Nazwa wydziału	Wydział Elektroniki i Technik Informacyjnych
Nazwa kierunku	Cyberbezpieczeństwo
Poziom studiów	drugiego stopnia
Profil studiów	Ogólnoakademicki
Forma studiów	stacjonarne
Język prowadzenia studiów	polski
Dyscypliny naukowe, do których przypisany jest kierunek (udział procentowy) (w przypadku przyporządkowania kierunku studiów do więcej niż 1 dyscypliny, wskazuje się dyscyplinę wiodącą, w ramach której będzie uzyskiwana ponad połowa efektów uczenia się)	Dziedzina nauk inżynieryjno-technicznych - dyscypliny: Informatyka techniczna i telekomunikacja - 100,00%
W przypadku zawodu, o którym mowa w art. 68 Ustawy, standardy kształcenia, na podstawie których będą prowadzone studia (opis standardów kształcenia (w przypadku zawodów uwzględniających standardy kształcenia, na podstawie których będą prowadzone studia ePW)	nie dotyczy
Liczba semestrów studiów	3
Tytuł zawodowy nadawany absolwentom	magister inżynier
Kierunkowe efekty uczenia się	**patrz tabela z efektami uczenia się**
Sposoby weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu kształcenia (należy uwzględnić również praktyki zawodowe, jeśli praktyka jest przewidziana	• egzamin pisemny • egzamin ustny • kolokwium pisemne • kolokwium ustne • test • sprawozdanie/raport pisemny • wykonanie i/lub obrona projektu • prezentacja • praca domowa • ocena aktywności w trakcie zajęć • konsultacje ..
Łączna liczba godzin zajęć	1170

Liczba punktów ECTS konieczna do ukończenia studiów (wraz z obowiązkowymi praktykami)	90
Liczba punktów ECTS, którą student musi uzyskać na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia	45
Liczba punktów ECTS jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych, w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż dziedziny nauk humanistycznych lub nauk społecznych	5
Liczba godzin zajęć z wychowania fizycznego na studiach prowadzonych w formie stacjonarnej	Nie dotyczy
Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć podlegających wyborowi przez studenta (w wymiarze nie mniejszym niż 30% liczby punktów ECTS koniecznych do ukończenia studiów na danym poziomie)	43 (48%)
Dla studiów o profilu praktycznym: Łączna liczba punktów ECTS, którą student musi uzyskać w ramach przedmiotów/zajęć kształtujących umiejętności praktyczne (w wymiarze większym niż 50% liczby punktów ECTS koniecznych do ukończenia studiów na danym poziomie)	Nie dotyczy
Dla studiów o profilu ogólnoakademickim: Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć związanych z prowadzoną w Uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów (w wymiarze większym niż 50% liczby punktów ECTS wymaganej do ukończenia studiów na danym poziomie), z uwzględnieniem udziału studentów w zajęciach przygotowujących do prowadzenia działalności naukowej lub udziału w tej działalności	83 (92%)

Liczba punktów ECTS, jaka może być uzyskana w ramach kształcenia z wykorzystaniem metod i technik kształcenia na odległość: (liczba punktów ECTS nie może być większa niż 50% liczby punktów ECTS koniecznej do ukończenia studiów - w przypadku studiów o profilu praktycznym albo 75% liczby punktów ECTS koniecznej do ukończenia studiów - w przypadku studiów o profilu ogólnoakademickim).	27 (30%)
Łączna liczba godzin z matematyki	Nie dotyczy
Łączna liczba punktów ECTS z matematyki	Nie dotyczy
Łączna liczba godzin z fizyki	Nie dotyczy
Łączna liczba punktów ECTS z fizyki	Nie dotyczy
Łączna liczba godzin z języków obcych	60
Łączna liczba punktów ECTS z języków obcych	4
Liczba punktów ECTS za pracę dyplomową	20
WYMIAR, ZASADY, FORMA PRAKTYK ZAWODOWYCH	Nie dotyczy
Opis przedmiotów obieralnych	• Przedmioty obieralne (cyberbezpieczeństwo | teleinformatyka), ECTS(4),SUMA GODZ(60) W trakcie studiów student musi uzyskać 8 ECTS z grupy przedmiotów obieralnych. 4 ECTS w sem. I, 4 ECTS w sem. II. W programie studiów zamieszczono przykładowe przedmioty obieralne, przedmiotem obieralnym może być przedmiot spoza przedstawionej listy. • Przedmioty zaawansowane o różnym charakterze, ECTS(4),SUMA GODZ(60) W trakcie studiów student musi uzyskać 4 ECTS z grupy przedmiotów obieralnych. 4 ECTS w sem. III. W programie studiów zamieszczono przykładowe przedmioty obieralne, przedmiotem obieralnym może być przedmiot spoza przedstawionej listy.

EFEKTY UCZENIA SIĘ

(opis zakładanych efektów uczenia się dla kierunków w odniesieniu do charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji)

Jednostka: Wydział Elektroniki i Technik Informacyjnych
Nazwa kierunku studiów: Cyberbezpieczeństwo
Poziom kształcenia: drugiego stopnia
Profil kształcenia: Ogólnoakademicki

Kod efektu	Opis efektu	Odniesienie do uniwersalnych charakterystyk PRK	Odniesienie do charakterystyk II stopnia PRK
Wiedza			
W01	zna i rozumie główne tendencje rozwojowe informatyki technicznej i telekomunikacji, także w szerszym, społecznym kontekście	P7U_W	I_P7S_WG_O
W02	zna i rozumie procesy zachodzące w systemach teleinformatycznych, istotne dla zapewnienia bezpiecznego funkcjonowania takich systemów	P7U_W	III_P7S_WG I_P7S_WG_O
W03	zna metodologiczne podstawy prowadzenia badań naukowych; ma wiedzę dotyczącą metodyki prowadzenia prac o charakterze badawczym w dziedzinie nauk inżynieryjno-technicznych, w szczególności związanych z badaniami z zakresu cyberbezpieczeństwa	P7U_W	I_P7S_WG_O
W04	zna zaawansowane narzędzia informatyczne niezbędne do analizy wyników badań	P7U_W	I_P7S_WG_O
W05	ma zaawansowaną wiedzę z zakresu matematyki, obejmującą m.in. - metody i algorytmy algebry liniowej, - podstawy logiki temporalnej, - algorytmy kodowania i dekodowania dla liniowych kodów korekcyjnych, - podstawy teorii krat, - podstawy teoretyczne rozpoznawania wzorców, tworzącą podstawy do identyfikowania problemów i formułowania specyfikacji złożonych i nietypowych zadań inżynierskich oraz problemów badawczych, związanych z zapewnieniem cyberbezpieczeństwa oraz ich innowacyjnego rozwiązywania, dotyczących w szczególności analizy danych, weryfikacji formalnej i kryptografii postkwantowej	P7U_W	I_P7S_WG_O
W06	w pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu analizy danych w kontekście jej zastosowań w rozwiązywaniu problemów dotyczących cyberbezpieczeństwa	P7U_W	I_P7S_WG_O
W07	w pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu zapewniania bezpieczeństwa systemów Internetu Rzeczy	P7U_W	I_P7S_WG_O
W08	w pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu wybranych aspektów cyberbezpieczeństwa, w tym - bezpieczeństwa rozwiązań sprzętowych, - bezpieczeństwa komunikacji opartej na najnowszych standardach sieci bezprzewodowych	P7U_W	I_P7S_WG_O
W09	zna i rozumie procesy zachodzące w cyklu życia systemów teleinformatycznych, zwłaszcza związane z zapewnieniem bezpieczeństwa tych systemów	P7U_W	I_P7S_WG_O

W10	rozumie fundamentalne dylematy współczesnej cywilizacji, związane z rozwojem nauk inżynieryjno-technicznych, a zwłaszcza informatyki technicznej i telekomunikacji, oraz wykorzystaniem najnowszych osiągnięć nauki i techniki i wynikającymi z tego zagrożeniami, w szczególności osobiste i społeczne dylematy będące następstwem działań zagrażających bezpieczeństwu systemów teleinformatycznych	P7U_W	I_P7S_WK
W11	rozumie pozatechniczne (prawne, ekonomiczne, etyczne i inne) uwarunkowania działalności zawodowej w zakresie bezpośrednio lub pośrednio związanym z cyberbezpieczeństwem	P7U_W	I_P7S_WK
W12	zna zasady ochrony własności intelektualnej, w tym ochrony własności przemysłowej i prawa autorskiego, zwłaszcza w zakresie bezpośrednio lub pośrednio związanym z cyberbezpieczeństwem	P7U_W	I_P7S_WK
W13	zna i rozumie zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości, w tym związane przedsiębiorczością startupową	P7U_W	III_P7S_WK I_P7S_WK
Umiejętności			
U01	potrafi pozyskiwać informacje z właściwie dobranych źródeł, dokonywać ich krytycznej oceny, analizy, syntezy i twórczej interpretacji, wyciągać wnioski i wyczerpująco je uzasadniać	P7U_U	I_P7S_UW_O
U02	potrafi przeprowadzić krytyczną analizę sposobu funkcjonowania istniejących rozwiązań technicznych z zakresu bezpieczeństwa systemów teleinformatycznych i oceniać te rozwiązania	P7U_U	III_P7S_UW_O I_P7S_UW_O
U03	potrafi planować i przeprowadzać eksperymenty/ badania, w tym symulacje komputerowe dotyczące bezpieczeństwa systemów teleinformatycznych, oraz interpretować uzyskane wyniki	P7U_U	III_P7S_UW_O I_P7S_UW_O
U04	potrafi wykorzystać zaawansowane narzędzia informatyczne niezbędne do przeprowadzenia eksperymentów/badań związanych z zagadnieniami cyberbezpieczeństwa i analizy ich wyników		I_P7S_UW_O
U05	potrafi formułować i testować hipotezy związane z prostymi problemami badawczymi dotyczącymi m.in. zapewnienia bezpieczeństwa systemów teleinformatycznych	P7U_U	I_P7S_UW_O
U06	potrafi dokonać identyfikacji i sformułować specyfikację złożonych zadań dotyczących cyberbezpieczeństwa, a w szczególności: - analizy danych w kontekście jej zastosowań w rozwiązywaniu problemów związanych z zapewnieniem bezpieczeństwa systemów teleinformatycznych, - zapewniania bezpieczeństwa sieci bezprzewodowych najnowszych generacji i systemów Internetu Rzeczy.	P7U_U	I_P7S_UW_O
U07	potrafi zaprojektować - zgodnie z zadaną specyfikacją, używając właściwie dobranych metod i narzędzi - rozwiązanie zawierające elementy innowacyjności, związane z zapewnieniem bezpieczeństwa systemów teleinformatycznych, a także zweryfikować jego poprawność	P7U_U	III_P7S_UW_O I_P7S_UW_O
U08	potrafi przy identyfikacji i formułowaniu specyfikacji złożonych zadań dotyczących bezpieczeństwa systemów teleinformatycznych oraz ich rozwiązywaniu: - dostrzegać ich aspekty systemowe i pozatechniczne, w tym aspekty etyczne - oceniać aspekty ekonomiczne proponowanych rozwiązań i podejmowanych działań; potrafi wnieść wkład w opracowanie strategii zarządzania bezpieczeństwem na poziomie instytucjonalnym	P7U_U	III_P7S_UW_O I_P7S_UW_O

U09	potrafi - w pracach badawczych oraz przy rozwiązywaniu zadań dotyczących zapewnienia bezpieczeństwa systemów teleinformatycznych - wykorzystywać metody analityczne, symulacyjne i eksperymentalne - dokonać wyboru oraz zastosować właściwe metody, techniki i narzędzia, w tym zaawansowane techniki informacyjnokomunikacyjne - przystosować istniejące lub opracować nowe metody i narzędzia	P7U_U	III_P7S_UW_O I_P7S_UW_O
U10	potrafi przygotować opracowanie i przedstawić prezentację ustną, dotyczącą w szczególności zagadnień z zakresu cyberbezpieczeństwa, potrafi przygotować krótkie doniesienie naukowe	P7U_U	I_P7S_UK
U11	potrafi komunikować się przy użyciu różnych technik w środowisku zawodowym oraz w innych środowiskach; potrafi prowadzić debatę	P7U_U	I_P7S_UK
U12	potrafi posługiwać się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego	P7U_U	I_P7S_UK
U13	potrafi pracować indywidualnie oraz współdziałać z innymi osobami w ramach prac zespołowych; potrafi kierować pracą zespołu	P7U_U	I_P7S_UO
U14	potrafi określić kierunki dalszego uczenia się, zaplanować i zrealizować proces samokształcenia, a także ukierunkowywać innych w tym zakresie	P7U_U	I_P7S_UU
Kompetencje społeczne			
K01	jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści oraz do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu; jest gotów do stałego aktualizowania i wzbogacania posiadanej wiedzy	P7U_K	I_P7S_KK
K02	jest gotów do wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego oraz interesu publicznego, a zwłaszcza formułowania i przekazywania społeczeństwu – m.in. poprzez środki masowego przekazu – informacji i opinii dotyczących zagrożeń związanych z cyberbezpieczeństwem i sposobów przeciwdziałania tym zagrożeniom; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały	P7U_K	I_P7S_KO
K03	jest gotów do myślenia i działania w sposób przedsiębiorczy, przewodzenia grupie i ponoszenia odpowiedzialności za nią	P7U_K	I_P7S_KO
K04	jest gotów do odpowiedzialnego pełnienia ról zawodowych, z uwzględnieniem zmieniających się potrzeb społecznych, w tym: - rozwijania dorobku zawodu, - podtrzymywanie etosu zawodu, - przestrzegania etyki zawodowej oraz działania na rzecz przestrzegania tych zasad	P7U_K	I_P7S_KR

SYLABUS PRZEDMIOTU

Kod przedmiotu	103B-xxxxx-MSP-STUPA
Nazwa przedmiotu	Przedsiębiorczość startupowa
Wersja przedmiotu	2023L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty ekonomiczno-społeczne)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	3

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	20.00 h
Wykład	10.00 h

02. Bilans ECTS

Liczba punktów ECTS	3	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	44	1.76
Godziny i ECTS związane z pracą własną studenta	42	1.68
Razem	86	3.44 (3.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	30
Inne godziny kontaktowe	14
Razem	44

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	42

03. Treści kształcenia

Część I

Wykład	Zdobycie wiedzy na temat specyfiki przedsiębiorczości startupowej oraz w zakresie metodyki zarządzania startupem: Lean Startup. W ramach wykładu studenci zaliczają certyfikowany kurs online „Lean Canvas – stwórz swój pierwszy model biznesowy”, certyfikowany przez Polski Fundusz Rozwoju (PFR).Przygotowanie do każdego wykładu polega na zapoznaniu z wybranymi przez prowadzącego lekturami, które przygotują do i uzupełnią treści wykładowe, np. wybrane pozycje z bazy wiedzy PFR oraz raporty Fundacji Startup Poland i inne lektury wskazane i udostępnione przez prowadzącego. W1: Innowacje. Przedsiębiorczość innowacyjna a inne formy przedsiębiorczości. Startupy jako szczególne formy organizacji aktywności przedsiębiorczej; W2: Lean Startup jako metodyka zarządzania startupem i jej składowe: zwinny rozwój produktu (agile development), odkrywanie klienta (customer development) i modelowanie biznesowe; triada: klient-problem-rozwiązanie (CPS); W3: Modelowanie biznesowe na bazie kanwy modelu biznesowego oraz kanwy propozycji wartości wg Osterwaldera; struktura modelu i formułowanie hipotez biznesowych; W4: Weryfikowanie hipotez biznesowych w procesie modelowania biznesowego; odkrywanie klienta – zasady projektowania i przeprowadzania wywiadów z interesariuszami projektu; prototypowanie, koncepcja MVP; W5: Model biznesowy jako narzędzie wdrażania zmian i innowacji w przedsiębiorstwie.
Projekt	Praca nad projektem startupu – co najmniej zakończenie etapu Customer Discovery – na projekcie własnym (w grupach). W ramach zajęć projektowych studenci doświadczą mentoringu, który jest fundamentalnym źródłem wiedzy dla startupów oraz przejdą szkolenie z mentoringu, przewiduje się także wizytę studentów w Inkubatorze Innowacyjności PW i/lub spotkanie z przedsiębiorcą rezydującym w Inkubatorze. Przewiduje się, że do każdych zajęć projektowych student przygotowuje się przez co najmniej godzinę pracy samodzielnej lub zespołowej. Przygotowanie do próby generalnej i prezentacji końcowej w obecności gości z zewnątrz uczelni zajmuje w sumie 10h pracy samodzielnej lub zespołowej. P0: Selekcja pomysłów na projekty, elementy debaty; P1: Sformułowanie hipotez biznesowych: CPS i archetypu klienta (tworzenie persony), P2-P3: Kanwa propozycji wartości i kanwa modelu biznesowego – warsztaty projektowe w grupach, P4: Zaprojektowanie wywiadów i przeprowadzenie ich, P5: Weryfikacja hipotez biznesowych, analiza konkurencji, P6: Zajęcia mentoringowe, zajęcia z gościem i/lub w inkubatorze i akceleratorze innowacji PW, P7: Zasady prawidłowego „pitcha” projektu, prezentacji pomysłu i pracy nad jego weryfikacją i rozwojem, P8-P9: Prezentacja końcowa projektu (w obecności gości spoza uczelni – inwestorzy, przedsiębiorcy, eksperci).

