU_K01	Jest świadomy konieczności należytej współpracy z zespołem, wykazuje się świadomością swojej roli w projekcie oraz dbałością o terminową realizację powierzonych zadań.	K1_CBE_K04

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Nabycie umiejętności wykonania przydzielonych zadań inżynierskich w ramach realizacji złożonego zadania inżynierskiego.
2. Zdobycie doświadczeń w pracy zespołowej, w tym umiejętności planowania i harmonogramowania, komunikacji wewnątrz-zespołowej, pełnienia roli członka zespołu bądź lidera, możliwość wykazania się kreatywnością, otwartością na innowacyjne podejście do realizacji celu oraz zorientowaniem na sukces zespołu.

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

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
2025/2026

Kod przedmiotu
W4NCBECSIS.120PS.00095.25

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	1. 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_W16
PEU_W02	2. 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_W16

PEU_W03	3. 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_W16
Z zakresu umiejętności		
PEU_U01	1. 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_U24
PEU_U02	2. Tworzy procesy ekstrakcji, transformacji i ładowania danych (ETL), stosuje odpowiednie techniki raportowania analitycznego oraz dostosowuje narzędzia do specyficznych wymagań środowiska analitycznego.	K1_CBE_U24
PEU_U03	3. 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_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Program zajęć obejmuje szeroki zakres zagadnień związanych z przetwarzaniem danych, analizą danych oraz pozyskiwaniem wiedzy z dużych zbiorów danych. Na początku omawiane są kwestie rozwoju systemów baz/hurtowni danych oraz potrzeby przetwarzania dużych ilości danych, co prowadzi do zaprezentowania modeli logicznych systemów przetwarzających duże wolumeny danych. Następnie poruszane są tematy związane z analityką biznesową i hurtowniami danych, w tym potrzeba ich tworzenia oraz modele logiczne. Przedstawiony zostaje proces ETL, obejmujący ekstrakcję, transformację i ładowanie danych, a także raportowanie analityczne w określonym środowisku. Kolejne tematy koncentrują się na uczeniu maszynowym, w tym na terminologii, wprowadzeniu do Spark i PySpark oraz zarządzaniu cyklem życia eksperymentów za pomocą MLflow. Omówione są również procesy związane z pobieraniem danych, ich wstępnym przetwarzaniem oraz statystykami opisowymi, jak również inżynieria cech. Na zakończenie kursu przedstawione zostaje trenowanie modeli z wykorzystaniem Spark MLlib oraz wzorce wdrażania modeli uczenia maszynowego dla duzych zbiorów danych.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Projekt	15
Zaliczenie/Egzamin	4
Przygotowanie do egzaminu/zaliczenia	6
Samodzielne studiowanie tematyki zajęć	45
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

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
2025/2026

Kod przedmiotu
W4NCBECSIS.120PS.00096.25

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	Posiada podstawową wiedzę z zakresu: genezy, zastosowań, stanu badań i perspektyw rozwoju, architektury oraz warstwy fizycznej i protokołów wielodostępu stosowanych w systemach IoT	K1_CBE_W16
PEU_W02	Zna podstawowe systemy telekomunikacyjne IoT: z grupy 3GPP (NB-IoT, LTE-M/TC), rozwiązań firmowych (LoRa, Weightless, SigFox itp.)	K1_CBE_W16
PEU_W03	Zna zagrożenia wynikające ze stosowania systemów i podejścia IoT, zarówno pod kątem sprzętowym jak i programowym, oraz metody przeciwdziałania zagrożeniom w tych zakresach	K1_CBE_W16

