Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Algebra liniowa z geometrią analityczną** A
Nazwa w języku angielskim: **Linear algebra with analytic geometry A**
Kierunek studiów: **Telekomunikacja, Teleinformatyka, Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy): **……..**
Poziom i forma studiów: **I stopień / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu: **obowiązkowy / ~~wybieralny~~ / ~~ogólnouczelniany~~**
Kod przedmiotu: **W04CBE-SI0038G**
Grupa kursów **TAK / ~~NIE*~~**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75	75			
Forma zaliczenia	Egzamin	Zaliczenie na ocenę			
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**6**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-	2			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,4	1,3			

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

Znajomość matematyki odpowiadająca wymaganiom na egzaminie maturalnym na poziomie rozszerzonym.

CELE PRZEDMIOTU

C1. Przedstawienie podstaw teorii liczb zespolonych, wielomianów i funkcji wymiernych.
C2. Przedstawienie podstawowych struktur algebraicznych: przestrzeń liniowa, grupa, pierścień, ciało.
C3. Przedstawienie podstawowych twierdzeń i technik o charakterze algorytmicznym dotyczących teorii układów równań liniowych.
C4. Przedstawienie podstawowych pojęć dotyczących działań na macierzach, wektorów i wartości własnych macierzy.
C5. Prezentacja podstawowych pojęć geometrii analitycznej w przestrzeni trójwymiarowej.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ
Z zakresu wiedzy student: PEU_W01 zna podstawowe metody rozwiązywania równań liniowych PEU_W02 zna podstawowe własności liczb zespolonych PEU_W03 zna podstawowe własności algebraiczne wielomianów PEU_W04 zna metody opisu prostych i płaszczyzn. **Z zakresu umiejętności student:** PEU_U01 potrafi dodawać i mnożyć macierze, obliczać wyznaczniki PEU_U02 potrafi rozwiązywać układy równań liniowych PEU_U03 potrafi wyznaczać wektory i wartości własne macierzy PEU_U04 potrafi przeprowadzać obliczenia z wykorzystaniem liczb zespolonych PEU_U05 potrafi wyznaczać równania płaszczyzn i prostych w przestrzeni. **Z zakresu kompetencji społecznych student:** PEU_K01 stara się precyzyjnie wysławiać i jest zdolny przekazywać informacje danej grupie PEU_K02 rozumie konieczność samodzielnej pracy

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		**Liczba godzin**
Wy1	Elementy logiki matematycznej. Indukcja matematyczna. Wzór dwumianowy Newtona.	1
Wy2	Struktury algebraiczne: grupa. ciało. Ciało liczb zespolonych. Postać algebraiczna liczby zespolonej. Liczba sprzężona. Działania na liczbach zespolonych.	2
Wy3	Interpretacja geometryczna liczby zespolonej. Moduł i argument liczby zespolonej. Postać trygonometryczna i wykładnicza liczby zespolonej. Wzór de Moivre'a. Pierwiastek n-tego stopnia z liczby zespolonej.	3
Wy4	Pojęcie wielomianu. Pierwiastki wielomianów. Twierdzenie Bezout. Zasadnicze twierdzenie algebry.	2
Wy5	Dzielnik liniowy i kwadratowy wielomianu rzeczywistego. Rozkład wielomianu na czynniki stopnia co najwyżej drugiego. Pojęcie funkcji wymiernej. Rozkład funkcji wymiernej na rzeczywiste ułamki proste.	2
Wy6	Przestrzenie wektorowe. Podprzestrzenie. Liniowa niezależność wektorów. Baza przestrzeni wektorowej. Przestrzeń Euklidesa.	1

Wy7	Pojęcie macierzy. Działania na macierzach. Macierz transponowana. Macierze: trójkątna, symetryczna, diagonalna.	1
Wy8	Obliczanie wyznacznika macierzy z zastosowaniem wzoru Sarrusa, rozwinięcia Laplace'a. Własności wyznaczników. Macierz nieosobliwa. Operacjie elementarne na macierzach. Twierdzenie Cauchy'ego.	2
Wy9	Pojęcie macierzy odwrotnej. Metody wyznaczania macierzy odwrotnych: metoda dopełnień algebraicznych, metoda bezwyznacznikowa. Własności macierzy odwrotnych. Równania macierzowe. Rząd macierzy. Wybrane zastosowania wyznaczników, związki z rzędem i odwracalnością macierzy	3
Wy10	Układ równań liniowych i ich związek z równaniami macierzowymi. Twierdzenie Kroneckera-Capellego. Wzory Cramera. Metoda eliminacji Gaussa.	3
Wy11	Funkcje i odwzorowania liniowe. Wektory i wartości własne. Diagonalizacja macierzy.	2
Wy12	Geometria analityczna w przestrzeni R^3. Działania na wektorach. Długość wektora. Iloczyny: skalarny, wektorowy, mieszany i ich zastosowania.	2
Wy13	Niekartezjańskie układy współrzędnych. Współrzędne sferyczne i cylindryczne (walcowe).	2
Wy14	Płaszczyzna. Wektor normalny. Równanie płaszczyzny: ogólne, parametryczne, wyznacznikowe. Prosta. Równanie prostej: parametryczne, kierunkowe, krawędziowe.	2
Wy15	Wzajemne położenie płaszczyzn i prostych. Odległość punktu od prostej i od płaszczyzny. Rzut punktu na prostą i na płaszczyznę.	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Cw1	Przekształcanie wyrażeń algebraicznych. Wzór dwumianowy Newtona.	1

Cw2	Działania na liczbach zespolonych.	2
Cw3	Wyznaczanie postaci trygonometrycznej i wykładniczej liczb zespolonych. Interpretacja geometryczna liczby zespolonej.	2
Cw4	Potęgowanie i pierwiastkowanie liczb zespolonych. Rozwiązywanie równań, nierówności i układów liniowych w ciele liczb zespolonych.	2
Cw5	Wyznaczanie pierwiastków wielomianów o współczynnikach rzeczywistych i zespolonych. Rozkład wielomianu na czynniki liniowe.	2
Cw6	Rozkład funkcji wymiernych na sumę wielomianów i ułamków prostych.	1
Cw7	Działania na macierzach.	1
Cw8	Obliczanie własności wyznaczników metodą: Sarrusa i z zastosowaniem wzoru na rozwinięcie Laplace'a. Wyznaczanie macierzy odwrotnych. Równania macierzowe.	2
Cw9	Kolokwium.	1
Cw10	Rozwiązywanie układów równań liniowych metodą macierzy odwrotnej i metodą Cramera.	3
Cw11	Obliczanie rzędu macierzy. Rozwiązywanie układów równań liniowych metodą eliminacji Gaussa i z wykorzystaniem twierdzenia Kroneckera-Capellego.	3
Cw12	Wyznaczanie wektorów i wartości własnych macierzy. Diagonalizacja macierzy.	2
Cw13	Działania na wektorach. Wyznaczanie iloczynów (skalarnego, wektorowego, mieszanego). Zastosowania iloczynów: skalarnego, wektorowego i mieszanego.	2
Cw14	Wyznaczanie równań płaszczyzn, prostych, rzutów na proste i płaszczyzny. Badanie wzajemnego położenia płaszczyzn i prostych.	4
Cw15	Kolokwium	2
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład – metoda tradycyjna. N2. Ćwiczenia problemowe i rachunkowe – metoda tradycyjna. N3. Praca własna studenta. N4. Konsultacje.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01,PEU_W02, PEU_W03, PEU_W04	Aktywność na wykładach, egzamin pisemny.

F2	PEU_U01, PEU_U02, PEU_U03, PEU_U04, PEU_U05, PEU_K01, PEU_K02	Aktywność na ćwiczeniach, Zaliczenie prac pisemnych (w tym kolokwiów i ew. krótkich sprawdzianów).
P=0.6*F1+0.4*F2, warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1 i F2.		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] T. Jurlewicz, Z. Skoczylas, Algebra i geometria analityczna. Definicje, twierdzenia, wzory. Oficyna Wydawnicza GiS, Wrocław 2016.

[2] T. Jurlewicz, Z. Skoczylas, Algebra i geometria analityczna. Przykłady i zadania. Oficyna Wydawnicza GiS, Wrocław 2015.

[3] F. Leja, Geometria analityczna, PWN, Warszawa 1972.

[4] A. Mostowski, M. Stark, Elementy algebry wyższej, PWN, Warszawa 1963.

[5] J. Rutkowski, Algebra liniowa w zadaniach, PWN, 2008.

LITERATURA UZUPEŁNIAJĄCA:

[6] J. Jureczko, M. Turzański, Elementy matematyki wyższej. Teoria i zadania, Wydawnictwo WSB, Poznań 2011.

[7] J. Stankiewicz, K. Wilczek, Algebra z geometrią. Teoria, przykłady, zadania, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2011.

[8] M. Zakrzewski, Markowe wykłady z matematyki, Algebra z geometrią, Oficyna Wydawnicza GiS, Wrocław 2015.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr Joanna Jureczko, joanna.jureczko@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Analiza matematyczna 1.2A**
Nazwa w języku angielskim: **Mathematical Analysis 1.2A**
Kierunek studiów: **Telekomunikacja, Teleinformatyka, Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy): **……..**
Poziom i forma studiów: **I stopień / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu: **obowiązkowy / ~~wybieralny~~ / ~~ogólnouczelniany~~**
Kod przedmiotu: **W04CBE-SI0036G**
Grupa kursów **TAK / ~~NIE*~~**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	100	150			
Forma zaliczenia	Egzamin	Zaliczenie na ocenę			
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**10**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)		3			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,4	1,3			

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

Zalecana jest znajomość matematyki odpowiadająca wymaganiom na egzamin maturalny na poziomie rozszerzonym.

CELE PRZEDMIOTU

C1. Zapoznanie z podstawowymi funkcjami elementarnymi i ich własnościami.
C2. Zapoznanie z podstawowymi pojęciami i twierdzeniami rachunku różniczkowego funkcji jednej zmiennej.
C3. Zapoznanie z podstawowymi pojęciami i twierdzeniami rachunku różniczkowego funkcji wielu zmiennych.
C4. Zapoznanie z pojęciem całki oznaczonej, jej podstawowymi własnościami, metodami Obliczania i jej zastosowaniami.
C5. Zapoznanie się z pojęciami całki podwójnej i potrójnej oraz jej zastosowaniami

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ
Z zakresu wiedzy student PEU_W01 zna wykresy i własności podstawowych funkcji elementarnych, PEU_W02 zna podstawowe pojęcia i twierdzenia rachunku różniczkowego funkcji jednej zmiennej, PEU_W03 zna podstawowe pojęcia i twierdzenia rachunku różniczkowego funkcji wielu zmiennych, PEU_W04 zna pojęcie całki oznaczonej, jej własności i podstawowe zastosowania. PEU_W05 zna pojęcie całki podwójnej i potrójnej, jej własności i podstawowe zastosowania. **Z zakresu umiejętności student** PEU_U01 umie rozwiązywać typowe równania i nierówności z funkcjami elementarnymi, PEU_U02 umie badać zbieżność szeregów liczbowych. PEU_U03 umie stosować elementy badania przebiegu zmienności funkcji do rozwiązywania typowych zadań, PEU_U04 umie stosować pochodne cząstkowe, wyznaczać gradient i pochodną kierunkową oraz wyznaczać ekstrema lokalne i warunkowe funkcji dwóch zmiennych. PEU_U05 umie obliczać typowe całki oznaczone i nieoznaczone, PEU_U06 umie obliczać typowe całki podwójne i potrójne, PEU_U07 umie stosować rachunek różniczkowy i całkowy do rozwiązywania wybranych zagadnień praktycznych. **Z zakresu kompetencji społecznych student** PEU_K01 mieć świadomość konieczności systematycznej i samodzielnej pracy w celu zdobycia wiedzy

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Pojęcie funkcji, funkcji odwrotnej i złożonej. Wykres funkcji. Dziedzina, obraz i przeciwobraz funkcji. Podstawowe własności funkcji: monotoniczność, okresowość, różnowartościowość, „na". Funkcje elementarne (wielomianowa, wymierna, trygonometryczna, cyklometryczna, wykładnicza, logarytmiczna).	2
Wy2	Ciągi liczbowe. Granica ciągu. Twierdzenia o granicach ciągów liczbowych. Wyrażenia nieoznaczone. Liczba e.	2
Wy3	Szeregi liczbowe. Podstawowe rodzaje i własności. Szereg harmoniczny. Zbieżność szeregów (podstawowe warunki).	2
Wy4	Granica funkcji. Asymptoty. Ciągłość funkcji w punkcie i w przedziale. Podstawowe własności funkcji ciągłych. Zastosowania.	2
Wy5	Definicja pochodnej funkcji, jej interpretacja geometryczna i fizyczna. Styczna. Różniczka. Wzory na obliczanie pochodnych funkcji elementarnych. Pochodna funkcji złożonej.	2

Wy6	Ekstrema funkcji: lokalne i globalne. Twierdzenia o monotoniczności i wypukłości funkcji. Punkty przegięcia. Twierdzenie de l'Hospitala. Ekstrema funkcji: lokalne i globalne.	2
Wy7	Przebieg zmienności funkcji jednej zmiennej. Przykłady zastosowań rachunku różniczkowego.	2
Wy8	Funkcja dwu i trzech zmiennych. Granica i ciągłość funkcji dwu zmiennych.	2
Wy9	Pochodne cząstkowe funkcji dwu i trzy zmiennych. Różniczka zupełna.	2
Wy10	Pochodne cząstkowe wyższych rzędów. Ekstrema lokalne i globalne funkcji dwu i trzy zmiennych.	2
Wy11	Definicja całki nieoznaczonej i jej własności. Wzory na obliczanie całek funkcji elementarnych. Całkowanie przez podstawienie i przez części.	2
Wy12	Całkowanie funkcji wymiernych i trygonometrycznych.	1
Wy13	Definicja całki oznaczonej i jej własności. Twierdzenie Newtona-Leibniza. Przykłady zastosowań całki oznaczonej (np. średnia wartość funkcji na przedziale, pole obszaru, objętość bryły obrotowej, długość krzywej, etc).	2
Wy14	Całki podwójne. Interpretacja geometryczna. Własności całek podwójnych. Zamiana całek podwójnych na iterowane, Zamiana zmiennych w całce podwójnej. Zastosowania: objętość bryły, pole powierzchni.	3
Wy15	Całki potrójne. Zamiana całki potrójnej na iterowaną. Zamiana współrzędnych prostokątnych na współrzędne biegunowego, sferyczne i walcowe. Obliczanie całki potrójnej Zastosowania w technice.	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Cw1	Badanie podstawowych własności funkcji, składanie funkcji, wyznaczanie funkcji odwrotnej, przekształcanie wykresów,	2
Cw2	Obliczanie granic ciągów liczbowych.	1
Cw3	Badanie zbieżności szeregów	1
Cw4	Obliczanie granicy funkcji. Wyznaczanie asymptot. Badanie ciągłości funkcji w punkcie i w przedziale.	2
Cw5	Wyznaczanie z definicji pochodnej funkcji. Obliczanie różniczki. Obliczanie pochodnych funkcji elementarnych z wykorzystaniem podstawowych wzorów oraz pochodnych funkcji złożonych.	2
Cw6	Wyznaczanie przedziałów monotoniczności i wypukłości funkcji.	2

	Obliczanie granic funkcji korzystając z reguły de l'Hospitala. Wyznaczanie ekstremów funkcji.	
Cw7	Badanie przebiegu zmienności funkcji jednej zmiennej. Zastosowanie rachunku różniczkowego do rozwiązywania zadań optymalizacyjnych.	3
Cw8	Obliczanie granic i badanie ciągłości funkcji dwu zmiennych.	1
Cw9	Wyznaczanie pochodnych cząstkowych funkcji dwu i trzy zmiennych. Obliczanie różniczki zupełnej. Wyznaczanie ekstremów funkcji dwu i trzy zmiennych.	3
Cw10	Kolokwium	1
Cw11	Obliczanie całek niezonaczonych funkcji elementarnych. Całkowanie przez podstawienie i przez części. Całkowanie funkcji wymiernej i trygonometrycznej.	3
Cw12	Obliczanie całek oznaczonych. Rozwiązywanie zadań z zastosowaniem całki oznaczonej (np. średnia wartość funkcji na przedziale, pole obszaru, objętość bryły obrotowej, długość krzywej, etc).	3
Cw13	Obliczanie całek podwójnych. Zamiana całek podwójnych na iterowane, zamiana zmiennych. Obliczanie objętość bryły i jej pola powierzchni. Rozwiązywanie zadań z zastosowaniem całek podwójnych.	2
Cw14	Obliczanie całek potrójnych. Zamiana całek potrójnych na iterowane, zamiana współrzędnych prostokątnych na współrzędne biegunowego, sferyczne i walcowe. Obliczanie całki potrójnej Zastosowania w technice.	2
Cw15	Kolokwium	2
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład – metoda tradycyjna. N2. Ćwiczenia problemowe i rachunkowe – metoda tradycyjna. N3. Praca własna studenta. N4. Konsultacje.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01,PEU_W02, PEU_W03,PEU_W04, PEU_W05.	Aktywność na wykładach, egzamin pisemny
F2	PEU_U01, PEU_U02, PEU_U03, PEU_U04, PEU_U05, PEU_U06, PEU_U07, PEU_K01	Aktywność na ćwiczeniach, zaliczenie prac pisemnych (kolokwiów)

P=0.6*F1+0.4*F2, warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1 i F2

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] M. Gewert, Z. Skoczylas, Analiza matematyczna 1. Definicje, twierdzenia, wzory, Oficyna Wydawnicza GiS, Wrocław 2015.
[2] M. Gewert, Z. Skoczylas, Analiza matematyczna 1. Przykłady i zadania, Oficyna Wydawnicza GiS, Wrocław 2015.
[3] M. Gewert, Z. Skoczylas, Analiza matematyczna 2. Definicje, twierdzenia, wzory, Oficyna Wydawnicza GiS, Wrocław 2015.
[4] M. Gewert, Z. Skoczylas, Analiza matematyczna 2. Przykłady i zadania, Oficyna Wydawnicza GiS, Wrocław 2015.
[5] W. Krysicki, L. Włodarski, Analiza matematyczna w zadaniach, Cz. I i II, PWN, Warszawa 2006.
[6] F. Leja, Rachunek różniczkowy i całkowy, PWN 2012.

LITERATURA UZUPEŁNIAJĄCA:

[7] R. Leitner, Zarys matematyki wyższej dla studiów technicznych, cz.1-2, WNT, Warszawa 2006.
[8] M. Zakrzewski, Markowe wykłady z matematyki. Analiza, Oficyna Wydawnicza GiS, Wrocław 2013.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr Joanna Jureczko, joanna.jureczko@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim Bezpieczeństwo elektromagnetyczne
Nazwa w języku angielskim Electromagnetic safety
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo (CB)
Specjalność (jeśli dotyczy):

Poziom i forma studiów: **I / ~~II stopień~~ / ~~jednolite studia magisterskie*~~, stacjonarna / ~~niestacjonarna*~~**
Rodzaj przedmiotu: **obowiązkowy / ~~wybieralny / ogólnouczelniany~~ ***
Kod przedmiotu **W04CBE-SI0054G**
Grupa kursów **TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		75		
Forma zaliczenia	zaliczenie na ocenę		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	5				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			3		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6		1,2		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Zaliczony kurs i „Miernictwo 1" „Miernictwo 2"
2. Posiadanie wiedzy na temat podstawowej metrologii wielkości takich jak moc i napięcie
3. Znajomość zagadnień szacowania niepewności pomiarowej

CELE PRZEDMIOTU

C1. Zdobycie podstawowej wiedzy z zakresu bezpieczeństwa elektromagnetycznego, obejmujące identyfikację zagrożeń wynikających z elektromagnetycznego ulotu informacji jak i możliwych zagrożeń i ataków elektromagnetycznych na urządzenia, systemy, sieci oraz ich części oraz zaznajomienie się z typowymi rozwiązaniami technicznymi i organizacyjnymi, które poprawiają bezpieczeństwo elektromagnetyczne i niezawodność działania urządzeń, systemów, sieci i instalacji.

C2. Zdobycie umiejętności: wyboru technik badawczych, konfigurowania stanowisk testowych, wyznaczania parametrów technicznych i skuteczności stosowanych zabezpieczeń i ich klasyfikacji, wykonywania podstawowych badań emisyjności i podatności na zaburzenia elektromagnetyczne oraz opracowywania i interpretacji otrzymanych wyników badań. Zdobycie umiejętności pomiaru rozwiązań technicznych ograniczających ulot informacji.

C3. Nabywanie i utrwalanie kompetencji społecznych obejmujących inteligencję emocjonalną polegającą na umiejętności współpracy w grupie studenckiej, których celem jest efektywne rozwiązywanie problemów i wyzwań. Odpowiedzialność, uczciwość i rzetelność w postępowaniu; przestrzeganie obyczajów obowiązujących w środowisku akademickim i społeczeństwie.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – Ma podstawową wiedzę z zakresu bezpieczeństwa elektromagnetycznego, obejmującą identyfikację zagrożeń oraz skutków wynikających z elektromagnetycznego ulotu informacji jak i oddziaływania zaburzeń elektromagnetycznych wytwarzanych celowo i w sposób niezamierzony w środowisku użytkowania urządzeń, systemów i sieci, w tym możliwych ataków elektromagnetycznych.