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Student zna i rozumie zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości, a zwłaszcza innowacyjnych, ambitnych i dynamicznych form organizacji typu startup
Powiązane kierunkowe efekty uczenia się	W13
Kod efektu	W02

Część I

Opis	Student zna zasady ochrony własności intelektualnej w kontekście tworzenia i rozwijania startupów – innowacyjnych form przedsiębiorczości
Powiązane kierunkowe efekty uczenia się	W12

Umiejętności

Kod efektu	U01
Opis	Student potrafi przygotować opracowanie i przedstawić prezentację ustną (w języku polskim lub w języku angielskim), tzw. prezentację inwestorską: „pitch” na temat tworzonego startupu i jego modelu biznesowego.
Powiązane kierunkowe efekty uczenia się	U10
Kod efektu	U02
Opis	Student potrafi komunikować się przy użyciu różnych technik multimedialnych w środowisku zawodowym oraz w innych środowiskach (w języku polskim lub w języku angielskim) w zakresie tworzenia i walidacji startupu i modelu biznesowego.
Powiązane kierunkowe efekty uczenia się	U11
Kod efektu	U03
Opis	Student potrafi pracować indywidualnie oraz współdziałać z innymi osobami w ramach prac zespołowych nad tworzeniem i walidacją koncepcji startupu.
Powiązane kierunkowe efekty uczenia się	U13
Kod efektu	U04
Opis	Student potrafi określić kierunki dalszego uczenia się, zaplanować i zrealizować proces samokształcenia, a także ukierunkowywać innych w tym zakresie – w ramach prac nad tworzeniem startupu.
Powiązane kierunkowe efekty uczenia się	U14

Kompetencje społeczne

Kod efektu	K01
Opis	Student jest gotów do myślenia i działania w sposób innowacyjny i przedsiębiorczy, przewodzenia grupie i ponoszenia odpowiedzialności za nią.
Powiązane kierunkowe efekty uczenia się	K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-CBxxx-MSP-MACY
Nazwa przedmiotu	Metody matematyczne w cyberbezpieczeństwie
Wersja przedmiotu	2024L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Matematyki i Nauk Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Podstawy teoretyczne)-Cyberbezpieczeństwo-mgr.-EITI, (Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 1 modelowy)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	4

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	30.00 h
Wykład	15.00 h
Ćwiczenia	15.00 h

02. Bilans ECTS

Liczba punktów ECTS	4	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	65	2.60
Godziny i ECTS związane z pracą własną studenta	55	2.20
Razem	120	4.80 (4.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	60
Inne godziny kontaktowe	5
Razem	65

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	55

03. Treści kształcenia

Część I

Wykład	1. **Faktoryzacja macierzy (4 godz.)** Nieujemna i dodatnia określoność macierzy kwadratowej, związek z wartościami własnymi. Rozkłady macierzy: QR, LU, SVD (wg wartości osobliwych), rozkład spektralny macierzy. Normy macierzowe. 1. **Wprowadzenie do logik temporalnych (4 godz.)** Elementy logiki modalnej. Podstawy logiki temporalnej: aspekty syntaktyki oraz semantyka (np. modele Kripkego). Postać normalna formuł. Reguły wnioskowania i równoważność formuł. Automaty Büchi a logika temporalna. Logiki temporalne z liniową strukturą czasu (LTL) oraz z rozgałęzioną strukturą czasu (CTL). Przykładowe modele. 1. **Kody korekcyjne (4 godz.)** Kody liniowe nad dowolnymi ciałami skończonymi. Kody BCH jako kody poprawiające błędy wielokrotne. Niebinarne kody Reeda-Solomona. Uogólnione kody RS. Kody alternujące. 1. **Kraty stosowane w kryptografii (3 godz.)** Wprowadzenie pojęć dotyczących krat, kraty q-arne, wyznacznik kraty. Istnienie niezerowych wektorów o minimalnej długości. Twierdzenie Blichfeldta, twierdzenia Minkowskiego.
Ćwiczenia	Ćwiczenia audytoryjne będą ilustracją problemów poruszanych na wykładach. Ponadto będą stanowiły uzupełnienie wykładów o następujące zagadnienia: 1. Funkcje macierzy. Eksponenta macierzy. 2. Operatory sprzężone i unitarne. Macierze Householdera. 3. Własności ciał skończonych. Wielomiany nad ciałami skończonymi. 4. Kody Goppa w kryptografii. System McEliece z kluczem publicznym. 5. Zredukowana baza w 2-wymiarowej kracie. Uogólniony algorytm Gaussa.

Część I

Projekt	W ramach projektu kilkuosobowe zespoły będą opracowywać prezentacje zastosowań praktycznych zagadnień omawianych na wykładach lub na ćwiczeniach. W zakres tematyki projektów będą wchodziły między innymi: 1. Metody numeryczne znajdywania wartości własnych. 2. Wybrane implementacje i zastosowania algorytmów rozkładu macierzy do zagadnień związanych z cyberbezpieczeństwem. 3. Rozwiązywanie układów równań z wykorzystaniem faktoryzacji macierzy. 4. Metody formalne analizy bezpieczeństwa protokołów z wykorzystaniem logiki temporalnej. 5. Zastosowanie wybranych metod kodowania korekcyjnego w praktyce. 6. Przykładowe techniki kryptoanalizy dla systemów kryptograficznych opartych na kodach liniowych (np. atak Sidelnikov-Shestakov). 7. Wybrane algorytmy aproksymacyjne problemów kratowych: problem najkrótszego wektora w kracie (SVP), problem najbliższego wektora w kracie (CVP), problem najkrótszych wektorów liniowo niezależnych (SIVP). 8. Zastosowanie metody Coppersmitha znajdowania rozwiązań równań wielomianowych do ataków na system RSA. Ponadto elementem projektu będzie przygotowanie materiałów z danego zakresu dla studentów z pozostałych grup projektowych. czy w ramach zajęć praktycznych przewidziane jest prezentowanie ich stosowania w ramach problemów cyberbezpieczeństwa? Np. dobrym uzupełnieniem byłoby zwrócenie na to uwagi w ramach projektu, gdy wykład + ćwiczenia potratkować jako wprowadzenie i ugruntowanie aparatu matematycznego jeżeli odpowiedź na powyższe byłaby twierdząca, to zalecane byłoby umieszczenie przy projekcie wzmianek odnoszących się do zastosowań w cyberbezpieczeństwe danego tematu (tak jak przy drugim zagadnieniu wykładowym). przykład: https://www.microsoft.com/en-us/research/video/the-mathematics-of-side-channel-attacks/

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Ma wiedzę ogólną w zakresie metod i algorytmów stosowanych w algebrze liniowej.
Powiązane kierunkowe efekty uczenia się	W05
Kod efektu	W02
Opis	Zna podstawy logiki temporalnej.
Powiązane kierunkowe efekty uczenia się	W05
Kod efektu	W03
Opis	Zna algorytmy kodowania i dekodowania dla wybranych liniowych kodów korekcyjnych.
Powiązane kierunkowe efekty uczenia się	W05
Kod efektu	W04
Opis	Zna zagadnienia dotyczące krat.
Powiązane kierunkowe efekty uczenia się	W05

Umiejętności

Kod efektu	U01

Część I

Opis	Potrafi wykorzystać nabytą wiedzę z algebry liniowej do zagadnień z zakresu analizy danych.
Powiązane kierunkowe efekty uczenia się	U01, U11, U13
Kod efektu	U02
Opis	Potrafi wykorzystać metody logiki temporalnej do weryfikacji własności prostych systemów zmiennych w czasie.
Powiązane kierunkowe efekty uczenia się	U01, U10
Kod efektu	U03
Opis	Posiada umiejętność zastosowania krat oraz kodów korekcyjnych w kryptografii postkwantowej.
Powiązane kierunkowe efekty uczenia się	U01, U10, U13

Kompetencje społeczne

Kod efektu	K01
Opis	Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz ich weryfikacji w możliwych zastosowaniach.
Powiązane kierunkowe efekty uczenia się	K01
Kod efektu	K02
Opis	Umie współpracować w grupie.
Powiązane kierunkowe efekty uczenia się	K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103D-CBxxx-MSP-EPART
Nazwa przedmiotu	Pattern Recognition
Wersja przedmiotu	2024L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Podstawy teoretyczne)-Cyberbezpieczeństwo-mgr.-EITI, (Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 1 modelowy)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	angielski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	2

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Wykład	30.00 h

02. Bilans ECTS

Liczba punktów ECTS	2

Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**
Liczba godzin i ECTS pracy studenta:		
Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	40	1.60
Godziny i ECTS związane z pracą własną studenta	20	0.80
Razem	60	2.40 (2.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	30
Inne godziny kontaktowe	10
Razem	40

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	20

03. Treści kształcenia

Wykład	.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	knows basic pattern classification methods
Powiązane kierunkowe efekty uczenia się	W05, W06
Kod efektu	W02

Część I

Opis	knows preliminary data analysis and clustering methods
Powiązane kierunkowe efekty uczenia się	W05, W06
Kod efektu	W03
Opis	knows basic classifiers ensemble construction methods
Powiązane kierunkowe efekty uczenia się	W05, W06

Umiejętności

Kod efektu	U01
Opis	is able to critically evaluate the solution of the classification problem and propose its improvement
Powiązane kierunkowe efekty uczenia się	U01, U06, U09, U12

SYLABUS PRZEDMIOTU

Kod przedmiotu	103B-CBxxx-MSP-TBD
Nazwa przedmiotu	Techniki i technologie Big Data
Wersja przedmiotu	2024L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Podstawy teoretyczne)-Cyberbezpieczeństwo-mgr.-EITI, (Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 1 modelowy)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	2

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Wykład	30.00 h

02. Bilans ECTS

Liczba punktów ECTS	2	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	36	1.44
Godziny i ECTS związane z pracą własną studenta	20	0.80
Razem	56	2.24 (2.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	30
Inne godziny kontaktowe	6
Razem	36

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	20

03. Treści kształcenia

Część I

Wykład	1. Wprowadzenie do zagadnień przetwarzania Big Data. (2 godz). Wprowadzenie do przedmiotu, omówienie spraw organizacyjnych, cele zajęć oraz ich program. Omówienie przyczyn zmian w podejściu do retencji danych. Przedstawienie rysu historycznego metod składowania oraz analizy dużych zbiorów danych. Omówienie najważniejszych zagadnień związanych z Big Data: architektura lambda, przetwarzanie strumieniowe vs przetwarzanie batchowe, orkiestracja, serializacja i deserializacja danych, bazy NoSQL. Przedstawienie czołowych projektów z obszaru Big Data: Hadoop, Spark, Cassandra. 2. Podstawowe komponenty ekosystemu Hadoop: wprowadzenie do YARN i HDFS. (2 godziny) 3. Sposób organizacji danych: pojęcie jeziora danych (data lake), analityka oraz bazy klucz-wartość, serializacja i deserializacja danych, formaty (ORC, Parquet), Cassandra, HBase, pojęcie schematu danych i ewolucji na przykładzie Avro, wsparcie dla ACID na przykładzie DeltaLake czy Iceberg. Porównanie wydajności różnych konfiguracji dla rzeczywistych przypadków użycia, pochodzących z projektów badawczych. (4 godziny) 4. Apache Spark. Omówienie koncepcji i zastosowań RDD (historycznie) i DataFrame. Architektura Spark (cluster manager, executor'y). Porównanie przetwarzania z Hadoop MapReduce oraz dyskusja dotycząca optymalizacji. Powiązanie z platformą Hadoop poprzez Resource Manger'a oraz wersja standalone (local). Omówienie API na podstawie przykładowego job'a. (4 godziny) 5. Analityka Big Data - SQL w środowisku Big Data (na przykładzie SparkSQL, Hive). Analiza danych z Hadoop za pomocą R i innych środowisk analitycznych (pyspark + jupyter). (4 godziny) 6. Wizualizacja danych - środowisko R/Python + narzędzia D3, Leaflet, Vega, deck.gl. Omówienie podstawowych pojęć i strategii wizualizacji danych z uwzględnieniem przede wszystkim danych ilościowych i danych geograficznych. (2 godziny) 7. Przetwarzanie strumieniowe. Wprowadzenie do narzędzi służących przetwarzaniu strumieni danych: Kafka, Spark Streaming, Apache Flink, Apache Beam. Przykład algorytmu strumieniowego z wykorzystaniem struktur danych takich jak: count min sketch, bloom filter. (4 godziny) 8. Big Data w chmurze. Przedstawienie architektur chmurowych, wirtualizacji i kontenerów, systemów zarządzania chmurą (OpenShift, K8S), Przykładowe osadzenie projektu big data w chmurze. Przedstawienie heterogenicznych środowisk obliczeniowych i zarządzania zasobami oraz ich izolacji za pomocą konteneryzacji. (2 godziny) 9. Zapewnienie bezpieczeństwa w środowisku rozproszonym – [KK2](Kerberos) oraz scentralizowana autoryzacja dostępu do zasobów (Apache Ranger. Integracja z istniejącymi systemami bezpieczeństa, wykorzystanie impersonacji uzytkowników, bezpieczeństwo w środowisku kontenerowym. (2 godziny)

Część I

	10. Uczenie maszynowe w środowiskach rozproszonych z wykorzystaniem bilbiotek TensorFlow. Wprowadzenie do uczenia maszynowego na przykładzie sieci neuronowych oraz głębokich sieci neuronowych. Wprowadzenie do TensorFlow oraz przykłady implementacji rozproszonej m.in. w oparciu o rozwiązania chmurowe. (4 godziny)

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	zna mechanizmy zapewnienia bezpieczeństwa w systemach rozproszonych
Powiązane kierunkowe efekty uczenia się	W02
Kod efektu	W02
Opis	zna metody stosowane w implementacji rozproszonych narzędzi wykorzystujących metody uczenia maszynowego
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W03
Opis	zna sposoby organizacji danych w systemach Big Data, w tym formaty i silniki zapytań stosowane w rozproszonych bazach danych
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W04
Opis	zna metody stosowane w analityce Big Data, w tym metody integracji potoków przetwarzania danych
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W05
Opis	zna typowe architektury stosowane w systemach chmur obliczeniowych, sposoby konteneryzacji oraz systemy zarządzania chmurą
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W06
Opis	zna istotne komponenty ekosystemu Hadoop
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W07
Opis	zna koncepcję przetwarzania w Apache Spark, w tym stosowane struktury danych RDD, dataframe
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W08
Opis	zna metody stosowane do wizualizacji danych Big Data
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W09
Opis	zna koncepcje i metody stosowane do przetwarzania strumieniowego w systemach Big Data
Powiązane kierunkowe efekty uczenia się	W06

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-CBxxx-MSP-ADAC
Nazwa przedmiotu	Analiza danych w cyberbezpieczeństwie
Wersja przedmiotu	2024L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Kształcenie oparte o projekty)-Cyberbezpieczeństwo-mgr.-EITI,(Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 1 modelowy)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	8

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Zajęcia zintegrowane	90.00 h
Projekt	30.00 h

02. Bilans ECTS

Liczba punktów ECTS	8	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	150	6.00
Godziny i ECTS związane z pracą własną studenta	85	3.40
Razem	235	9.40 (8.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	120
Inne godziny kontaktowe	30
Razem	150

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	85

03. Treści kształcenia

Część I

Projekt	Projekt będzie wykonywany w zespołach 3-5 osobowych. Zakłada się sześć etapów projektu, każdy z etapów będzie dotyczył kolejnego etapu procesu analizy danych w zastosowaniach w różnych obszarach cyberbezpieczeństwa. Wykonanie każdego etapu będzie potwierdzone napisaniem krótkiego raportu cząstkowego, zaś raporty cząstkowe będą stanowiły kolejne rozdziały raportu finalnego. Raport finalny będzie prezentował wyniki całego projektu w ramach przedmiotu. Zakłada się następujące etapy projektu: 1. Analiza literatury dotyczącej: wybranego problemu/ zagadnienia, sposobów analizy danych, narzędzi do analizy danych i ich zastosowania w różnych obszarach cyberbezpieczeństwa; 2. Stawianie hipotez dotyczących problemu np. możliwość lokalizacji/momentu nieuprawnionego dostępu do zasobów; 3. Badanie zależności między podzbiorami danych a hipotezami; 4. Budowa modeli informacyjnych dotyczących testowania i weryfikacji hipotez; 5. Testowanie i weryfikacja poprawności hipotez; ocena stosowalności opracowanych rozwiązań w praktyce cyberbezpieczeństwa; 6. Synteza wyników. Ze względu na charakter badawczy projektu, studenci będą stawiali kolejne hipotezy („prototypy”), testowali je, a następnie ulepszali je bądź ponownie formułowali. Powyższe etapy nie będą realizowane liniowo i możliwe będą nawroty. Wymagane będzie przeprowadzenie co najmniej jednego nawrotu. Zakłada się, że na każdy etap będzie przeznaczone około 2-3 tygodni. Każdy ze studentów będzie oceniany indywidualnie (za wykonaną pracę indywidualną) oraz za wyniki pracy całego zespołu projektowego. Wyraźny podział zadań między członków zespołu będzie jednym z zadań projektowych. Część zespołowa będzie oceniać: wykonaną pracę, wyniki, współpracę nad poszczególnymi elementami raportu i jego spójność. Synteza wyników projektu zostanie opublikowana w wybranej sieci społecznościowej i będzie stanowiła integralną część raportu.

Część I

Zajęcia zintegrowane	Zajęcia zintegrowane uzupełniają tworzenie projektu przez studentów. Zajęcia te będą odbywały się co tydzień. Ich celem jest przedyskutowanie bieżącej pracy studentów, dostarczenie im wiedzy i wskazówek dotyczącej prowadzonego projektu. Na wybranych zajęciach zintegrowanych studenci otrzymają pracę domową, którą będą musieli zrealizować na kolejne zajęcia. Zgodnie z zasadami PBL na pierwszych zajęciach studenci otrzymają informacje na temat dostępnych zbiorów danych odnoszących się do różnych obszarów cyberbezpieczeństwa i zestaw niedookreślonych zagadnień/problemów, potencjalnie możliwych do rozwiązania przy pomocy tych zbiorów. Propozycja harmonogramu zajęć zintegrowanych: 1. Zajęcia wstępne, podział studentów na zespoły, . 1. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): źródła, struktury danych, metody pozyskania i agregacja danych, przegląd algorytmów w kontekście postawionego problemu badawczego. 2. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): preprocessing, techniki manipulacji na dużych zbiorach danych i modelowanie zbiorów danych na potrzeby np. uczenia maszynowego, 3. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): budowa, specyfikacja i implementacja modeli w odniesieniu do wypracowanej hipotezy. 4. Zajęcia w formule otwartych prezentacji, na których studenci przedstawiają: charakterystykę analizowanych danych, problem do rozwiązania, sformułowane hipotezy i sformułowanie dalszych kroków. 5. Zajęcia w formule otwartych prezentacji: wstępny rekonensans opracowanych rozwiązań, weryfikacja założeń względem osiągniętych wyników. 6. Remodelowanie rozwiązań, rozszerzenie badań literaturowych. 7. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): trening, parametryzacja modeli. 8. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): modelowanie testowania oraz technik weryfikacyjnych. 9. Zajęcia otwarte w formie prezentacji: prezentacja wyników uzyskanych do tego etapu projektu, omówienie problemów, kwestii technicznych, metodycznych itd.

Część I

	10. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): poprawa modeli, omówienie toku realizacji projektu tj. retrospecja działań, możliwe kroki, które usprawniłyby pracę itd. 11. Zajęcia w formie demonstracyjno-dyskusyjnej: synteza wyników, tworzenie dokumentacji. 12. Zajęcia otwarte w formie prezentacji, podczas których studenci przedstawiają wyniki swojej pracy, wyniki swoich eksperymentów i wnioski.

Część I

Zajęcia zintegrowane	Zajęcia zintegrowane uzupełniają tworzenie projektu przez studentów. Zajęcia te będą odbywały się co tydzień. Ich celem jest przedyskutowanie bieżącej pracy studentów, dostarczenie im wiedzy i wskazówek dotyczącej prowadzonego projektu. Na wybranych zajęciach zintegrowanych studenci otrzymają pracę domową, którą będą musieli zrealizować na kolejne zajęcia. Zgodnie z zasadami PBL na pierwszych zajęciach studenci otrzymają informacje na temat dostępnych zbiorów danych odnoszących się do różnych obszarów cyberbezpieczeństwa i zestaw niedookreślonych zagadnień/problemów, potencjalnie możliwych do rozwiązania przy pomocy tych zbiorów. Propozycja harmonogramu zajęć zintegrowanych: 1. Zajęcia wstępne, podział studentów na zespoły, . 1. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): źródła, struktury danych, metody pozyskania i agregacja danych, przegląd algorytmów w kontekście postawionego problemu badawczego. 2. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): preprocessing, techniki manipulacji na dużych zbiorach danych i modelowanie zbiorów danych na potrzeby np. uczenia maszynowego, 3. Zajęcia w formie demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): budowa, specyfikacja i implementacja modeli w odniesieniu do wypracowanej hipotezy. 4. Zajęcia w formule otwartych prezentacji, na których studenci przedstawiają: charakterystykę analizowanych danych, problem do rozwiązania, sformułowane hipotezy i sformułowanie dalszych kroków. 5. Zajęcia w formule otwartych prezentacji: wstępny rekonensans opracowanych rozwiązań, weryfikacja założeń względem osiągniętych wyników. 6. Remodelowanie rozwiązań, rozszerzenie badań literaturowych. 7. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): trening, parametryzacja modeli. 8. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): modelowanie testowania oraz technik weryfikacyjnych. 9. Zajęcia otwarte w formie prezentacji: prezentacja wyników uzyskanych do tego etapu projektu, omówienie problemów, kwestii technicznych, metodycznych itd.