Z zakresu umiejętności		
PEU_U01	Potrafi odpowiednio skonfigurować układ mikroprocesorowy (np. Arduino, Raspberry Pi) do rejestracji odczytów rozmaitych czujników analogowych i cyfrowych	K1_CBE_U24
PEU_U02	Potrafi dobrać oraz skonfigurować 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_U24
PEU_U03	Potrafi dobrać oraz skonfigurować 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_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci uzyskają podstawową wiedzę z zakresu istoty i roli Internetu Rzeczy (IoT) we współczesnych realiach gospodarczych i technologicznych, zastosowań, specyfiki i zasad działania systemów stosowanych w Internecie Rzeczy, wiodących standardów transmisyjnych IoT, zagrożeń dla prywatności, urządzeń i sieci IoT oraz metod przeciwdziałania im oraz umiejętności instalowania i zarządzania 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	15
Przygotowanie raportu/sprawozdania/prezentacji/referatu	25
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
2025/2026

Kod przedmiotu
W4NCBECSIS.120PS.00037.25

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	Student klasyfikuje elementy usługi internetowej	K1_CBE_W16
PEU_W02	Student definiuje architektoniczny wzorzec projektowy REST	K1_CBE_W16
PEU_W03	Student rozpoznaje krytyczne ryzyka dla bezpieczeństwa sieciowych interfejsów programistycznych	K1_CBE_W16
PEU_W04	Student odtwarza dobre praktyki projektowania sieciowych interfejsów programistycznych	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Student konstruuje bazę danych dla usługi internetowej	K1_CBE_U24

PEU_U02	Student kwestionuje zasadność poszczególnych elementów interfejsu programistycznego	K1_CBE_U24
PEU_U03	Student dokumentuje wykonany samodzielnie sieciowy interfejs programistyczny	K1_CBE_U24
PEU_U04	Student współpracuje w grupie	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Kurs wprowadza osoby studenckie w tematykę projektowania współczesnych usług internetowych opartych o architektoniczny wzorzec projektowy REST, przeprowadzając je od podstaw komunikacji z wykorzystaniem protokołu HTTP do narzędzi produkcji takich systemów. Niezbędne tło teoretyczne stanowi introdukcję do podstaw protokolarnych internetu rozumianego z perspektywy WWW, zgodnie z wytycznymi ustanowionymi w regułach Representational State Transfer, stanowiącego architektoniczną specyfikację jednolitego interfejsu programistycznego usług sieciowych. Kurs rozwija się później do opisu realizacji praktycznej ~ opartej o nowoczesne frameworki budowy aplikacji internetowych ~ szczególną uwagę przykładając do tematyki planowania architektury informacji systemu, reprezentacji danych oraz dokumentacji kodu. Zajęcia projektowe stanowią narzędzie weryfikacji samodzielności osób studenckich w realizacji złożonego zadania projektowego i są weryfikowane w oparciu o wytyczne prezentowane na poszczególnych wykładach.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	15
Przygotowanie projektu	19
Zaliczenie/Egzamin	1
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 50

Politechnika Wrocławska

Projekt zespołowy

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
2025/2026

Kod przedmiotu
W4NCBECIKS.120PS.00051.25

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

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Potrafi wykonać zadania w ramach realizacji złożonego projektu informatycznego.	K1_CBE_U24
PEU_U02	Umie zastosować zasady zarządzania projektem do realizacji złożonego projektu informatycznego.	K1_CBE_U24
PEU_U03	Umie opracować dokumentację projektu.	K1_CBE_U24
Z zakresu kompetencji społecznych		
PEU_K01	Jest świadomy konieczności należytej współpracy z zespołem, wykazuje się świadomością swojej roli w projekcie oraz dbałością o terminową realizację powierzonych zadań.	K1_CBE_K04

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Nabycie umiejętności wykonania przydzielonych zadań inżynierskich w ramach realizacji złożonego zadania inżynierskiego.
2. Zdobycie doświadczeń w pracy zespołowej, w tym umiejętności planowania i harmonogramowania, komunikacji wewnątrz-zespołowej, pełnienia roli członka zespołu bądź lidera, możliwość wykazania się kreatywnością, otwartością na innowacyjne podejście do realizacji celu oraz zorientowaniem na sukces zespołu.