PEU_W02 – Ma podstawową wiedzę o stosowanych rozwiązaniach technicznych i organizacyjnych, które poprawiają bezpieczeństwo elektromagnetyczne i niezawodność działania urządzeń, systemów, sieci.

PEU_W03 – Wie, jak scharakteryzować wymagania w zakresie bezpieczeństwa elektromagnetycznego, stosowanych zabezpieczeń i środków ochrony, jak i określić zagrożenia elektromagnetyczne występujące w różnych środowiskach elektromagnetycznych.

PEU_W04 – Zna rodzaje i charakterystyki zaburzeń elektromagnetycznych oraz zna mechanizmy i drogi ich rozprzestrzeniania.

PEU_W05 – Zna pojęcia odporność i podatność na zaburzenia elektromagnetyczne oraz emisję elektromagnetyczną i kanały ulotu informacji. Wie, jak wskazać właściwe metody ich pomiaru i testowania oraz wyjaśnić kryteria ich wyboru.

PEU_W06 – Zna architekturę bezpieczeństwa sieci oraz systemów oraz potrafi zidentyfikować elementy architektury (infrastruktury, urządzeń końcowych i aplikacji) szczególnie istotne dla bezpieczeństwa elektromagnetycznego;

PEU_W07 – Zna metody szacowania ryzyka czasowego lub całkowitego uszkodzenia lub zaburzenia pracy infrastruktury, jej elementów, w tym urządzeń końcowych i aplikacji.

PEU_W08 – Wie jakie metody ochrony organizacyjnej i technicznej są stosowane m.in. dla osób, w budynkach i pomieszczeniach oraz urządzeniach, systemach, sieciach i instalacjach, aby ograniczyć poziomy narażeń elektromagnetycznych i skutki ich oddziaływania, a także skutecznie chronić się przez elektromagnetycznym ulotem informacji;

Z zakresu umiejętności:

PEU_U01 – Potrafi wytypować odpowiednią metodę pomiarową, przygotować stanowiska pomiarowe, wykonywać podstawowe pomiary emisji ujawniających i badania podatności urządzeń na zaburzenia elektromagnetyczne, sprzężenia elektromagnetyczne oraz wyznaczać parametry techniczne stosowanych zabezpieczeń;

PEU_U02 – Potrafi opracować i zinterpretować otrzymane wyniki badań, w tym dokonać klasyfikacji zagrożeń i efektywności stosowanych zabezpieczeń;

PEU_U03 – Potrafi rozwiązywać problemy związane z bezpieczeństwem elektromagnetycznym, w tym zastosować w praktyce podstawowe techniki ograniczające poziomy zaburzeń elektromagnetycznych i poprawiające niezawodność działania i bezpieczeństwo w obecności narażeń elektromagnetycznych;

PEU_U04 – Potrafi posługiwać się: podstawowymi przyrządami pomiarowymi (m.in., analizatorem widma, oscyloskopem) oraz metodami pomiarowymi w celu lokalizacji i identyfikacji źródła „wycieków" elektromagnetycznych, wykonania podstawowych pomiarów z zakresu ulotu elektromagnetycznego oraz określania skuteczności zastosowanych technik ograniczania ulotu informacji;

PEU_U05 – Potrafi krytycznie ocenić rozwiązania naukowo-techniczne stosowane dla oceny i zapewnienia bezpieczeństwa elektromagnetycznego.

Z zakresu kompetencji społecznych:

PEU_K01 – poszerzanie wiedzy z zakresu bezpieczeństwa elektromagnetycznego poprzez wyszukiwanie informacji oraz jej krytyczna analiza;

PEU_K02 – przestrzeganie obyczajów i zasad obowiązujących w środowisku akademickim;

PEU_K03 – wykorzystywania i upowszechnianie wiedzy o zagrożeniach elektromagnetycznych i stosowanych metodach zapewniania bezpieczeństwa elektromagnetycznego.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do przedmiotu: zagrożenia celowe i przypadkowe w środowisku elektromagnetycznym, ulot informacji, systemy i sieci chronione przed problemami i zagrożeniami elektromagnetycznymi. Przyczyny i wymogi formalne w zakresie ochrony informacji przed zjawiskami elektromagnetycznymi. Charakterystyka podstawowych zjawisk fizycznych.	2
Wy2	Emisyjność urządzeń i ulot informacji. Zjawisko rozprzestrzeniania się zaburzeń elektromagnetycznych. Metody pomiaru emisyjności elektromagnetycznej (ulotu informacji). Przykłady metod podsłuchu urządzeń teleinformatycznych oraz wykrywania urządzeń podsłuchowych.	2
Wy3	Metody ochrony urządzeń teleinformatycznym przed ulotem elektromagnetycznym (TEMPEST)	2
Wy4	Odziaływanie pól elektromagnetycznych na urządzenia elektroniczne. Zjawiska fizyczne. Pola stacjonarne. Narażenia impulsowe. Przykłady skutków narażeń elektromagnetycznych. Intencjonalnie generowane zaburzenia elektromagnetyczne dużej energii (np. NEMP, HPEM, HPM) i terroryzm elektromagnetyczny	2
Wy5	Ochrona urządzeń przed narażeniami elektromagnetycznymi z wykorzystaniem: symetryzacji, ekranowania, filtracji, absorbcji zaburzeń EM. Sposoby pomiaru skuteczności ekranowania.	2

Wy6	Ochrona obiektów informatycznych przed wyładowaniami elektrostatycznymi i zaburzeniami elektromagnetycznymi	2
Wy7	Bezpieczeństwo elektromagnetyczne infrastruktury krytycznej. Zasady poprawnej konstrukcji i zabezpieczeń: etapy, wykorzystanie wcześniej omówionych sposobów w docelowych aplikacjach, analiza ryzyka, ograniczenie infiltracji, uwzględnienie udziału człowieka jako najsłabszego ogniwa.	2
Wy8	Ochrona ludzi przed polami elektromagnetycznymi. Uwarunkowania formalno-prawne. Dopuszczalne poziomy oraz sposoby sprawdzania dotrzymania dopuszczalnych poziomów pól elektromagnetycznych w środowisku.	1
	Suma godzin	**15**

Forma zajęć - laboratorium		**Liczba godzin**
La1	Zajęcia wstępne – wprowadzenie, zapoznanie z aparaturą, zasadami bezpieczeństwa.	2
La2	Pomiar podstawowych zjawisk elektromagnetycznych (przesłuchy, niedopasowania…)	4
La3	Pomiar ujawniających emisji promieniowanych	4
La4	Lokalizacja i identyfikacja „wycieków” elektromagnetycznych	4
La5	Pomiar skuteczności redukcji ulotu informacji przez elementy absorpcyjne	4
La6	Pomiar skuteczności redukcji ulotu informacji przez filtry	4
La7	Pomiar tłumienności / skuteczności ekranowania materiałów	4
La8	Badanie wpływu zaburzeń elektromagnetycznych na transmisję danych	4
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem slajdów oraz narzędzi symulacyjnych N2. Materiały do wykładu (https://eportal.pwr.edu.pl) N3. Konsultacje N4. Praca własna – samodzielne studia i przygotowanie do zajęć i kolokwium N5. Praca własna – samodzielne przygotowanie do laboratorium N6. Studia literaturowe N7. Stanowiska laboratoryjne w Laboratorium Kompatybilności Elektromagnetycznej N8. Materiały do laboratorium – instrukcje i materiały uzupełniające (https://eportal.pwr.edu.pl)

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 - PEU_W08 PEU_K01 - PEU_K03	Sprawdziany cząstkowe, pisemny lub/i ustny egzamin
F2	PEU_U01 - PEU_U05	Sprawdziany z przygotowania do zajęć, dyskusje,

	PEU_K01 -PEU_K03	pisemne sprawozdania z ćwiczeń

P=F1*0,6+F2*0,4
Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Grzesiak K., Kubiak I., Musiał S. Przybysz A.,: Elektromagnetyczne Bezpieczeństwo informacji, WAT, 2009
[2] L. Nowosielski: Minimalizacja elektromagnetycznej podatności infiltracyjnej urządzeń informatycznych, WAT 2019
[3] Liderman K.: Bezpieczeństwo teleinformatyczne, Warszawa 2001
[4] Charoy A.: Zakłócenia w urządzeniach elektronicznych, WNT, Warszawa, 1999.
[5] Ott H.W.: Electromagnetic Compatibility Engineering, John Willey & Sons, 2009
[6] Więckowski T.W.: Badania kompatybilności elektromagnetycznej urządzeń elektrycznych i elektronicznych, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2001.
[7] Więckowski T.W.: Pomiar emisyjności urządzeń elektrycznych i elektronicznych, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 1997.
[8] Paul C.R.: Introduction to Electromagnetic Compatibility, John Willey & Sons, New Jersey, 2006
[9] Williams T.: EMC for Product Designers, 2017

LITERATURA UZUPEŁNIAJĄCA:

[1] http://ieeexplore.ieee.org/
[2] www.etsi.org,
[3] www.cenelec.eu

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Tadeusz W. Więckowski, Tadeusz.wieckowski@pwr.edu.pl
Zbigniew Jóskiewicz, zbigniew.joskiewicz@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim ***Bezpieczeństwo sieci komputerowych***
Nazwa w języku angielskim ***Computer network security***
Kierunek studiów (jeśli dotyczy): ***Cyberbezpieczeństwo***
Specjalność (jeśli dotyczy):
Poziom i forma studiów: **I ~~/ II stopień*,~~ stacjonarna ~~/ niestacjonarna~~***
Rodzaj przedmiotu: **obowiązkowy ~~/ wybieralny / ogólnouczelniany~~ ***
Kod przedmiotu **W04CBE-SI0014G**
Grupa kursów **TAK ~~/ NIE*~~**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		60		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		100		
Forma zaliczenia	Egzamin / ~~zaliczenie na ocenę*~~	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**6**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			4		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,4		2,4		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1.
2.
3.

\

CELE PRZEDMIOTU

C1. Zdobycie podstawowej wiedzy o metodach i mechanizmach bezpieczeństwa w sieciach komputerowych, ochrony dostępu, filtrowania ruchu oraz utajniania treści.
C2. Zdobycie podstawowej wiedzy o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom.
C3. Zdobycie umiejętności konfigurowania i uruchamiania mechanizmów bezpieczeństwa na ruterach, tuneli szyfrowanych i mechanizmów zapobiegania atakom z sieci

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – posiada podstawową wiedze o zagrożeniach i zabezpieczaniu urządzeń teleinformatycznych. Zna koncepcję uwierzytelniania, kontroli dostępu i rozliczalności (AAA).

PEU_W02 – zna metody zabezpieczania sieci LAN oraz techniki szyfrowania używane w połączeniach VPN.

PEU_W03 – zna koncepcję zarządzania bezpieczną siecią oraz funkcjonalność dedykowanych zapór sieciowych.

Z zakresu umiejętności:

PEU_U01 – potrafi zabezpieczać dostęp administracyjny na ruterach.

PEU_U02 – potrafi konfigurować zapory sieciowe

PEU_U03 – potrafi konfigurować funkcje bezpieczeństwa na urządzeniach warstwy 2.

PEU_U04 – potrafi konfigurować sieci VPN i tunelowanie ruchu na ruterach i dedykowanych zaporach sieciowych

Z zakresu kompetencji społecznych:

PEU_K01 – umiejętność współpracy w grupie

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1,2,3	Zabezpieczanie sieci. Zagrożenia sieciowe. Łagodzenie zagrożeń i bezpieczny dostęp do urządzeń	4
Wy3	Przypisywanie ról administracyjnych oraz monitorowanie i zarządzanie urządzeniami	2
Wy4	Uwierzytelnianie, autoryzacja i rozliczanie (Authentication, Authorization and Accounting)	2
Wy5	Listy kontroli dostępu (AAA)	2
Wy6	Zapory sieciowe i bezpieczeństwo urządzeń końcowych	2
Wy7	Bezpieczeństwo urządzeń końcowych i sieci w drugiej warstwie	2
Wy8	Zabezpieczenia kryptograficzne	2
Wy9	Prywatne wirtualne sieci (VPN)	2
Wy10,11	Dedykowane urządzenia do zabezpieczania sieci	4
Wy12,13	Testowanie bezpieczeństwa sieci. Technika IPS	4
Wy14,15	Nowe trendy w bezpieczeństwie sieci	4
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1,2	Ćwiczenia wprowadzające do pracy w laboratorium bezpieczeństwa sieci	8

La3	Zabezpieczanie dostępu administracyjnego do urządzeń sieciowych	4
La4	Konfiguracja ról administracyjnych	4
La5	Konfiguracja zabezpieczeń OSPF. Zarządzanie odporrnością i raportowanie w systemie Cisco IOS	4
La6	Zabezpieczanie dostępu administracyjnego przy pomocy AAA i protokołu RADIUS	4
La7	Konfiguracja i weryfikacja rozszerzonych list kontroli dostępu	4
La8	Konfiguracja firewall zgodnie z polityką podziału na strefy (zone-based policy)	4
La9	Konfiguracja zabezpieczeń na przełącznikach warstwy drugiej	4
La10	Praktyczne zastosowania kryptografii	4
La11	Konfiguracja VPN pomiędzy siedzibami firmy Podstawowa konfiguracja dedykowanego urządzenia typu firewall przy użyciu interfejsu tekstowego	4
La12	Podstawowa konfiguracja dedykowanego urządzenia typu firewall przy użyciu interfejsu graficznego.	4
La13,La14, La15	Repetytorium. Test umiejętności	12
	Suma godzin	60

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem transparencji i slajdów oraz narzędzi symulacyjnych N2. Materiały i instrukcje laboratoryjne on-line na stronach Akademii Cisco (www.netacad.com) N3. Ćwiczenia rachunkowe – dyskusja rozwiązań zadań. N4. Ćwiczenia praktyczne – konfiguracja urządzeń sieciowych i testy funkcjonalne N5. Udział w e-testach przeprowadzanych w laboratoriach komputerowych (www.netacad.com, kursy.pwr.wroc.pl) N6. Konsultacje N7. Praca własna – przygotowanie do ćwiczeń laboratoryjnych N8. Praca własna – samodzielne studia i przygotowanie do kolokwium

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się

– podsumowująca (na koniec semestru)		
F1, F2	PEU_W01, PEU_W02, PEU_W03	F1 - e-testy cząstkowe, F2 - e-test podsumowujący
F3,F4	PEU_U01, PEU_U02, PEU_U03, PEU_U04, PEU_K01,	F3 - ocena realizacji ćwiczeń (sprawozdania) F4 - praktyczny test umiejętności
P= 30/100*(50/100*F1+50/100*F2)+70/100*(40/100*F3+60/100*F4) Ocena jest pozytywna po uzyskaniu 70 procent oceny maksymalnej. Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu.		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] 1. Podręcznik interaktywny kursu Network Security 1.0, www.netacad.com (wersja angielska), www.netacad.com

LITERATURA UZUPEŁNIAJĄCA:

[1] Adam Józefiok, "Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco", Wydawnictwo Helion, Gliwice 2016
[2] Omar Santos, John Stuppi,” CCNA Security 210-260 Oficjalny przewodnik”, Wydawnictwo Naukowe PWN,Warszawa 2016

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Jarosław Janukiewicz, Jaroslaw.Janukiewicz@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ ELEKTRONIKI

KARTA PRZEDMIOTU

Nazwa w języku polskim BAZY DANYCH
Nazwa w języku angielskim DATABASES
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy):
Poziom i forma studiów: I / ~~II~~ stopień*, stacjonarna ~~/ niestacjonarna*~~
Rodzaj przedmiotu: obowiązkowy / ~~wybieralny~~ ~~/ ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0050G
Grupa kursów TAK ~~/ NIE~~*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75		75		
Forma zaliczenia	~~Egzamin~~ / zaliczenie na ocenę*			~~Egzamin /~~ zaliczenie na ocenę*	
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	6				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0		2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2		1,2		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

Podstawowa wiedza z zakresu kodowania i szyfrowania danych (np. kurs Kodowanie i Kryptografia I), wiedza z zakresu bezpieczeństwa systemów operacyjnych, z zakresu ochrony informacji, protokołów sieciowych oraz znajomość obsługi systemów operacyjnych z rodziny Unix.

\

CELE PRZEDMIOTU

C1 Nabycie wiedzy dotyczącej technik fizycznej i logicznej organizacji danych oraz zapoznanie z różnymi typami baz danych i ich mechanizmami.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Student ma wiedzę o architekturze i zasadzie działania podstawowych komponentów SZBD.
PEU _W02 Student potrafi omówić i porównać podstawowe metody organizacji danych, indeksowania danych oraz przetwarzania i optymalizacji transakcji i zapytań w SZBD.

Z zakresu umiejętności:

PEU _U01 Student potrafi wybrać i dostosować odpowiednie do wymagań narzędzia tworzenia aplikacji baz danych.
PEU _U02 Student potrafi samodzielnie zaprojektować i zaimplementować bazę danych.

Z zakresu kompetencji społecznych:

PEU _K01 – Student posiada kompetencje w zakresie indywidualnej
Realizacji prostych systemów baz danych.

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		**Liczba godzin**
Wyk1	Wprowadzenie.	2
Wyk2	Bazy danych relacyjne – zastosowanie i architektura.	2
Wyk3	Bazy danych relacyjne – mechanizmy i operacje	2
Wyk4	Bazy danych relacyjne - mechanizmy i operacje	2
Wyk5	Usługi katalogowe – zastosowanie, architektura, operacje	2
Wyk6	Usługi katalogowe – zastosowanie, architektura, operacje	2
Wyk7	Bazy danych grafowe – zastosowanie i architektura.	2
Wyk8	Bazy danych grafowe – zastosowanie i architektura.	2
Wyk9	Modele usługowe a bazy danych	2
Wyk10	Bazy obiektowe – zastosowanie i architektura.	2
Wyk11	Bazy danych NoSQL – zastosowanie i architektura	2
Wyk12	Bazy danych NoSQL – zastosowanie i architektura	2
Wyk13	Uwierzytelnianie i autoryzacja w bazach danych	2
Wyk14	Wykorzystanie ORM w zarządzaniu bazami danych	2
Wyk15	Kolokwium zaliczeniowe	2
	Suma godzin	30

Forma zajęć – laboratorium		Liczba godzin
Lab1	Sprawy organizacyjne, omówienie usług sieciowych wspomagających realizację laboratorium	2
Lab2	Instalacja i konfiguracja relacyjnej bazy danych	2
Lab3	Operacje na relacyjnych bazach danych	2
Lab4	Operacje na relacyjnych bazach danych	2
Lab5	Operacje na relacyjnych bazach danych	2
Lab6	Instalacja i konfiguracja usług katalogowych	2
Lab7	Operacje na usłudze katalogowej	2
Lab8	Instalacja i konfiguracja grafowej bazy danych	2
Lab9	Operacje na grafowej bazie danych	2
Lab10	Operacje na grafowej bazie danych	2
Lab11	Instalacja i konfiguracja bazy typu NoSQL	2
Lab12	Operacje na bazie NoSQL	2
Lab13	Operacje na bazie NoSQL	2
Lab14	Instalacja i konfiguracja silników wyszukiwania	2
Lab15	Indeksowanie treści silnikami wyszukiwania	2
	Suma godzin	30

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych N2. Studia literaturowe N3. Konsultacje N4. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02	1. Ocena z kolokwium (wykład)
F2	PEU_U01 PEU_U02 PEU _K01	1. Realizacja zadań w trakcie laboratorium
P=0.3*F1+0.7*F2, warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] R. Elmasri, S. B. Navathe - "Wprowadzenie do systemów baz danych", Helion 2005
[2] Garcia-Molina. H., Ullman J.D., Widom J., Systemy baz danych. Pełnywykład, WNT, 2006.
[3] Stencel, Krzysztof - "Obiektowe i półstrukturalne bazy danych", Wydawnictwo Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych 2012

LITERATURA UZUPEŁNIAJĄCA:

[1] David Litchfield, Chris Anley, John Heasman, Bill Grindlay, „The Database Hacker's Handbook: Defending Database Servers”, Wiley 2005

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Mateusz Tykierko mateusz.tykierko@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	**Chmury obliczeniowe**
Nazwa w języku angielskim:	**Cloud computing**
Kierunek studiów:	**Cyberbezpieczeństwo**
Stopień studiów i forma:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**obowiązkowy**
Kod przedmiotu:	**W04CBE-SI0049G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		45		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		75		
Forma zaliczenia	Zaliczenie na ocenę		Zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**5**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-		4		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6		1,8		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

CELE PRZEDMIOTU

C1. Zdobycie podstawowej wiedzy dotyczącej infrastruktury chmur obliczeniowych oraz aplikacji i usług w chmurach.