Część I

	10. Zajęcia w formule demonstracyjno-dyskusyjnej z naciskiem na zaangażowanie studentów (mikro prezentacje problemów cząstkowych, przygotowywanie schematów, (info)grafik, map myśli wraz z omówieniem): poprawa modeli, omówienie toku realizacji projektu tj. retrospecja działań, możliwe kroki, które usprawniłyby pracę itd. 11. Zajęcia w formie demonstracyjno-dyskusyjnej: synteza wyników, tworzenie dokumentacji. 12. Zajęcia otwarte w formie prezentacji, podczas których studenci przedstawiają wyniki swojej pracy, wyniki swoich eksperymentów i wnioski.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Zna i potrafi poprawnie zidentyfikować i zastosować metody analizy danych
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W02
Opis	Zna i rozumie główne tendencje rozwojowe cyberbezpieczeństwa, w szczególności dotyczące analizy danych
Powiązane kierunkowe efekty uczenia się	W01, W06
Kod efektu	W03
Opis	Zna i rozumie różne modele informatyczne służące do analizy danych w szczególności dotyczące cyberbezpieczeństwa
Powiązane kierunkowe efekty uczenia się	W03, W04, W06
Kod efektu	W04
Opis	Zna i rozumie metody i narzędzia informatyczne służące do weryfikacji hipotez dotyczących analizy danych
Powiązane kierunkowe efekty uczenia się	W03, W04, W06

Umiejętności

Kod efektu	U01
Opis	Potrafi, na podstawie analizy istniejących uwarunkowań, formułować i testować hipotezy dotyczące analizowanych danych, przy wykorzystaniu właściwych narzędzi informatycznych
Powiązane kierunkowe efekty uczenia się	U02, U04, U05, U06
Kod efektu	U02
Opis	Potrafi używać, formułować i parametryzować modele informatyczne służące do analizy danych
Powiązane kierunkowe efekty uczenia się	U04, U06
Kod efektu	U03
Opis	Potrafi dobrać i skutecznie wykorzystać metody i narzędzia służące do weryfikacji postawionych hipotez
Powiązane kierunkowe efekty uczenia się	U04, U05, U06
Kod efektu	U04
Opis	Potrafi planować i przeprowadzać eksperymenty i badania, w tym symulacje komputerowe, w celu weryfikacji postawionych hipotez
Powiązane kierunkowe efekty uczenia się	U03, U06, U09

Część I

Kod efektu	U05
Opis	Potrafi poprawnie identyfikować, selekcjonować i wybierać dane z różnych źródeł, także dane w języku angielskim
Powiązane kierunkowe efekty uczenia się	U01, U12
Kod efektu	U06
Opis	Potrafi realizować zadanie projektowe w zespole, podejmować różne role w zespole
Powiązane kierunkowe efekty uczenia się	U13

Kompetencje społeczne

Kod efektu	K01
Opis	Jest gotów do zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemów związanych z projektem
Powiązane kierunkowe efekty uczenia się	K01
Kod efektu	K02
Opis	Jest gotów do formułowania i przekazywania społeczeństwu, poprzez wybrane sieci społecznościowe – informacji i opinii dotyczących zagrożeń związanych z cyberbezpieczeństwa i opracowanych sposobów ich im przeciwdziałania
Powiązane kierunkowe efekty uczenia się	K02
Kod efektu	K03
Opis	Jest gotów do ponoszenia odpowiedzialności za pracę całej grupy
Powiązane kierunkowe efekty uczenia się	K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-CBxxx-MSP-BSC
Nazwa przedmiotu	Bezpieczne systemy cyfrowe
Wersja przedmiotu	2024L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty kierunkowe)-Cyberbezpieczeństwo-mgr.-EITI, (Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 1 modelowy)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	5

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Laboratorium	30.00 h
Wykład	30.00 h
Projekt	15.00 h

02. Bilans ECTS

Liczba punktów ECTS	5	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	87	3.48
Godziny i ECTS związane z pracą własną studenta	60	2.40
Razem	147	5.88 (5.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	75
Inne godziny kontaktowe	12
Razem	87

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	60

03. Treści kształcenia

Część I

Wykład	**Mikroelektroniczne systemy cyfrowe – przegląd.** System zintegrowany (System-on-Chip): przykłady architektur, w tym układy wielordzeniowe i wieloprocesorowe. Układy rekonfigurowalne. Bloki IP. Komunikacja: magistrale, sieć zintegrowana (Network-on-Chip). Układy wejścia/wyjścia. **Modelowanie i synteza bloków IP.** Języki opisu sprzętu (Verilog, VHDL) i synteza logiczna. Języki opisu systemu (SystemC, SystemVerilog) i synteza behawioralna: harmonogramowanie i wybór mikroarchitektury systemu. Modelowanie systemów na poziomie transakcji (TLM). Ograniczenia i możliwości syntezy behawioralnej, logicznej i syntezy topografii. **Problemy projektowania dużych systemów jednoukładowych SoC.** Dystrybucja sygnałów zegarowych. Szacowanie poboru mocy dynamicznej i zarządzanie poborem mocy (bramkowanie zegara i adaptacyjne sterowanie częstotliwością taktowania itp.). Techniki minimalizacji poboru mocy statycznej, adaptacyjne sterowanie napięciem zasilania i polaryzacją podłoża itp. **Weryfikacja i testowanie.** Metody weryfikacji formalnej i funkcjonalnej na różnych poziomach abstrakcji, weryfikacja wykorzystująca systemy asercji (PSL, SystemVerilog), metodyka UVM. Jakość weryfikacji a bezpieczeństwo systemu. Zarys problemów testowania i projektowania systemów łatwo testowalnych. **Bezpieczeństwo systemów VLSI.** Układy funkcji fizycznie nieklonowalnych PUF i generatorów liczb prawdziwie losowych TRNG. Zabezpieczanie bloków IP. Projektowanie i weryfikacja systemów wykorzystujących zabezpieczone bloki IP. Kompromisy projektowe wynikające z konfliktów pomiędzy wymaganiami dotyczącymi funkcjonalności, bezpieczeństwa, weryfikowalności i testowalności. Zabezpieczenia układów scalonych przed atakami typu hardware trojan, side-channel, via JTAG, microprobing itp. Integralność procesu projektowania układu scalonego.
Projekt	W ramach zajęć projektowych wykonywane są zadania wyrabiające umiejętności implementacji systemów, na podstawie wiedzy uzyskanej na wykładach. W ramach pracy zespołowej studenci wykonują projekt prostego systemu cyfrowego. Tematy projektów będą nawiązywać do przykładowych praktycznych zastosowań.
Laboratorium	Zajęcia laboratoryjne będą polegać na wykonywaniu zadań indywidualnie przydzielanych każdemu studentowi, które ilustrują główne zagadnienia poruszane na wykładzie: modelowanie systemów z wykorzystaniem języka opisu sprzętu, synteza behawioralna, synteza logiczna, weryfikacja formalna i funkcjonalna.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Zna metody projektowania bloków cyfrowych IP i systemów jednoukładowych wykorzystujące narzędzia syntezy behawioralnej, syntezy logicznej i syntezy topografii.
Powiązane kierunkowe efekty uczenia się	W03, W08
Kod efektu	W02
Opis	Zna techniki weryfikacji cyfrowych bloków IP i systemów jednoukładowych wykorzystujące metody formalne oraz metodykę UVM
Powiązane kierunkowe efekty uczenia się	W03, W08, W12
Kod efektu	W03

Część I

Opis	Zna metody zabezpieczania bloków IP i systemów jednoukładowych przed atakami.
Powiązane kierunkowe efekty uczenia się	W03, W07, W08, W12

Umiejętności

Kod efektu	U01
Opis	Potrafi formułować i analizować specyfikacje projektu oraz przeprowadzić weryfikację zrealizowanego projektu.
Powiązane kierunkowe efekty uczenia się	U01, U03, U06
Kod efektu	U02
Opis	Potrafi zaprojektować specjalizowany cyfrowy układ scalonych z wykorzystaniem narzędzi do syntezy behawioralnej, syntezy logicznej i syntezy topografii.
Powiązane kierunkowe efekty uczenia się	U03, U04, U07
Kod efektu	U03
Opis	Potrafi wykorzystać technikę układów funkcji fizycznie nieklonowalnych PUF.
Powiązane kierunkowe efekty uczenia się	U07, U09
Kod efektu	U04
Opis	Potrafi zrealizować sprzętowy generator liczb prawdziwie losowych.
Powiązane kierunkowe efekty uczenia się	U07, U09
Kod efektu	U05
Opis	Potrafi samodzielnie rozwiązywać problemy projektowe oraz pracować w zespole
Powiązane kierunkowe efekty uczenia się	U13

Kompetencje społeczne

Kod efektu	K01
Opis	Umie współpracować w grupie
Powiązane kierunkowe efekty uczenia się	K01, K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-xxxxx-MSP-PPMGR
Nazwa przedmiotu	Pracownia problemowa magisterska
Wersja przedmiotu	2022Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Dyplomowanie)-Cyberbezpieczeństwo-mgr.-EITI, (Dyplomowanie)-Informatyka biomedyczna-mgr.-EITI, (Dyplomowanie)--mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	2

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	30.00 h

02. Bilans ECTS

Liczba punktów ECTS	2	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	30	1.20
Godziny i ECTS związane z pracą własną studenta	20	0.80
Razem	50	2.00

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	30
Inne godziny kontaktowe	0
Razem	30

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	20

03. Treści kształcenia

Część I

Treści kształcenia	Pracownia problemowa to początek współpracy Dyplomanta i Promotora. W ramach zajęć ustalane są: • tematyka, zakres i cel pracy dyplomowej, • narzędzia i metodologia wykorzystywana w pracy, • zasady i formy współpracy Dyplomanta i Promotora. • Opracowywany jest harmonogram prac. Dyplomant dokonuje przeglądu literatury i w zależności od specyfiki pracy określa wstępną dokumentację pracy w postaci algorytmów, schematów blokowych, opisów eksperymentów, itp. Efekty pracy przedstawia Promotorowi w postaci raportu. Treści kształcenia Pracowni Problemowej obejmują: 1. Wprowadzenie do pracy dyplomowej Cel i struktura pracy dyplomowej.Wymagania formalne i merytoryczne.Etapy realizacji pracy dyplomowej. 1. Metodyka badań naukowych Przegląd literatury i źródeł naukowych. Formułowanie hipotez badawczych. Metody zbierania danych Techniki analizy danych.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Student wie jak korzystać z ogólnodostępnych baz literaturowych i patentowych w celu określenia tematyki, zakresu i harmonogramu działań związanych z wybraną tematyką pracy dyplomowej.
Powiązane kierunkowe efekty uczenia się	W01
Kod efektu	W02
Opis	Student wie jak opracować plan badawczy i zna sposoby weryfikacji, analizy i interpretacji wyników.
Powiązane kierunkowe efekty uczenia się	W03
Kod efektu	W03
Opis	Student zna aktualny stan wiedzy i trendy rozwojowe związane z wybraną tematyką pracy dyplomowej.
Powiązane kierunkowe efekty uczenia się	W08, W09, W10
Kod efektu	W04
Opis	Student ma uporządkowaną wiedzę z zakresu obejmującego tematykę pracy dyplomowej.
Powiązane kierunkowe efekty uczenia się	W11, W12

Umiejętności

Kod efektu	U01
Opis	Student potrafi pozyskiwać informacje z literatury, baz danych oraz innych właściwie dobranych źródeł, także w języku angielskim; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny
Powiązane kierunkowe efekty uczenia się	U01, U02, U12
Kod efektu	U02
Opis	Student potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia.
Powiązane kierunkowe efekty uczenia się	U14
Kod efektu	U03
Opis	Student potrafi stawiać hipotezy badawcze i poddawać je weryfikacji.
Powiązane kierunkowe efekty uczenia się	U02, U07, U10

Część I

Kompetencje społeczne

Kod efektu	K01
Opis	Student potrafi przedstawić i uzasadnić przyjęte założenia i plan działania związany z pisaniem pracy magisterskiej.
Powiązane kierunkowe efekty uczenia się	K01, K03, K04

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-CBxxx-MSP-ARCY
Nazwa przedmiotu	Archiwa cyfrowe
Wersja przedmiotu	2023Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty obieralne)-Cyberbezpieczeństwo-mgr.-EITI, (Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI
Status przedmiotu	Wybieralny
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	4

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	30.00 h
Wykład	15.00 h

02. Bilans ECTS

Liczba punktów ECTS	4

Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**
Liczba godzin i ECTS pracy studenta:		
Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	49	1.96
Godziny i ECTS związane z pracą własną studenta	70	2.80
Razem	119	4.76 (4.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	45
Inne godziny kontaktowe	4
Razem	49

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	70

03. Treści kształcenia

Część I

Projekt	**PROJEKT** • Projekt prowadzony będzie w zespołach 4-6 osobowych, z wyznaczonymi rolami poszczególnych uczestników (w tym kierownika zespołu). • Każdy zespół zaproponuje zadanie archiwizacji, wg precyzyjnie określonych wytycznych. • Następnie dla tego zadania opracuje strukturę archiwum, wraz z projektem pakietów archiwalnych, dopuszczonych formatów archiwizowanych zasobów, ze szczegółowymi scenariuszami procesów ingest, outgest i procesów konserwacji archiwum oraz ze szczegółowym projektem metadanych w formatach zgodnych z uznanymi standardami. • W ramach projektu opracowywane też będą zasady organizacyjne działania archiwum. • Opcjonalnie wykonywane będzie częściowe oprogramowanie wspierające działanie archiwum, np. zarządzające wybranymi rodzajami metadanych.
Wykład	**WYKŁAD** • Organizacja zajęć i regulamin przedmiotu. • Wprowadzenie do archiwów cyfrowych: pojęcie archiwum, rodzaje archiwów cyfrowych, podstawowe zasady archiwizacji. • Wymagania dla archiwów cyfrowych: standaryzacja, replikacja, dyslokacja, dywersyfikacja itp. • Standard OAIS – omówienie i wnioski. Inne standardy dotyczące archiwów cyfrowych. • Budowa archiwum cyfrowego: formaty zasobów, zespoły archiwalne, pakiety archiwalne, procesy ingest i outgest, procesy konserwacji archiwum. Procedury organizacyjne w archiwum cyfrowym. • Metadane w archiwach cyfrowych: podstawy, rodzaje metadanych, metadane zagłębione – rodzaje i sposoby pozyskiwania. • Wprowadzenie do technologii XML. • Standardy metadanych dla archiwów cyfrowych. •

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Zna i rozumie rosnące znaczenie zasobów cyfrowych dla kultury i gospodarki.
Powiązane kierunkowe efekty uczenia się	W01
Kod efektu	W02
Opis	Zna i rozumie procesy związane z długoterminowym bezpiecznym przechowywaniem danych cyfrowych.
Powiązane kierunkowe efekty uczenia się	W02
Kod efektu	W03
Opis	W pogłębionym stopniu zna i rozumie wybrane fakty i metody, stanowiące wiedzę z zakresu analizy systemów w kontekście jej zastosowań w rozwiązywaniu problemów dotyczących bezpieczeństwa zasobów cyfrowych.
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W04

Część I

Opis	W pogłębionym stopniu zna i rozumie wybrane fakty i metody z zakresu bezpieczeństwa przechowywania zasobów cyfrowych, w tym: - bezpieczeństwa rozwiązań sprzętowych, - bezpiecznego długoterminowego składowania danych cyfrowych, - dostępności informacji cyfrowej na długim horyzoncie, - rozwiązań organizacyjnych sprzyjających bezpieczeństwu przechowywania zasobów cyfrowych
Powiązane kierunkowe efekty uczenia się	W08
Kod efektu	W05
Opis	Zna i rozumie procesy zachodzące w cyklu życia archiwów cyfrowych, zwłaszcza związane z zapewnieniem bezpieczeństwa tych systemów.
Powiązane kierunkowe efekty uczenia się	W09
Kod efektu	W06
Opis	Rozumie dylematy współczesnej cywilizacji, związane z upowszechnieniem i rozwojem cyfrowej reprezentacji informacji.
Powiązane kierunkowe efekty uczenia się	W10
Kod efektu	W07
Opis	Rozumie pozatechniczne (prawne, ekonomiczne, etyczne i inne) uwarunkowania archiwizacji zasobów
Powiązane kierunkowe efekty uczenia się	W11
Kod efektu	W08
Opis	zna zasady ochrony własności intelektualnej w zakresie związanym z przechowywaniem zasobów cyfrowy
Powiązane kierunkowe efekty uczenia się	W12

Umiejętności

Kod efektu	U01
Opis	Potrafi przeprowadzić krytyczną analizę sposobu funkcjonowania istniejących rozwiązań technicznych z zakresu przechowywania zasobów cyfrowych i oceniać te rozwiązania.
Powiązane kierunkowe efekty uczenia się	U02
Kod efektu	U02
Opis	Potrafi wykorzystać narzędzia informatyczne służące dobadań i implementacji rozwiązań związanych z archiwizacją zasobów cyfrowych
Powiązane kierunkowe efekty uczenia się	U04
Kod efektu	U03
Opis	Potrafi dokonać identyfikacji i sformułować specyfikację złożonych zadań dotyczących bezpieczeństwa zasobów cyfrowych, a w szczególności: - analizy systemów w kontekście problemów związanych z zapewnieniem bezpieczeństwa zasobów cyfrowych, - zapewniania bezpieczeństwa przechowywania oraz długoterminowej dostępności zasobów cyfrowych
Powiązane kierunkowe efekty uczenia się	U06
Kod efektu	U04
Opis	Potrafi zaprojektować – używając właściwie dobranych metod i narzędzi – rozwiązania związane z długoterminowym przechowywaniem zasobów cyfrowych, a także zweryfikować ich poprawność.
Powiązane kierunkowe efekty uczenia się	U07