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	15
Zaliczenie/Egzamin	5
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

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
2025/2026

Kod przedmiotu
W4NCBECIKS.120PS.00105.25

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	Zna sposoby realizacji łączności pomiędzy zabezpieczeniami elektroenergetycznymi, układami sterowania i regulacji oraz stanowiskiem dyspozytorskim.	K1_CBE_W16
PEU_W02	Zna środki stosowane w systemach elektroenergetycznych w celu zapewnienia bezpieczeństwa ich pracy.	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Potrafi dobrać i dokonać nastaw wartości rozruchowych wielkości kryterialnych zabezpieczeń oraz wyznaczyć charakterystyki podstawowych kryteriów zabezpieczeń elektroenergetycznych	K1_CBE_U24

PEU_U02	Ma umiejętności związane z nawiązywaniem komunikacji cyfrowej między zabezpieczeniem elektroenergetycznym a sterownikiem polowym (koncentratorem), jako elementem Systemu Sterowania i Nadzoru.	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Treści programowe obejmują:
1. Zapoznanie studenta z nowoczesnymi zabezpieczeniami elektroenergetycznymi sieci elektroenergetycznych, koncentratorami oraz stanowiskiem dyspozytorskim.
2. Nabycie praktycznej wiedzy i umiejętności nastawiania wielkości rozruchowych wybranych kryteriów zabezpieczeń linii w zależności od układu pracy sieci elektroenergetycznej
3. Wyrobienie umiejętności zastosowania nowoczesnych metod, technik i narzędzi do badania zabezpieczeń elektroenergetycznych.
4. Rozwój kompetencji związanych z szeroko rozumianymi aplikacjami SCADA (protokoły komunikacyjne, koncentratory, stanowisko dyspozytorskie).

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	10
Samodzielne studiowanie tematyki zajęć	5
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 100

Politechnika Wrocławska

Cyberbezpieczeństwo inteligentnych sieci elektroenergetycznych

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2025/2026
Specjalność bezpieczeństwo infrastruktury krytycznej	**Kod przedmiotu** W4NCBECIKS.120PS.00106.25
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Grupa zajęć** Tak
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Języki wykładowe** polski
Forma studiów studia stacjonarne	**Obligatoryjność** Obowiązkowy specjalnościowy
Profil studiów profil ogólnoakademicki	**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	Zna i rozumie przyczyny i skutki zagrożeń informatycznych dla infrastruktury inteligentnych sieci elektroenergetycznych	K1_CBE_W16
PEU_W02	Ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie identyfikacji i reagowania na incydenty cybernetyczne w systemach IIoT [Industrial Internet of Things]	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Potrafi opracowywać procedury wspierające bezpieczeństwo informatyczne systemów IIoT [Industrial Internet of Things]	K1_CBE_U24

PEU_U02	Potrafi podejmować działania związane z naruszeniem poufności informacji przetwarzanych w inteligentnych sieciach elektroenergetycznych	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Cele, zadania oraz zagrożenia dot. inteligentnych sieci elektroenergetycznych (ISE), jako podsystemu infrastruktury krytycznej.
2. Podstawy prawne, podstawowe definicje i klasyfikacja systemów informacyjnych. Cel i strategia bezpieczeństwa informacji.
3. Wybrane zagadnienia z teorii bezpieczeństwa informacji przetwarzanych w systemach IIot [Industrial Internet of Things].
4. Bezpieczeństwo informacji w inteligentnych sieciach domowych (HAN - Home Area Network).
5. Zarządzanie bezpieczeństwem informacji w systemach zdalnego odczytu liczników (AMI – Advanced Metering Infrastructure)
6. Wybrane zagadnienia z zakresu zarządzania rozproszonymi źródłami energii.
7. Utrzymanie ciągłości działania systemów informacyjnych IIoT oraz procesy wznowienia działania systemów informacyjnych po przerwie spowodowanej czynnikami naturalnymi lub wywołanej przez człowieka.