C2. Zdobycie umiejętności uruchamiania usług teleinformatycznych w oparciu o infrastrukturę chmury, a także formułowania charakterystyki chmury obliczeniowej.

C3. Identyfikuje zagrożenia oraz zna metody związane z zachowaniem cyberbezpieczeństwa.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01- Zna koncepcję wirtualizacji oraz kluczowe zagadnienia związane z platformą sprzętową oraz oprogramowaniem, modelem warstwowym, a także cechy charakterystycznych chmur obliczeniowych.

PEU_W02- Posiada podstawową koncepcję kontenerów oraz wiedzę o ich środowiskach uruchomieniowych.

PEU_W03- Zna modele dostarczania usług chmury oraz zakresy odpowiedzialności dostawcy i klienta.

PEU_W04- Identyfikuje chmury prywatne, publiczne oraz hybrydowe, zna typowe zastosowania oraz zalety i wady poszczególnych rozwiązań oraz identyfikuje zagrożenia oraz zna metody związane z zachowaniem cyberbezpieczeństwa.

Z zakresu umiejętności:

PEU_U01- Potrafi zarządzać zasobami hipervisorów, tworzyć maszyny wirtualne oraz instalować systemy operacyjne.

PEU_U02- Potrafi instalować środowiska uruchomieniowe kontenerów oraz uruchamiać przykładowe aplikacje wielo-kontenerowe.

PEU_U03- Potrafi zarządzać zasobami chmury obliczeniowej z pozycji klienta chmury, tworzyć projekty oraz zamawiać maszyny wirtualne.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie. Rys historyczny, terminologia i podstawowa koncepcja. Wirtualizacja w chmurach obliczeniowych.	1
Wy2	Charakterystyka chmur obliczeniowych. Skalowanie.	2
Wy3	Koncepcja kontenerów oraz środowisko uruchomieniowe Docker.	2
Wy4	Model warstwowy.Usług XaaS w chmurach obliczeniowych. Granice odpowiedzialności dostawcy i klienta.	2
Wy5	Usługi udostępniania infrastruktury na przykładzie AWS Compute	2
Wy6	Usługi przechowywania danych na przykładzie AWS Storage. Chmury prywatne, publiczne i hybrydowe. Zalety i wady różnych rozwiązań. Zastosowania.	2
Wy7	Usługi tworzenia prywatnej sieci na przykładzie AWS VPC.	2
Wy8	Repetytorium	2
	Suma godzin	**15**

Forma zajęć - laboratorium		**Liczba godzin**
La1	Wprowadzenie. Wirtualizacja lokalna z użyciem hypervisora typu II. Tworzenie maszyn wirtualnych, instalacja systemu operacyjnego gościa wraz z dodatkowym oprogramowaniem sterowników.	3
La2	Importowanie obrazów maszyn wirtualnych. Tworzenie migawek i klonowanie maszyn wirtualnych. Rozwiązania oparte o wiele maszyn wirtualnych.	3
La3	Komunikacja sieciowa w środowisku wirtualnym.	3
La4	Środowiska produkcyjne– wirtualizacja z użyciem hypervisora typu I. Tworzenie VM, instalacja systemów operacyjnych gościa.	3
La5	Instalacja środowiska uruchomieniowego Docker. Obrazy i kontenery.	3

La6	Tworzenie własnych obrazów kontenerów za pomocą Dockerfile. Tworzenie projektów wielokontenerowych. Narzędzie Docker-compose	3
La7,8	Rozwiązania oparte o wiele kontenerów. Komunikacja sieciowa w środowisku uruchomieniowym.Zarządzanie pojedynczym Dockerem oraz klastrem Dockerów	6
La9	Wybrane usługi na AWS Amazon - EC2 i EFS	3
La10	Wybrane usługi AWS Amazon - Auto Scaling i Elastic Load Balancing	3
La11	Wybrane usługi AWS Amazon - VPC	3
La12	Wybrane usługi na AWS Amazon - Elastic Beanstalk oraz S3 z CF	3
La13	Wybrane usługi AWS Amazon - Cloud Formation	3
La14	Wybrane usługi na AWS Amazon - ECS	3
La15	Repetytorium	3
	Suma godzin	45

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem transparencji i slajdów oraz narzędzi symulacyjnych N2. Materiały i instrukcje laboratoryjne on-line na stronach PWR N3. Ćwiczenia praktyczne – konfiguracja urządzeń i testy funkcjonalne N4. Konsultacje N5. Praca własna – przygotowanie do ćwiczeń laboratoryjnych N6. Praca własna – samodzielne studia i przygotowanie do kolokwium

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01-04	Kolokwium końcowe
F2	PEU_U01-03	Realizacja ćwiczeń laboratoryjnych
P= (F1+F2)/2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Kurs e-learningowy „Cloud Computing Introduction” dostępny na portalu Otwartych Zasobów Edukacyjnych OZE PWR.

LITERATURA UZUPEŁNIAJĄCA:

[1] Materiały ze strony https://www.ibm.com/cloud-computing/

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Marcin Głowacki, Marcin.Glowacki@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Etyka inżynierska**
Nazwa w języku angielskim: **Engineering Ethics**
Kierunek studiów (jeśli dotyczy): **Cyberbezpieczeństwo, Telekomunikacja, Teleinformatyka**
Specjalność (jeśli dotyczy): **……..**
Poziom i forma studiów: **I stopień / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu: **obowiązkowy / ~~wybieralny~~ / ogólnouczelniany~~**
Kod przedmiotu **W08W04-SI0001W**
Grupa kursów **~~TAK~~ / NIE***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25				
Forma zaliczenia	Zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**1**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-				
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0.6				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1: Zdobycie przez studentów elementarnej wiedzy z etyki ogólnej i zawodowej;
C2: Ukształtowanie wrażliwości na dylematy moralne w pracy inżyniera;
C3: Zapoznanie studentów z kodeksami etyki inżynierskiej.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ
Z zakresu wiedzy: PEU_W01: Po zakończeniu kursu student ma wiedzę niezbędną do rozumienia etyczno-społecznych uwarunkowań działalności inżynierskiej, takich jak: filozoficzny namysł nad istotą techniki i konkretne rozstrzygnięcia na gruncie „wartościowania techniki" (*technology assessment*).

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Etyka jako dyscyplina filozoficzna	1
Wy2	Główne szkoły metaetyczne	1
Wy3	Problem sumienia	1
Wy4	Podstawowe pojęcia etyczne – problem uzasadnienia norm etycznych	1
Wy5	Sposoby uzasadnienia norm w etykach deontologicznych	1
Wy6	Sposoby uzasadnienia norm w etyce utylitarystycznych	1
Wy7	Problemy działalności technicznej	1
Wy8	Determinizm techniczny w świetle sporu o możliwość wolności	1
Wy9	Elementy socjologii zawodu	1
Wy10	Status etyki inżynierskiej	1
Wy11	Problem odpowiedzialności zawodowej inżyniera	1
Wy12	Etyczna ocena wdrażania nowych technologii (TA)	1
Wy13	Struktura i funkcja kodeksów inżynierskiej etyki zawodowej	1
Wy14	Prezentacja wybranych inżynierskich kodeksów etycznych cz. 1.	1
Wy15	Prezentacja wybranych inżynierskich kodeksów etycznych cz. 2.	1
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Prezentacja multimedialna N2. Wykład informacyjny N3. Dyskusja

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
P	PEU_W01:	Kolokwium pisemne z materiału wykładów

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

1) Agazzi E., *Dobro, zło i nauka*, tłum. E. Kałuszyńska, Warszawa 1997.
2) Anzenbacher A., *Wprowadzenie do etyki*, 2008.
3) Birnbacher D., *Odpowiedzialność za przyszłe pokolenia*, Kraków 1999.
4) Chyrowicz B. [red.], *Etyka i technika w poszukiwaniu ludzkiej doskonałości*, Lublin 2004.
5) Galewicz W. [red.], *Moralność i profesjonalizm. Spór o pozycję etyk zawodowych*, Kraków 2010.
6) Gasparski W., *Dobro, zło i technika*, [w:] *Problemy etyczne techniki*, Instytut Problemów Współczesnej Cywilizacji, Warszawa 1999, s. 17-26.
7) Gasparski W., *Dobro, zło i technika*, „Zagadnienia Naukoznawstwa" 1999 nr 3-4, s. 386-391.
8) Gościkowski J. Pigoń K., *Etyka zawodowa ludzi nauki*, Wrocław 1991.
9) Jonas H., *Zasada odpowiedzialności. Etyka dla cywilizacji technologicznej*, tłum. M. Klimowicz, Kraków 1996.
10) Kiepas A., *Człowiek – technika – środowisko: człowiek współczesny wobec wyzwań końca wieku*, Katowice 1999.
11) Kiepas A., *Człowiek wobec dylematów filozofii techniki*, Katowice 2000.
12) Kiepas A., *Nauka – technika – kultura: studium z zakresu filozofii techniki*, Katowice 1984.
13) Ossowska M., *Normy moralne. Próba systematyzacji*, Warszawa 2003.
14) Postman N., *Technolpol: triumf techniki nad kulturą*, Warszawa 1995.
15) Styczeń T., *Wprowadzenie do etyki*, Lublin 1993.

LITERATURA UZUPEŁNIAJĄCA:

1) Bober, W. J., *Powinność w świecie cyfrowym: etyka komputerowa w świetle współczesnej filozofii moralnej*, 2008.
2) Kotarbiński T., *Dzieła wszystkie. Prakseologia*, Ossolineum 2003.
3) Lisak M. Elementy etyki w zawodzie architekta, 2006.
4) Słowiński B., *Podstawy sprawnego działania*, Koszalin 2007.
5) Sołtysiak G., *Kodeksy etyczne w Polsce*, Warszawa 2006.
6) Sułek M., Swiniarski J., *Etyka jako filozofia dobrego działania zawodowego*, Warszawa 2001.
7) Ślipko T., *Zarys etyki ogólnej*, Kraków 2004.
8) Ślipko T., *Zarys etyki szczegółowej*: t.1: *Etyka osobowa*, t.2: *Etyka społeczna*, Kraków 2005.
9) Wawszczak, W., *Humanizacja Inżynierów*, „Forum Akademickie" nr 9, wrzesień 2003, s. 38-40.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr Krzysztof Serafin, krzysztof.serafin@pwr.wroc.pl

WYDZIAŁ ZARZĄDZANIA (K-81)

KARTA PRZEDMIOTU

Nazwa w języku polskim **Filozofia**
Nazwa w języku angielskim **Philosophy**
Kierunek studiów (jeśli dotyczy): **Telekomunikacja, Teleinformatyka Cyberbezpieczeństwo,**

Specjalność (jeśli dotyczy): **……..**
Poziom i forma studiów: **I stopień / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu: **obowiązkowy / ~~wybieralny~~ / ogólnouczelniany**
Kod przedmiotu **W08W04-SI0004W**
Grupa kursów **~~TAK~~ / NIE***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50				
Forma zaliczenia	zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	2				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0				
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1.W zakresie wiedzy – nie ma
2. W zakresie umiejętności – nie ma
3. W zakresie innych kompetencji – nie ma

\

CELE PRZEDMIOTU

1. Przedstawienie specyfiki filozofii jako rodzaju ludzkiej wiedzy o świecie.
2.Rozwijanie umiejętności krytycznego myślenia
3.Przedstawienie uwarunkowań działalności inżynierskiej oraz ukazanie problemu społecznej odpowiedzialności nauki i techniki

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01: Zna podstawowe metody wnioskowania (indukcja, dedukcja, abdukcja). Ma podstawową wiedzę w zakresie społecznych i filozoficznych uwarunkowań działalności inżynierskiej.

Z zakresu kompetencji społecznych:

PEU_K01: Ma świadomość ważności i zrozumienie humanistycznych aspektów i skutków działalności inżynierskiej. Poznaje skutki wpływu działalności technicznej na środowisko i związaną z tym odpowiedzialność społeczną nauki i techniki.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie (plan, cel i warunki zaliczenia)	2
Wy2	Co to jest filozofia?	2
Wy3	Filozofia a inne dziedziny wiedzy (1)	2
Wy4	Filozofia a inne dziedziny wiedzy (2)	2
Wy5	Wybrane zagadnienia z filozofii nauki i techniki (1)	2
Wy6	Wybrane zagadnienia z filozofii nauki i techniki (2)	2
Wy7	Poznanie jako klasyczny problem filozofii	2
Wy8	Wybrane zagadnienia z etyki	2
Wy9	Wybrane zagadnienia z filozofii społecznej (1)	2
Wy10	Wybrane zagadnienia z filozofii społecznej (2)	2
Wy11	Wybrane zagadnienia z filozofii polityki	2
Wy12	Elementy teorii argumentacji	2
Wy13	Pytanie o człowieka	2
Wy14	Kolokwium	2
Wy15	Podsumowanie i zaliczenie kursu	2
	Suma godzin:	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład informacyjny N2. Prezentacja multimedialna N3. Film dokumentalny N4. Dyskusja

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu kształcenia	Sposób oceny osiągnięcia efektu kształcenia
F1	PEU_W01 PEU_K01	Aktywność w dyskusji
F2	PEU_W01 PEU_K01	Kolokwium, prezentacja
P = F1 + F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Blackburn S., *Oksfordzki słownik filozoficzny*, Warszawa 2004;
[2] Chalmers A., *Czym jest to, co zwiemy nauką*, Wrocław 1997;
[3] Grobler A., *Metodologia nauk*, Kraków 2004;
[4] Fry H., *Hello World. Jak być człowiekiem w dobie maszyn?*, Warszawa 2019.
[5] Martens E., Schnädelbach H., *Filozofia. Podstawowe pytania*, Warszawa 1995;
[6] Zuboff S., *Wiek kapitalizmu inwigilacji*, Warszawa 2020.

LITERATURA UZUPEŁNIAJĄCA

[1] Anzenbacher A., *Wprowadzenie do filozofii*, Kraków 2000;
[2] Buksiński T., *Współczesne filozofie polityki*, Poznań 2006;
[3] *Stanford Encyclopedia of Philosophy*, https://plato.stanford.edu/
[4] Tegmark, M., *Życie 3.0. Człowiek w erze sztucznej inteligencji*, Warszawa 2019.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Marek Sikora m.sikora@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim **Fizyka 1.1. A**
Nazwa przedmiotu w języku angielskim **Physics 1.1. A**
Kierunek studiów (jeśli dotyczy): **Telekomunikacja, Teleinformatyka, Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy): ……..
Poziom i forma studiów: **I stopień / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu: **obowiązkowy / ~~wybieralny~~ / ~~ogólnouczelniany~~ ***
Kod przedmiotu **W04CBE-SI0032G**
Grupa kursów **TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	15			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75	50			
Forma zaliczenia	Egzamin / ~~zaliczenie na ocenę~~*	~~Egzamin~~ / zaliczenie na ocenę*			
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**5**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)		2			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,3	0,7			

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Znajomość podstaw analizy matematycznej i algebry

\

CELE PRZEDMIOTU

C1. Nabycie podstawowej wiedzy z zakresu podstaw fizyki, ruchu drgającego i falowego, modeli optycznych, elektrostatyki, prądu elektrycznego, pola magnetycznego.
C2. Zdobycie umiejętności jakościowego rozumienia, interpretacji oraz ilościowej analizy – w oparciu o prawa fizyki – wybranych zjawisk i procesów fizycznych z zakresu podstaw fizyki, ruchu drgającego i falowego, modeli optycznych, elektrostatyki, prądu elektrycznego, pola magnetycznego.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna i potrafi stosować podstawowe modele fizyczne, wskazuje ich ograniczenia
PEU_W02 Zna i potrafi wyjaśnić podstawowe prawa związane z ruchem drgającym i zjawiskami falowymi, także w ujęciu optycznym.
PEU_W03 Zna i potrafi wyjaśnić podstawowe prawa elektrostatyki, elektromagnetyzmu.
PEU_W04 Zna i potrafi wyjaśnić podstawowe zagadnienia elektryczności oraz informatyki optycznej.

Z zakresu umiejętności:

PEU_U01 Potrafi ilościowo i jakościowo opisywać zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się podstawowymi prawami również dotyczącymi ruchu obiektów oraz ruchu drgającego i falowego.
PEU_U02 Potrafi ilościowo i jakościowo opisywać zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się podstawowymi prawami związanych z ruchem naładowanych cząstek.
PEU_U03 Potrafi ilościowo i jakościowo opisywać zjawiska i procesy z zakresu praktyki inżynierskiej, posługując się podstawowymi prawami optyki.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie: zakres i metodologia fizyki; metoda naukowa. Podstawowe prawa i zasady fizyki.	2
Wy2	Podstawowe prawa i zasady fizyki – siły, praca i energia mechaniczna. Zasada zachowania energii mechanicznej, zasada zachowania pędu	2
Wy3	Oscylator harmoniczny, drgania harmoniczne i swobodne, Drgania tłumione i wymuszone (rezonans) oraz składanie drgań, analiza Fouriera.	2
Wy4	Fale mechaniczne, równanie falowe, fala stojąca, energia fal, nakładanie fal, paczka falowa, prędkości w ruchu falowym, fale akustyczne, efekt Dopplera	2
Wy5, 6	Pole grawitacyjne. Prędkości kosmiczne. Podstawy elektrostatyki i elektromagnetyzmu	4
Wy7	Podstawowe prawa i definicje dla przepływu prądu stałego	2
Wy8	Kondensator – ładowanie i rozładowanie oraz magazynowanie energii, obwody prądu sinusoidalnego, moc prądu zmiennego	2
Wy9	Zjawiska i prawa optyki geometrycznej, metamateriały	2
Wy10	Elementy i przyrządy optyczne, wady odwzorowań w ujęciu inżynierskim	4
Wy11	Podstawy modelu falowego w ujęciu skalarnym, interferencja, interferometry	2
Wy12	Dyfrakcja – podstawowe prawa i podstawy przetwarzania sygnału optycznego. Dyfrakcja w ujęciu bliskiego i dalekiego pola.	2
Wy13	Elementy zapisu i odtwarzania informacji falowej w ujęciu przestrzennym, holografia	2
Wy14	Polaryzacja – podstawy modelu, stany polaryzacji, metody polaryzacji, anizotropia i dwójłomność	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		Liczba godzin
Ćw1	Rozwiązywanie zadań: wielkości wektorowe	1
Ćw 2	Rozwiązywanie zadań: podstawowe prawa i zasady fizyki	2
Ćw 3	Rozwiązywanie zadań: energia w problemach fizycznych	2
Ćw 4	Rozwiązywanie zadań: ruch drgający i fale	2
Ćw 5	Rozwiązywanie zadań: elektryczność	2
Ćw 6,7	Rozwiązywanie zadań: optyka geometryczna i falowa, przetwarzanie sygnałów optycznych	4
Ćw 8	Zajęcia uzupełniające lub zaliczeniowe	2
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE

N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych
N2. Ćwiczenia rachunkowe – metoda tradycyjna, dyskusja nad rozwiązaniami zadań
N3. Ćwiczenia rachunkowe – sprawdziany pisemne
N4. Ćwiczenia rachunkowe – zadania domowe
N5. Ćwiczenia rachunkowe – praca na zajęciach
N6. Konsultacje
N7. Praca własna – przygotowanie do ćwiczeń
N8. Praca własna – wskazana lektura dodatkowa
N9. Praca własna – przygotowanie do egzaminu

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01,PEU_W02, PEU_W03, PEU_W04	Aktywność na wykładach, prace dodatkowe, egzamin pisemny lub ustny o dopuszczeniu do egzaminu decyduje pozytywna ocena z F2
F2	PEU_U01, PEU_U02, PEU_U03	Aktywność na ćwiczeniach, ocena z pracy na zajęciach lub kolokwium końcowe
P=0.6*F1+0.4*F2, warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1 i F2, o dopuszczeniu do egzaminu decyduje pozytywna ocena z F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] D. Halliday, R. Resnick, J. Walker, Podstawy fizyki, Wydawnictwo Naukowe PWN, Warszawa 2003
[2] J. Orear, Fizyka, Wydawnictwo Naukowo-Techniczne, Warszawa 2008
[3] I.W. Sawieliew, Wykłady z fizyki, Wydawnictwo Naukowe PWN, Warszawa 2003
[4] Listy zadań publikowane przez wykładowcę

LITERATURA UZUPEŁNIAJĄCA:

[5] H.D. Young, R.A. Freedman, University Physics, Pearson-Addison Wesley 2014
[6] W. Korczak, M. Trajdos, Wektory, pochodne, całki, Wydawnictwo Naukowe PWN, Warszawa 2013

OPIEKUN PRZEDMIOTU: dr inż. Ewa Frączek, ewa.fraczek@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim	**INFORMATYKA ŚLEDCZA**
Nazwa przedmiotu w języku angielskim	**IT FORENSICS**
Kierunek studiów (jeśli dotyczy):	**CYBERBEZPIECZEŃSTWO**
Specjalność (jeśli dotyczy):	
Poziom i forma studiów:	**I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu:	**obowiązkowy/ ~~wybieralny~~ / ~~ogólnouczelniany~~***
Kod przedmiotu	W04CBE-SI0053G
Grupa kursów	**TAK / ~~NIE*~~**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15	---	30	---	---
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	---	75	---	---
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin / zaliczenie na ocenę*~~
Dla grupy kursów zaznaczyć kurs końcowy (X)	X	---	---	---	---
Liczba punktów ECTS	5	---		---	---
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0	---	2	---	---
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6	---	1,2	---	---

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Poszerzona wiedza z zakresu kodowania i szyfrowania danych (np. kurs Kodowanie i Kryptografia II), wiedza z zakresu bezpieczeństwa systemów operacyjnych (np. kurs Bezpieczeństwo Systemów Operacyjnych) oraz z zakresu ochrony informacji (np. kurs Ochrona Informacji).