Część I

Kod efektu	U05
Opis	potrafi przy identyfikacji, formułowaniu specyfikacji i rozwiązywaniu zadań dotyczących archiwizacji zasobów cyfrowych: - dostrzegać ich aspekty systemowe i pozatechniczne, w tym aspekty społeczne, prawne i etyczne, - oceniać aspekty ekonomiczne proponowanych rozwiązań i podejmowanych działań. Potrafi wnieść wkład w opracowanie strategii zarządzania długoterminowym przechowywaniem zasobów cyfrowych na poziomie instytucjonalnym
Powiązane kierunkowe efekty uczenia się	U08
Kod efektu	U06
Opis	Potrafi przy rozwiązywaniu zadań dotyczących przechowywania zasobów cyfrowych: - dokonać wyboru oraz zastosować właściwe metody, techniki i narzędzia, w tym zaawansowane rozwiązania techniczno-organizacyjne, - przystosować i wykorzystać istniejące lub opracować nowe metody i narzędzia.
Powiązane kierunkowe efekty uczenia się	U09
Kod efektu	U07
Opis	Potrafi przygotować opracowanie i przedstawić prezentację ustną, dotyczącą zagadnień z zakresu archiwizacji cyfrowej.
Powiązane kierunkowe efekty uczenia się	U10
Kod efektu	U08
Opis	Potrafi współdziałać z innymi osobami w ramach prac zespołowych; potrafi kierować pracą zespołu
Powiązane kierunkowe efekty uczenia się	U13

Kompetencje społeczne

Kod efektu	K01
Opis	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści oraz do uznawania znaczenia wiedzy w rozwiązywaniu problemów praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu.
Powiązane kierunkowe efekty uczenia się	K01
Kod efektu	K02
Opis	Jest gotów do myślenia i działania w sposób przedsiębiorczy przewodzenia grupie i ponoszenia odpowiedzialności za nią
Powiązane kierunkowe efekty uczenia się	K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103B-INISY-MSP-PORR
Nazwa przedmiotu	Programowanie równoległe i rozproszone
Wersja przedmiotu	2022Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty obieralne)-Cyberbezpieczeństwo-mgr.-EITI, (Przedmioty zaawansowane obieralne)-Informatyka biomedyczna-mgr.-EITI,(Wytwarzanie)-Inteligentne systemy-mgr.-EITI,(Przedmioty zaawansowane techniczne)--mgr.-EITI,(Przedmioty techniczne)---EITI
Status przedmiotu	Wybieralny
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S1-MSP-103B
Liczba punktów ECTS	4

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	30.00 h
Wykład	30.00 h

02. Bilans ECTS

Liczba punktów ECTS	4	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	62	2.40
Godziny i ECTS związane z pracą własną studenta	55	2.20
Razem	117	4.60 (4.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	60
Inne godziny kontaktowe	2
Razem	62

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	55

03. Treści kształcenia

Część I

Wykład	1. Zagadnienia podstawowe: klasyfikacja i architektura komputerów równoległych; procesory wielordzeniowe, dodatkowe jednostki wykonawcze AVX oraz GPU i akceleratory; obliczenia: wektorowe, współbieżne, równoległe, rozproszone, strumieniowe; rodzaje oprogramowania realizującego równoległość, istotne paradygmaty i modele programowania równoległego. 2. Miary oceny efektywności obliczeń równoległych (współczynniki przyśpieszenia oraz wydajności, prawa Amdahla i Gustafsona-Barsisa, sprawność i skalowalność). 3. Zagadnienia synchronizacji i wymiany informacji w obliczeniach równoległych i rozproszonych, podstawowe mechanizmy: zamek, semafor, monitor, bariera klasyczna i dwuczęściowa, zmienne specyficzne, zmienne i operacje atomowe, zmienne warunków, komunikaty (synchroniczne, asynchroniczne, blokujące, nieblokujące, buforowane, operacje kolektywne, itd.), tablice rozproszone. 4. Wektoryzacja obliczeń we współczesnych komputerach opartych na architekturze x64, sposób wykorzystania jednostek wykonawczych AVX. Podstawowe informacje o obliczeniach ogólnego przeznaczenia wykorzystujących karty graficzne (GPGPU), pojęcia strumienia i jądra; najważniejsze cechy środowisk oprogramowania: CUDA, OpenACC, OpenMP od wersji 4. 5. Elementy programowania współbieżnego na maszynach z pamięcią wspólną, narzędzia: klasyczne systemu UNIX, programowania wielowątkowego (wątki POSIX, wątki języka C według standardu C23, korutyny, język dyrektyw OpenMP. 6. Elementy programowania na maszynach z pamięcią lokalną oraz w sieciach komputerowych, klastrach, gridach, chmurach; narzędzia: środowisko MPI, rodzina narzędzi RPC (w tym dokładniej gRPC). 7. Obliczenia w klastrach i gridach, metody szeregowania zadań i alokacji zasobów, systemy zarządzające obciążeniem (PBS/Torque, Slurm), systemy zarządzania klastrami i gridami (Mosix, Unicore), energooszczędne centra obliczeniowe. 8. Przetwarzanie Big Data – modele, paradygmat MapReduce, środowiska i platformy (Hadoop, Apach Spark). Modele przetwarzania w chmurze, architektura chmury obliczeniowej, technologie (OpenStack). 9. Algorytmy synchroniczne: podstawowe algorytmy algebry liniowej w wersji równoległej, rozwiązywanie układów równań nieliniowych, równoległe metody optymalizacji. 10. Algorytmy całkowicie lub częściowo asynchroniczne: założenia, zbieżność, zastosowanie do rozwiązywania dużych układów równań liniowych i nieliniowych, optymalizacji statycznej, routingu, szeregowania linków w wyszukiwarkach.

Część I

Projekt	Celem projektu jest zdobycie podstawowych praktycznych umiejętności w posługiwaniu się równoległym środowiskiem do obliczeń oraz wykonanie przykładowych obliczeń na maszynach równoległych, wielordzeniowych (także z wykorzystaniem AVX i GPU), jak również w klastrze stacji roboczych. Przewidywane są zadania związane z: 1. badaniem algorytmów synchronicznych z wykorzystaniem dyrektyw zrównoleglających kompilatora (OpenMP) oraz mechanizmu wątków (POSIX, C23, Java/Julia/Rust/itd. threads) na maszynie równoległej z pamięcią wspólną; 2. badaniem algorytmów rozproszonych w klastrze z wykorzystaniem oprogramowania: MPI, gRPC, Java RMI; 3. badaniem efektywności obliczeń hybrydowych - ze zrównolegleniem na wiele rdzeni oraz simdyzacją (AVX, GPU); 4. oceną efektywności różnych narzędzi do zrównoleglania programów napisanych w: Javie, C++, C#, , Julii, Pythonie, Rust, Go, itd., uruchamianych na maszynie wielordzeniowej, pracującej pod kontrolą systemu UNIX/ Linux/macOS albo w sieci PC pod kontrolą MS Windows; 5. oceną różnych platform przetwarzania Big data (Hadoop, Apache Spark, OpenStack, itp.); 6. oceną symulacyjną różnych technik alokacji zasobów do zadań.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Student zna i rozumie główne tendencje rozwojowe informatyki technicznej i telekomunikacji w zakresie komputerów równoległych oraz systemów rozproszonych.
Powiązane kierunkowe efekty uczenia się	W01, W10
Kod efektu	W02
Opis	Student zna i rozumie podstawowe procesy zachodzące w równoległych i rozproszonych systemach informatycznych.
Powiązane kierunkowe efekty uczenia się	W02, W10
Kod efektu	W03
Opis	Student w pogłębionym stopniu zna i rozumie wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę z zakresu matematyki, dotyczące algorytmów i obliczeń równoległych i rozproszonych
Powiązane kierunkowe efekty uczenia się	W05
Kod efektu	W04
Opis	Student w pogłębionym stopniu zna i rozumie wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę ogólną z zakresu projektowania, i integracji rozproszonych systemów informatycznych.
Powiązane kierunkowe efekty uczenia się	W03, W06
Kod efektu	W05

Część I

Opis	Student w pogłębionym stopniu zna i rozumie wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę z zakresu programowania równoległego i rozproszonego.
Powiązane kierunkowe efekty uczenia się	W04, W08

Umiejętności

Kod efektu	U01
Opis	Student potrafi komunikować się na tematy specjalistyczne ze zróżnicowanymi kręgami odbiorców, prowadzić debatę dotyczącą programowania równoległego i rozproszonego.
Powiązane kierunkowe efekty uczenia się	U10, U11
Kod efektu	U02
Opis	Student potrafi kierować pracą zespołu programistów oraz współdziałać z innymi osobami w ramach prac zespołowych nad aplikacją równoległą i rozproszoną.
Powiązane kierunkowe efekty uczenia się	U13
Kod efektu	U03
Opis	Student potrafi planować i realizować uczenie się przez całe życie nowych API do programowania równoległego i rozproszonego a także środowisk klastrowych i chmurowych oraz ukierunkowywać innych w tym zakresie.
Powiązane kierunkowe efekty uczenia się	U03, U09, U14
Kod efektu	U04
Opis	Student potrafi wykorzystać posiadaną wiedzę - formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania, także z innych dziedzin, w nieprzewidywalnych warunkach z zakresu systemów równoległych i rozproszonych poprzez: - właściwy dobór źródeł i informacji z nich pochodzących, dokonywanie oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji - dobór oraz stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik programowania równoległego i rozproszonego - przystosowanie istniejących lub opracowanie nowych metod i narzędzi programowania równoległego i rozproszonego.
Powiązane kierunkowe efekty uczenia się	U02, U03, U10
Kod efektu	U05
Opis	Student potrafi planować i przeprowadzać eksperymenty, w tym pomiary i obliczenia komputerowe z zakresu przetwarzania równoległego i rozproszonego, interpretować uzyskane wyniki.
Powiązane kierunkowe efekty uczenia się	U03, U04
Kod efektu	U06
Opis	Student potrafi przy identyfikacji i formułowaniu specyfikacji zadań inżynierskich z zakresu systemów oraz obliczeń równoległych i rozproszonych a także przy ich rozwiązywaniu: - wykorzystywać metody analityczne, symulacyjne i eksperymentalne - dostrzegać ich aspekty systemowe i pozatechniczne, w tym aspekty etyczne - oceniać aspekty ekonomiczne proponowanych rozwiązań i podejmowanych działań inżynierskich.
Powiązane kierunkowe efekty uczenia się	U07, U08, U09
Kod efektu	U07

Część I

Opis	Student potrafi przeprowadzić krytyczną analizę sposobu funkcjonowania istniejących rozwiązań technicznych z zakresu systemów równoległych i rozproszonych oraz programowania równoległego i rozproszonego i oceniać te rozwiązania.
Powiązane kierunkowe efekty uczenia się	U02, U03
Kod efektu	U08
Opis	Student potrafi projektować - zgodnie z zadaną specyfikacją - oraz tworzyć aplikacje równoległe i rozproszone, używając odpowiednio dobranych metod, technik i narzędzi.
Powiązane kierunkowe efekty uczenia się	U06, U08, U09

Kompetencje społeczne

Kod efektu	K01
Opis	Student jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści oraz do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu z zakresu systemów równoległych i rozproszonych.
Powiązane kierunkowe efekty uczenia się	K01
Kod efektu	K02
Opis	Student jest gotów do myślenia i działania w sposób przedsiębiorczy, przewodzenia grupie twórców systemów oraz aplikacji równoległych i rozproszonych i ponoszenia odpowiedzialności za nią.
Powiązane kierunkowe efekty uczenia się	K03
Kod efektu	K03
Opis	Student jest gotów do odpowiedzialnego pełnienia ról zawodowych, z uwzględnieniem zmieniających się potrzeb społecznych w dziedzinie systemów równoległych i rozproszonych, w tym: - rozwijania dorobku zawodu informatyka zajmującego się programowaniem równoległym i rozproszonym - podtrzymywanie etosu zawodu programisty aplikacji równoległych i rozproszonych, - przestrzegania etyki zawodowej oraz działania na rzecz przestrzegania tych zasad w systemach rozproszonych, w tym w chmurach oraz sieciach społecznych w Internecie.
Powiązane kierunkowe efekty uczenia się	K04

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-xxxxx-MSP-CYPR
Nazwa przedmiotu	Cyberprzestępczość - wyzwania prawne
Wersja przedmiotu	2024Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty ekonomiczno-społeczne)-Cyberbezpieczeństwo-mgr.-EITI,(Semestr 2 modelowy)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S2-MSP-103B
Liczba punktów ECTS	2

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Ćwiczenia	30.00 h

02. Bilans ECTS

Liczba punktów ECTS	2

Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**
Liczba godzin i ECTS pracy studenta:		
Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	30	1.20
Godziny i ECTS związane z pracą własną studenta	28	1.12
Razem	58	2.32 (2.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	30
Inne godziny kontaktowe	0
Razem	30

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	28

03. Treści kształcenia

Część I

Ćwiczenia	Przedmiot opiera się na założeniu, że praca zawodowa oraz prowadzenie działalności gospodarczej w sektorze informatycznym wymaga znajomości podstawowych koncepcji prawnych oraz ryzyka prawnego związanego z obszarem cyberprzestępczości. Podczas zajęć omówione zostaną teoretyczne i praktyczne aspekty zwalczania i zapobiegania cyberprzestępczości przy wykorzystaniu narzędzi prawnych oraz współpracy z wymiarem sprawiedliwości, w tym organami ścigania. Studenci zapoznają się także z tendencjami rozwojowymi prawa i procesu karnego w obszarze cyberprzestępczości. Przedmiot ma na celu dostarczenie wiedzy oraz kształtowanie umiejętności praktycznych i kompetencji społecznych w tym zakresie. Zamierzone cele dydaktyczne można podzielić na dwie grupy - merytoryczne (opanowanie kluczowych pojęć, zrozumienie instytucji prawnych i zasad prawa karnego materialnego i procesu karnego, prawne aspekty prowadzenia audytów bezpieczeństwa informatycznego) oraz osiągnięcie określonych umiejętności praktycznych (identyfikowanie ryzyka prawnego w obszarze cyberprzestępczości, identyfikowanie ryzyka niezgodności z prawem prowadzonej działalności gospodarczej lub zawodowej, dokonywanie wykładni przepisów w zakresie prawa karnego materialnego i postępowania karnego umożliwiające ich poprawne zastosowanie w praktyce, umiejętność opracowania rozwiązań prawnych sytuacji kryzysowych związanych z cyberprzestępczością). Podczas zajęć studenci zostaną zapoznani z zagrożeniami wynikającymi z wykorzystywania rozwoju telekomunikacji przez pojedynczych przestępców i zorganizowane grupy przestępcze.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	zna i rozumie problemy prawne związane z cyberprzestępczością, jej wykrywaniem i zwalczaniem
Powiązane kierunkowe efekty uczenia się	W01, W10
Kod efektu	W02
Opis	posiada podstawową wiedzę o narzędziach prawnych służących do dochodzenia odpowiedzialności sprawców cyberprzestępstw
Powiązane kierunkowe efekty uczenia się	W01, W10, W11
Kod efektu	W03
Opis	rozumie etyczne, prawne i społeczny aspekty zwalczania cyberprzestępczości
Powiązane kierunkowe efekty uczenia się	W10, W11
Kod efektu	W04
Opis	posiada wiedzę na temat ryzyka prawnego związanego z bezprawnym lub nieprawidłowym przetwarzaniem danych
Powiązane kierunkowe efekty uczenia się	W01, W10, W11
Kod efektu	W05
Opis	posiada wiedzę na temat ryzyka prawnego związanego z naruszeniem prawa w zakresie ochrony własności intelektualnej, własności przemysłowej oraz z czynami nieuczciwej konkurencji
Powiązane kierunkowe efekty uczenia się	W12

Część I

Umiejętności

Kod efektu	U01
Opis	potrafi interpretować normy prawne w stopniu umożliwiającym identyfikację ryzyka prawnego w obszarze cyberbezpieczeństwa
Powiązane kierunkowe efekty uczenia się	U01
Kod efektu	U02
Opis	potrafi przygotować opracowanie i przedstawić prezentację ustną przedstawiającą praktyczne aspekty postępowania zgodnie z przepisami prawa w sytuacjach ryzyka prawnego w obszarze cyberbezpieczeństwa
Powiązane kierunkowe efekty uczenia się	U10
Kod efektu	U03
Opis	potrafi ocenić aspekty etyczne i prawne odnoszące się do zjawiska cyberprzestępczości i uwzględnić czynniki społeczne w zapobieganiu cyberprzestępczości
Powiązane kierunkowe efekty uczenia się	U08
Kod efektu	U04
Opis	potrafi zidentyfikować aktualne problemy prawne odnoszące się do zjawiska cyberprzestępczości oraz uwzględnić ryzyka prawne w tym zakresie w przyszłej działalności zawodowej
Powiązane kierunkowe efekty uczenia się	U08, U13

Kompetencje społeczne

Kod efektu	K01
Opis	umie w zrozumiały sposób prezentować rozwiązania i strategie cyberbezpieczeństwa odbiorcom nietechnicznym z uwzględnieniem podstawowych aspektów prawnych
Powiązane kierunkowe efekty uczenia się	K02
Kod efektu	K02
Opis	potrafi planować rozwój swoich kompetencji zawodowych, oraz przewidywać i rozwijać nowe trendy z zakresu cyberbezpieczeństwa, biorąc pod uwagę ich aspekty prawne i etyczne
Powiązane kierunkowe efekty uczenia się	K04

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-CBxxx-MSP-BESG
Nazwa przedmiotu	Bezpieczeństwo sieci 5G i 6G
Wersja przedmiotu	2024Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty kierunkowe)-Cyberbezpieczeństwo-mgr.-EITI, (Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 2 modelowy)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S2-MSP-103B
Liczba punktów ECTS	4

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Wykład	30.00 h
Projekt	15.00 h

02. Bilans ECTS

Liczba punktów ECTS	4	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	58	2.32
Godziny i ECTS związane z pracą własną studenta	52	2.08
Razem	110	4.40 (4.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	45
Inne godziny kontaktowe	13
Razem	58