Nakład pracy studenta

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

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
2025/2026

Kod przedmiotu
W4NCBECIKS.120PS.00107.25

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	Ma wiedzę dotyczącą mechanizmu rozwoju wyładowań piorunowych oraz rodzajów wyładowań doziemnych; zna zasady ochrony przepięciowej w instalacjach elektroenergetycznych i sygnałowych; ma podstawową wiedzę z zakresu ekranowania pola elektromagnetycznego	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Posiada umiejętności praktyczne potrzebne do wykonywania prób i badań urządzeń wysokimi napięciami udarowymi, symulującymi przepięcia piorunowe i łączeniowe	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

Treści programowe obejmują:
Zaznajomienie z zasadami i technikami realizacji zabezpieczeń instalacji elektrycznych zasilających urządzenia lokalnych sieci komputerowych
Nabycie praktycznej umiejętności wykonywania badań elementów zabezpieczeniowych

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

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
2025/2026

Kod przedmiotu
W4NCBES.120PK.00085.25

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	Ma podstawową wiedzę na temat metod zarządzania projektami	K1_CBE_W10
PEU_W02	Ma wiedzę odnośnie monitorowania postępu projektu	K1_CBE_W10
Z zakresu umiejętności		
PEU_U01	Potrafi dobrać i stosować metodykę zarządania projektami	K1_CBE_U10
PEU_U02	Potrafi przygotować harmonogramy i alokować zasoby.	K1_CBE_U10
PEU_U03	Potrafi monitorować realizację projektu	K1_CBE_U10

Treści programowe zapewniające uzyskanie efektów uczenia się

Poznanie podstawowych zasad zarządania projektami IT. Przegląd róznych metodologii. Umiejętność wyborumetodologii do konkretnego przojektu.

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Projekt	15
Samodzielne studiowanie tematyki zajęć	20
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
2025/2026

Kod przedmiotu
W4NCBES.120PK.00086.25

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	Zna koncepcję oraz cele testowania penetracyjnego.	K1_CBE_W11
PEU_W02	Posiada wiedzę o sposobach i narzędziach do prowadzania testów penetracyjnych.	K1_CBE_W11
Z zakresu umiejętności		
PEU_U01	Potrafi planować i przygotowywać procedury testowania penetracyjnego.	K1_CBE_U13

PEU_U02	Umie przeprowadzać podstawowe testy penetracyjne w obszarze infrastruktury teleinformatycznej oraz na poziomie aplikacji internetowych.	K1_CBE_U13
PEU_U03	Umie zaprezentować i omówić w sposób logiczny i zrozumiały opracowane koncepcje oraz dokumentację techniczną.	K1_CBE_U13

Treści programowe zapewniające uzyskanie efektów uczenia się

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

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	15
Laboratorium	45
Przygotowanie raportu/sprawozdania/prezentacji/referatu	40
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** 2025/2026
Specjalność -	**Kod przedmiotu** W4NCBES.120PK.00087.25
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Grupa zajęć** Tak
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Języki wykładowe** polski
Forma studiów studia stacjonarne	**Obligatoryjność** Obowiązkowy
Profil studiów profil ogólnoakademicki	**Blok zajęciowy** Przedmioty kierunkowe
	Przedmiot powiązany z badaniami naukowymi Tak

Semestr Semestr 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	zna najważniejsze metody sztucznej inteligencji (AI) i uczenia maszynowego (ML) stosowane w modelowaniu i wykrywaniu zagrożeń / ataków na systemy komputerowe zna najważniejsze metody wykrywania anomalii / nietypowych profili w danych z monitoringu ruchu sieciowego, monitoringu zdarzeń i obciążenia urządzeń i z innych źródeł zna strukturę i specyfikę zbiorów i źródeł danych wykorzystywanych w modelowaniu i wykrywaniu zagrożeń w systemach komputerowych	K1_CBE_W14
Z zakresu umiejętności		

PEU_U01	potrafi dobrać i wykorzystać właściwe metody analizy danych w zadaniu analizy zagrożeń lub wykrywania anomalii w zależności od specyfiki ataku i specyfiki źródła danych	K1_CBE_U14