\

CELE PRZEDMIOTU

C1. Nabycie wiedzy z zakresu prowadzenia analizy powłamaniowej.
C2. Nabycie wiedzy z zakresu obsługi incydentu teleinformatycznego.

C3.	Nabycie wiedzy z zakresu pozyskiwania i zabezpieczania dowodów cyfrowych w celach własnej analizy oraz przedstawienia tych dowodów innym podmiotom.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01	Zna zasady prowadzenia analizy powłamaniowej.
PEU_W02	Zna zagadnienia i procedury obsługi incydentu teleinformatycznego.
PEU_W03	Zna zagadnienia i metody analizy i przetwarzania dowodów cyfrowych.
PEU_W04	Rozumie i określa parametry dowodów cyfrowych
PEU_W05	Zna metody zapewniania rzetelności i niezaprzeczalności dowodów cyfrowych.

Z zakresu umiejętności:

PEU_U01	Potrafi przeprowadzić i udokumentować analizę powłamaniową incydentu teleinformatycznego.
PEU_U02	Potrafi stosować techniki pozyskiwania dowodów cyfrowych z różnych źródeł.
PEU_U03	Potrafi rozróżnić różne typy zapisu i formatów źródeł dowodów cyfrowych.
PEU_U04	Potrafi stosować zabezpieczenia dowodów cyfrowych.
PEU_U05	Potrafi określić potrzebne źródła i uzyskać określone informacje na zadane kwestie

Z zakresu kompetencji społecznych:

PEU_K01	Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.
PEU_K02	Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.

TREŚCI PROGRAMOWE

	Forma zajęć – wykład	**Liczba godzin**
Wy1	Wprowadzenie do analizy danych i informatyki śledczej. Omówienie podstawowych procesów i procedur w informatyce śledczej.	2
Wy2	Wskazanie prawnych aspektów IT pod kątem przygotowania materiałów do postępowań karnych, cywilnych oraz wewnątrz korporacyjnych: zasady pozyskiwania danych, nienaruszalność dowodów.	2
Wy3	Podstawy analizy danych: rozpoznawanie, pozyskiwanie istotnych informacji, rozpoznawanie typów plików, analizowanie tożsamości i aktywności użytkowników. Przedstawienie funkcjonalności narzędzi OSS / komercyjnych.	2
Wy4	Metodyka obejścia zabezpieczeń dostępu oraz analizy zdarzeń, techniki zabezpieczeń przed analizami.	2
Wy5	Metody i procedury obsługi incydentu teleinformatycznego (regulacje prawne i korporacyjne, standardy Cyber Security Incident Response Team). Raportowanie (konstrukcja raportu, raportowanie wybraną metodą na przykładzie metody KISS oraz wg zaleceń DFA).	2
Wy6	Analiza danych potokowych, śledzenie danych w sieciach.	2
Wy7	Techniki OSINT oraz zakres użycia.	2
Wy8	Kolokwium zaliczeniowe	1

	Suma godzin	**15**

Forma zajęć – ćwiczenia		**Liczba godzin**
Ćw1	---	
Ćw2	---	
Ćw3	---	
…		
	Suma godzin	

Forma zajęć – laboratorium		**Liczba godzin**
La1	Typy, formaty i zawartość plików, analizy z użyciem prostych narzędzi analitycznych.	2
La2	Metadane: ekstrakcja, podejście, metodyki.	2
La3	Standardy dekodowania i rozszyfrowywania danych, rozpoznawanie i metody oraz narzędzia.	2
La4	Pozyskiwanie danych z nośników: tworzenie i zabezpieczanie obrazów, metodyka i podejście.	2
La5	Metody i sposoby pozyskiwania danych z urządzeń różnego typu: komputerów, ruterów, przełączników, telefonów, rejestratorów.	2
La6	Narzędzia analityczne: wykorzystanie do pozyskiwania informacji klasy OSS – podstawowe funkcje, porównanie systemów.	2
La7	Narzędzia analizujące i śledzące transmisje sieciowe. Wyzwalacze, detektory. Analiza ruchu sieciowego i połączeń.	2
La8	Odzyskiwanie skasowanych i uszkodzonych danych: formaty plików, podejście i narzędzia.	2
La9	Niszczenie/wymazywanie danych metodami niedestrukcyjnymi: analiza skuteczności.	2
La10	Metodyka OSINT – białego wywiadu.	2
La11	Analizy systemów mobilnych Android oraz iOS. Podejście.	2
La12	Analizy systemów i formatów zapisu potokowego, systemy CCTV	2
La13	Zaawansowane systemy do analiz danych.	2
La14	Wykonanie pełnej analizy powłamaniowej / procesu pozyskania, zabezpieczenia i opisania dowodów cyfrowych zgodnie z przyjętą metodyką.	2
La15	Raportowanie i zabezpieczanie danych raportowych.	2
	Suma godzin	**30**

Forma zajęć – projekt		**Liczba godzin**
Pr1	---	
Pr2	---	
Pr3	---	
…		
	Suma godzin	

Forma zajęć – seminarium		**Liczba godzin**
Se1	---	
Se2	---	
Se3	---	

…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych. N2. Prezentacja syntetyczna (10 minut) zadania laboratoryjnego przez prowadzącego. N3. Realizacja zadania laboratoryjnego (wg instrukcji) na stanowisku laboratoryjnym. N4. Konsultacje. N5. Praca własna.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02 PEU_W03 PEU_W04 PEU_W05 PEU_K01	1. Ocena z kolokwium (wykład). 2. Proste zadania domowe dotyczące zagadnień przetwarzania danych.
F2	PEU_U01 PEU_U02 PEU_U03 PEU_U04 PEU_U05 PEU_K01 PEU_K02	1. Krótkie prace pisemne – testy sprawdzające przygotowanie teoretyczne do laboratoriów. 2. Proste zadania domowe dotyczące przerabianych zagadnień. 3. Rozwiązania zadań realizowanych w trakcie zajęć. 4. Sprawozdania w wykonywanych ćwiczeń.
F1 – wykład – ocena z kolokwium F2 – laboratorium – średnia ważona z ocen za poszczególne zadania wymienione w opisie F2 P = 0,6*F1 + 0,4*F2 Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu.		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
<u>LITERATURA PODSTAWOWA:</u> [1] Bruce Nikkel, „Practical forensic imaging”, No Starch Press 2016 [2] Harlan Carvey, „Analiza śledcza i powłamaniowa”, Helion 2013 **<u>LITERATURA UZUPEŁNIAJĄCA:</u>** [1] Phil Polstra, „Linux Forensics”, Pentester Academy 2015 [2] Adam Ziaja, Praktyczna analiza powłamaniowa, Wydawnictwo Naukowe PWN 2017
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
dr inż. Robert Czechowski, robert.czechowski@pwr.edu.pl,

mgr inż. Marcin Kaczmarek, marcin.kaczmarek@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim **Inżynierskie zastosowania statystyki**
Nazwa w języku angielskim **Mathematical Statistics with Applications in Engineering**
Kierunek studiów (jeśli dotyczy): **Cyberbzepieczeństwo, Telekomunikacja, Teleinformatyka**
Specjalność (jeśli dotyczy): **……..**
Poziom i forma studiów: **I stopień / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu: **obowiązkowy / ~~wybieralny~~ / ~~ogólnouczelniany~~**
Kod przedmiotu **W04CBE-SI0035G**
Grupa kursów **TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	15			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75	50			
Forma zaliczenia	Zaliczenie na ocenę	Zaliczenie na ocenę			
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**5**				
w tym liczba punktów ECTS odpowiadająca zajęciom o charakterze praktycznym (P)	-	3			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2	0,7			

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

Podstawowa wiedza w zakresie analizy matematycznej, algebry liniowej i rachunku prawdopodobieństwa

CELE PRZEDMIOTU

C1 Nabycie wiedzy na temat zadań testowania hipotez statystycznych i podstawowych testów o parametrach rozkładów oraz wybranych testów nieparametrycznych
C2 Nabycie podstawowej wiedzy na temat wymagań nakładanych na estymatory parametrów rozkładów i klasycznych metod ich konstruowania oraz stosowania.

C3 Nabycie wiedzy w zakresie zastosowań estymacji i testowania hipotez w systemach przetwarzania informacji i telekomunikacji
C4 Zdobycie umiejętności doboru i stosowania podstawowych testów statystycznych
C5 Nabycie umiejętności stosowania i doboru metody estymacji dla prostych modeli statystycznych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 posiada wiedzę na temat zadań testowania hipotez statystycznych i podstawowych testów o parametrach rozkładów oraz wybranych testów nieparametrycznych
PEU_W02 posiada wiedzę na temat wymagań nakładanych na estymatory parametrów rozkładów i klasycznych metod ich konstruowania oraz stosowania.
PEU_W03 posiada wiedzę w zakresie zastosowań estymacji i testowania hipotez w systemach przetwarzania informacji i telekomunikacji

Z zakresu umiejętności:

PEU_U01 potrafi dobrać i zastosować podstawowe testy statystyczne
PEU_U02 potrafi stosować i dobierać metod estymacji dla prostych modeli statystycznych

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Zarys tematyki wykładu i zastosowań statystyki matematycznej w systemach monitorowania jakości produkcji, automatyce, informatyce, elektronice i telekomunikacji	2
Wy2	Podstawowe pojęcia statystyki, pojęcie testu statystycznego, testy istotności, błędy I i II rodzaju, przykład prostego testu	2
Wy3	Rozkłady niezbędne do testowania hipotez, testy dla wartości średniej, porównania kilku wartosci średnich, test dla wariancji oraz ich zastosowania	2
Wy4	Test dla współczynnika korelacji,wybrane testy nieparametryczne – testy zgodności rozkładów, przykłady doboru testów i ich zastosowań	2
Wy5	Elementy teorii estymacji parametrów – wymagania stawiane estymatorom ((asymptotyczna) nieobciążoność, zgodność, wariancja estymatora i nierówność Rao-Cramera)	2
Wy6	Klasyczne metody konstruowania estymatorów (metody: momentów i największej wiarygodności, wzmianka o podejściu bayesowskim) z przykładami zastosowań	2
Wy7	Wielowymiarowy rozkład normalny i estymacja macierzy kowariancji	2
Wy8	Wstęp do estymacji regresji liniowej i testowanie hipotez z nią związanych	2
Wy9	Dobór postaci i struktury funkcji regresji	2
Wy10	Podstawowe informacje o nieliniowej i nieparametrycznej regresji	2
Wy11	Przykłady zastosowań – estymacja parametrów systemów dynamicznych	2
Wy12	Entropia i odporne metody statystyki.	2
Wy13	Wstęp do statystyki procesów stochastycznych – procesy stacjonarne	2
Wy14	Wstęp do statystyki procesów stochastycznych – dyskretne procesy Markowa	2
Wy15	Pakiety statystyczne, Big data i repretytorium.	2
	Razem	**30**

Forma zajęć - ćwiczenia		Liczba godzin
Cw1	Sprawy organizacyjne. Powtórka elementów rachunku prawdopodobieństwa.1 – zadania ilustrujące pojęcia dystrybuanty i gęstości rozkładu prawdopodobieństwa oraz ich podstawowe własności. Przykłady histogramów rzeczywistych danych (np. długości rozmów telefonicznych, danych biometrycznych, rozmiarów defektów itp.) Zadania ilustrujące rolę parametrów położenia i skali i najprostsze wersje ich estymacji, inne parametry (mediana, moda itd.).	2
Cw2	Przykłady formułowania problemów z różnych dziedzin techniki w formie testów statystycznych. Klasyfikacja rodzajów testów wraz z przeglądem repertuaru testów dostępnych w typowym pakiecie oprogramowania statystycznego. Przykłady ilustrujące pojęcie statystyki testowej, obszaru odrzucenia hipotezy, wpływu doboru poziomu istotności testu na praktyczne skutki decyzji	2
Cw3	Szczegółowa analiza testu dla wartości średniej w rozkładzie normalnym przy znanej i nieznanej wariancji z graficzną interpretacją. Rozwiązywanie zadań ilustrujących zastosowania testu dla wartości oczekiwanej przy nieznanej wariancji i porównania średnich z kilku populacji o rozkładzie normalnym (z przykładami praktycznymi badania istotności wpływu jednego czynnika).	2
Cw4	Zadania ilustrujące podstawowe własności rozkładów: chi^2, t-Studenta i F-Snedecora. Wyznaczanie ich kwantyli w pakiecie statystycznym i z tablic. Zadania ilustrujące zastosowania testu dla wariancji w rozkładzie normalnym, np. do oceny stabilności procesu produkcyjnego.	2
Cw5	Przykłady zastosowań testu Kołmogorowa-Smirnowa i testu chi^2 Pearsona do oceny rozkładu – na przykładach danych z kontroli jakości, czasów trwania rozmów telefonicznych i danych zebranych przez studentów.	2
Cw6	Testowanie istnienia zależności dla pary zmiennych losowych – test dla współczynnika korelacji i regresja liniowa.	2
Cw 7	Repetytorium	2
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z użyciem środków multimedialnych N2. Prezentacja syntetyczna problematyki ćwiczeń (ok. 10 min - przez prowadzącego) N3. Ćwiczenia rachunkowe z dyskusją rozwiązań zadań N4 Ćwiczenia rachunkowe – krótki sprawdzian pisemny N5. Konsultacje N6. Praca własna – przygotowanie do ćwiczeń N7. Praca własna – samodzielne studia, przygotowanie do końcowego sprawdzianu

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01,PEU_W02, PEU_W03	aktywność na wykładach, ocena z końcowego sprawdzianu

F2	PEU_U01, PEU_U02	aktywność na ćwiczeniach, oceny sprawdzianów pisemnych na ćwiczeniach
P = 0.5*F1 + 0.5*F2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Koronacki J., Mielniczuk J., Statystyka dla kierunków technicznych i przyrodniczych. WNT Warszawa, 2001.

[2] Gajek, Kałuszka, "Wnioskowanie statystyczne", WNT, Warszawa, 2000

[3] Wybrane rozdziały z podręczników prof. Magiery i prof. Krzyśko (będą wskazane na wykładzie)

LITERATURA UZUPEŁNIAJĄCA:

[1] Kordecki W., Rachunek prawdopodobieństwa Oficyna Wydawnicza PWr, Wrocław 2003.
[2] Krysicki W. i inni, Rachunek prawdopodobieństwa i statystyka matematyczna w zadaniach, Część I i II, PWN, Warszawa, 1996.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Prof. dr hab. inż. Ewaryst Rafajłowicz, ewaryst.rafajlowicz@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	***Kryptografia stosowana***
Nazwa w języku angielskim:	***Applied cryptography***
Kierunek studiów (jeśli dotyczy):	***Cyberbezpieczeństwo***
Specjalność (jeśli dotyczy):	
Poziom i forma studiów:	***I stopień, stacjonarna***
Rodzaj przedmiotu:	***obowiązkowy***
Kod przedmiotu	**W04CBE-SI0046G**
Grupa kursów	***TAK***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	**30**		**30**		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	**75**		**75**		
Forma zaliczenia	Egzamin		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**6**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			**2**		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	**1,4**		**1,2**		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Wiedza z zakresu wielomianów, rachunku macierzowego

\

CELE PRZEDMIOTU

C1. Zdobycie wiedzy na temat systemów kryptograficznych w telekomunikacji oraz zdobycie wiedzy umożliwiającej rozróżnianie metod szyfrowania informacji.

*niepotrzebne skreślić

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01-	Posiada wiedzę na temat miejsca zastosowania elementów kryptograficznych w kanale telekomunikacyjnym
PEU_W02-	Posiada wiedzę na temat wyznaczania odwrotności liczb w ciałach skończonych, znaczenia liczb pierwszych w kryptografii oraz wyznaczania statystycznych parametrów informacji
PEU_W03-	Zna podstawowe pojęcia stosowane w kryptografii
PEU_W04-	Posiada ogólna wiedzę na temat systemów kryptograficznych stosowanych przed erą systemów obliczeniowych.
PEU_W05-	Posiada podstawową wiedzę na temat metod kryptoanalizy algorytmów kryptograficznych
PEU_W06-	Posiada wiedzę na temat współczesnych symetrycznych algorytmów kryptograficznych oraz standardów wykorzystywanych w świecie.
PEU_W07-	Posiada wiedzę na temat niesymetrycznych systemów kryptograficznych.
PEU_W08-	Posiada wiedzę na temat sposobów realizacji podpisów cyfrowych, ich bezpieczeństwie oraz niepodrabialności
PEU_W09-	Posiada wiedzę na temat sposobów progowych i bezprogowych sposobów dzielenia tajemnicy pomiędzy większą ilość osób.
PEU_W10-	Zna podstawy kryptografii kwantowej oraz jej wykorzystanie praktyczne.
PEU_W11-	Zna pojęcie protokołu kryptograficznego i potrafi go analizować.
PEU_W12-	Zna podstawowe implementacje protokołów kryptograficznych we współczesnych systemach telekomunikacyjnych
PEU_W13-	Zna metody generowania i wykorzystania liczb pierwszych.
PEU_W14-	Zna metody zabezpieczenia i protokoły we współczesnych systemach sieciowych i komputerowych oraz systemach ochronny.

TREŚCI PROGRAMOWE

Forma zajęć – wykład		**Liczba**
Wy1	Wprowadzenie w tematykę przedmiotu oraz przypomnienie istotnych informacji na temat cyfrowego kanału telekomunikacyjnego.	2
Wy2	Elementy teorii informacji oraz operacje w ciałach skończonych. Generowanie liczb pierwszych	2
Wy3	Wprowadzenie do kryptografii. Zapoznanie się z podstawowymi pojęciami	2
Wy4	Szyfry klasyczne	2
Wy5	Symetryczne algorytmy kryptograficzne	2
Wy6	Niesymetryczne algorytmy kryptograficzne	2
Wy7	Podpisy cyfrowe, funkcje skrótu, system PKI	2
Wy8	Kryptoanaliza klasyczna oraz współczesna	2

Wy9	Współdzielenie tajemnicy, steganografia	2
Wy10	Kryptografia kwantowa	2
Wy11	Protokoły kryptograficzne	2
Wy12	Blockchain-elektroniczne pieniądze	2
Wy 13	Szyfry strumieniowe, generatory ciągów pseudolosowych.	2
Wy14	Zastosowanie praktyczne systemów kryptograficznych. Kryptografia w systemach telefonii komórkowej, w sieciach teleinformatycznych, w systemach operacyjnych. Systemy kryptograficzne z kluczem dynamicznym	2
Wy 15	Repetytorium	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		1
Ćw2		2
Ćw3		2
	Suma godzin	0

Forma zajęć - laboratorium		**Liczba godzin**
La1	Obserwacja i analiza ruchu sieciowego w oparciu o programy „tcpdump” i Wireshark.	2
La2	Implementacja w języku skryptowym wybranych szyfrów klasycznych	4
La3	Łamanie szyfrów klasycznych znanymi metodami	4
La4	Generowanie funkcji skrótu i łamanie funkcji skrótu	2
La5	Analiza siły haseł poprzez użycie gotowego oprogramowania do ich łamania np. John the Ripper, Cain &Abel	2
La6	Analiza działania współczesnych algorytmów szyfrujących	4
La7	Składanie i weryfikacja podpisu cyfrowego.	2
La8	Porównanie działania współczesnych algorytmów symetrycznych i niesymetrycznych	2
La9	Implementacja w języku skryptowym metody podziału tajemnicy w systemach progowych oraz bezprogowych. Odzyskiwanie tajemnicy oraz wskazywanie oszusta w systemach progowych.	4
La10	Łamanie szyfrów strumieniowych w sieciach bezprzewodowych	2
La11	Termin zapasowy	2
	Suma godzin	30

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	**0**

Forma zajęć - seminarium		Liczba godzin
	Suma godzin	0

STOSOWAE NARZĘDZIA DYDAKTYCZNE
1. Wykład z wykorzystaniem tablicy i slajdów 2. Materiały do wykładu na serwerze dydaktycznym https://eportal.pwr.edu.pl/). 3. Konsultacje 5. Praca własna – samodzielne studia i przygotowanie do zaliczenia końcowego/. 6. Realizacja ćwiczeń laboratoryjnych

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01PEU_W14	Egzamin
F2	PEU_W01PEU_W14	Ocena z laboratorium
70% (F1)+30% (F2). *Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu*		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] William Buchanan, Cryptography, River Publishers, 2017
[2] Roger J.Shutton Bezpieczeństwo w telekomunikacji, WKŁ, Warszawa 2004
[3] D. E. R. Denning, Kryptografia i ochrona danych, WNT, Warszawa, 1993.
[4] B. Schneier, Kryptografia dla praktyków, WNT, Warszawa, 2009
[5] M. R. Ogiela, Podstawy Kryptografii, Wydawnictwa AGH, Kraków 2000 r.