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	52

03. Treści kształcenia

Część I

Wykład	Wprowadzenie Wprowadzenie do przedmiotu. Omówienie zasad zaliczania przedmiotu i zakresu projektu. Omówienie zagadnień bezpieczeństwa sieciowego i klas typowych ataków sieciowych. Rekomendacje dotyczące bezpieczeństwa sieci (m.in. ITU-T, NGMN). 1. Omówienie sieci 2G, 3G i 4G oraz ich mechanizmów bezpieczeństwa Zwięzłe wprowadzenie do sieci 2G, 3G, 4G omówienie i rola usług oferowanych przez omawiane sieci, omówienie ewolucji mechanizmów bezpieczeństwa w w/w sieciach. 1. Architektura sieci 5G Omówienie architektury sieci 5G (wersje Non-Stand-Alone i Stand-Alone) oraz podsystemu radiowego NR. Łącze radiowe w systemach 5G. Protokoły w łączu radiowym. Wykorzystanie techniki network slicing do tworzenia wirtualnych sieci usługowych (programowanie płaszczyzny sterowania). 1. Architektura bezpieczeństwa sieci 5G Zwięzłe wprowadzenie do omawianych rozwiązań sieciowych, omówienie i rola usług oferowanych przez omawiane systemy. Podkreślenie roli bezpieczeństwa omawianych systemów. 1. Bezpieczeństwo łącza radiowego Omówienie aspektów bezpieczeństwa łącza radiowego oraz podsystemu radiowego NR. Uwierzytelnianie. Szyfrowanie i kontrola integralności. Numery tymczasowe stacji ruchomych. Generacja i dystrybucja kluczy kryptograficznych. Odporność łącza radiowego na zakłócenia i zagłuszanie. 1. Bezpieczeństwo wirtualizacji Sieci 5G i 6G budowane są/będą z wykorzystaniem technik wirtualizacyjnych w rozproszonym środowisku chmurowym. W ramach wykładu zostaną omówione aspekty bezpieczeństwo rozwiązań ETSI NFV (MANO) i Kubernetes w przypadku sieci 5G i 6G. 1. Usługi i architektura sieci 6G W ramach wykładu przedstawione zostaną wymagania, usługi i szkic architektury sieci 6G (architektura docelowa spodziewana jest w roku 2030). 1. Mechanizmy bezpieczeństwa sieci 6G W ramach wykładu przedstawione zostaną mechanizmy bezpieczeństwa (uwierzytelniania, szyfrowania, integralności danych) oraz wiarygodności wymiany danych w środowisku wielooperatorskim (np. Gaia-X) wymagania, usługi i szkic architektury bezpieczeństwa sieci 6G
Projekt	W ramach projektu 2-3 osobowe zespoły będą odpowiedzialne za rozwiązanie wybranego problemu z zakresu tematyki wykładów. Projekt zakończy się raportem oraz prezentacją wyników prac. Każda grupa projektowa dostanie inny temat projektu.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	zna i rozumie główne tendencje rozwojowe sieci komunikacji ruchomej
Powiązane kierunkowe efekty uczenia się	W01
Kod efektu	W02
Opis	ma wiedzę dotyczącą zagrożeń bezpieczeństwa sieci 5G i 6G
Powiązane kierunkowe efekty uczenia się	W02

Część I

Kod efektu	W03
Opis	ma wiedzę dotyczącą architektury bezpieczeństwa sieci 5G i 6G
Powiązane kierunkowe efekty uczenia się	W08
Kod efektu	W04
Opis	ma wiedzę dotyczącą bezpieczeństwa techniki network slicing i wirtualizacji
Powiązane kierunkowe efekty uczenia się	W08, W09
Kod efektu	W05
Opis	ma wiedzę z zakresu przetwarzania danych osobowych w sieciach 5Gi 6G
Powiązane kierunkowe efekty uczenia się	W10, W11

Umiejętności

Kod efektu	U01
Opis	potrafi planować i przeprowadzać symulacje komputerowe dotyczące bezpieczeństwa sieci komunikacji ruchomej
Powiązane kierunkowe efekty uczenia się	U03
Kod efektu	U02
Opis	potrafi skonfigurować i zoptymalizować podstawowe mechanizmy bezpieczeństwa w sieciach 5G
Powiązane kierunkowe efekty uczenia się	U07, U08

Kompetencje społeczne

Kod efektu	K01
Opis	ma świadomość konieczności komunikowania się z podmiotami ekosystemu 5G w calu zapewnienia jego pełnego bezpieczeństwa
Powiązane kierunkowe efekty uczenia się	K03
Kod efektu	K02
Opis	jest świadomy konieczności ciągłej aktualizacji wiedzy o sieciach komunikacji ruchomej w związku z pojawianiem się ich nowych generacji
Powiązane kierunkowe efekty uczenia się	K01

SYLABUS PRZEDMIOTU

Kod przedmiotu	103B-xxxxx-MSP-PDMGR
Nazwa przedmiotu	Pracownia dyplomowa magisterska
Wersja przedmiotu	2022Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Dyplomowanie)-Cyberbezpieczeństwo-mgr.-EITI, (Dyplomowanie)-Informatyka biomedyczna-mgr.-EITI, (Dyplomowanie)--mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S2-MSP-103B
Liczba punktów ECTS	6

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	90.00 h

02. Bilans ECTS

Liczba punktów ECTS	6	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	100	4.00
Godziny i ECTS związane z pracą własną studenta	50	2.00
Razem	150	6.00

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	90
Inne godziny kontaktowe	10
Razem	100

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	50

03. Treści kształcenia

Część I

Treści kształcenia	W ramach Pracownia Dyplomowej Student pod nadzorem Promotora realizuje ustalone wcześniej zadania. W szczególności Dyplomant zapoznaje się z dostępną bazą dydaktyczną, która będzie wykorzystywana w trakcie realizacji pracy (aparatura pomiarowa, systemy komputerowe i pomiarowe, specjalistyczne oprogramowanie, itp.). W razie konieczności określane są brakujące zasoby i ustalany jest sposób i czas uzyskania dostępu do nich. W ramach pracowni Dyplomant stale dokształca się w zakresie odpowiadającym tematyce pracy. Uzyskane rezultaty prac na bieżąco poddawane są analizie i weryfikacji i w razie potrzeby, we współpracy z Promotorem, podejmowane są decyzje o modyfikacji ustalonych wcześniej zadań badawczych. Oceniana jest także zgodność postępów prac z przyjętym harmonogramem. Dyplomant przedstawia Promotorowi wyniki pracy w postaci raportu lub prezentacji.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Ma podbudowaną teoretycznie szczegółową wiedzę ogólną obejmującą kluczowe zagadnienia związaną z tematyką dyplomowania
Powiązane kierunkowe efekty uczenia się	W02, W03
Kod efektu	W02
Opis	Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu złożonych zadań inżynierskich związanych z tematyką pracy magisterskiej
Powiązane kierunkowe efekty uczenia się	W04, W05, W06
Kod efektu	W03
Opis	Zna aktualny stan wiedzy i trendy rozwojowe związane z wybraną tematyką pracy dyplomowej
Powiązane kierunkowe efekty uczenia się	W01, W08

Umiejętności

Kod efektu	U01
Opis	Potrafi porozumiewać się przy użyciu różnych technik w środowisku zawodowym oraz w innych środowiskach, także w języku angielskim.
Powiązane kierunkowe efekty uczenia się	U10, U11, U12
Kod efektu	U02
Opis	Potrafi pozyskiwać informacje z literatury, baz danych oraz innych właściwie dobranych źródeł, także w języku angielskim; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny
Powiązane kierunkowe efekty uczenia się	U01, U02
Kod efektu	U03
Opis	Potrafi stawiać hipotezy badawcze i poddawać je weryfikacji
Powiązane kierunkowe efekty uczenia się	U09
Kod efektu	U04
Opis	Potrafi planować i przeprowadzać eksperymenty, w tym zaawansowane pomiary i symulacje komputerowe oraz opracowywać i interpretować uzyskane wyniki i wyciągać wnioski
Powiązane kierunkowe efekty uczenia się	U06, U07

Kompetencje społeczne

Część I

Kod efektu	K01
Opis	Potrafi myśleć i działać kreatynie rozwiązując napotkane problemy. Potrafi także działać w zespole oraz umie przedstawić i uzasadnić przyjętą metodologię działań.
Powiązane kierunkowe efekty uczenia się	K01, K02, K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103B-CBxxx-MSP-BIRC
Nazwa przedmiotu	Bezpieczeństwo internetu rzeczy
Wersja przedmiotu	2026Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Kształcenie oparte o projekty)-Cyberbezpieczeństwo-mgr.-EITI,(Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 2 modelowy)-Cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S2-MSP-103B
Liczba punktów ECTS	12

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Zajęcia zintegrowane	120.00 h
Projekt	60.00 h

02. Bilans ECTS

Liczba punktów ECTS	12	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	227	9.08
Godziny i ECTS związane z pracą własną studenta	120	4.80
Razem	347	13.88 (12.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	180
Inne godziny kontaktowe	47
Razem	227

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	120

03. Treści kształcenia

Część I

Projekt	Projekt realizowany jest w kilkuosobowych zespołach. Zajęcia związane z realizacją projektu odbywają w wymiarze 2 godz. w każdym tygodniu wspólnie dla całej grupy oraz 2 godz. w każdym tygodniu w formie konsultacji poszczególnych zespołów z opiekunami. Projekt składa się z dwóch odrębnie ocenianych części. Część 1 – projekt i implementacja sieci IoT Zadaniem każdego z kilkuosobowych zespołów studenckich jest zaprojektowanie i zaimplementowanie uproszczonego modelu niskobudżetowej, możliwie bezpiecznej sieci IoT, realizującej zadania z zakresu akwizycji danych lub / i sterowania, zgodne z zarysem założeń funkcjonalnych określonym przez prowadzącego zajęcia. Istotą zadania jest zaprojektowanie własnego sposobu komunikacji bezprzewodowej wykorzystującego scalone transceiwery Sub-1GHz lub / i urządzenia SDR (wykluczone jest stosowanie fabrycznych rozwiązań oferujących wbudowane szyfrowanie, np. WiFi, BLE, LTE itp.). Zadanie obejmuje wybór schematu modulacji, projekt ramki radiowej, wybór lub projekt protokołu warstwy aplikacji, decyzje o tym, czy system jest jedno – czy dwukierunkowy (z potwierdzeniami), wybór algorytmu szyfrowania (lub jego braku) itp. oraz implementację modelu sieci z wykorzystaniem dostępnych komponentów (np. minikomputer jednoukładowy Raspberry Pi plus dołączony interfejs bezprzewodowy, czujnik lub / i element wykonawczy). Elementem zadania jest także wyposażenie sieci w mechanizmy pozwalające zorientować się, że ktoś próbuje naruszać jej integralność (monitorowanie ruchu). Zadanie kończy się przygotowaniem dokumentacji technicznej systemu, obejmującej m.in. specyfikację opracowanego protokołu radiowego, szczegóły implementacji, podjęte działania i zastosowane rozwiązania mające na celu podniesienie poziomu bezpieczeństwa sieci. Część 2 – przegląd bezpieczeństwa sieci IoT Działający model sieci dany zespół studentów przekazuje w ręce innego zespołu, w celu zweryfikowania jej bezpieczeństwa. Względem swojej sieci zespół występuje w roli Zespołu Broniącego, natomiast względem obcej sieci zespół pełni rolę Testera. Zadaniem Testera jest przeprowadzenie przeglądu bezpieczeństwa sieci podążając za zaleceniami (np. zgodnie z wybranym frameworkiem bezpieczeństwa) przedstawionymi przez prowadzącego zajęcia. Zespół Broniący udostępnia Testerom kod źródłowy stworzonego oprogramowania (np. poprzez repozytorium), ale nie hasła czy innego rodzaju klucze autoryzujące. Przegląd bezpieczeństwa polega zarówno na analizie kodu źródłowego jak również przeprowadzeniu prób spenetrowania sieci oraz złamania jej zabezpieczeń, w tym tych dotyczących komunikacji radiowej. Przeprowadzane próby są odnotowywane w sprawozdaniu, z uwzględnieniem typu, dokładnej daty i godziny prowadzonych działań, oraz szczegółów technicznych pozwalających na odtworzenie ataku w późniejszym terminie np. przez prowadzącego zajęcia lub Zespół Broniący w ramach zabezpieczania swojego rozwiązania. Tester przedstawia sprawozdanie z przeprowadzonych badań, wskazując na wykryte podatności analizowanego systemu. Zadaniem Zespołu Broniącego na tym etapie jest przede wszystkim wychwycenie prób spenetrowania oraz złamania zabezpieczeń własnej sieci. Do tego celu wykorzystane

Część I

	powinny zostać wbudowane w sieć rozwiązania monitorujące podejrzane zachowania (np. zaimplementowane w części 1 monitorowanie ruchu). Zespół Broniący przedstawia sprawozdanie, w którym zamieszcza wiarygodne zestawienie wykrytych prób naruszenia integralności swojej sieci.

Część I

Zajęcia zintegrowane	Zajęcia zintegrowane mają charakter zajęć praktycznych, prowadzonych w wymiarze 2 razy po 4 godz. w każdym tygodniu, z bogatą częścią wprowadzającą w dane zagadnienie. „Minimisja” określa przykładową aktywność, jaką studenci mogą zrealizować podczas zajęć lub/i w ramach pracy samodzielnej w danym tygodniu. W1: Wprowadzenie do zagadnień bezpieczeństwa sieci IoT, modelowanie zagrożeń. Specyfika systemów IoT i kwestie bezpieczeństwa, przykłady incydentów. Standardy, frameworki, protokoły, stan prawny, kierunki rozwoju. Pojęcia constrained-node, constrained-networks. Identyfikacja zagrożeń. Łączność w sieciach IoT – przewodowa i bezprzewodowa. Tablica przeznaczeń częstotliwości. Źródła informacji o urządzeniach IoT (np. FCC ID, inżynieria odwrotna). Technika Software Defined Radio – charakterystyka i rola w systemach IoT. Minimisja: Na przykładzie specyfikacji wybranych urządzeń elektronicznych z najbliższego otoczenia – samodzielna próba identyfikacji sposobu i parametrów komunikacji (np. częstotliwość, moc, standard telekomunikacyjny). W2: Protokoły sieciowe w IoT. Podstawy najpopularniejszych protokołów sieciowych wykorzystywanych w sieciach IoT np. HTTP, MQTT, CoAP. Narzędzia do generowania żądań i analizy komunikacji (np. Postman, MQTT Explorer, Mosquitto, Wireshark). Biblioteki wspomagające implementację klienta/serwera np. w Pythonie. Podgląd komunikacji na poziomie pakietów TCP/IP – program Wireshark. Minimisja: Klient/serwer w Pythonie – uruchomienie i modyfikacja przykładów. Analiza przechwyconych żądań i odpowiedzi za pomocą Wireshark dla protokołów sieci IoT. Minimisja: Wykorzystując dostępne online odbiorniki SDR, odebrać i spróbować zidentyfikować wybrane sygnały radiowe. W3: Podstawy komunikacji radiowej. Fale elektromagnetyczne – właściwości propagacyjne, modele propagacji. Obliczanie bilansu łącza. Sygnał radiowy – definicja, miary jakości, cechy charakterystyczne. Typowe schematy modulacji analogowych i cyfrowych. Częste problemy związane z przesyłaniem informacji za pomocą sygnału radiowego (np. stosunek sygnał-szum, zniekształcenia, synchronizacja, publiczność przekazu). Reprezentacja sygnału radiowego w domenie cyfrowej – sygnał kwadraturowy (IQ). Wizualizacja sygnału w dziedzinie czasu, częstotliwości, czasu-częstotliwości. Parametry widmowe sygnałów różnych standardów, identyfikacja sygnałów. Minimisja: Zainstalować i uruchomić odbiornik SDR na własnym komputerze. Przy jego pomocy odebrać i spróbować zidentyfikować wybrane sygnały dostępne lokalnie w eterze. Minimisja: Analiza literaturowa obecnego stanu techniki w zakresie bezpieczeństwa systemów bezprzewodowych powszechnego użytku. W4: Narzędzia do testów penetracyjnych w sieciach radiowych IoT Architektura Zero-IF w systemach SDR. Przykłady dostępnych komercyjnie urządzeń odbiorczych i nadawczo-odbiorczych SDR – przegląd, wady, zalety ze szczególnym uwzględnieniem cech szczególnie ważnych dla badania bezpieczeństwa sieci IoT. Analizator widma. Oprogramowanie

Część I

	do odbioru i analizy sygnałów radiowych, np. Universal Radio Hacker, GNU Radio Companion, Gqrx, SDR#, SDR Console, Audacity. Minimisja: Odbiór sygnałów z wybranego otwartego standardu za pomocą mobilnej platformy SDR. Dyskusja nad potencjalnymi zagrożeniami wynikającymi z otwartości przekazu. W5: Testy bezpieczeństwa w sieciach IoT. Badanie bezpieczeństwa systemu IoT w różnych warstwach: rekonesans sieciowy (odkrywanie hostów, identyfikacja systemów operacyjnych oraz wersji narzędzi, mapowanie topologii), badanie protokołów w łączach bezprzewodowych i przewodowych, atakowanie usług/protokołów, przegląd konfiguracji hostów, testowanie aplikacji mobilnych / webowych / chmurowych, warstwa sprzętowa, rekonesans pasywny / OSINT. Rekonesans pasywny w sieci bezprzewodowej na przykładzie nasłuchu transmisji radiowych przy użyciu odbiorników SDR oraz ogólnodostępnego oprogramowania. Źródła wiedzy o sygnałach radiowych. Ulot elektromagnetyczny, urządzenia klasy TEMPEST. Minimisja: Wykorzystanie narzędzi do automatycznego skanowania sieci i podatności urządzeń IoT. Minimisja: Przechwytywanie i analiza emisji ujawniającej – ulot elektromagnetyczny. W6: Rekonesans systemu radiowego. Zagrożenia wynikające z możliwości przechwycenia transmisji, zarejestrowania sygnału, jego analizy/ dekodowania i retransmisji. Inżynieria odwrotna protokołów radiowych na przykładzie urządzeń klasy Sub-1GHz. Typowe elementy ramki radiowej (np. preambuła, payload, suma kontrolna). Systemy o stałym i zmiennym kluczu. Minimisja: Dekodowanie sygnałów z urządzeń powszechnego użytku, np. stacje pogodowe, wodomierze, piloty zdalnego sterowania. W7: Ingerowanie w działanie systemów radiokomunikacyjnych – nadawanie sygnałów. Aspekty prawne. Przegląd urządzeń i podzespołów pozwalających wytwarzać sygnały radiowe: dedykowane dla określonych schematów modulacji oraz generatory przebiegów arbitralnych (określanych na podstawie próbek IQ). Odtwarzanie zarejestrowanego sygnału – atak typu replay. Modyfikacja zarejestrowanego sygnału. Ataki typu brute-force, jamming, spoofing, tampering. Minimisja: Zaimplementować nadajnik podszywający się pod oryginalny czujnik stacji pogodowej (atak typu spoofing). Minimisja: Przeprowadzić atak typu brute-force oraz jamming na wskazanym systemie IoT. W8: Sieci WiFi / Bluetooth Organizacja łączności, charakterystyka komunikacji w warstwie radiowej, techniki zabezpieczeń. Znane podatności, narzędzia i techniki ataku. Minimisja: Przeprowadzenie ataków typu deauthentication, jamming sieci WiFi. Minimisja: Podsłuchiwanie klawiatury / myszki bezprzewodowej. W9: Systemy ZigBee i BLE Organizacja łączności, charakterystyka komunikacji w warstwie radiowej, techniki zabezpieczeń. Znane podatności, narzędzia i techniki ataku. Minimisja: Podsłuch oraz atak typu replay względem wybranego urządzenia konsumenckiego pracującego w