Treści programowe zapewniające uzyskanie efektów uczenia się

Poznanie metod AI i uczenia maszynowego w zadaniach związanych z modelowaniem i wykrywaniem zagrożeń w systemach komputerowych

Nakład pracy studenta

Rodzaje zajęć studenta	**Średnia liczba godzin przeznaczonych na zrealizowane aktywności**
Wykład	30
Laboratorium	30
Przygotowanie do zajęć	65
Całkowity nakład pracy studenta (CNPS)	**Liczba godzin** 125

Politechnika Wrocławska

Wykrywanie zagrożeń i reakcja na incydenty

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
2025/2026

Kod przedmiotu
W4NCBES.120PK.00088.25

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: 30 Laboratorium: 30	4.0

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Ma ogólną wiedzę na temat organizacji i usług bezpieczeństwa realizowanych w ramach Security Operation Center (SOC) oraz sposobów i metod monitorowania oraz detekcji zagrożeń w systemach informatycznych	K1_CBE_W22
PEU_W02	Ma ogólną wiedzę na temat struktury organizacji i architektury systemów wykrywania zagrożeń.	K1_CBE_W22
PEU_W03	Zna systemy wykrywające zagrożenia oraz systemy prewencyjne, rozumie analizę korelacji zdarzeń w systemach komputerowych, wie jak dobrać oraz skonfigurować narzędzia monitorujące zagrożenia.	K1_CBE_W22

Z zakresu umiejętności		
PEU_U01	Umie zaimplementować narzędzia monitorujące zdarzenia oraz bezpieczeństwo w systemie komputerowym.	K1_CBE_U22
PEU_U02	Potrafi przygotować system składający się z wielu komponentów do monitorowania zagrożeń.	K1_CBE_U22
PEU_U03	Umie korelować zdarzenia pochodzące z wielu źródeł danych i używać wskaźników jakościowych i ilościowych, np. ocenić skuteczność wdrożonego systemu monitorowania.	K1_CBE_U22
PEU_U04	Umie projektować rozwiązania mające na celu monitorowanie oraz wykrywanie zagrożeń w systemach informatycznych.	K1_CBE_U22

Treści programowe zapewniające uzyskanie efektów uczenia się

C1. Poznanie sposobów monitorowania oraz detekcji zagrożeń w systemach informatycznych.
C2. Poznanie systemów wykrywających zagrożenia oraz systemów prewencyjnych, zrozumienie korelacji zdarzeń w systemach komputerowych.
C3. Poznanie metodologii doboru oraz parametryzacji narzędzi monitorujących zagrożenia.

Nakład pracy studenta

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

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
2025/2026

Kod przedmiotu
W4NCBECSIS.140PS.00097.25

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	Ma wiedzę na temat stosowanych metod audytu formalnego oraz technicznego a w szczególności podstawowe założenia norm ISO rodziny 27000.	K1_CBE_W16
PEU_W02	Ma ogólną wiedzę na temat struktury organizacji i architektury systemów wykrywania zagrożeń	K1_CBE_W16
PEU_W03	Ma wiedzę na temat narzędzi i metod audytu technicznego oraz zna wybrane metody audytu technicznego oraz zastosowanie wybranych narzędzi do audytu technicznego i testów penetracyjnych.	K1_CBE_W16

PEU_W04	Ma wiedzę ogólną w zakresie metodyk zarządzania ryzykiem	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Potrafi używać narzędzi audytu technicznego do przetestowania bezpieczeństwo aplikacji sieciowej	K1_CBE_U24
PEU_U02	Potrafi zaplanować poszczególne etapy testu penetracyjnego i określić ich kryteria	K1_CBE_U24
PEU_U03	Potrafi wykonać poszczególne etapy testu penetracyjnego i przygotować raport	K1_CBE_U24
PEU_U04	Potrafi dokonać mapowania potrzeb (formalnych i związanych z cechami organizacji) oraz niezbędnego poziomu organizacji usług bezpieczeństwa	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci uzyskają wiedzę z zakresu audytu bezpieczeństwa sieci komputerowych, metodologii audytów i testów penetracyjnych oraz umiejetności umożliwiające organizacje i prowadzenie audytów i testów penetracyjnych.