LITERATURA UZUPEŁNIAJĄCA:

[1] Kutyłowski, M. Strothmann, W.B. Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, Oficyna Wydawnicza Read Me, Warszawa 1999.
[2] W. Mochnacki, Kody korekcyjne i kryptografia, Wyd. Politechniki Wrocławskiej, 1997.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Robert Borowiec, Robert.Borowiec@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ Informatyki i Telekomunikacji

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim Metody AI w badaniu zagrożeń w systemach komputerowych

Nazwa przedmiotu w języku angielskim AI methods for threat analysis in computer systems

Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo

Specjalność (jeśli dotyczy): ……..

Poziom i forma studiów: I ~~/ II~~ stopień ~~/ jednolite studia magisterskie*, stacjonarna / niestacjonarna*~~

Rodzaj przedmiotu: obowiązkowy / ~~wybieralny~~ / ~~ogólnouczelniany~~ *

Kod przedmiotu W04CBE-SI0057G

Grupa kursów TAK / ~~NIE~~*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		75		
Forma zaliczenia	Egzamin / ~~zaliczenie na ocenę*~~	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**5**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,4		1,2		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

\

CELE PRZEDMIOTU

C1 Nabycie wiedzy z zakresu metod sztucznej inteligencji (AI) i metod uczenia maszynowego (ML) wykorzystywanych w modelowaniu i wykrywaniu zagrożeń / ataków na systemy komputerowe.

C2 Nabycie wiedzy dotyczącej metod wykrywania anomalii / nietypowych profili w oparciu o dane z monitoringu ruchu sieciowego, monitoringu zdarzeń i obciążenia urządzeń i z innych źródeł.

C3 Nabycie umiejętności doboru i zastosowania właściwych metod analizy danych w zadaniu analizy zagrożeń / wykrywania anomalii w zależności od specyfiki analizowanych danych.

C4 Nabycie umiejętności samodzielnego poszerzania wiedzy w zakresie metod AI w analizie i modelowaniu zagrożeń w systemach komputerowych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – zna najważniejsze metody sztucznej inteligencji (AI) i uczenia maszynowego (ML) stosowane w modelowaniu i wykrywaniu zagrożeń / ataków na systemy komputerowe

PEU_W02 – zna najważniejsze metody wykrywania anomalii / nietypowych profili w danych z monitoringu ruchu sieciowego, monitoringu zdarzeń i obciążenia urządzeń i z innych źródeł

PEU_W03 – zna strukturę i specyfikę zbiorów i źródeł danych wykorzystywanych w modelowaniu i wykrywaniu zagrożeń w systemach komputerowych

Z zakresu umiejętności:

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

Z zakresu kompetencji społecznych:

PEU_K01 – rozumie konieczność samodzielnego poszerzania wiedzy i umiejętności w zakresie rozwijanych metod analizy, modelowania i wykrywania zagrożeń i anomalii w systemach komputerowych

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Przegląd podstawowych metod AI i uczenia maszynowego w zadaniach związanych z modelowaniem i wykrywaniem zagrożeń w systemach komputerowych	2
Wy2	Wybrane metody analizy danych i uczenia maszynowego (uczenie nadzorowane)	4
Wy3	Uczenie nienadzorowane - wybrane metody	2
Wy4	Redukcja wymiaru	2
Wy5	Uczenie w oparciu o dane niezbalansowane i ocena jakości modeli	2
Wy6	Metody wykrywania anomalii	2
Wy7	Uczenie głębokie	4
Wy8	Metody grafowe	3
Wy9	Wizualizacja danych wielowymiarowych	2
W10	Metody modelowania szeregów czasowych	3
W11	Wyjaśnialność modeli uczenia maszynowego (XAI)	2
W12	Bezpieczeństwo systemów AI	2

	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Wprowadzenie do proponowanych zagadnień laboratoryjnych – omówienie wybranych problemów analizy zagrożeń badanych metodami AI	2
La2-3	Wprowadzenie do Pythona	3
La4	Wprowadzenie do wybranych narzędzi obliczeniowych	3
La5	Sformułowanie założeń, uszczegółowienie zadań dla poszczególnych grup laboratoryjnych	2
La6-14	Realizacja kolejnych etapów zadania laboratoryjnego (preprocesiong danych / przygotowanie środowiska analizy / budowanie modeli dot. zagrożeń / badania empiryczne dot. wykrywania zagrożeń i anomalii, itd.)	18
La15	Prezentacja i dyskusja wyników uzyskanych przez grupy laboratoryjne	2
	Suma godzin	**30**

Forma zajęć - projekt		**Liczba godzin**

Forma zajęć - seminarium		**Liczba godzin**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem prezentacji N2. Konsultacje N3. Praca własna – przygotowanie zagadnień seminaryjnych N4. Praca własna – rozwiązywanie zadań projektowych

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01 PEU_K01	Ocena wykonanych zadań laboratoryjnych,
F2	PEU_W01-03 PEU_K01	Kolokwium pisemne
P = 0.5*F1+0.5*F2, o ile F1>2 i F2>2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] T. Hastie, R. Tibshirani, J. H. Friedman, The Elements of Statistical Learning : Data Mining, Inference, and Prediction, Second Edition , Springer
[2] J. Han, M. Kamber, Data Mining: Concepts and Techniques, Second Edition, Elsevier
[3] Robert H Shumway, Time series analysis and its applications, Springer

LITERATURA UZUPEŁNIAJĄCA:

[1] N. Heard (ed), Data Science for Cybersecurity, World Scientific
[2] Shishir K Shandilya (ed), Advances in cyber security analytics and decision system, Springer
[3] Razan Abdulhammed, et al., Features dimensionality reduction approaches for machine learning based network intrusion detection, Electronics 8 (2019), no. 3, 322
[4] Asrul H Yaacob et al., Arima based network anomaly detection, 2010 Second International Conference on Communication Software and Networks, IEEE, 2010, pp. 205–209
[5] Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." ACM computing surveys (CSUR) 41.3 (2009): 1-58
[6] Amodei, Dario, et al., Concrete Problems in AI Safety. arXiv preprint arXiv:1606.06565 (2016)
[7] Agarwal, Chirag, et al., Probing GNN explainers: A rigorous theoretical and empirical analysis of GNN explanation methods. International Conference on Artificial Intelligence and Statistics. PMLR, 2022

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Henryk Maciejewski, henryk.maciejewski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA KARTA PRZEDMIOTU

Nazwa w języku polskim Metody monitorowania jakości produkcji
Nazwa w języku angielskim Methods of production quality monitoring
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): ……..
Poziom i forma studiów: I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna~~*
Rodzaj przedmiotu: obowiązkowy / ~~wybieralny~~ / ~~ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0017W
Grupa kursów ~~TAK~~ / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50				
Forma zaliczenia	~~Egzamin~~ / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**2**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)					
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Brak
2.
3.

\

CELE PRZEDMIOTU

C1 Nabycie wiedzy na temat podstawowych metod monitorowania jakości produkcji
C2

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:
PEU_W01 wiedza na temat podstawowych metod monitorowania jakości produkcji
…
Z zakresu umiejętności:
…
Z zakresu kompetencji społecznych:

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Historia i rola monitorowania jakości produkcji	2
Wy2	Podstawowa wiedza na temat metod statystycznych wykorzystywanych do monitorowania jakości produkcji cz 1	2
Wy3	Podstawowa wiedza na temat metod statystycznych wykorzystywanych do monitorowania jakości produkcji cz 2	2
Wy4	Wykrywanie zmian jakości – pojęcie karty kontrolnej i kryteria oceny kart kontrolnych, rodzaje błędów	2
Wy5	Podstawowe karty do oceny zmian wartości średniej procesu (karty: Shewharta, EWMA, CUSUM)	2
Wy6	Karty do oceny liczby i prawdopodobieństwa liczby wadliwych produktów	2
Wy7	Karty kontrolne dla wariancji	2
Wy8	Inne narzędzia statystyczne wykorzystywane w kontroli jakości cz 1	2
Wy9	Inne narzędzia statystyczne wykorzystywane w kontroli jakości cz 2	2
Wy10	Informacje o normach kontroli jakości	**2**
Wy11	Inne obszary zastosowań kart kontrolnych – wykrywanie ataków w sieciach komputerowych	**2**
Wy12	Kamery przemysłowe w monitorowaniu jakości produkcji	**2**
Wy13	Kamery na podczerwień w monitorowaniu jakości produkcji	**2**
Wy14	Inne sposoby obrazowania w monitorowaniu jakości produkcji (UV, RTG….)	**2**
Wy15	Podsumowanie	**2**
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		Liczba godzin
La1		
La2		
La3		
La4		
La5		
…		
	Suma godzin	

Forma zajęć - projekt		Liczba godzin
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Prezentacja slajdów N2. N3.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01	Aktywność w odpowiadaniu na pytania na wykładzie i sprawdzian pisemny
F2		
F3		
P=F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Rafajłowicz Ewaryst: Optymalizacja eksperymentu z zastosowaniami w monitorowaniu jakości produkcji Wrocław : Oficyna Wydawawnicza Politechniki Wrocławskiej, 2005,
[2] Rafajłowicz Ewaryst, Rafajłowicz Wojciech: Wstęp do przetwarzania obrazów przemysłowych, Wrocław : Oficyna Wydawnicza Politechniki Wrocławskiej, [2010]. 235 stron Lokalizacja elektroniczna: http://www.dbc.wroc.pl/publication/13832
[3] Thompson J.R., Koronacki J., "Statystyczne sterowanie procesami . Metoda Deminga etapowej optymalizacji jakości", AOW-PLJ, Warszawa, 1994.
[4] Hryniewicz O., Współczesne metody statystyczne w sterowaniu jakością. IBS PAN, W-wa 2006

LITERATURA UZUPEŁNIAJĄCA:

[1] Montgomery D.C. Introduction to Statistical Quality Control, Wiley, 6-th Ed/ 2009

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Prof. Ewaryst Rafajłowicz, ewaryst.rafajlowicz@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim Miernictwo 1
Nazwa przedmiotu w języku angielskim Metrology 1
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): ……..
Poziom i forma studiów: I / ~~II~~ stopień / ~~jednolite studia magisterskie*~~, stacjonarna / ~~niestacjonarna~~*
Rodzaj przedmiotu: obowiązkowy / ~~wybieralny / ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0020W
Grupa kursów TAK ~~/ NIE*~~

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75				
Forma zaliczenia	~~Egzamin~~ / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**3**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0				
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

\

CELE PRZEDMIOTU

C1. Poznanie i zrozumienie istoty pomiarów ze szczególnym uwzględnieniem roli pomiarów, ich niepewności i rzetelności na koszty jakości w jednostkach gospodarczych
C2. Poznanie zasad pomiarów i nabycie wiedzy dotyczącej niepewności pomiarów i umiejętności jej szacowania
C3. Nabycie wiedzy dotyczącej parametrów sygnałów elektrycznych, metod pomiarów i przyrządów pomiarowych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – Zna podstawowe zasady pomiarów, teorię niepewności pomiarów i techniki pomiarów wybranych sygnałów elektrycznych

PEU_W02 - Zna metody pomiarowe i sprzęt stosowany w pomiarach sygnałów elektrycznych. Jest w stanie scharakteryzować potrzeby pomiarowe pod kątem oceny parametrów sygnałów elektrycznych, wskazać wielkości mierzone, dobrać metodę pomiaru i określić miarodajność wyników

…

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Podstawowe pojęcia metrologii – definicja pomiaru, wielkości mierzonej, metodyki pomiarów, jednostki i układy miar.	2
Wy2	Spójność pomiarowa, wzorce wielkości elektrycznych, metrologia prawna i techniczna – uwierzytelnienie, wzorcowanie	2
Wy3	Teoria błędu, rodzaje błędów, niepewność pomiaru, budżet niepewności, zasady zapisu wyników i podstawy statystycznej analizy wyniku	3
Wy4	Metody pomiaru – pomiary bezpośrednie i pośrednie, rodzaje przyrządów pomiarowych	3
Wy5	Miary liniowe i logarytmiczne (decybele)	2
Wy6	Wybrane wielkości elektryczne i ich parametry – amplituda, wartość średnia, skuteczna, widmo sygnału (szereg Fouriera).	2
Wy7	Pomiary prądu i napięcia stałego oraz przemiennego małych częstotliwości	4
Wy8	Przetworniki pomiarowe – przetwarzania A/C i C/A, wpływ parametrów wejściowych przetwornika na wynik pomiaru.	2
Wy9	Przetworniki sygnałów zmiennych na sygnały stałe (peak, average, RMS), scalone przetworniki TRMS	2
Wy10	Pomiary impedancji elektrycznej i mocy dla sygnałów stałych i przemiennych	2
Wy11	Obrazowanie sygnałów elektrycznych - oscyloskop analogowy	2
Wy12	Pomiar okresu, częstotliwości i fazy	1
Wy13	Systemy pomiarowe. Interfejsy pomiarowe	1
Wy14	Podsumowanie wiadomości	2
	Suma godzin	30

STOSOWANE NARZĘDZIA DYDAKTYCZNE

N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych
N2. Ćwiczenia rachunkowe – dyskusja rozwiązań w trakcie wykładu
N3. Konsultacje
N4. Praca własna – powtórzenie wyłożonego materiału

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 – W02	Kolokwium
P = F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Chwaleba A., Poniński M., Siedlecki A.: Metrologia elektryczna. WNT, Warszawa 2003.
[2] A. Marcyniuk „Podstawy miernictwa elektrycznego dla kierunku elektronika", Wydawnictwo Politechniki Śląskiej, Gliwice 2002
[3] J. Parchański: Miernictwo elektryczne i elektroniczne, WSiP, Warszawa

LITERATURA UZUPEŁNIAJĄCA:

[1] Praca zbiorowa „Współczesna metrologia. Zagadnienia wybrane", WNT, Warszawa 2004.
[2] Dusza J. Gortat G., Leśniewski A.: Podstawy miernictwa. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 1998.
[3] Jaworski J., Morawski R., Olędzki J.: Wstęp do metrologii i techniki eksperymentu. WNT, Warszawa 1992.
[4] Piotrowski J.: Podstawy miernictwa. Wydawnictwo Politechniki Śląskiej, Gliwice 1997.
[5] Nadachowski M., Kulka Z: Przetworniki analogowo cyfrowe i cyfrowo-analogowe.
[6] Taylor J.: Wstęp do analizy błędu pomiarowego. PWN, Warszawa 1995.
[7] Międzynarodowy słownik metrologii. Pojęcia podstawowe i ogólne terminy z nimi związane (VIM); PKN-ISO/IEC Guide 99:2010
[8] Wyrażanie niepewności pomiaru. Przewodnik. Główny Urząd Miar, Warszawa 1999

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

dr hab. inż. Paweł Bieńkowski, prof. uczelni, pawel.bienkowski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim Miernictwo 2
Nazwa przedmiotu w języku angielskim Metrology 2
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): ……..
Poziom i forma studiów: I / ~~II~~ stopień / ~~jednolite studia magisterskie*~~, stacjonarna / ~~niestacjonarna~~*
Rodzaj przedmiotu: obowiązkowy / ~~wybieralny / ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0021L
Grupa kursów ~~TAK /~~ NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)			15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)			50		
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS			**2**		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)			0,6		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Wykład Miernictwo 1

\

CELE PRZEDMIOTU

C1. Nabycie umiejętności planowania i wykonywania pomiarów
C2 Nabycie umiejętności doboru metody i sprzętu pomiarowego w pomiarach wielkości elektrycznych
C3 Nabycie umiejętności zestawienia stanowiska pomiarowego, pomiarów i analizy wyników
C4. Nabycie umiejętności pomiarów napięć i prądów w obwodach prądu stałego i przemiennego
C5. Nabycie umiejętności wykorzystania oscyloskopu w pomiarach wielkości elektrycznych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu umiejętności:

PEU_U01 – potrafi wykorzystywać i obsługiwać podstawowe analogowe i cyfrowe przyrządy do pomiarów wielkości elektrycznych

PEU_U02 - Potrafi dobrać i uzasadnić metodę pomiaru podstawowych wielkości elektrycznych i oszacować niepewność wybranej metody

PEU_U03 - Potrafi zestawić stanowisko pomiarowe, dokonać pomiarów i przeanalizować wyniki tych pomiarów

PEU_U04 – potrafi zastosować oscyloskop do obrazowania i podstawowych pomiarów sygnałów elektrycznych.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
La1	Spawy organizacyjne, przepisy BHP i regulamin laboratorium	1
La2	Pomiary rezystancji i impedancji	2
La3	Pomiary napięcia i prądu stałego przyrządami analogowymi i cyfrowymi	2
La4	Pomiary wartości średniej, szczytowej i skutecznej sygnałów okresowych	2
La5	Pomiary seryjne i statystyczna analiza danych	2
La6	Oscyloskop – obsługa, dobór nastaw, obrazowanie i pomiary wybranych przebiegów elektrycznych	4
La7	Termin odróbczy lub ćwiczenie dodatkowe	2
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Praca własna – przygotowanie do ćwiczeń laboratoryjnych
N2. Sprawdzanie wiadomości przed lub w trakcie zajęć (pisemnie lub usnie)
N3. Ćwiczenia laboratoryjne – zestawianie stanowisk i pomiary
N4. Opracowanie wyników – protokoły z pomiarów
N5. Konsultacje

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01÷PEU_U04	Sprawdzanie wiadomości do poszczególnych ćwiczeń, ocena poprawności i sprawności realizacji pomiarów, protokoły z pomiarów i analiza wyników
P = F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Chwaleba A., Poniński M., Siedlecki A.: Metrologia elektryczna. WNT, Warszawa 2003.
[2] A. Marcyniuk „Podstawy miernictwa elektrycznego dla kierunku elektronika", Wydawnictwo Politechniki Śląskiej, Gliwice 2002
[3] J. Parchański: Miernictwo elektryczne i elektroniczne, WSiP, Warszawa

LITERATURA UZUPEŁNIAJĄCA:

[1] Praca zbiorowa „Współczesna metrologia. Zagadnienia wybrane", WNT, Warszawa 2004.
[2] Dusza J. Gortat G., Leśniewski A.: Podstawy miernictwa. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 1998.
[3] Jaworski J., Morawski R., Olędzki J.: Wstęp do metrologii i techniki eksperymentu. WNT, Warszawa 1992.
[4] Piotrowski J.: Podstawy miernictwa. Wydawnictwo Politechniki Śląskiej, Gliwice 1997.
[5] Nadachowski M., Kulka Z: Przetworniki analogowo cyfrowe i cyfrowo-analogowe.
[6] Taylor J.: Wstęp do analizy błędu pomiarowego. PWN, Warszawa 1995.
[7] Międzynarodowy słownik metrologii. Pojęcia podstawowe i ogólne terminy z nimi związane (VIM); PKN-ISO/IEC Guide 99:2010
[8] Wyrażanie niepewności pomiaru. Przewodnik. Główny Urząd Miar, Warszawa 1999

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

dr hab. inż. Paweł Bieńkowski, prof. uczelni, pawel.bienkowski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim	**OCHRONA INFORMACJI**
Nazwa przedmiotu w języku angielskim	**PROTECTION OF INFORMATION**
Kierunek studiów (jeśli dotyczy):	**CYBERBEZPIECZEŃSTWO**
Specjalność (jeśli dotyczy):	**BEZPIECZENSTWO SIECI/DANYCH**
Poziom i forma studiów:	**I / ~~II~~ stopień / ~~jednolite studia magisterskie*,~~ stacjonarna / ~~niestacjonarna*~~**
Rodzaj przedmiotu:	**obowiązkowy ~~/ wybieralny~~ / ~~ogólnouczelniany~~***
Kod przedmiotu	**W04CBE-SI0042G**
Grupa kursów	**TAK / ~~NIE*~~**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	---	---	---	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	---	---	---	50
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X	---	---	---	
Liczba punktów ECTS	**4**	---	---	---	
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0	---	---	---	2
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2	---	---	---	0,7

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Znajomość zagadnień odpowiedzialności w ochronie informacji (np. kurs Etyka Inżynierska I).