Część I

	standardzie ZigBee. Minimisja: Analiza komunikacji BLE. Odczyt deskryptorów, autentykacja, MAC spoofing. W10: Systemy łączności dalekiego zasięgu (np. LoRa, GPS, DCF77, publiczne emisje rozsiewcze) Organizacja łączności, charakterystyka komunikacji w warstwie radiowej, techniki zabezpieczeń. Właściwości i propagacja fal elektromagnetycznych w różnych zakresach częstotliwości i na dużych dystansach. Modele propagacyjne. Znane podatności, narzędzia i techniki ataku. Minimisja: przeprowadzić wybrany atak na sieć LoRa np. bitflip, replay, ack spoofing). Minimisja: przeprowadzić atak GPS spoofing. W11: Systemy łączności bliskiego zasięgu (np. RFID, NFC) Organizacja łączności, charakterystyka komunikacji w warstwie radiowej, techniki zabezpieczeń. Systemy RFID aktywne i pasywne. Tagi RFID i ich zabezpieczenia. Znane podatności, narzędzia i techniki ataku. Minimisja: Klonowanie tagów. Modyfikowanie zawartości tagów. Podsłuchiwanie transmisji pomiędzy czytnikiem a tagiem. W12: Inżynieria odwrotna urządzeń IoT – część 1. Komunikacja i diagnostyka za pomocą interfejsów szeregowych. Inżynieria odwrotna urządzenia IoT: inspekcja zewnętrzna, pozyskiwanie wszelkich informacji o urządzeniu z różnych źródeł, inspekcja wewnętrzna, identyfikacja roli kluczowych komponentów. FCC ID. Wyszukiwanie oraz czytanie not katalogowych komponentów elektronicznych. Komunikacja szeregowa UART – odczyt informacji diagnostycznych. Standardy RS-232 / RS-485 i sieci przemysłowe. Protokół Modbus – podgląd transmisji, sterowanie urządzeniami. Minimisja: Inżynieria odwrotna wskazanego urządzenia IoT. Minimisja: Komunikacja w sieci przemysłowej Modbus – nasłuch i ingerencja. W13: Inżynieria odwrotna urządzeń IoT – część 2. Komunikacja pomiędzy podzespołami urządzenia IoT (np. SPI, I2C, 1-Wire). Komunikacja pomiędzy komponentami składowymi urządzeń IoT – protokoły szeregowe SPI, I2C, 1-Wire itp. Podglądanie komunikacji z układami peryferyjnymi – wykorzystanie oscyloskopu, analizatora stanów logicznych itp. Pozyskiwanie listy zajętych adresów na magistrali I2C. Inżynieria odwrotna protokołu komunikacji w przypadku, gdy nota katalogowa układu nie jest dostępna. Wysyłanie własnych komend do sprzętu. Minimisja: odczyt, modyfikacja i zapis szeregowej pamięci EEPROM przechowującej nastawy lub firmware urządzenia. Minimisja: podgląd komunikacji szeregowej pomiędzy mikrokontrolerem a czujnikiem. W14: Bezpieczeństwo IoT – aspekty prawne, moralne i praktyczne. Audyt bezpieczeństwa. Regulacje prawne (w tym planowane regulacje EU) dotyczące bezpieczeństwa urządzeń i systemów IoT. Kwestia ochrony prywatności użytkowników urządzeń IoT, anonimizacja danych, ochrona danych przed podsłuchaniem, szyfrowanie. Nieoczywiste drogi do utraty/zabrania komuś elementów prywatności, np. profilowanie zachowań ludzi na podstawie pomiarów zużycia energii elektrycznej, wody itp., ulot elektromagnetyczny, kamery i analiza obrazu za pomocą sztucznej inteligencji. Wykorzystywanie publicznie dostępnych danych do nieoczywistych zastosowań, np.

Część I

	https://dictatoralert.org/. Dalsze kierunki rozwoju dla inżynierów bezpieczeństwa IoT, rynek pracy. Minimisja: przygotowanie i poprowadzenie prelekcji lub dyskusji na wybrany temat dotyczący bezpieczeństwa IoT. W15 – Rezerwa, prezentacje końcowe projektów semestralnych. Seminarium podsumowujące zrealizowane projekty semestralne. Każdy z zespołów prezentuje przygotowane rozwiązanie techniczne oraz uzyskane wyniki z zakresu bezpieczeństwa i stabilności działania sieci. Omawiane są logi wykrytych i przeprowadzonych prób naruszeń integralności systemów. Dyskusja nad potencjalnymi podatnościami poszczególnych rozwiązań.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Zna i rozumie główne kierunki rozwoju urządzeń oraz sposobów łączności w sieciach urządzeń Internetu Rzeczy.
Powiązane kierunkowe efekty uczenia się	W01
Kod efektu	W02
Opis	Zna i rozumie procedury bezpieczeństwa stosowane w popularnych standardach komunikacyjnych wykorzystywanych w systemach IoT
Powiązane kierunkowe efekty uczenia się	W02
Kod efektu	W03
Opis	Ma wiedzę dotyczącą metodyki prowadzenia rekonesansu w sieciach pakietowych oraz w systemach radiowych, pozwalającą na wykrywanie i analizowanie podatności systemów IoT.
Powiązane kierunkowe efekty uczenia się	W03
Kod efektu	W04
Opis	Ma wiedzę dotyczącą metodyki prowadzenia prac z zakresu inżynierii wstecznej urządzeń IoT w zakresie pozyskiwania informacji o wykorzystywanych sposobach łączności pomiędzy komponentami urządzenia oraz pomiędzy urządzeniami.
Powiązane kierunkowe efekty uczenia się	W03
Kod efektu	W05
Opis	zna specjalistyczne narzędzia informatyczne niezbędne do analizy ruchu w sieciach IoT przewodowych i bezprzewodowych
Powiązane kierunkowe efekty uczenia się	W04
Kod efektu	W06
Opis	W pogłębionym stopniu zna i rozumie zasady wymiany informacji pomiędzy urządzeniami komunikującymi się bezprzewodowo (sposób formowania sygnału radiowego, modulacji, budowy ramki itp.) dla różnych standardów telekomunikacyjnych w kontekście wyszukiwania potencjalnych luk w obszarze cyberbezpieczeństwa.
Powiązane kierunkowe efekty uczenia się	W06
Kod efektu	W07

Część I

Opis	W pogłębionym stopniu zna i rozumie możliwości wpływania na nadawany sygnał i działanie nadajnika radiowego i jego podstawowych podzespołów oraz wybranych techniki dostępu i modulacji, a także aspekty prawne dot. transmisji radiowej.
Powiązane kierunkowe efekty uczenia się	W07
Kod efektu	W08
Opis	Zna przykłady incydentów bezpieczeństwa dotyczących systemów IoT dotyczących rozwiązań sprzętowych oraz łączności bezprzewodowej, rozumie przyczyny ich zaistnienia oraz zna metody wykrywania i zapobiegania.
Powiązane kierunkowe efekty uczenia się	W08

Umiejętności

Kod efektu	U01
Opis	Potrafi pozyskiwać informacje o działaniu urządzeń IoT na podstawie ogólnodostępnych źródeł oraz analizie układu „z natury”, dokonywać ich krytycznej oceny źródeł, wyciągać wnioski i wyczerpująco je uzasadniać.
Powiązane kierunkowe efekty uczenia się	U01
Kod efektu	U02
Opis	Potrafi przeprowadzić krytyczną analizę sposobu funkcjonowania istniejących standardów komunikacji w sieciach IoT z zakresu bezpieczeństwa systemów teleinformatycznych i oceniać te rozwiązania.
Powiązane kierunkowe efekty uczenia się	U02
Kod efektu	U03
Opis	Potrafi planować i przeprowadzać eksperymenty polegające na wygenerowaniu zasymulowanych sygnałów radiowych w celu ich wstrzyknięcia do sieci bezprzewodowej oraz potrafi interpretować uzyskane wyniki.
Powiązane kierunkowe efekty uczenia się	U03
Kod efektu	U04
Opis	Potrafi wykorzystać specjalistyczne oprogramowanie do analizy sygnałów radiowych w celu analizy protokołów bezprzewodowych pod kątem cyberbezpieczeństwa i analizy ich wyników.
Powiązane kierunkowe efekty uczenia się	U04
Kod efektu	U05
Opis	Potrafi formułować i testować hipotezy odnośnie bezpieczeństwa danego systemu oraz skuteczności zabezpieczeń.
Powiązane kierunkowe efekty uczenia się	U05
Kod efektu	U06
Opis	Potrafi identyfikować potencjalne wektory ataku oraz formułować wymagania dotyczące poziomu bezpieczeństwa w projektowanym lub analizowanym systemie.
Powiązane kierunkowe efekty uczenia się	U06
Kod efektu	U07
Opis	Potrafi zaprojektować – zgodnie z zadaną specyfikacją – bezpieczną sieć urządzeń IoT komunikujących się ze sobą bezprzewodowo za pomocą autorskiego protokołu, a także zweryfikować poprawność projektu.
Powiązane kierunkowe efekty uczenia się	U07

Część I

Kod efektu	U08
Opis	Potrafi dostrzegać aspekty dotyczące ochrony prywatności użytkowników w trakcie projektowania nowych sieci urządzeń IoT lub analizy istniejących sieci.
Powiązane kierunkowe efekty uczenia się	U08
Kod efektu	U09
Opis	Potrafi dokonać wyboru oraz zastosować właściwe metody, techniki i narzędzia do przeprowadzenia badań bezpieczeństwa sieci urządzeń IoT.
Powiązane kierunkowe efekty uczenia się	U09
Kod efektu	U10
Opis	Potrafi pracować indywidualnie oraz współdziałać z innymi osobami w ramach prac zespołowych; potrafi kierować pracą zespołu.
Powiązane kierunkowe efekty uczenia się	U13
Kod efektu	U11
Opis	Potrafi określić kierunki dalszego uczenia się, zaplanować i zrealizować proces samokształcenia, a także ukierunkowywać innych w tym zakresie.
Powiązane kierunkowe efekty uczenia się	U14

Kompetencje społeczne

Kod efektu	K01
Opis	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści oraz do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu; jest gotów do stałego aktualizowania i wzbogacania posiadanej wiedzy.
Powiązane kierunkowe efekty uczenia się	K01

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-CBxxx-MSP-EMET
Nazwa przedmiotu	Methodological and Ethical Issues of Technoscientific Research
Wersja przedmiotu	2024Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Dyplomowanie)-Cyberbezpieczeństwo-mgr.-EITI, (Dyplomowanie)-Inżynieria Internetu Rzeczy-mgr.-EITI, (Courses in English)--eng.-EITI,(Semestr 2 modelowy)-Cyberbezpieczeństwo-mgr.-EITI,(Semestr 2 modelowy)-Inżynieria internetu rzeczy-mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	angielski
Kod etapu studiów	CB000-S2-MSP-103B
Liczba punktów ECTS	2

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Wykład	20.00 h
Ćwiczenia	10.00 h

02. Bilans ECTS

Liczba punktów ECTS	2	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	30	1.20
Godziny i ECTS związane z pracą własną studenta	30	1.20
Razem	60	2.40 (2.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	30
Inne godziny kontaktowe	0
Razem	30

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	30

03. Treści kształcenia

Część I

Wykład	1. Pojęcia związane z metodologią badań naukowych (2 h): 2. nauka i dyscypliny naukowe, 3. informacja i wiedza naukowa. 4. Modelowanie matematyczne i pomiar (3 h): – zasady modelowania matematycznego, – identyfikacja modeli matematycznych, – matematyczny metamodel pomiaru. 5. Metoda naukowa i proces badawczy (3 h): 6. pojęcia podstawowe, 7. naiwna interpretacja metody naukowej i krytyka tej interpretacji, – kontekst odkrycia i kontekst uzasadnienia, 8. niepewność wiedzy naukowej. 9. Elementy metaetyki i etyki ogólnej (2 h): 10. podstawowe pojęcia etyki i metaetyki, 11. etyka a inne obszary aktywności intelektualnej. 12. Etyczne aspekty eksperymentowania (2 h): 13. formułowanie problemu badawczego, – planowanie i przeprowadzanie eksperymentów, 14. zbieranie i obróbka danych eksperymentalnych. 15. Etyczne aspekty procesów informacyjnych w badaniach naukowych (2 h): 16. prowadzenie dyskusji technonaukowej, 17. ochrona własności intelektualnej, – recenzowanie prac naukowych, 18. wnioskowanie o środki na badania. 19. Etyczne aspekty użytkowania nowych technik (2 h): 20. zarys problematyki etycznej związanej z technikami, 21. problemy etyczne związane z cyberbezpieczeństwem, sztuczną inteligencją i robotyką. 22. Sprawdziany (4 h): – Sprawdzian 1 i Sprawdzian1 dotyczące pierwszej połowy wykładu, –Sprawdzian 2 i Sprawdzian 2 dotyczące drugiej połowy wykładu.

Część I

Ćwiczenia	**Contents of lectures (16 h):** • Basic concepts of research methodology (2 h): • science and sciences • scientific information and scientific knowledge • Mathematical modelling and measurement (3 h): • principles of mathematical modelling, • identification of mathematical models • mathematical meta-model of measurement • Scientific method and research process (3 h): • basic concepts and approaches • naïve understanding of scientific method and its critics • context of discovery and context of justification • uncertainty of scientific knowledge • Elements of meta-ethics and general ethics (2 h): • basic concepts of ethics and meta-ethics • relation of ethics to other forms of intellectual activity. • Ethical aspects of key research operations (2 h): • formulation of a research problem • design and execution of experiments • acquisition and processing of experimental data • Ethical aspects of research-related information processes (2 h): • technoscientific discussion • protection of intellectual property • reviewing process • research grant application • Ethical aspects of new technologies (2 h): • basic approaches of ethical problems related to new technologies • ethical issues related to cybersecurity, AI and robotics • **Contents of tutorials (10 h):** • Art and science of meta-scientific discourse (2h) • Modern approaches to research methodology (2h) • Methodological issues related to scientific justification (2h) • Ethical dilemmas related to data processing and publication (2h) • Ethical dilemmas related to new technologies (2h) • **Contents of tests (4 h):** • Class Test.1 and Class Test .1. cover the first half of the contents of lectures • Class Test .2 and Class Test .2. cover the second half of the contents of lectures

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Ma wiedzę dotyczącą: – pojęć metodologii badań, – modelowania matematycznego i pomiaru, – metody naukowej i procesu badawczego.
Powiązane kierunkowe efekty uczenia się	W03, W05
Kod efektu	W02
Opis	Ma wiedzę dotyczącą: –najważniejszych pojęć etyki i metaetyki, – etycznych aspektów pracy inżyniera, – etycznych aspektów procesów informacyjnych związanych z działalnością badawczorozwojową, – etycznych aspektów ochrony własności intelektualnej, – etycznych aspektów wykorzystywania technik informacyjnych w działalności badawczorozwojowej.
Powiązane kierunkowe efekty uczenia się	W10, W11, W12

Część I

Umiejętności

Kod efektu	U01
Opis	Potrafi: – identyfikować i krytycznie analizować problemy metodologiczne i etyczne związane z działalnością badawczo-rozwojową, – podchodzić metodycznie do dylematów etycznych związanych z działalnością badawczo-rozwojową, – omawiać problemy etyczne związane z działalnością badawczo-rozwojową i bronić własnej postawy etycznej.
Powiązane kierunkowe efekty uczenia się	U01, U08, U11, U12
Kod efektu	U02
Opis	Potrafi porozumiewać się w języku angielskim, w szczególności na temat metodologicznych i etycznych problemów badań technonaukowych.
Powiązane kierunkowe efekty uczenia się	U12

Kompetencje społeczne

Kod efektu	K01
Opis	Jest: – bardziej wrażliwy na wartości moralne związane z działalnością badawczo- rozwojową, – lepiej przygotowany do podejmowania odpowiedzialności za działalność badawczorozwojową, – lepiej przygotowany do rozwiązywania dylematów etycznych pojawiających się w praktyce badawczo-rozwojowej, – bieglejszy w kształtowaniu indywidualnej postawy etycznej w odniesieniu do działalności badawczo-rozwojowej, – bardziej skłonny do systematycznej refleksji nad etycznymi aspektami życia codziennego.
Powiązane kierunkowe efekty uczenia się	K01, K03, K04

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-ARxxx-DSP-MISK
Nazwa przedmiotu	Modelowanie i symulacja komputerowa
Wersja przedmiotu	2024L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty zaawansowane)-Automatyka i robotyka-dr.-EITI,(Przedmioty zaawansowane obieralne)-Automatyka i robotyka-mgr.-EITI,(Przedmioty zaawansowane)-Automatyka i robotyka-mgr.-EITI,(Przedmioty obieralne)-Cyberbezpieczeństwo-mgr.-EITI,(Przedmioty zaawansowane techniczne)--mgr.-EITI,(Przedmioty techniczne)---EITI
Status przedmiotu	Wybieralny
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S2-MSP-103B
Liczba punktów ECTS	5

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	30.00 h
Wykład	30.00 h

02. Bilans ECTS

Liczba punktów ECTS	5	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	75	3.00
Godziny i ECTS związane z pracą własną studenta	50	2.00
Razem	125	5.00

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	60
Inne godziny kontaktowe	15
Razem	75

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	50

03. Treści kształcenia

Część I

Wykład	Wykład składa się z czterech części. Część pierwsza dotyczy zagadnień ogólnych modelowania matematycznego, tworzenia modeli systemów oraz budowy modeli symulacyjnych, bliźniaków cyfrowych i emulatorów. Szczególna uwaga jest zwrócona na modelowanie systemów zdarzeń dyskretnych. Przedstawione są trzy sposoby prezentacji graficznej układów dynamicznych. Część druga jest poświęcona technikom symulacji. Omówione są różne techniki symulacyjne, etapy tworzenia i weryfikacji modeli symulacyjnych, metody wnioskowania statystycznego, planowania eksperymentu, symulacja metodą Monte Carlo oraz metoda bootstrap. Zaprezentowane są techniki projektowania symulatorów w wersji równoległej i rozproszonej. Część trzecia jest poświęcona prezentacji przykładowych zastosowań symulacji komputerowej w projektowaniu, optymalizacji, komputerowej analizie systemów sterowania oraz systemach wspomagania decyzji i planowania. Uwaga koncentruje się na przykładach zastosowań w złożonych strukturach sterowania systemem wodnym, systemach kolejkowych, sieciach komputerowych, w tym mobilnych sieciach ad hoc, sieciach społecznych i innych. Przedstawione jest zastosowanie modeli symulacyjnych w złożonych zadaniach optymalizacji. Omówiony jest schemat symulator-optymalizator oraz podstawowe algorytmy do rozwiązywania tak sformułowanych problemów, w tym heurystyki i metaheurystyki. Część czwarta wykładu jest poświęcona architekturze blockchain, krypto walucie Bitcoin oraz wybranym technologiom blockchain. 1. Wprowadzenie do modelowania i symulacji. 2. Klasyfikacja modeli i metody opisu. 3. Budowa modeli symulacyjnych. 4. Techniki symulacyjne. 5. Rozproszona symulacja zdarzeń dyskretnych. 6. Wnioskowanie statystyczne w badaniach symulacyjnych 7. Modelowanie eksperymentów losowych i ocena wyników symulacji. 8. Symulacja komputerowa w projektowaniu układów sterowania i sterowaniu operacyjnym. 9. Układ symulator-optymalizator – metody obliczeniowe. 10. Symulacyjna analiza systemów kolejkowych. 11. Metody analityczne i symulacja analiza sieci społecznych. 12. Modelowanie i symulacja sieci ad hoc. 13. Technologia Blockchain. Krypto waluta Bitcon.
Projekt	Wykonanie symulatora dla zadanego przykładu (np. systemy robotyczne, inteligentne miasto, sieci mobilne ad hoc, sieci bezprzewodowych czujników, klastry obliczeniowe). Aplikacja będzie mogła być zrealizowana w jednym z wybranych języków programowania bądź z wykorzystaniem udostępnionego lub wybranego przez studenta środowiska do symulacji.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Wiedza na temat modelowania i symulacji komputerowej systemów fizycznych, w tym na temat budowy modeli formalnych, konstruowania modeli symulacyjnych, środowisk informatycznych do symulacji.
Powiązane kierunkowe efekty uczenia się	W01, W04