Nakład pracy studenta

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

Politechnika Wrocławska

Rozproszone systemy automatyki

Karta przedmiotu

Informacje podstawowe

Kierunek studiów cyberbezpieczeństwo	**Cykl kształcenia** 2025/2026
Specjalność bezpieczeństwo infrastruktury krytycznej	**Kod przedmiotu** W4NCBECIKS.140PS.00108.25
Jednostka organizacyjna Wydział Informatyki i Telekomunikacji	**Grupa zajęć** Tak
Poziom kształcenia studia pierwszego stopnia (inżynier)	**Języki wykładowe** polski
Forma studiów studia stacjonarne	**Obligatoryjność** Obowiązkowy specjalnościowy
Profil studiów profil ogólnoakademicki	**Blok zajęciowy** Przedmioty specjalnościowe
	Przedmiot powiązany z badaniami naukowymi Tak

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

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Ma wiedzę w zakresie stosowania sterowników PLC oraz sieci komunikacyjnych w rozproszonych systemach automatyki	K1_CBE_W16
PEU_W02	Wie, jakie są charakterystyczne cechy rozproszonego systemu automatyki	K1_CBE_W16
Z zakresu umiejętności		
PEU_U01	Potrafi zastosować sterowniki PLC w rozproszonych systemach automatyki	K1_CBE_U24

PEU_U02	Potrafi sformułować algorytm sterowania w rozproszonym systemie automatyki oraz napisać program sterujący na wybrany sterownik	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Zapoznanie z podstawową wiedzą dotyczącą rozproszonych systemów automatyki
2. Zapoznanie z wybranymi rodzajami przemysłowych sieci komunikacyjnych wykorzystywanymi w rozproszonych systemach automatyki
3. Praktyczne zapoznanie z urządzeniami wykorzystywanymi w rozproszonych systemach automatyki

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	7
Przygotowanie do egzaminu/zaliczenia	5
Zaliczenie/Egzamin	1
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
2025/2026

Kod przedmiotu
W4NCBES.140HS.00089.25

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	Student posiada wiedzę na temat podstawowych metod monitorowania jakości produkcji	K1_CBE_W04
Z zakresu kompetencji społecznych		
PEU_K01	Student posiada wiedzę w zakresie kontroli jakości.	K1_CBE_K05

Treści programowe zapewniające uzyskanie efektów uczenia się

Nabycie wiedzy na temat podstawowych metod monitorowania jakości produkcji

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Wykład	30
Przygotowanie do zajęć	20
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
2025/2026

Kod przedmiotu
W4NCBES.140PK.00090.25

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	Zna ryzyka w systemach informatycznych.	K1_CBE_W08
PEU_W02	Zna zasady określania oraz definiowania obszarów ryzyka w systemach.	K1_CBE_W08
PEU_W03	Zna zasady tworzenia matryc ryzyka w oparciu o prawdopodobieństwo oraz wpływ.	K1_CBE_W08
PEU_W04	Rozumie i określa parametry ryzyka: istotność, wpływ, prawdopodobieństwo.	K1_CBE_W08
PEU_W05	Zna metodykę i zasady tworzenia i analiz polityk bezpieczeństwa.	K1_CBE_W08

Z zakresu umiejętności		
PEU_U01	Potrafi zdefiniować i wskazać ryzyka związane z procesami przetwarzania informacji.	K1_CBE_U19
PEU_U02	Potrafi utworzyć stosowne matryce ryzyka dla procesów przetwarzania danych.	K1_CBE_U19
PEU_U03	Potrafi rozróżnić różne typy ryzyk oraz odnieść je do warstwy technologicznej.	K1_CBE_U19
PEU_U04	Potrafi rozpoznać i określić ryzyka związane z użytkowaniem systemów informatycznych.	K1_CBE_U19
PEU_U05	Potrafi rozróżnić ryzyka procesowe oraz technologiczne.	K1_CBE_U19