\

CELE PRZEDMIOTU

C1. Nabycie wiedzy z zakresu ochrony informacji

C2.	Nabycie umiejętności z zakresu przeprowadzania analizy procesów biznesowych i zasobów teleinformatycznych
C3.	Nabycie wiedzy z zakresu wdrażania Systemów Zarządzania Bezpieczeństwem Informacji

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy: (K1CBE_W20)

PEU_W01	Student ma ogólną, spójną wiedzę teoretyczną na temat dostępu do informacji oraz konstrukcji ochrony informacji niejawnych, danych osobowych i informacji objętych tajemnicą przedsiębiorstwa
PEU_W02	Potrafi określić hierarchię i metody dostępu do informacji niejawnej.
PEU_W03	Ma ogólną wiedzę dotyczącą systemów zarządzania bezpieczeństwem informacji (SZBI) zgodnych z normami/regulacjami europejskimi (NIS) i krajowymi (ustawa KSC), budowy systemów ochrony: informacji niejawnych, danych osobowych i informacji objętych tajemnicą zawodową.
PEU_W04	Potrafi określić wymagania ogólne dotyczące wdrażania systemów zarządzania bezpieczeństwem informacji zgodnych z odpowiednimi normami oraz potrafi określić wymagania oraz obszary związane z projektowaniem i wdrażaniem Polityki Bezpieczeństwa Informacji w zależności od charakteru przedsiębiorstwa
PEU_W05	Potrafi określić ogólne ramy obowiązków osób odpowiedzialnych za ochronę informacji i systemów informatycznych w organizacji.
PEU_W06	Rozumie mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację

Z zakresu umiejętności:(K1CBE_U16)

PEU_U01	Umie dokonać wstępnego przeglądu standardów ochrony informacji, potrafi przedstawić założenia poszczególnych dokumentów normatywnych i prawnych.
PEU_U02	Umie omówić niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację.
PEU_U03	Umie dokonać wstępnego przeglądu standardów ochrony informacji
PEU_U04	Potrafi określić założenia i zakres Polityki Bezpieczeństwa Informacji organizacji

Z zakresu kompetencji społecznych: (K1CBE_K10)

PEU_K01	Ma świadomość znaczenia ochrony informacji, ochrony dostępu do informacji oraz konstrukcji systemów ochrony informacji niejawnych, danych osobowych i informacji objętych tajemnicą zawodową.
PEU_K02	Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.
PEU_K03	Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		**Liczba godzin**
Wy1	Wiedza, informacje i dane jako zasoby społeczeństwa informacji	2
Wy2	Prawne aspekty ochrony informacji – charakterystyka	2

	europejskich i krajowych regulacji prawnych. Publicznoprawna ochrona informacji	
Wy3	Pojęcie informacji chronionej i klasyfikacja rodzajów chronionych informacji	2
Wy4	Systemowe zarządzanie bezpieczeństwem informacji – założenia i koncepcja systemu zarządzania bezpieczeństwem informacji Polityka bezpieczeństwa informacji. Odpowiedzialność i uprawnienia – role w ISMS struktura SZBI	2
Wy5	Struktura normy ISO 27001 – interpretacja wymagań normy	2
Wy6	Proces szacowania ryzyka bezpieczeństwa informacji	2
Wy7	Ogólna charakterystyka metodyk szacowania ryzyka bezpieczeństwa informacji	2
Wy8	Wdrożenie, utrzymanie i rozwój SZBI w organizacji – analiza wybranych przypadków	2
Wy9	Modele bezpieczeństwa i ochrony informacji w przedsiębiorstwie	2
Wy10	Bezpieczeństwo teleinformatyczne jako element kompleksowej ochrony informacji	2
Wy11	Praktyczne aspekty wdrażania Systemu Zarządzania Bezpieczeństwem Informacji	2
Wy12	Audyt bezpieczeństwa informacji	2
Wy13	Konstrukcja i zawartość polityki bezpieczeństwa informacji dla organizacji.	2
Wy14	Przechowywanie i usuwanie informacji. Metody destrukcyjne i niedestrukcyjne trwałego usuwania informacji z nośników fizycznych (szczególnie magnetycznych).	2
Wy15	Kolokwium zaliczeniowe	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1	---	
Ćw2	---	
Ćw3	---	
Ćw4	---	
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	---	
La2	---	
La3	---	
La4	---	
La5	---	
…		
	Suma godzin	

Forma zajęć - projekt		**Liczba godzin**
Pr1	---	

Pr2	---	
Pr3	---	
Pr4	---	
…		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
Se1	Omówienie tematyki seminarium oraz zalecanych pozycji literaturowych.	1
Se2 – Se8	Prezentacje studentów dotyczące przedmiotowych zagadnień. Dyskusja w grupie seminaryjnej.	14
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład problemowy N2. Dyskusja problemowa N3. Studia literaturowe N4. Opracowanie pisemne N5. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01-06, PEU_K01-02	wykład – ocena z kolokwium
F2	PEU_U01-04, PEU_K01-03	laboratorium – średnia ważona z ocen za poszczególne zadania wymienione w opisie
P = 0,6F1 + 0,4F2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Normy ISO rodziny 27000, PKN 2014 lub późniejsze
[2] Mikołaj Karpiński oraz zespół, „Bezpieczeństwo Informacji", PAK 2012
[3] Polityka bezpieczeństwa i ochrony informacji, Tadeusz Kifner
[4] Ochrona danych osobowych na podstawie RODO, Andrzej Krasuski
[5] Audyt bezpieczeństwa informacji w praktyce, Romasz Polaczek, Helion ebook 2014

LITERATURA UZUPEŁNIAJĄCA:

[1] Jakub J. Brdulak, Przemysław Sobczak, „Wybrane problemy zarządzania bezpieczeństwem informacji", OW SGH 2014
[2] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
[3] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
[4] Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Łuczak M., Tyburski J.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

dr inż. Jacek Oko jacek.oko@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim	**OCHRONA SYSTEMÓW OPERACYJNYCH**
Nazwa przedmiotu w języku angielskim	**SECURITY OF THE OPERATING SYSTEMS**
Kierunek studiów (jeśli dotyczy):	**CYBERBEZPIECZEŃSTWO**
Specjalność (jeśli dotyczy):	
Poziom i forma studiów:	**I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu:	**~~obowiązkowy~~/ wybieralny /~~ogólnouczelniany *~~**
Kod przedmiotu	**W04CBE-SI0052G**
Grupa kursów	**TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	---	45	---	---
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75	---	75	---	---
Forma zaliczenia	Egzamin / ~~zaliczenie na ocenę~~*	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X	---	---	---	---
Liczba punktów ECTS	6	---	---	---	---
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0	---	3	---	---
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,4	---	1,8	---	---

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Zaawansowana wiedza z zakresu systemó w operacyjnych (np. kurs Systemy Operacyjne), wiedza z zakresu kryptografii i kodowania (np. kurs Kryptografia i Kodowanie) oraz z zakresu ochrony informacji (np. kurs Ochrona Informacji).

\

CELE PRZEDMIOTU

C1. Poznanie metod ochrony systemów operacyjnych przed atakami naruszającymi bezpieczeństwo tych systemów.
C2. Poznanie ataków komputerowych na systemy operacyjne oraz metod wykrywania ataków z tych źródeł.
C3. Poznanie metod zapobiegania atakom oraz minimalizowania zagrożeń z nich wynikających.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy: (K1CBE_W26)

PEU_W01 Zna podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych.
PEU_W02 Zna podstawowe pojęcia audytu technicznego i testów penetracyjnych.
PEU_W03 Zna zastosowanie narzędzi: monitorowania bezpieczeństwa systemów, audytu technicznego i testów penetracyjnych.
PEU_W04 Zna zastosowanie narzędzi: monitorowania bezpieczeństwa systemów, audytu technicznego i testów penetracyjnych.

Z zakresu umiejętności:

PEU_U01 Potrafi przeanalizować sposoby ochrony systemu operacyjnego (w tym konfiguruje komponenty bezpieczeństwa systemu) oraz rozpoznać podstawowe zagrożenia oraz ataki.
PEU_U02 Potrafi wdrożyć zalecenia norm i rekomendacji do systemu operacyjnego oraz mierzyć ich skuteczność - wykonać audyt bezpieczeństwa.

Z zakresu kompetencji społecznych:

PEU_K01 Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.
PEU_K02 Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.
PEU_K03 Ma świadomość znaczenia umiejętności wyszukiwania informacji oraz jej krytycznej analizy.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		**Liczba godzin**
Wy1	Bezpieczeństwo systemów komputerowych przedstawienie i omówienie pojęć	2
Wy2	Architektura systemu operacyjnego: jądro, pliki, użytkownicy, procesy, komunikacja sieciowa.	2
Wy3	Mechanizmy uwierzytelniania stosowane w systemach operacycjnych: w oparciu o hasło, token, dane biometryczne. Zdalne uwierzytelnianie. Bezpieczeństwo uwierzytelniania. PAM, usługi katalogowe.	2
Wy4	Użytkownicy w systemie operacyjnym (modele uprawnień, ACL Access Control List, RBAC Role Base Access Control).	2
Wy5	Ochrona pamięci w systemie operacyjnym. Ochrona plików, kontrola procesów i dostęp do zasobów.	2
Wy6	Modele dotępu do zasobów: mandatory access control (MAC) discretionary access control (DAC).	2

Wy7	Planowanie i wzmacnianie bezpieczeństwa („utwardzanie") systemu operacyjnego.	2
Wy8	Rodzaje zagrożeń bezpieczeństwa w systemach operacyjnych Zagrożenia i ataki na system operacyjny.	2
Wy9	Rodzaje zagrożeń bezpieczeństwa w systemach operacyjnych Zagrożenia i ataki na system operacyjny.	2
Wy10	Bezpieczeństwo systemu Linux/Unix. Implementacje mechanizmów w głównych dystrybucjach. Najlepsze praktyki	2
Wy11	Zagrożenia sieciowe na poziomie warstw 1-4 modelu OSI	2
Wy12	Bezpieczeństwo środowisk zwirtualizowanych (bezpieczeństwo a wydajność, kierunki rozwoju mechanizmów bezpieczeństwa w środowiskach wirtualnych, dobór zestawów funkcji i narzędzi w układach hybrydowych).	2
Wy13	Bezpieczeństwo aplikacji (z uwzględnieniem bezpiecznego programowania).	2
Wy14	Narzędzia ochrony sieciowej (zapory sieciowe bezstanowe, stanowe, aplikacyjne).	2
Wy15	Kolokwium zaliczeniowe.	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1	---	
Ćw2	---	
Ćw3	---	
Ćw4	---	
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1 - 3	Analiza ruchu sieciowego (analiza pakietów, poznawanie protokołów). Zapora sieciowa (planowanie oraz konfiguracja polityk bezpieczeństwa). Monitoring skuteczności zapory.	9
La4-5	Analiza dzienników zdarzeń (logów systemowych oraz aplikacyjnych) - wykrywanie ataków (znanych wzorców ataków, anomalii, nietypowych zapisów stanowiących potencjalne zagrożenie).	6
La6	Utwardzanie systemu operacyjnego i monitoring skuteczności wykonanych działań i operacji (dobór metody do przyjętych założeń)	3
La7	Metody uwierzytelniania (PAM, RADIUS, usługi katalogowe).	3
La8-9	Szyfrowanie danych oraz implementacja bezpiecznych protokołów sieciowych.	6
La10	Symulowanie ataków i obrona przed nimi.	3
La11-15	Zadanie projektowe związane z bezpiecznym programowaniem aplikacji sieciowych	15
	Suma godzin	**45**

Forma zajęć - projekt		**Liczba godzin**
Pr1	---	
Pr2	---	
Pr3	---	

Pr4	---	
…		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1	---	
Se2	---	
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem prezentacji multimedialnych. N2. Prezentacja syntetyczna (10 minut) zadania laboratoryjnego przez prowadzącego. N3. Realizacja zadania laboratoryjnego (wg instrukcji) na stanowisku laboratoryjnym. N4. Konsultacje. N5. Praca własna.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02 PEU_W03 PEU_W04	1. Ocena z kolokwium (wykład) 2. Proste zadania domowe dotyczące zagadnień tematu wykładu
F2	PEU_U01 PEU_U02 PEU_K01 PEU_K02 PEU_K03	1. Proste zadania domowe dotyczące zagadnień laboratoryjnych 2. Rozwiązania zadań realizowanych w trakcie zajęć 3. Sprawozdania w wykonywanych ćwiczeń
F1 – wykład – ocena z kolokwium F2 – laboratorium – średnia ważona z ocen za poszczególne zadania wymienione w opisie F2 P = 0,5F1 + 0,5F2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWCBEK00027-OCHRONASYSTEMOWOPERACYJNYCH_F.DOCXA:

[1] W. Stallings, L. Brown, *Computer Security. Principles and Practice*, 3th ed., Pearson, 2015.
[2] S. Garfinkel, G. Spafford, „Bezpieczeństwo w Unixie i Internecie"
[3] A. Silberschatz, P.B. Gavin, G. Gagne, *Podstawy systemów operacyjnych*, WNT, 2005, 2006 (tł. 6th ed.).
[4] W. Stallings, *Cryptography and Network Security. Principles and Practice*, 5th ed., Pearson, 2011.
[5] G. Weidman, *Bezpieczny system w praktyce - Wyższa szkoła hackingu i testy penetracyjne*, wyd. Helion 2015
[6] A. S. Tanenbaum, H. Bos, *Systemy operacyjne*, Helion, 2016
[7] W. Stallings, *Data and Computer Communications*, 10th ed., Pearson, 2014.
[8] A. Silberschatz, *Operating System Concepts*, 8th ed., Wiley, 2010.
[9] RHCSA/RHCE Red Hat Linux Certification Study Guide (Exams EX200 & EX300), 6th Edition, **McGraw-Hill, 2011**
[10] D.J. Barrett, R.E. Silverman, R.G. Byrnes, *Linux Security Cookbook*, O'Reilly Media, 2003

LITERATURA UZUPEŁNIAJĄCA:

[1] William (Chuck) Easttom II, *Computer Security Fundamentals*, 3th ed., Pearson, 2016
[2] S. Rass, D. Slamanig, *Cryptography for Security and Privacy in Cloud Computing*, Artech House, 2014.
[3] C. P. Pfleeger, S. L. Pfleeger - *Analyzing Computer Security. A threat/Vulnerabiliity/ Countermeasure Approach* , Pearson, 2012

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

dr inż. Tomasz Surmacz, Tomasz.Surmacz@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	**Podstawy cyberbezpieczeństwa**
Nazwa w języku angielskim:	**Cybersecurity essentials**
Kierunek studiów:	**Cyberbepieczeństwo**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**obowiązkowy**
Kod przedmiotu:	**W04CBE-SI0041W**
Grupa kursów:	**NIE**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50				
Forma zaliczenia	~~Egzamin~~ / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**2**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-				
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1.

\

CELE PRZEDMIOTU

C1 Poznanie podstawowych pojęć i kategorii cyberbezpieczeństwa
C2 Nabycie podstawowej wiedzy w zakresie bezpieczeństwa systemów i sieci teleinformatycznych
C3 Nabycie podstawowej wiedzy w zakresie zagrożeń występujących w sieciach teleinformatycznych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 posiada wiedzę o podstawowych zagadnieniach cyberbezpieczeństwa
PEU_W02 posiada wiedzę o zagrożeniach w infrastrukturze teleinformatycznej
PEU_W03 posiada wiedzę o bezpieczeństwie sieci i systemów teleinformatycznych
PEU_W04 posiada wiedzę o bezpieczeństwie systemów operacyjnych

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do cyberbezpieczeństwa	2
Wy2	Zagrożenia, luki i ataki w cyberbezpieczeństwie	2
Wy3	Triada CIA, podstawy ochrony danych	2
Wy4	Kryptografia i kontrola dostępu	2
Wy5	Integralność danych, dostępność usług	2
Wy6	Podstawy działania systemów komputerowych, systemy liczbowe	2
Wy7-8	Podstawy ochrony systemów operacyjnych	4
Wy9-10	Bezpieczeństwo sieci komputerowych przewodowych i bezprzewodowych	4
Wy11	Ochrona urządzeń końcowych i sieciowych, urządzenia zapewniające bezpieczeństwo sieci	2
Wy12-13	Wykrywanie zagrożeń, reakcja na incydenty, informatyka śledcza	2
Wy14 - 15	Zaliczenie	4
	Suma godzin	**30**

Forma zajęć - laboratorium		**Liczba godzin**
	Suma godzin	
Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych N2. Konsultacje N3. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01,PEU_W02, PEU_W03, PEU_W04	Aktywność na wykładach, kolokwium zaliczeniowe
P=F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
LITERATURA PODSTAWOWA: [1] William Stallings, Lawrie Brown – Bezpieczeństwo systemów informatycznych, zasady i praktyka, Wydanie 4, Helion 2019 [2] Krzysztof Lidermann, Bezpieczeństwo informacyjne. Nowe wyzwania, PWN 2017 [3] Jan Zych, Teleinformatyka dla bezpieczeństwa 2.0, FNCE 2019 [4] Kevin Lam, David LeBlanc, Ben Smith, Ocena bezpieczeństwa sieciowego, Microsoft Press 2005 **LITERATURA UZUPEŁNIAJĄCA:** [1] Pozycje literaturowe dotyczące polityki i strategii bezpieczeństwa
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
dr inż. Sławomir Kubal (slawomir.kubal@pwr.edu.pl)

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim: Podstawy programowania
Nazwa przedmiotu w języku angielskim: The basics of programming
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy):
Poziom i forma studiów: I stacjonarna
Rodzaj przedmiotu: obowiązkowy
Kod przedmiotu: W04CBE-SI0030L
Grupa kursów: NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)			45		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)			75		
Forma zaliczenia			Zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS			3		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)			1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

\

CELE PRZEDMIOTU

C1 Zdobycie umiejętności posługiwania się językiem Python z użyciem narzędzi kontroli przepływu
C2 Zdobycie umiejętności obsługi plików w skryptach stworzonych w języku Python
C3 Zdobycie umiejętności automatyzacji zadań systemowych z wykorzystaniem języka Python

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu umiejętności:
PEU_U01 Potrafi napisać prosty skrypt w języku Python
PEU_U02 Potrafi przygotować skrypty do automatyzacji zadań systemowych
PEU_U03 Potrafi stworzyć skrypty do obsługi plików i przetwarzania danych
PEU_U04 Potrafi zaprojektować interfejs graficzny w języku Python

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1		
Wy2		
Wy3		
Wy4		
….		
	Suma godzin	

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Wprowadzenie do kursu: • wprowadzenie do języka Python • tematyka zajęć, harmonogram pracy oraz zasady zaliczania • prezentacja wybranego środowiska programistycznego	3
La2	Podstawy – typy danych, wprowadzanie wyrażeń, podstawowe funkcje, pierwszy program	3
La3	Instrukcje warunkowe, pętle, operacje logiczne i bitowe	3
La4	Definiowanie własnych funkcji, zakresy, listy, krotki, słowniki, operacje na łańcuchach znaków	3
La5	Moduły, metody list i łańcuchów znaków, wyjątki	3
La6	Programowanie obiektowe: klasy, metody, obiekty	3
La7	Obsługa plików w skryptach oraz organizacja plików	3
La8	Czas, harmonogram zadań, wielowątkowość, uruchamianie programów	3

La9	Praca z obrazami, arkuszami kalkulacyjnymi i dokumentami tekstowymi	3
La10,11	Analiza danych z wykorzystaniem modułów języka Python	6
La12	Kontrolowanie myszy i klawiatury za pomocą skryptów	3
La13,14	Projektowanie interfejsu graficznego w języku Python	6
La15	Kolokwium	3
	Suma godzin	45

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1 – Laboratorium, dyskusja i omówienie przykładów oraz metod ich analizy N2 – Laboratorium, rozwiązanie danego problemu za pomocą komputera N3 – Praca własna, przygotowanie się do ćwiczeń laboratoryjnych N4 – Konsultacje N5 – Materiały pomocnicze do wykładu i ćwiczeń laboratoryjnych udostępnione w Internecie

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01-PEU_U04	Ocena z laboratorium
P=F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Al Sweigart, Automatyzacja nudnych zadań z Pythonem. Nauka programowania. Wydanie II.
[2] Mark Lutz, Python. Wprowadzenie. Wydanie V.
[3] Dokumentacja języka Python: https://docs.python.org/

LITERATURA UZUPEŁNIAJĄCA:

[1] Wes McKinney, Python w analizie danych. Przetwarzanie danych za pomocą pakietów Pandas i NumPy oraz środowiska IPython. Wydanie II.
[2] Steven F. Lott, Python. Programowanie funkcyjne.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Mateusz Mądry, mateusz.madry@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	**Podstawy telekomunikacji**
Nazwa w języku angielskim:	**Introduction to Telecommunications**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**……**
Poziom i forma studiów:	**I, stacjonarna**
Rodzaj przedmiotu:	**obowiązkowy**
Kod przedmiotu	**W04CBE-SI0023W**
Grupa kursów:	**NIE**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	**30**	**—**	**—**	**—**	**—**
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	**—**	**—**	**—**	**—**
Forma zaliczenia	Zaliczenie na ocenę	**—**	**—**	**—**	**—**
Dla grupy kursów zaznaczyć kurs końcowy (X)	**—**	**—**	**—**	**—**	**—**
Liczba punktów ECTS	**2**	**—**	**—**	**—**	**—**
Liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	**—**	**—**	**—**	**—**	**—**
Liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	1,2	**—**	**—**	**—**	**—**

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Ogólna, podstawowa wiedza w zakresie zastosowania i użyteczności systemów telekomunikacyjnych (przewodowych i bezprzewodowych) w życiu codziennym, na potrzeby indywidualne i do celów gospodarczych.