Część I

Kod efektu	W02
Opis	Znajomość różnych technik symulacji komputerowej, możliwości i obszaru zastosowań współczesnych narzędzi do symulacji.
Powiązane kierunkowe efekty uczenia się	W09, W10
Kod efektu	W03
Opis	Wiedza jak opracować oraz przeprowadzić eksperyment symulacyjny i przedstawić jego wyniki.
Powiązane kierunkowe efekty uczenia się	W01, W04, W09

Umiejętności

Kod efektu	U01
Opis	Umiejętność pozyskiwania informacji z literatury krajowej i zagranicznej oraz dostępnych baz danych.
Powiązane kierunkowe efekty uczenia się	U01, U02
Kod efektu	U02
Opis	Umiejętność sformułowania modelu formalnego i przygotowania projektu modelu symulacyjnego procesów zachodzących w systemie.
Powiązane kierunkowe efekty uczenia się	U03, U04, U05
Kod efektu	U03
Opis	Umiejętność zaprojektowania i wykonania systemu oprogramowania do symulacji komputerowej.
Powiązane kierunkowe efekty uczenia się	U07, U09
Kod efektu	U04
Opis	Umiejętność przeprowadzenia eksperymentu symulacyjnego, dokonania analizy wyników i udokumentowania ich.
Powiązane kierunkowe efekty uczenia się	U05, U06, U07

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-INISY-MSP-WSO
Nazwa przedmiotu	Wirtualne środowiska obliczeniowe
Wersja przedmiotu	2022Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty obieralne)-Cyberbezpieczeństwo-mgr.-EITI, (Wytwarzanie)-Inteligentne systemy-mgr.-EITI,(Przedmioty zaawansowane techniczne)--mgr.-EITI,(Przedmioty techniczne)---EITI
Status przedmiotu	Wybieralny
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S2-MSP-103B
Liczba punktów ECTS	4

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Wykład	30.00 h
Projekt	15.00 h

02. Bilans ECTS

Liczba punktów ECTS	4	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	50	1.80
Godziny i ECTS związane z pracą własną studenta	50	2.80
Razem	100	4.60 (4.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	45
Inne godziny kontaktowe	5
Razem	50

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	50

03. Treści kształcenia

Część I

Wykład	Wykład: • Wprowadzenie do zagadnień związanych z wirtualizacją i konteneryzacją, przykłady typowych architektur klastrowych i chmurowych, systemy operacyjne, przykłady zastosowań • Wirtualizacja: rodzaje wirtualizacji, zasada działania, tworzenie obrazów systemów, standardy, typowe operacje: migracja, klonowanie, metody przydzielania zasobów: thin provisioning. • Omówienieczęsto stosowanych środowisk wirtualizacyjnych: KVM, VMWare, Xen – porównanie architektur i możliwości, przykłady zastosowania. • Zagadnienia związane z przygotowaniem pamięci dyskowej – technologie: RAID, JBOD, LVM, macierze dyskowe, rozproszone systemy plików – zasady wykorzystania i projektowania, technologie transmisji danych, przechowywanie danych blokowych i plikowych, przykłady wykorzystania. • Organizacja sieci dla klastrów i chmur: przegląd technologii sieciowych (Ethernet 1/10/100Gb, InfiniBand, sieci dla pamięci masowych), topologie sieci w ramach klastra – metody zapewnienia wysokiej dostępności, wydajności i skalowalności. Wykorzystanie redundancji łącz i urządzeń sieciowych, przegląd typowych topologie sieci. • Sieci wirtualne w ramach pojedynczego gospodarza wirtualizacji - zarządzanie w warstwie 2 ISO/OSI. Wykorzystanie protokołów: 802.1Q (sieci wirtualne VLAN), 802.1ad (Q-in-Q). Wykorzystanie możliwości warstwy 3 ISO/OSI: ruting statyczny i dynamiczny, polityki rutingowe, kształtowanie i filtrowanie ruchu - elementy bezpieczeństwa. Porównanie technologii dla KVM i VMWare. • Budowa sieci dla klastra, wykorzystanie narzędzi dla uproszczenia zarządzania i automatyzacji provisioningu. Sieci definiowane programowo (SDN) - wykorzystanie w dużych klastrach – przegląd jakiś rozwiązań: OpenFlow, VMWare NSX • Zagnieżdżona wirtualizacja: przykłady, problemy: ograniczenia w budowie sieci wirtualnych. • Systemy zarządzania klastrami i chmurami: OpenStack, oVirt • Konteneryzacja: zasada, przykłady rozwiązań: Docker, Kubernetes. • Modelowanie środowisk klastrowych i chmurowych, wybrane metody optymalizacji przydziału zasobów i alokacji zadań. Równoważenie obciążeń i szeregowanie zadań jako metody bezpośredniego sterowania wydajnością. • Symulacja środowisk klastrowych i chmurowych. Symulator Cloudsim. • Zagadnienie związane z oszczędnością energii: sterowanie wydajnością na poziomie procesora, systemu operacyjnego i klastra. Przykłady definicji i metod rozwiązania zadań. Uwzględnienie zużycia energii przez sieć. Przegląd technologii i standardów związanych z energooszczędnością: ACPI, 802.3az, energooszczędne sterowniki procesora w Linuksie, energooszczędne topologie sieci.

Część I

Projekt	Projekt polega na zaprojektowaniu i implementacji w postaci prototypu o ograniczonych możliwościach lub modułu symulatora wybranych fragmentów typowego systemu wykorzystującego architekturę klastra bądź chmury. W realizacji projektu mogą być wykorzystane elementy rozwiązań rozwijanych przez zespół autorski w ramach prowadzonych projektów badawczych takie jak np. energooszczędne algorytmy przydziału zasobów. Przykładowe tematy projektu: • Projekt 1: Zaprojektuj architekturę klastra dla systemu przetwarzającego dane z dużego zestawu czujników. Architektura powinna uwzględniać możliwość wydajnego zapisywania i udostępniania danych do dalszej obróbki, oraz wysoką skalowalność. Sprawdź istotne założenia architektury wdrażając kluczowe elementy w ograniczonym środowisku (pojedynczy komputer z wirtualiztorem). • Projekt 2: Zaprojektuj architekturę małego klastra umożliwiającego przetwarzanie zadań obliczeniowych w ramach pewnej organizacji. Zadbaj o wysoki poziom bezpieczeństwa i niskie koszty operacyjne. Sprawdź istotne założenia architektury wdrażając kluczowe elementy w ograniczonym środowisku (pojedynczy komputer z wirtualiztorem). • Projekt 3: Zaimplementuj wskazany algorytm szeregowania zadań w symulatorze CloudSim. • Projekt 4: Zaimplementuj wskazany algorytm alokacji zasobów w symulatorze CloudSim.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Zna zagadnienia związane z metodami alokacji zadań w klastrach i chmurach.
Powiązane kierunkowe efekty uczenia się	W01, W02, W04
Kod efektu	W02
Opis	Zna zagadnienia związane z wirtualizacją i konteneryzacją.
Powiązane kierunkowe efekty uczenia się	W01, W02, W04
Kod efektu	W03
Opis	Zna metody służące zapewnieniu bezpieczeństwa w rozproszonych środowiskach obliczeniowych. Zna metody pozwalające ograniczyć zużycie energii przez systemy komputerowe
Powiązane kierunkowe efekty uczenia się	W03, W06, W08

Umiejętności

Kod efektu	U01
Opis	Potrafi kierować pracą zespołu oraz współdziałać z innymi osobami w ramach prac zespołowych
Powiązane kierunkowe efekty uczenia się	U13
Kod efektu	U02
Opis	Potrafi zastosować odpowiednie metody alokacji zadań
Powiązane kierunkowe efekty uczenia się	U11, U14
Kod efektu	U03
Opis	Potrafi zweryfikować przez symulację bądź eksperyment obliczeniowy efektywność algorytmów zarządzania klastrem obliczeniowym

Część I

Powiązane kierunkowe efekty uczenia się	U06, U07, U09
Kod efektu	U04
Opis	Potrafi dobierać odpowiednią technologie umożliwiającą wydajną i ekonomiczną budowę środowisk obliczeniowych poprzez m.in. właściwe wymiarowanie zasobów sprzętowych.
Powiązane kierunkowe efekty uczenia się	U06, U07, U09
Kod efektu	U05
Opis	Potrafi przeprowadzić testy zaproponowanego rozwiązania i wyciągać wnioski odnośnie jego skalowalności.
Powiązane kierunkowe efekty uczenia się	U06, U07, U09
Kod efektu	U06
Opis	Potrafi projektować środowiska obliczeniowe wykorzystujące wirtualizację i konteneryzację
Powiązane kierunkowe efekty uczenia się	U06, U07, U09

Kompetencje społeczne

Kod efektu	K01
Opis	Poprzez wprowadzenie nawyku praktycznego weryfikowania dokumentacji poprzez prowadzenie testów i korzystanie z doświadczeń społeczności użytkowników i ekspertów jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści
Powiązane kierunkowe efekty uczenia się	K01
Kod efektu	K02
Opis	Poprzez świadome wymiarowanie projektowanych rozwiązań i wprowadzanie algorytmów energooszczędnych minimalizuje koszty i oddziaływanie na środowisko
Powiązane kierunkowe efekty uczenia się	K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103X-xxxxx-MSP-SDM2
Nazwa przedmiotu	Seminarium dyplomowe magisterskie 2
Wersja przedmiotu	2024L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Dyplomowanie)--mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S3-MSP-103B
Liczba punktów ECTS	2

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Seminarium	30.00 h

02. Bilans ECTS

Liczba punktów ECTS	2	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	40	1.60
Godziny i ECTS związane z pracą własną studenta	20	0.40
Razem	60	2.00

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	30
Inne godziny kontaktowe	10
Razem	40

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	20

03. Treści kształcenia

Część I

Seminarium	1. Wykład na temat "po co i jak piszemy pracę magisterską i prezentację", tekst techniczny a tekst naukowy. 2. Przygotowanie streszczenia do swoich prac magisterskich i wspólna (całą grupą dziekańską) praca nad ich redakcją - merytoryczną, logiczną, gramatyczną. 3. Opracowanie prezentacji na obronę pracy a następnie wspólna (całą grupą dziekańską) praca pod nadzorem koordynatora nad redakcją - merytoryczną, logiczną, gramatyczną i wizualną. 4. Opracowanie własnej publikację konferencyjnej na „pozorowaną” konferencję, przy spełnieniu wszystkich formalizmów „prawdziwej” publikacji (recenzje p2p, umieszczanie materiałów na serwerze wydawnictwa, itd.). 5. Jak przygotować recenzje? Recenzja trzech prac konferencyjnych pod okiem koordynatora seminarium. 6. Omawianie w/w publikacji i ich recenzji

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Student wie w jaki sposób przeprowadzić eksperyment poprawny z punktu widzenia metodologii badań naukowych
Powiązane kierunkowe efekty uczenia się	W01, W02
Kod efektu	W02
Opis	Student zna i rozumie podstawy metodologii badań naukowych w dyscyplinach powiązanych z kierunkiem
Powiązane kierunkowe efekty uczenia się	W03, W04

Umiejętności

Kod efektu	U01
Opis	Student potrafi wykorzystywać wybrane teorie, metody i narzędzia w praktyce projektowania i realizacji badań.
Powiązane kierunkowe efekty uczenia się	U06, U07, U08
Kod efektu	U02
Opis	Student potrafi prowadzić prace badawcze w celu przygotowania pracy magisterskiej
Powiązane kierunkowe efekty uczenia się	U05
Kod efektu	U03
Opis	Student potrafi przygotować krótki dokument techniczny lub doniesienie naukowe w języku angielskim
Powiązane kierunkowe efekty uczenia się	U01, U10, U11
Kod efektu	U04
Opis	Student potrafi stawiać hipotezy badawcze i poddawać je weryfikacji
Powiązane kierunkowe efekty uczenia się	U02, U04, U09

Kompetencje społeczne

Kod efektu	K01
Opis	Absolwent jest gotów do uzasadniania własnych poglądów w pracy magisterskiej i innych formach komunikacji.
Powiązane kierunkowe efekty uczenia się	K01, K02, K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103X-xxxxx-MSP-PDYM
Nazwa przedmiotu	Przygotowanie pracy dyplomowej magisterskiej
Wersja przedmiotu	2024L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Dyplomowanie)--mgr.-EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S3-MSP-103B
Liczba punktów ECTS	20

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	150.00 h

02. Bilans ECTS

Liczba punktów ECTS	20	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	150	12.00
Godziny i ECTS związane z pracą własną studenta	350	12.00
Razem	500	24.00 (20.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	150
Inne godziny kontaktowe	0
Razem	150

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	350

03. Treści kształcenia

Część I

Treści kształcenia	Przygotowanie Pracy Dyplomowej Magisterskiej to najintensywniejsza część procesu dyplomowania. W ramach zajęć w zależności od specyfiki realizowanej pracy wykonywane są zasadnicze działania badawcze z wykorzystaniem przewidzianej bazy dydaktycznej (aparatura pomiarowa, systemy komputerowe i pomiarowe, specjalistyczne oprogramowanie, itp.). Uzyskane rezultaty prac na bieżąco poddawane są analizie i weryfikacji. We współpracy z Promotorem, podejmowane są decyzje o sposobie opisu i wykorzystania uzyskanych wyników w pracy magisterskiej. Oceniana jest zgodność postępów prac z przyjętym harmonogramem. Uzyskane wyniki prac są na bieżąco oceniane przez Promotora. Ich końcowym efektem jest zredagowana praca magisterska przygotowana do przeprowadzenia obrony

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Ma podbudowaną teoretycznie szczegółową wiedzę ogólną obejmującą zagadnienia związaną z tematyką dyplomowania
Powiązane kierunkowe efekty uczenia się	W02, W03
Kod efektu	W02
Opis	Ma rozszerzoną i pogłębioną wiedzę z matematyki w zakresie związanym z wybraną tematyką pracy dyplomowej
Powiązane kierunkowe efekty uczenia się	W05
Kod efektu	W03
Opis	Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu złożonych zadań inżynierskich związanych z tematyką pracy magisterskiej
Powiązane kierunkowe efekty uczenia się	W04, W05, W06
Kod efektu	W04
Opis	Zna aktualny stan wiedzy i trendy rozwojowe związane z wybraną tematyką pracy dyplomowej.
Powiązane kierunkowe efekty uczenia się	W01, W08

Umiejętności

Kod efektu	U01
Opis	Potrafi porozumiewać się przy użyciu różnych technik w środowisku zawodowym oraz w innych środowiskach, także w języku angielskim.
Powiązane kierunkowe efekty uczenia się	U10, U11, U12
Kod efektu	U02
Opis	Potrafi pozyskiwać informacje z literatury, baz danych oraz innych właściwie dobranych źródeł, także w języku angielskim; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny
Powiązane kierunkowe efekty uczenia się	U01, U02
Kod efektu	U03
Opis	Potrafi stawiać hipotezy badawcze i poddawać je weryfikacji
Powiązane kierunkowe efekty uczenia się	U09
Kod efektu	U04
Opis	Potrafi planować i przeprowadzać eksperymenty, w tym zaawansowane pomiary i symulacje komputerowe oraz opracowywać i interpretować uzyskane wyniki i wyciągać wnioski

Część I

Powiązane kierunkowe efekty uczenia się	U06, U07
Kod efektu	U05
Opis	Potrafi wykorzystać metody analityczne, symulacyjne oraz eksperymentalne do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych związanych z tematyką pracy dyplomowej.
Powiązane kierunkowe efekty uczenia się	U04
Kod efektu	U06
Opis	Potrafi przygotować i przedstawić w języku polskim i języku angielskim prezentację ustną, dotyczącą szczegółowych zagadnień z zakresu kierunku studiowania
Powiązane kierunkowe efekty uczenia się	U10, U11, U12

Kompetencje społeczne

Kod efektu	K01
Opis	Potrafi myśleć i działać kreatynie rozwiązując napotkane problemy. Potrafi także działać w zespole oraz umie przedstawić i uzasadnić przyjętą metodologię działań
Powiązane kierunkowe efekty uczenia się	K01, K02, K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-CBxxx-MSP-PROCY
Nazwa przedmiotu	Projekt badawczy w cyberbezpieczeństwie
Wersja przedmiotu	2027L
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty kierunkowe)-Cyberbezpieczeństwo-mgr.-EITI, (Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S3-MSP-103B
Liczba punktów ECTS	4

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	60.00 h

02. Bilans ECTS

Liczba punktów ECTS	4	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	70	2.80
Godziny i ECTS związane z pracą własną studenta	50	2.00
Razem	120	4.80 (4.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	60
Inne godziny kontaktowe	10
Razem	70