Treści programowe zapewniające uzyskanie efektów uczenia się

1. Nabycie wiedzy z zakresu zarządzania ryzykiem w systemach informatycznych.
2. Nabycie wiedzy z zakresu analizy i wyceny ryzyk.
3. Nabycie wiedzy z zakresu określania i tworzenia 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	12
Zaliczenie/Egzamin	3
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
2025/2026

Kod przedmiotu
W4NCBES.140PD.00057.25

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: 150 godz., 12 ECTS, Zaliczenie na ocenę

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu umiejętności		
PEU_U01	Student wyszukuje informacje z różnych źródeł, dokonuje ich krytycznej analizy, syntezy oraz twórczej interpretacji.	K1_CBE_U24
PEU_U02	Student konstruuje i testuje hipotezy dotyczące prostych problemów badawczych.	K1_CBE_U24
PEU_U03	Student 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_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zapoznają się z wytycznymi formalnymi odnośnie przygotowania pracy pisemnej, opisu literatury i struktury pracy dyplomowej. Zdobędą również poszerzoną 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	150
Przygotowanie pracy dyplomowej	120
Przeprowadzenie badań literaturowych	30
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
2025/2026

Kod przedmiotu
W4NCBES.140PZ.00058.25

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	Ma umiejętność pracy indywidualnej i zespołowej.	K1_CBE_U23
PEU_U02	Ma umiejętność korzystania ze zdobytej wiedzy do twórczego analizowania i rozwiązywania różnych problemów inżynierskich.	K1_CBE_U23
PEU_U03	Ma świadomość odpowiedzialności za pracę własną, jest otwarty na wymianę myśli i nowe wyzwania.	K1_CBE_U23

Treści programowe zapewniające uzyskanie efektów uczenia się

Konfrontacja wiedzy, zdobytej podczas zajęć dydaktycznych objętych planem studiów, z rzeczywistymi wymaganiami stawianymi przez pracodawców.
Zdobycie doświadczenia praktycznego i zawodowego, poznanie podstawowego wyposażenia technicznego i technologicznego firmy, procesów i procedur, a także poznanie specyfiki pracy dozoru technicznego.
Zapoznanie się ze specyfiką środowiska zawodowego oraz kształtowanie konkretnych umiejętności zawodowych związanych

bezpośrednio z miejscem realizacji praktyki.
Doskonalenie umiejętności organizacji pracy własnej i zespołowej, efektywnego zarządzania czasem, sumienności, odpowiedzialności za powierzone zadania.
Profesjonalizacja zachowań zawodowych, przestrzegania zasad etyki zawodowej i poszanowania różnorodności technicznych (otwartości na nowe technologie i świadomości związanej z ochroną środowiska).

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
2025/2026

Kod przedmiotu
W4NCBES.140PS.00056.25

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	Student opracowuje prezentację zawierającą wyniki rozwiązań	K1_CBE_U24
PEU_U02	Student prowadzi rzeczową dyskusję uzasadniającą swoje oryginalne pomysły i rozwiązania	K1_CBE_U24
PEU_U03	Student krytycznie ocenia rozwiązania naukowo-techniczne innych osób	K1_CBE_U24

Treści programowe zapewniające uzyskanie efektów uczenia się

W ramach przedmiotu studenci zdobędą umiejętności poszukiwania selektywnej wiedzy niezbędnej do tworzenia własnych oryginalnych rozwiązań, przygotowania prezentacji pozwalającej w sposób komunikatywny przekazać słuchaczom swoje oryginalne pomysły, koncepcje i rozwiązania, kreatywnej dyskusji, w której w sposób rzeczowy i merytoryczny można uzasadnić i obronić swoje stanowisko a także pisania dzieła prezentującego własne osiągnięcia, w tym prezentacji własnych osiągnięć na tle rozwoju myśli światowej.

Nakład pracy studenta

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