CELE PRZEDMIOTU

C1. Nabycie wiedzy z zakresu podstaw telekomunikacji w kontekście aspektów cyberbezpieczeństwa

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – zna główne elementy, pojęcia, etapy oraz procesy zachodzące w kolejnych etapach nadawania i odbioru sygnału, z uwzględnieniem kontekstu cyberbezpieczeństwa, czyli podstawowych schematów uwierzytelniania i autoryzacji. Posiada wiedzę dot. organizacji standaryzacyjnych właściwych branży telekomunikacyjnej.

PEU_W02 – zna podstawy reprezentacji sygnałów w dziedzinie czasu i częstotliwości, w tym: zagadnienia związane konwersją analogowo-cyfrową, parametry opisujące sygnału telekom., przestrzeń widmową. Zna i rozumie definicję metryk oceny transmisji, takich jak: pojemność, przepustowość, opóźnienie, jitter. Wartości tych metryk umie interpretować w kontekście detekcji potencjalnych cyberataków.

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

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		**Liczba godzin**
Wy1	Sprawy organizacyjne. Cel i rola telekomunikacji.	2
Wy2	Pojęcie systemu telekomunikacyjnego z podstawami bezpieczeństwa.	2
Wy3	Generacja informacji z elementami przetwarzania sygnałów.	2
Wy4	Kodowanie źródłowe i kanałowe, modulacje, zwielokrotnianie kanału i dostępu, kryptografia	2
Wy5	Tor (kanał) transmisyjny	2
Wy6	Przewodowe media transmisyjne w kontekście cyberbezpieczeństwa	2
Wy7	Bezprzewodowe media transmisyjne w kontekście cyberbezpieczeństwa	2
Wy8	Sieci komputerowe, bezpieczeństwo urządzeń sieciowych i transmisji	2
Wy9	Sieci dostępowe i szkieletowe	3
Wy10	Sieci komórkowe (2G-5G) w kontekście cyberbezpieczeństwa	2
Wy11	Sieci satelitarne w kontekście cyberbezpieczeństwa	2
Wy12	Sieci rozsiewcze (DVB, DAB, FM)	2
Wy13	Sieci bezprzewodowe w kontekście cyberbezpieczeństwa	3
Wy14	Repetytorium	2
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem środków multimedialnych N2. Dyskusja problemowa N3. Konsultacje N4. Praca własna – samodzielne studia i przygotowanie do sprawdzianu końcowego.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W10	Pisemne kolokwium zaliczeniowe
P = F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
LITERATURA PODSTAWOWA [1] Krzysztof Wesołowski, *Podstawy cyfrowych systemów telekomunikacyjnych*, Wydawnictwa Komunikacji i Łączności, Warszawa 2006 [2] Simon Haykin, *Systemy telekomunikacyjne*. Cz. 1. i 2., Wydawnictwa Komunikacji i Łączności, Warszawa 2004. LITERATURA UZUPEŁNIAJĄCA [1] Ryszard Zieliński, *Satelitarne sieci teleinformatyczne*, Wydawnictwa Naukowo-Techniczne, Warszawa 2011.
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
Prof. dr hab. inż. Tadeusz Więckowski, tadeusz.wieckowski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim **Praktyka zawodowa**
Nazwa w języku angielskim **Internship**
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy):
Poziom i forma studiów: **I stopień / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu: **~~obowiązkowy~~ / wybieralny / ~~ogólnouczelniany~~ ***
Kod przedmiotu **W04CBE-SI0029Q**
Grupa kursów **~~TAK~~ / NIE***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)				175	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)				175	
Forma zaliczenia				zaliczenie na ocenę*	
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS				7	
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)				7	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)				7	

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

1. Dopuszczenie do realizacji praktyki przez pełnomocnika ds. praktyk

CELE PRZEDMIOTU

C1 Konfrontacja wiedzy, zdobytej podczas zajęć dydaktycznych objętych planem studiów, z rzeczywistymi wymaganiami stawianymi przez pracodawców.
C2 Zdobycie doświadczenia praktycznego i zawodowego, poznanie podstawowego wyposażenia technicznego i technologicznego firmy, procesów i procedur, a także poznanie specyfiki pracy dozoru technicznego.
C3 Zapoznanie się ze specyfiką środowiska zawodowego oraz kształtowanie konkretnych umiejętności zawodowych związanych bezpośrednio z miejscem realizacji praktyki.
C4 Doskonalenie umiejętności organizacji pracy własnej i zespołowej, efektywnego zarządzania czasem, sumienności, odpowiedzialności za powierzone zadania.

C5 Profesjonalizacja zachowań zawodowych, przestrzegania zasad etyki zawodowej i poszanowania różnorodności technicznych (otwartości na nowe technologie i świadomości związanej z ochroną środowiska).

*niepotrzebne skreślić

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

Z zakresu umiejętności:

PEU_U01 Ma umiejętność pracy indywidualnej i zespołowej.

PEU_U02 Ma umiejętność korzystania ze zdobytej wiedzy do twórczego analizowania i rozwiązywania różnych problemów inżynierskich.

Z zakresu kompetencji społecznych:

PEU_K01 Ma świadomość odpowiedzialności za pracę własną, jest otwarty na wymianę myśli i nowe wyzwania.

TREŚCI PROGRAMOWE

Forma zajęć - projekt		Liczba godzin
Pr1	Indywidualne zadania dla każdego studenta w zależności od wyboru miejsca realizacji praktyki	160
	Suma godzin	160

STOSOWANE NARZĘDZIA DYDAKTYCZNE

N1. Prezentacja wprowadzająca w działalność firmy.
N2. Konsultacje.
N3. Specjalistyczny sprzęt i oprogramowanie stosowane w firmie.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01, PEU_U02, PEU_K01	Ocena indywidualna (2,0....5,5) na podstawie pisemnego sprawozdania z odbytej praktyki oraz wymagań zawartych w „Regulaminie praktyk”
P= F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Sławomir Sambor (slawomir.sambor@pwr.edu.pl)

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim: Programowanie skryptowe
Nazwa przedmiotu w języku angielskim: Scripting programming
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy):
Poziom i forma studiów: I stacjonarna
Rodzaj przedmiotu: obowiązkowy
Kod przedmiotu: W04CBE-SI0044L
Grupa kursów: NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)			45		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)			125		
Forma zaliczenia			Zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS			5		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			3		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)			1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Podstawowa wiedza w zakresie języka Python

\

CELE PRZEDMIOTU

C1 Zdobycie umiejętności pisania skryptów w Bashu i PowerShellu
C2 Zdobycie umiejętności tworzenia skryptów w języku Python do pobierania i przetwarzania danych z Internetu
C3 Zdobycie umiejętności posługiwania się językiem Python do testowania podatności serwerów i aplikacji na ataki sieciowe

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu umiejętności:

PEU_U01 Potrafi napisać skrypty automatyzujące zadania systemowe za pomocą Basha albo PowerShella

PEU_U02 Potrafi napisać skrypty w języku Python, które pobierają i przetwarzają dane pobrane z Internetu

PEU_U03 Potrafi testować podatności serwerów i aplikacji na ataki sieciowe za pomocą skryptów w języku Python

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1		
Wy2		
Wy3		
Wy4		
….		
	Suma godzin	

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Wprowadzenie do kursu: • tematyka zajęć • harmonogram pracy i zasady zaliczania	3
La2,3,4	Bash – wprowadzenie, skrypty, automatyzacja zadań	9
La5,6,7	Powershell – wprowadzenie, skrypty, automatyzacja zadań	9
La8,9	Pobieranie i przetwarzanie danych pobranych z Internetu	6
La10	Usługi FTP i SSH realizowane za pomocą skryptów	3
La11	Uzyskiwanie informacji geolokalizacyjnych i wyodrębnianie metadanych z dokumentów z wykorzystaniem skryptów	3
La12	Techniki kryptograficzne w modułach języka Python	3
La13,14	Język Python do testowania podatności serwerów i aplikacji na ataki sieciowe	6
La15	Kolokwium	3
	Suma godzin	45

Forma zajęć - projekt		Liczba godzin
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1 – Laboratorium, dyskusja i omówienie przykładów oraz metod ich analizy N2 – Laboratorium, rozwiązanie danego problemu za pomocą komputera N3 – Praca własna, przygotowanie się do ćwiczeń laboratoryjnych N4 – Konsultacje N5 – Materiały pomocnicze do wykładu i ćwiczeń laboratoryjnych udostępnione w Internecie

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01-PEU_U03	Ocena z laboratorium
P=F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] José Manuel Ortega, Bezpieczeństwo sieci w Pythonie. Rozwiązywanie problemów za pomocą skryptów i bibliotek. Wydanie II.
[2] Mateusz Lach, Bash. Praktyczne skrypty.
[3] Adam Bertram, PowerShell dla administratorów systemów.

LITERATURA UZUPEŁNIAJĄCA:

[1] Jaworski Michał, Tarek Ziade, Profesjonalne programowanie w Pythonie. Poznaj najlepsze praktyki kodowania i zaawansowane koncepcje programowania.
[2] Ramalho Luciano, Zaawansowany Python. Wyd. 2.
[3] Seitz Justin, Arnold Tim, Black Hat Python. Język Python dla hakerów i pentesterów.
[4] Donald W. Jones, Jeffrey Hicks, Windows PowerShell w miesiąc. Wydanie III.
[5] Arnold Robbins, Bash. Leksykon kieszonkowy. Przewodnik dla użytkowników i administratorów systemów.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Mateusz Mądry, mateusz.madry@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ Informatyki i Telekomunikacji

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim Programowanie Systemowe
Nazwa przedmiotu w języku angielskim Systems Programming
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): ……..
Poziom i forma studiów: I / ~~II~~ stopień ~~/ jednolite studia magisterskie*, stacjonarna / niestacjonarna~~*
Rodzaj przedmiotu: obowiązkowy ~~/ wybieralny~~ / ~~ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0047G
Grupa kursów TAK / ~~NIE~~*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75		75		
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin~~ / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**6**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			3		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2		1,2		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Ogólna znajomość budowy systemów operacyjnych
2. Podstawowa znajomość środowiska UNIX
3. Podstawowa umiejętność programowania w języku C/Python

\

CELE PRZEDMIOTU

C1 Nabycie praktycznej wiedzy z zakresu programowania w środowisku UNIX
C2 Nabycie wiedzy dotyczącej komunikacji między procesami i programowania współbieżnego

C3 Nabycie wiedzy i umiejętności praktycznych dotyczących stosowania mechanizmów synchronizacji procesów
C4 Nabycie wiedzy dotyczącej modelu OSI i protokołów sieciowych w sieciach TCP/IP
C5 Nabycie wiedzy i umiejętności praktycznych dotyczących gniazdek sieciowych BSD i programowania komunikacji sieciowej w trybach klient-serwer i peet-to-peer
C6 Nabycie umiejętności wyszukiwania i korzystania z dokumentacji technicznej

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01. Znajomość modelu OSI: student, potrafi zidentyfikować poszczególne warstwy i przynależność do nich odpowiednich części oprogramowania systemowego i programów użytkownika.

PEU_W02 – student wie na czym polega kontrola procesów, sposoby uruchamiania procesów w systemie UNIX orak metody komunikacji między nimi

PEU_W02 – student zna i potrafi opisać metody synchronizacji wątków za pomocą moniotorów i zmiennych warunkowych.

PEU_W03 – student zna i kojarzy podstawowe protokoły sieciowe TCP/IP, potrafi scharakteryzować sposób komunikacji przy użyciu TCP i UDP, zna funkcje systemowe dotyczące gniazdek sieciowych pozwalające na pisanie programów sieciowych

PEU_W04 - zna model działania klient-serwer oraz peer-to-peer

Z zakresu umiejętności:

PEU_U01 Umiejętność kompilacji programów w języku C na platformie UNIX, korzystanie z edytora vim i plików projektowych Makefile

PEU_U01 Praktyczna znajomość systemów i narzędzi służących uruchamianiu procesów, komunikacji między nimi, a take mechanizmów synchronizacji zadań, monitorów, semaforów i zmiennych warunkowych.

PEU_U03 Praktyczna umiejętność pisania i testowania aplikacji sieciowych działających w architekturze klient-serwer i peer-to-peer z użyciem TCP i UDP.

Z zakresu kompetencji społecznych:

PEU_K01 Świadomość znaczenia wagi przykładanej do poprawnego pisania programów z zastosowaniem kontroli błędów i deterministycznego zachowania aplikacji.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wstęp, wprowadzenie do wykładu, wymagania	1
Wy1, Wy2	System plików, prawa dostępu, blokowanie, biblioteki systemowe, skrypty, komendy.	3
Wy3	Procesy, sterowanie procesami. Standardowe wejście i wyjście.	2

Wy4	Komunikacja między procesami za pomocą łącz nazwanych i nienazwanych..	2
Wy5	Wzajemne wykluczanie procesów, atomiczność operacji, sekcja krytyczna, niesystemowe i systemowe metody synchronizacji procesów	2
Wy6	Problemy współbieżności: zakleszczenie i zagłodzenie, synchronizacja w modelu producent-konsument	2
Wy7	Aplikacje wielowątkowe, semafory IPC i POSIX, monitory i zmienne warunkowe	2
Wy8	Komunikacja między procesami z użyciem pamięci wspólnej SHM, pamięć wirtualna	2
Wy9	Komunikacja sieciowa - adresy w sieci Internet, warstwy ISO/OSI.	2
Wy10	Protokoły sieciowe warstw 2-3, gniazda sieciowe BSD, funkcje systemowe związane z komunikacją sieciową	2
Wy11	Protokół TCP - właściwości, schemat blokowy aplikacji, funkcje systemowe, programowanie komunikacji sieciowej z użyciem gniazdek BSD	2
Wy12	Protokół UDP - właściwości, schemat aplikacji, przykłady.	2
Wy13	Zaawansowane zagadnienia sieciowe - zwielokrotnione wejście, funkcje specjalne	2
Wy14	Komunikacja RPC, standard XDR - schemat blokowy aplikacji, przykłady. Funkcje tłumaczenia nazw (DNS), protokoły sieciowe.	2
Wy15	Kolokwium zaliczeniowe	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Zajęcia wstępne – określenie tematyki zajęć, założenie kont dostępowych w laboratorium, poznanie/przypomnienie podstawowych komend systemu Unix, opanowanie pracy w systemie	2
La2-3	Opanowanie edycji tekstów, kompilacja i linkowanie przykładowych programów	4
La4	Poznanie reguł kompilacji za pomocą programu make, uruchomienie programów testujących kontrolę zadań (funkce fork, exec)	2
La5	Komunikacja międzyzadaniowa z użyciem strumieni PIPE i FIFO	2
La6	Komunikacja międzyzadaniowa z użyciem pamięci wspólnej i semaforów IPC	2
La7	Obsługa terminali i urządzeń specjalnych, sygnały	2
La8-10	Mechanizmy synchronizacji w programach wielowątkowych – biblioteka lPthreads, semafory, monitory, zmienne warunkowe	6
La11-13	Komunikacja sieciowa z użyciem TCP, aplikacje klient-serwer i peer-to-peer	6
La14-15	Komunikacja sieciowa z użyciem UDP	4

	Suma godzin	30

Forma zajęć - projekt		Liczba godzin

Forma zajęć - seminarium		Liczba godzin

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład – prezentacja z wykorzystaniem przykładów z użyciem omawianych systemów i narzędzi. N2. System operacyjny Linux – dostępny podczas zajęć laboratoryjnych, pożądana instalacja na komputerach studentów. N3. Ttestowa sieć lokalna z wybranymi urządzeniami sieciowymi dostępna dla studentów. N4. Konsultacje i dyskusje podczas zajęć projektowych. N5. Praca własna – przygotowanie do laboratorium N6. Praca własna – samodzielne studia i przygotowanie do kolokwium zaliczeniowego.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01, PEU_W02, PEU_W03, PEU_W04	Test końcowy z wykładu
F2	PEU_U01, PEU_U02, PEU_U03, PEU_K01	Średnia ocen z wykonanych zadań laboratoryjnych
P = 50% test końcowy wykład (F1) + 50% ocena z laboratorium (F2) Test końcowy zaliczony jeśli wynik >= 55%. Ocena z projektu >= 3,0. Ocena z seminarium >= 3,0		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] SILBERSCHATS, ABRAHAM : Podstawy systemów operacyjnych.
[2] STEVENS : Programowanie zastosowań sieciowych w systemie UNIX.
[3] STALLINGS W. Organizacja i architektura systemu komputerowego, WNT, Warszawa 2004

LITERATURA UZUPEŁNIAJĄCA:

[1] Bach, Maurice J. -- Budowa systemu operacyjnego UNIX
[2] Ben-Ari, M. -- Podstawy programowania współbieżnego
[3] Dokumenty RFC (Request for Comments) dostępne na stronach IETF (www.ietf.org) oraz rtfm.mit.edu

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Tomasz Surmacz, Tomasz.Surmacz@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim *Sieci komputerowe 1*
Nazwa przedmiotu w języku angielskim *Computer networks 1*
Kierunek studiów (jeśli dotyczy): *Cyberbezpieczeństwo*
Specjalność (jeśli dotyczy):
Poziom i forma studiów: I ~~/ II~~ stopień ~~/ jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna*~~
Rodzaj przedmiotu: obowiązkowy ~~/ wybieralny / ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0043G
Grupa kursów TAK / ~~NIE~~*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		75		
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**5**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-		3		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6		1,2		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

\

CELE PRZEDMIOTU

C1. Zdobycie podstawowej wiedzy dotyczącej sieci komputerowych związanej z jej funkcjonowaniem, modelem odniesienia, topologią, elementami sieci i protokołami komunikacyjnymi.
C2. Zdobycie podstawowej wiedzy o działaniu urządzeń sieciowych.
C3. Zdobycie umiejętności konfigurowania hostów i ruterów do pracy w sieci lokalnej, stosowania narzędzi diagnostycznych, obserwacji i analizy zdarzeń sieciowych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – posiada podstawową wiedze o roli i zastosowaniach sieci komputerowej. Zna modele odniesienia ISO/OSI i TCP/IP.
PEU_W02 – zna funkcje warstwy fizycznej i łącza danych na przykładzie sieci Ethernet.
PEU_W03 – zna funkcje warstwy sieciowej, sposób adresacji IP i podział na podsieci.
PEU_W04 – jest w stanie zaplanować adresację IP dla sieci, zidentyfikować topologię oraz rodzaj okablowania.
PEU_W05 – zna funkcje warstwy transportowej i aplikacji

Z zakresu umiejętności:

PEU_U01 – potrafi konfigurować parametry urządzeń z Sieciowym Systemem Operacyjnym
PEU_U02 – potrafi posługiwać się narzędziami diagnostycznymi i analizatorem protokołów.
PEU_U03 – potrafi testować działanie rutera, funkcje wyboru trasy i sprawdzać zawartość tablicy rutowania.
PEU_U04 – potrafi testować działanie przełącznika i sprawdzać zawartość tablicy MAC.
PEU_U05 – potrafi skonfigurować ruter, podstawowe parametry i rutowanie statyczne
PEU_U06 – potrafi zaplanować, podłączyć i uruchomić niewielką sieć zawierającą hosty, ruter i przełącznik.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wstęp do sieci.	2
Wy2	Modele i protokoły komunikacyjne.	2
Wy3	Warstwa dostępu do sieci. Sieć Ethernet.	2
Wy4	Warstwa sieciowa.	2
Wy5	Adresacja IP.	2
Wy6	Budowa małej sieci z wykorzystaniem rutera i przełącznika.	2
Wy7	Warstwa transportowa i warstwa aplikacji.	2
Wy8	Repetytorium.	1
	Suma godzin	**15**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Wprowadzenie. Rozpoznanie usług konwergentnych dostępnych w sieci.	2

La2	Konfiguracja Sieciowego Systemu Operacyjnego. Budowa prostej sieci z przełącznikami.	2
La3	Przechwytywanie i monitorowanie zdarzeń sieciowych z użyciem analizatora protokołów Wireshark.	2
La4	Warstwa dostępu do sieci. Analiza adresacji MAC	2
La5	Odwzorowanie adresów, analiza protokołu ARP	2
La6	Ruter i tablica rutowania. Budowa prostej sieci z użyciem rutera i przełącznika.	2
La7	Wprowadzenie do adresacji IP.	2
La8	Schemat adresacji IP ze zmienną maską (VLSM).	2
La9	Adresacja IPv6	2
La10	Testowanie sieci przy użyciu protokołu ICMP	2
La11	Warstwa transportowa - komunikacja z użyciem protokołów TCP i UDP	2
La12,13	Konfiguracja urządzeń przy użyciu protokołu SSH. Analiza przypadku – projekt i budowa małej sieci z użyciem rutera i przełącznika.	4
La14,15	Repetytorium	4
	Suma godzin	**30**

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem transparencji i slajdów oraz narzędzi symulacyjnych N2. Materiały i instrukcje laboratoryjne on-line na stronach Akademii Cisco (www.netacad.com) N3. Ćwiczenia praktyczne – konfiguracja urządzeń sieciowych i testy funkcjonalne N4. Udział w e-testach przeprowadzanych w laboratoriach komputerowych N5. Konsultacje N6. Praca własna – przygotowanie do ćwiczeń laboratoryjnych N7. Praca własna – samodzielne studia i przygotowanie do kolokwium N8. Symulator działania sieci Cisco Packet Tracer

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01-05	F1 - e-testy z wiedzy, kolokwium
F2	PEU_U01-06	F2 – ocena z zaliczenia oraz ćwiczeń laboratoryjnych
P= 0,4*F1+0,6*F2 Ocena jest pozytywna po uzyskaniu 70 procent oceny maksymalnej. Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu.		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Podręcznik interaktywny kursu CCNA „Wprowadzenie do sieci", www.netacad.com

LITERATURA UZUPEŁNIAJĄCA:

[1] Adam Józefiok, CCNA 200-125. Zostań administratorem sieci komputerowych Cisco, Wydawnictwo Helion, Gliwice 2018

[2] Wendell Odom, „Oficjalny przewodnik Przygotowanie do egzaminu na certyfikat Cisco CCENT/CCNA", Wydawnictwo naukowe PWN, Warszawa 2015

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

dr inż. Sławomir Kubal (slawomir.kubal@pwr.edu.pl)

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim *Sieci komputerowe 2*
Nazwa w języku angielskim *Computer networks 2*
Kierunek studiów (jeśli dotyczy): *Cyberbezpieczeństwo*
Specjalność (jeśli dotyczy):
Poziom i forma studiów: I ~~/ II~~ stopień*, stacjonarna ~~/ niestacjonarna*~~
Rodzaj przedmiotu: obowiązkowy ~~/ wybieralny / ogólnouczelniany *~~
Kod przedmiotu W04CBE-SI0048G
Grupa kursów TAK ~~/ NIE*~~

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		45		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		75		
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**5**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			4		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6		1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1.
2.
3.