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	50

03. Treści kształcenia

Część I

Projekt	W ramach przedmiotu studenci dołączają do zespołów badawczych realizujących projekty naukowe w obszarze cyberbezpieczeństwa, prowadzone w warunkach odpowiadających rzeczywistemu środowisku pracy badawczej. Każdy zespół podejmuje temat badawczy wpisujący się w aktualne kierunki badań lub projekty o charakterze wdrożeniowym, obejmujące między innymi analizę podatności systemów, bezpieczeństwo aplikacji webowych, ochronę sieci, analizę incydentów bezpieczeństwa czy zastosowanie sztucznej inteligencji w systemach ochrony informacji. Na początkowym etapie pracy studenci dokonują przeglądu literatury naukowej i technicznej, aby określić stan wiedzy w danym obszarze oraz zdefiniować problem badawczy wraz z hipotezą. W kolejnych fazach uczestnicy opracowują i realizują plan badań, wykorzystując metody empiryczne, eksperymentalne lub symulacyjne, stosowane w rzeczywistych projektach naukowych i badawczo-rozwojowych. Następnie analizują uzyskane wyniki, interpretują je w kontekście przyjętych założeń oraz formułują wnioski istotne dla rozwoju dziedziny lub zastosowań praktycznych. Efektem końcowym jest opracowanie artykułu naukowego w języku polskim lub angielskim, spełniającego wymogi redakcyjne czasopism lub konferencji naukowych. **PROJEKT:** Organizacja projektu zakłada pracę studentów w niewielkich zespołach badawczych, które funkcjonują w strukturze odpowiadającej rzeczywistemu środowisku naukowemu. Każdy student w ramach zespołu realizuje część większego projektu badawczego prowadzonego w ramach jednostki naukowej lub we współpracy z partnerem zewnętrznym, dzięki czemu studenci uczestniczą w pełnym cyklu procesu badawczego – od koncepcji, przez eksperyment, aż po publikację wyników. Praca studentów odbywa się pod opieką kadry naukowej, która pełni rolę mentora, koordynując postępy i wspierając w zakresie metodologicznym, merytorycznym oraz redakcyjnym. Na początku semestru studenci wspólnie z opiekunami określają zakres projektu, plan badań, harmonogram działań oraz podział ról w zespole. Każdy uczestnik jest odpowiedzialny za wybrane zadania badawcze, takie jak analiza literatury, projektowanie eksperymentu, implementacja rozwiązań, opracowanie wyników czy przygotowanie fragmentów publikacji. Regularne spotkania projektowe umożliwiają bieżącą wymianę wiedzy, prezentację postępów oraz wspólne rozwiązywanie problemów badawczych. Praca ma charakter iteracyjny – studenci uczą się formułować hipotezy, weryfikować je za pomocą danych, a następnie krytycznie analizować rezultaty i modyfikować założenia badawcze w odpowiedzi na wyniki eksperymentów. Proces realizacji projektu kończy się przygotowaniem artykułu naukowego (w języku angielskim lub polskim) zgodnego z wymogami czasopism lub konferencji branżowych. Nacisk położony jest nie tylko na uzyskanie wyników, ale przede wszystkim na zrozumienie sposobu prowadzenia badań, ich planowania i dokumentowania. W wyniku realizacji projektu studenci nabywają szereg praktycznych umiejętności: potrafią planować i realizować badania w zespole, korzystać z nowoczesnych narzędzi analitycznych i środowisk badawczych, krytycznie interpretować dane, formułować wnioski oraz komunikować rezultaty w formie publikacji naukowej. Równocześnie rozwijają kompetencje miękkie – uczą się pracy zespołowej, zarządzania czasem i zadaniami

	oraz efektywnej komunikacji w środowisku badawczym. Celem realizowanego projektu jest nie tylko opanowanie warsztatu badawczego, lecz także rozwinięcie sposobu myślenia charakterystycznego dla współczesnego naukowca: otwartego, analitycznego, krytycznego i ukierunkowanego na rozwiązywanie problemów. Studenci uczą się samodzielności, dociekliwości oraz odpowiedzialności za jakość prowadzonych badań, co stanowi fundament ich przyszłej pracy naukowej lub zawodowej w obszarze cyberbezpieczeństwa.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Posiada – w pogłębionym stopniu – wiedzę i rozumienie podstawowych procesów zachodzących w systemach teleinformatycznych, istotne dla zapewnienia bezpiecznego funkcjonowania takich systemów
Powiązane kierunkowe efekty uczenia się	W01, W02, W06, W08
Kod efektu	W02
Opis	Posiada metodologiczne podstawy prowadzenia badań naukowych; ma wiedzę dotyczącą metodyki prowadzenia prac o charakterze badawczym w dziedzinie nauk inżynieryjno-technicznych, w szczególności związanych z badaniami z zakresu cyberbezpieczeństwa
Powiązane kierunkowe efekty uczenia się	W03, W10, W11
Kod efektu	W03
Opis	Posiada wiedzę dotyczącą zaawansowanych narzędzi informatycznych niezbędnych do analizy wyników badań
Powiązane kierunkowe efekty uczenia się	W04

Umiejętności

Kod efektu	U01
Opis	Potrafi pozyskiwać informacje z właściwie dobranych źródeł, dokonywać ich krytycznej oceny, analizy, syntezy i twórczej interpretacji, wyciągać wnioski i wyczerpująco je uzasadniać oraz przeprowadzić krytyczną analizę sposobu funkcjonowania istniejących rozwiązań technicznych z zakresu bezpieczeństwa systemów teleinformatycznych i oceniać te rozwiązania.
Powiązane kierunkowe efekty uczenia się	U01, U02, U10, U11, U13
Kod efektu	U02
Opis	Potrafi planować i przeprowadzać eksperymenty / badania, w tym symulacje komputerowe dotyczące bezpieczeństwa systemów teleinformatycznych, oraz interpretować uzyskane wyniki.
Powiązane kierunkowe efekty uczenia się	U03, U08, U10, U11, U13
Kod efektu	U03
Opis	Potrafi wykorzystać zaawansowane narzędzia informatyczne niezbędne do przeprowadzenia eksperymentów/badań związanych z zagadnieniami cyberbezpieczeństwa i analizy ich wyników.
Powiązane kierunkowe efekty uczenia się	U04, U05, U10, U11, U13
Kod efektu	U04
Opis	Potrafi – w pracach badawczych oraz przy rozwiązywaniu zadań dotyczących zapewnienia bezpieczeństwa systemów teleinformatycznych

Część I

Powiązane kierunkowe efekty uczenia się	U09, U10, U13
Kod efektu	U05
Opis	Potrafi posługiwać się językiem angielskim na poziomie przynajmniej B2+, aktywnie uczestnicząc w zajęciach prowadzonych w języku angielskim, opracowując zadania pisemne w tym języku i zapoznając się z obcojęzyczną literaturą i materiałami dostarczanymi przez prowadzącego
Powiązane kierunkowe efekty uczenia się	U12
Kod efektu	U06
Opis	Potrafi pracować indywidualnie oraz współdziałać z innymi osobami w ramach prac zespołowych; potrafi kierować pracą zespołu, określić kierunki dalszego uczenia się, zaplanować i zrealizować proces samokształcenia, a także ukierunkowywać innych w tym zakresie.
Powiązane kierunkowe efekty uczenia się	U13, U14

Kompetencje społeczne

Kod efektu	K01
Opis	Potrafi skutecznie współpracować z ekspertami zewnętrznymi i odbiorcami końcowymi rozwiązań, również spoza swojej macierzystej dyscypliny
Powiązane kierunkowe efekty uczenia się	K01, K02
Kod efektu	K02
Opis	Potrafi w klarowny sposób prezentować i popularyzować rozwiązania i strategie cyberbezpieczeństwa, również odbiorcom nietechnicznym
Powiązane kierunkowe efekty uczenia się	K02
Kod efektu	K03
Opis	Potrafi planować rozwój swoich kompetencji zawodowych oraz przewidywać i rozwijać nowe trendy z zakresu cyberbezpieczeństwa, biorąc pod uwagę ich aspekty społeczne
Powiązane kierunkowe efekty uczenia się	K03, K04

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-TLTIC-MSP-OAST
Nazwa przedmiotu	Optymalizacja i analiza sieci teleinformatycznych
Wersja przedmiotu	2024Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty zaawansowane)-Teleinformatyka i cyberbezpieczeństwo-mgr.-EITI,(Przedmioty zaawansowane obowiązkowe)-Teleinformatyka i cyberbezpieczeństwo-mgr.-EITI,(Przedmioty zaawansowane)-Telekomunikacja-dr.-EITI, (Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 2 modelowy)-Teleinformatyka i cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Wybieralny
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S3-MSP-103B
Liczba punktów ECTS	4

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	15.00 h
Wykład	15.00 h
Ćwiczenia	15.00 h

02. Bilans ECTS

Liczba punktów ECTS	4	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	52	2.08
Godziny i ECTS związane z pracą własną studenta	50	2.00
Razem	102	4.08 (4.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	45
Inne godziny kontaktowe	7
Razem	52

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	50

03. Treści kształcenia

Część I

Projekt	• Projekt 1. Wykorzystanie pakietu modelowania matematycznego AMPL oraz pakietów optymalizacyjnych CPLEX i GUROBI w celu zastosowania wprowadzonych metod optymalizacji do problemu WOST. • Projekt 2. Symulacja cyfrowa systemów teleinformatycznych. Weryfikacja użyteczności kolejkowych metod analitycznych przez porównanie ich wyników z wynikami uzyskanymi przy użyciu symulacji.˙
Ćwiczenia	• Projekt 1. Wykorzystanie pakietu modelowania matematycznego AMPL oraz pakietów optymalizacyjnych CPLEX i GUROBI w celu zastosowania wprowadzonych metod optymalizacji do problemu WOST. • Projekt 2. Symulacja cyfrowa systemów teleinformatycznych. Weryfikacja użyteczności kolejkowych metod analitycznych przez porównanie ich wyników z wynikami uzyskanymi przy użyciu symulacji.˙
Wykład	Nauczanie w ramach przedmiotu jest oparte na rozważaniu wybranych reprezentatywnych problemów (case studies) optymalizacji i analizy sieci teleinformatycznych. Każdy taki problem jest studiowany poczynając od sformułowania werbalnego, przez wprowadzenie jego modelu matematycznego (wraz z wariantami) i omówienie metod matematycznych prowadzących do jego rozwiazywania, kończąc na przykładach rozwiązań problemu dla konkretnych przypadków sieci. Przedmiot składa się z dwóch poniżej opisanych bloków programowych. • Blok 1: Optymalizacja sieci. Sieci przepływów wielotowarowych jako model matematyczny optymalizacji sieci teleinformatycznych. Zastosowanie modelu do problemów projektowania sieci dla wybranych technologii, na przykład do wymiarowania optycznych sieci transmisyjnych w technologii DWDM (problem WOST). Metody programowania liniowego (algorytm simpleks) i programowania całkowitoliczbowego (algorytm podziału i ograniczeń) w zastosowaniu do rozważanych problemów. • Blok 2: Analiza sieci. Zastosowanie podstawowych metod teorii kolejek do wybranych problemów badania wydajności i planowania zasobów w sieciach teleinformatycznych, na przykład do problemu estymacji wydajności węzła dystrybucji treści sieci CDN´ (WWDT). Zakres tematyczny: modelowanie napływu ruchu (proces Poissona), procesy urodzin i śmierci, wzór Little'a, podstawowe modele kolejkowe (M/M/1, M/M/n/m, M/G/1)´ oraz ich własności, sieci kolejek – sieci Jacksona.´

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Zna metody optymalizacji umożliwiające rozwiazywanie podstawowych problemów projektowania sieci teleinformatycznych
Powiązane kierunkowe efekty uczenia się	W01, W02
Kod efektu	W02
Opis	Zna najważniejsze pojęcia związane z modelowaniem matematycznym problemów optymalizacji sieci teleinformatycznych

Część I

Powiązane kierunkowe efekty uczenia się	W05
Kod efektu	W03
Opis	Zna podstawowe zadania optymalizacji związane z projektowaniem sieci teleinformatycznych
Powiązane kierunkowe efekty uczenia się	W02, W06
Kod efektu	W04
Opis	Zna wybrane metody matematyczne teorii kolejek, przydatne do analizy jakości działania systemów teleinformatycznych oraz wymiarowania ich zasobów
Powiązane kierunkowe efekty uczenia się	W05

Umiejętności

Kod efektu	U01
Opis	Potrafi sformułować zadania optymalizacji związane z projektowaniem sieci teleinformatycznych
Powiązane kierunkowe efekty uczenia się	U01, U02, U03
Kod efektu	U02
Opis	Potrafi wykorzystać odpowiednie metody optymalizacji do rozwiazywania podstawowych problemów projektowania sieci teleinformatycznych
Powiązane kierunkowe efekty uczenia się	U03
Kod efektu	U03
Opis	Umie ocenić efektywność potencjalnych metod optymalizacji w zastosowaniu do zadań optymalizacji związanych z projektowaniem sieci teleinformatycznych
Powiązane kierunkowe efekty uczenia się	U01, U02, U03
Kod efektu	U04
Opis	Umie zweryfikować skuteczność metod optymalizacji dla konkretnego zadania projektowania sieci teleinformatycznych
Powiązane kierunkowe efekty uczenia się	U01, U02, U03
Kod efektu	U05
Opis	Potrafi wykorzystać wybrane metody matematyczne teorii kolejek do analizy jakości działania systemów teleinformatycznych oraz wymiarowania ich zasobów
Powiązane kierunkowe efekty uczenia się	U02, U03
Kod efektu	U06
Opis	Potrafi zweryfikować zakres stosowalności poznanych modeli kolejkowych (przez porównanie z wynikami otrzymanymi przy wykorzystaniu symulacji cyfrowej)
Powiązane kierunkowe efekty uczenia się	U08, U09
Kod efektu	U07
Opis	Umie pozyskiwać informacje z literatury (głównie anglojęzycznej) dotyczące zagadnień rozwiązywanych w ramach zadań projektowych oraz krytycznie je analizować
Powiązane kierunkowe efekty uczenia się	U10
Kod efektu	U08
Opis	Potrafi przygotować i przedstawić prezentację dotyczącą uzyskanych wyników
Powiązane kierunkowe efekty uczenia się	U10, U11, U13

Kompetencje społeczne

Kod efektu	K01

Część I

Opis	Potrafi krytycznie analizować informacje pochodzące z różnych źródeł
Powiązane kierunkowe efekty uczenia się	K01, K03

SYLABUS PRZEDMIOTU

Kod przedmiotu	103A-TLTIC-MSP-SIS
Nazwa przedmiotu	Systemy i sieci światłowodowe
Wersja przedmiotu	2024Z
Poziom kształcenia	drugiego stopnia
Forma i tryb prowadzenia studiów	stacjonarne
Profil studiów	Ogólnoakademicki
Kierunek studiów	Cyberbezpieczeństwo
Specjalność	-
Jednostka prowadząca	Wydział Elektroniki i Technik Informacyjnych
Jednostka realizująca	Wydział Elektroniki i Technik Informacyjnych
Blok przedmiotów	nd
Grupy przedmiotów	(Przedmioty zaawansowane)-Teleinformatyka i cyberbezpieczeństwo-mgr.-EITI,(Przedmioty zaawansowane obowiązkowe)-Teleinformatyka i cyberbezpieczeństwo-mgr.-EITI,(Przedmioty zaawansowane techniczne)--mgr.-EITI, (Przedmioty techniczne)---EITI,(Semestr 3 modelowy)-Teleinformatyka i cyberbezpieczeństwo-mgr.-EITI
Status przedmiotu	Wybieralny
Język prowadzenia zajęć	polski
Kod etapu studiów	CB000-S3-MSP-103B
Liczba punktów ECTS	4

Część I

01. Efekty uczenia się i sposób prowadzenia zajęć

Efekty uczenia się	patrz tabela "Efekty uczenia się"

Formy zajęć i ich wymiar w semestrze

Projekt	30.00 h
Wykład	15.00 h

02. Bilans ECTS

Liczba punktów ECTS	4	
Rozliczenie godzinowo - punktowe przedmiotu	**Godziny**	**ECTS**

Liczba godzin i ECTS pracy studenta:

Godziny i ECTS za zajęcia związane z bezpośrednim udziałem nauczycieli akademickich	53	2.12
Godziny i ECTS związane z pracą własną studenta	50	2.00
Razem	103	4.12 (4.00)

Liczba godzin związanych z bezpośrednim udziałem nauczycieli akademickich:

Godziny związane z udziałem w zajęciach	45
Inne godziny kontaktowe	8
Razem	53

Liczba godzin związanych z pracą własną studenta:

Godziny przeznaczone na pracę własną studenta	50

03. Treści kształcenia

Część I

Wykład	1. Wprowadzenie Powtórzenie podstawowych wiadomości z transmisji światłowodowej: typy i właściwości światłowodów, podstawowe komponenty światłowodowego systemu transmisyjnego. 2. Systemy i sieci Budowa i właściwości użytkowe systemów światłowodowych takich jak PON, WDM czy OTN. 3. Transmisja koherentna Układy optycznych nadajników i odbiorników koherentnych. Cyfrowe przetwarzanie sygnałów w transmisji koherentnej. Budowa koherentnego systemu transmisyjnego. 4. RoF Światłowodowa transmisja sygnałów analogowych (RoF). Budowa systemu RoF i jego właściwości. Zastosowania i kierunki rozwoju RoF. 5. Bezpieczeństwo Techniki podsłuchu i możliwości zakłócenia pracy w transmisji światłowodowej. Metody wykrywania i przeciwdziałania zagrożeniom. Kryptografia i komunikacja kwantowa. 6. Systemy i sieci Budowa i właściwości użytkowe systemów światłowodowych takich jak PON, WDM czy OTN.
Projekt	• Projekt 1: Każdy z uczestników dostaje jedno lub dwa zagadnienia obliczeniowe (zadania) do samodzielnego rozwiązania, a następnie prezentuje swoje rozwiązania całej grupie w ramach zajęć projektowych. W dyskusji grupa ocenia poprawność rozwiązania. • Projekt 2: Każdy z uczestników dostaje do rozwiązania zagadnienie wymagające obliczeń wspomaganych komputerowo. Jego/jej zadaniem jest napisanie odpowiedniego oprogramowania w wybranym przez siebie środowisku, które rozwiązuje postawiony problem. W trakcie indywidulanych konsultacji prowadzący przeprowadza dyskusję na temat zastosowanego rozwiązania i sprawdza jego poprawność.

Tabela: Efekty uczenia się

Wiedza

Kod efektu	W01
Opis	Ma pogłębioną wiedzę teoretyczną z zakresu najważniejszych typów sieci telekomunikacji optycznej, a także działania kluczowych ich elementów wraz z określeniem ich roli
Powiązane kierunkowe efekty uczenia się	W01, W02
Kod efektu	W02
Opis	Ma pogłębioną wiedzę teoretyczną dotyczącą czynników ograniczających możliwości zastosowań poszczególnych elementów optycznych w sieciach i stopnia ich narażenia na ataki, a także ograniczeniach samej transmisji optyczne
Powiązane kierunkowe efekty uczenia się	W01, W02
Kod efektu	W03
Opis	Zna i rozumie aparat matematyki wyższej, w tym rachunek różniczkowo-całkowy, pozwalający obliczyć parametry transmitowanych sygnałów dla typowych systemów i sieci używanych w telekomunikacji optycznej
Powiązane kierunkowe efekty uczenia się	W05

Umiejętności

Kod efektu	U01

Część I

Opis	Potrafi zaprojektować złożony system transmisyjny przy uwzględnieniu najważniejszych zjawisk
Powiązane kierunkowe efekty uczenia się	U06, U07
Kod efektu	U02
Opis	Potrafi pozyskiwać informacje z literatury (głównie anglojęzycznej) dotyczące wybranych szczegółowych zagadnień na temat sieci telekomunikacji optycznej i ich bezpieczeństwa oraz krytycznie je analizować
Powiązane kierunkowe efekty uczenia się	U01
Kod efektu	U03
Opis	Potrafi rozwiązać postawione złożone zadanie projektowe dotyczące modelowania zjawisk zachodzących w sieciach telekomunikacji optycznej i ich narażenia na ataki, a wymagające syntezy metod analitycznych i symulacji/ obliczeń komputerowych
Powiązane kierunkowe efekty uczenia się	U02, U03, U09

Kompetencje społeczne

Kod efektu	K01
Opis	Potrafi przygotować i przedstawić prezentację oraz prowadzić dyskusję dotyczącą uzyskanych wyników projektu.
Powiązane kierunkowe efekty uczenia się	K01, K02
Kod efektu	K02
Opis	Ma orientację zawodową w obszarze systemów i sieci optycznych i jest świadomy procesu uczenia się w kierunku zwiększania kompetencji w tym obszarze
Powiązane kierunkowe efekty uczenia się	K01