CELE PRZEDMIOTU

C1 Zdobycie podstawowej wiedzy dotyczącej sieci komputerowych związanej z jej funkcjonowaniem, modelem odniesienia, topologią, elementami sieci i protokołami komunikacyjnymi.
C2. Zdobycie podstawowej wiedzy o działaniu urządzeń sieciowych.
C3. Zdobycie umiejętności konfigurowania hostów ruterów i przełączników do pracy w sieci lokalnej, stosowania narzędzi diagnostycznych, obserwacji i analizy zdarzeń sieciowych.
C4. Zdobycie umiejętności konfigurowania podstawowych funkcji bezpieczeństwa na urządzeniach sieciowych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – posiada podstawową wiedzę dotyczącą budowania sieci z przełącznikami i sieciami VLAN.

PEU_W02 - posiada podstawową wiedzę dotyczącą zagrożeń i bezpieczeństwa urządzeń

PEU_W03 – posiada podstawową wiedzę na temat mechanizmów nadmiarowości w sieciach lokalnych i działania usługi DHCP.

PEU_W04 – posiada podstawową wiedzę dotyczącą routingu statycznego i dynamicznego w sieciach IPv4 i IPv6

Z zakresu umiejętności:

PEU_U01 – potrafi konfigurować przełączniki Ethernet z użyciem techniki VLAN oraz rozwiązywać problemy w sieciach przełączanych.

PEU_U02 - potrafi konfigurować proste sieci z użyciem statycznego routingu w sieciach IPv4 i IPv6 oraz rozwiązywać problemy związane z działaniem sieci

PEU_U03– potrafi skonfigurować podstawowe funkcje bezpieczeństwa, mechanizmy nadmiarowości oraz usługi serwera i klienta protokołu DHCP.

Z zakresu kompetencji społecznych:

PEU_K01 – umiejętność pracy w grupie

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1,2	Koncepcja przełączania, sieci VLAN i routingu pomiędzy sieciami	4
Wy3	Nadmiarowość w sieci.	2
Wy4	Dostępność i niezawodność sieci	2
Wy5,6	Bezpieczeństwo warstwy 2 i sieci WLAN	4
Wy7,8	Koncepcja i konfiguracja routingu	3
	Suma godzin	**15**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Podstawowa konfiguracja sieciowa komputera, rutera i przełącznika	3
La2	Konfiguracja sieci VLAN i połączeń typu trunk	3
La3	Routing pomiędzy sieciami VLAN	3
La4	Badanie właściwości i konfiguracja protokołów STP, RPVST+	3
La5	Konfiguracja i diagnostyka Etherchannel	3
La6	Wdrożenie usługi DHCPv4 na urządzeniach sieciowych	3
La7	Konfiguracja DHCPv6. Konfiguracja protokołu HRSP	3
La8	Konfiguracja zabezpieczeń przełącznika	3
La9	Konfiguracja i rozwiązywanie problemów w sieci WLAN	3
La10	Konfiguracja routera i tras statycznych dla IPv4 i IPv6	3

La11	Rozwiązywanie problemów z trasami dla IPv4 i IPv6	3
La12	Repetytorium. Przygotowanie do testu umiejętności	3
La13,14,15	Test umiejętności i test końcowy	9
	Suma godzin	45

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE

N1. Wykład z wykorzystaniem transparencji i slajdów oraz narzędzi symulacyjnych
N2. Materiały i instrukcje laboratoryjne on-line na stronach Akademii Cisco (www.netacad.com)
N3. Ćwiczenia rachunkowe – dyskusja rozwiązań zadań.
N4. Ćwiczenia praktyczne – konfiguracja urządzeń sieciowych i testy funkcjonalne
N5. Udział w e-testach przeprowadzanych w laboratoriach komputerowych (www.netacad.com, eportal.pwr.edu.pl)
N6. Konsultacje
N7. Praca własna – przygotowanie do ćwiczeń laboratoryjnych
N8. Praca własna – samodzielne studia i przygotowanie do kolokwium

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01, PEU_W02, PEU_W03, PEU_W04	F1 - e-testy z wiedzy, kolokwium
F2, F3,F4,F5	PEU_U01, PEU_U02, PEU_U03, PEU_K01	F2 - ocena realizacji ćwiczeń (sprawozdania) F3 – praktyczny test umiejętności F4 - e-testy cząstkowe F5 - e-test podsumowujący
P= 30/100*F1+70/100*(30/100*F2+60/100*F3+5/100*F4+5/100*F5) Ocena jest pozytywna po uzyskaniu 70 procent oceny maksymalnej. Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu.		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Podręcznik interaktywny na kursie CCNA v.7 Switching, Routing and Wireless Essentials" (SRWE) wersja polska lub angielska, www.netacad.com

LITERATURA UZUPEŁNIAJĄCA:

[1] Adam Józefiok,CCNA 200-125. Zostań administratoterm sieci komputerowych Cisco, Wydawnictwo HELION 2018
[2] Wendell Odom,"CCNP ROUTE z CD-ROM, Oficjalny przewodnik certyfikacji", Wydawnictwo Naukowe PWN, 2014
[3] David Hucaby,"CCNP SWITCH z CD-ROM, Oficjalny przewodnik certyfikacji", Wydawnictwo Naukowe PWN, 2012

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Jarosław Janukiewicz, Jaroslaw.Janukiewicz@pwr.edu.pl

Załącznik nr 6 do ZW …….

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim Sieci komputerowe 3
Nazwa w języku angielskim Computer networks 3
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): nd
Poziom i forma studiów: I ~~/ II stopień*,~~ stacjonarna ~~/ niestacjonarna*~~
Rodzaj przedmiotu: obowiązkowy ~~/ wybieralny / ogólnouczelniany *~~
Kod przedmiotu W04CBE-SI0051G
Grupa kursów TAK ~~/ NIE*~~

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		45		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		75		
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**5**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0		4		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6		1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1.
2.
3.

\

CELE PRZEDMIOTU

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

C4. Zdobycie umiejętności konfigurowania połączeń do i w sieciach WAN, stosowania narzędzi diagnostycznych, obserwacji i analizy zdarzeń sieciowych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – posiada wiedze z zakresu skalowania sieci oraz działania sieci w topologii nadmiarowej z przełącznikami z użyciem VLAN.

PEU_W02 – posiada wiedze z zakresu ograniczania zagrożeń i zwiększania bezpieczeństwa sieci, korzystając z list kontroli dostępu IPv4 do filtrowania ruchu i bezpiecznego dostępu administracyjnego oraz najlepszych praktyk w zakresie zabezpieczeń.

PEU_W03 – rozumie i potrafi planować ruting statyczny i dynamiczny oraz zna zasady działania protokołów routingu dynamicznego, stanu łącza OSPF oraz wektora odległości EIGRP w sieciach IPv4 i IPv6.

PEU_W04 – posiada wiedzę dotyczącą projektowania sieci hierarchicznych i architektury sieci biznesowych oraz technik zapewniających skalowalność adresów i bezpieczny dostęp zdalny dla sieci WAN.

PEU_W05 - posiada wiedzę dotyczącą metod dołączania sieci LAN do ISP oraz typowych protokołów stosowanych w publicznych i prywatnych sieciach WAN (protokoły PPP, sieci VPN, usługa translacji adresów NAT).

PEU_W06 – posiada wiedzę dotyczącą zarządzania siecią (monitorowania i diagnostyki sieci), wie jak urządzenia sieciowe implementują QoS oraz w jaki sposób technologie takie jak wirtualizacja, sieci programowalne i automatyzacja wpływają na rozwijające się sieci.

Z zakresu umiejętności:

PEU_U01 – potrafi posługiwać się narzędziami diagnostycznymi i analizatorem protokołów.

PEU_U02 – potrafi konfigurować i diagnozować przełączniki i rutery.

PEU_U03 – potrafi konfigurować i diagnozować sieci VLAN, agregację łączy w technologii EtherChannel, protokół STP oraz porty brzegowe przy użyciu PortFast i BPDU Guard.

PEU_U04 - potrafi konfigurować proste sieci z użyciem statycznego wyboru trasy i protokołów dynamicznego wyboru tras, stanu łącza OSPF i wektora odległości EIGRP w sieciach IPv4 i IPv6 oraz rozwiązywać problemy związane z działaniem sieci

PEU_U05 – potrafi konfigurować podłączenia do sieci WAN na ruterach i ograniczać zagrożenia i zwiększać bezpieczeństwo sieci, korzystając z list kontroli dostępu ACL.

PEU_U06– potrafi skonfigurować usługę Network Address Translation na ruterach oraz zabezpieczenia na połączeniach site-to-site (łacza VPN).

Z zakresu kompetencji społecznych:

PEU_K01 – umiejętność pracy w grupie

TREŚCI PROGRAMOWE

	Forma zajęć - wykład	**Liczba godzin**
Wy1	Dynamiczne protokoły wyboru trasy na przykładzie OSPF.	2
Wy2	Koncepcje bezpieczeństwa sieci i listy kontroli dostępu ACL.	2
Wy3	Sieci rozległe (WAN) - techniki transmisji i protokoły oraz NAT	2
Wy4	Koncepcja VPN i IPsec. Pojęcie QoS.	2
Wy5	Projektowanie sieci i zarządzanie siecią.	2
Wy6	Rozwiązywanie problemów z sieciami.	2
Wy7	Nowe techniki sieciowe - automatyzacja i wirtualizacja sieci.	2
Wy8	Kolokwium z wykładu	1

	Suma godzin	**15**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Nadmiarowość w sieciach LAN – powtórka: • Budowa sieci przełączanej z połączeniami nadmiarowymi. • Konfiguracja Rapid PVST+, PortFast i BPDU Guard.	3
La2	Znajdowanie trasy w sieciach – powtórka: • Konfiguracja HSRP i GLBP. • Podstawowa konfiguracja RIPv2 i RIPng.	3
La3	Jednoobszarowy protokół OSPF: • Konfiguracja jednoobszarowego OSPFv2. • Konfiguracja zaawansowanych funkcji OSPFv2.	3
La4	Wieloobszarowy protokół OSPF: • Konfigurowanie wieloobszarowego OSPFv2. • Konfigurowanie wieloobszarowego OSPFv3.	3
La5	Protokół EIGRP: • Podstawowa konfiguracja EIGRP dla IPv4. • Podstawowa konfiguracja EIGRP dla IPv6.	3
La6	Bezpieczeństwo sieci: • Zabezpieczenie rutera dla dostępu administracyjnego. • Eksploracja ruchu DNS. • Badania socjotechnik.	3
La7	Listy kontroli dostępu ACL • Konfiguracja i weryfikacja rozszerzonych list ACL IPv4. • Usuwanie błędów w konfiguracji i położeniu list ACL.	3
La8	Usługa translacji adresów NAT: • Konfiguracja NAT dla IPv4. • Konfiguracja NAT dla IPv4 – sprawdzian umiejętności.	3
La9	Zarządzanie siecią: • Użycie protokołów CDP I LLDP do mapowania sieci. • Konfiguracja i weryfikacja NTP. • Stosowanie TFTP, Flash i USB do zarządzania plikami konfiguracyjnymi. • Procedury odzyskiwania hasła i przywracania konfiguracji domyślnej. • Użycie Tera Term do zarządzania plikami konfiguracyjnymi routera.	3
La10	Wirtualizacja: • Instalacja Linuksa na maszynie wirtualnej i poznanie graficznego interfejsu użytkownika.	3

	• Konfigurowanie połączeń sieciowych w środowisku wirtualnym.	
La11	Połączenia w sieci WAN, połączenia punkt-punkt: • Konfiguracja i weryfikacja protokołu eBGP. • Podstawy konfiguracji protokołu PPP z uwierzytelnianiem.	3
La12	Repetytorium	3
La13	Praktyczny test umiejętności (max. 8 osób)	3
La14	Praktyczny test umiejętności (max. 8 osób)	3
La15	E-test podsumowujący	3
	Suma godzin	60

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem transparencji i slajdów oraz narzędzi symulacyjnych. N2. Materiały i instrukcje laboratoryjne on-line na stronach eportal.pwr.wroc.pl i Akademii Sieci Komputerowych Cisco (www.netacad.com) N3. Ćwiczenia praktyczne – konfiguracja urządzeń sieciowych i testy funkcjonalne N4. Udział w e-testach przeprowadzanych w laboratoriach komputerowych (www.netacad.com) N5. Konsultacje N6. Praca własna – przygotowanie do ćwiczeń laboratoryjnych N7. Praca własna – samodzielne studia i przygotowanie do kolokwium, praktycznego testu umiejętności i e-testu podsumowującego.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01, PEU_W02, PEU_W03, PEU_W04, PEU_W05, PEU_W06	F1 - e-testy z wiedzy, kolokwium
F2, F3,F4,F5	PEU_U01,	F2 - ocena realizacji ćwiczeń (sprawozdania)

	PEU_U02, PEU_U03, PEU_U04, PEU_U05, PEU_U06, PEU_K01	F3 – praktyczny test umiejętności F4 - e-testy cząstkowe F5 - e-test podsumowujący
P= 30/100*F1+70/100*(30/100*F2+60/100*F3+5/100*F4+5/100*F5) Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie poziomu co najmniej 70 procent oceny maksymalnej z każdej z ocen formujących		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Podręcznik interaktywny kursu CCNAv7 „Sieci korporacyjne, bezpieczeństwo i automatyzacja (ENSA)", www.netacad.com

LITERATURA UZUPEŁNIAJĄCA:

[1] Wendell Odom, „Oficjalny przewodnik Przygotowanie do egzaminu na certyfikat Cisco CCENT/CCNA", Wydawnictwo naukowe PWN, Warszawa 2015
[2] Adam Józefiok, CCNA 200-125. Zostań administratorem sieci komputerowych Cisco, Wydawnictwo Helion, Gliwice 2017
[3] Adam Józefiok, CCNA 200-120. Zostań administratorem sieci komputerowych Cisco, Wydawnictwo Helion, Gliwice 2015
[4] Douglas E. Comer, Sieci komputerowe i intersieci, WNT, Warszawa 2000
[5] Andrew S. Tanenbaum, Sieci komputerowe, HELION, Gliwice 2004

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Waldemar Grzebyk, Waldemar.Grzebyk@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim Systemy operacyjne
Nazwa w języku angielskim Operating Systems
Kierunek studiów (jeśli dotyczy): Cyberpezpieczeństwo
Specjalność (jeśli dotyczy): Bezpieczeństwo sieci, Bezpieczeństwo danych
Poziom i forma studiów: I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna~~*
Rodzaj przedmiotu: obowiązkowy / ~~wybieralny / ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0005G
Grupa kursów TAK / ~~NIE~~*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		45		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75		75		
Forma zaliczenia	~~Egzamin~~ / zaliczenie na ocenę*		~~Egzamin~~ / zaliczenie na ocenę*		
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**6**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2		1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Umiejętności pracy w systemie operacyjnym z rodziny Linux.
Umiejętności pisania skryptów powłoki.

\

CELE PRZEDMIOTU

C1 Nabycie zaawansowanej wiedzy w zakresie użytkowania systemu z rodziny Linux
C2 Nabycie wiedzy z zakresu lokalnego administrowania systemem z rodziny Linux
C3 Nabycie wiedzy z zakresu sieciowego administrowania systemem z rodziny Linux
C4 Nabycie podstawowej wiedzy z zakresu bezpieczeństwa systemu z rodziny Linux
C5 Nabycie wiedzy z zakresu wirtualizacji systemów operacyjnych
C6 Nabycie zaawansowanej umiejętności pracy w systemie operacyjnym z rodziny Linux
C7 Nabycie umiejętności administrowania systemem operacyjnym z rodziny Linux
C8 Nabycie umiejętności posługiwania się najbardziej popularnym darmowym systemem wirtualizacji

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Posiada zaawansowaną wiedzę z zakresu posługiwania się systemem Linux
PEU_W02 Posiada wiedzę z zakresu administrowania systemem Linux
PEU_W03 Posiada podstawową wiedzę z zakresu bezpieczeństwa systemów z rodziny Linux
PEU_W04 Posiada wiedzę na temat zagadnień związanych z wirtualizacją systemów operacyjnych

Z zakresu umiejętności:

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

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Linux: geneza, dystrybucje, architektura, cechy, zastosowanie, silne i słaby strony, historia bezpieczeństwa. Tryb tekstowy i graficzny.	2
Wy2	Sieć: pojęcie interfejsu,tablica rutingu, zarządzanie i diagnostyka połączeń sieciowych.	2
Wy3	Serwisy sieciowe, architektura klient-serwer, pojęcie demona i usługi, startowanie i zatrzymywanie usług.	2
Wy4	Podsystem składowania danych - koncepcja w systemie Linux. Tablice partycji MBR i GPT. BIOS i EFI .	2
Wy5	Proces bootowania. LILO i GRUB. Jądro, moduły, initrd, proces Init. Sytuacje krytyczne. Cron i skrypty startowe	2
Wy6	Systemy plików: ext4, vfat, NTFS, CIFS, NFS. Narzędzia NTFS-utils. Wprowadzenie do narzędzia losetup.	2
Wy7	Uprawnienia i zasady bezpieczeństwa w systemie Linux. Uprawnienia plików,	2

	pliki SUID i SGID. Identyfikatory i uprawnienia procesów.	
Wy8	Ochrona danych dyskowych. Kopie zapasowe i nadmiarowość nośników fizycznych. Tworzenie obrazów dysków. Narzędzia Tar i dd.	2
Wy9	System LVM. RAID programowy w Linux-ie, szyfrowanie dysków i partycji.	2
Wy10	Tunele i Wirtualne Sieci Prywatne. VPN – podstawy, OpenVPN, IPSec. Tunele SSH.	2
Wy11	Wirtualizacja: wprowadzenie, rodzaje wirtualizacji, możliwości i zastosowania.	2
Wy12	Implementacja środowisk w systemach wirtualnych. Popularne systemy wirtualizacji.	2
Wy13	Ochrona systemów wirtualizacji. Tworzenie kopii i przywracanie środowisk wirtualnych. Monitoring środowisk wirtualnych. Bootowanie BIOS i EFI.	2
Wy14	Dzienniki systemowe, syslog, logi jądra. Ochrona dzienników i centralne logowanie.	2
Wy15	Kolokwium zaliczeniowe	
	Razem	**30**

Forma zajęć - laboratorium		Liczba godzin
La1	Informacje organizacyjne, zasady pracy w laboratorium, zasady oceniania. Narzędzia wykorzystywane podczas zajęć.	3
La2	Instalacja i personalizacja systemu Linux. Konsola graficzna. Menedżery pulpitu i okien. Graficzne narzędzia zarządzania systemem.	3
La3-4	Konfiguracja sieci i usług w systemie operacyjnym. Połączenia klient-serwer.	6
La5-6	Partycjonowanie dysków. Kompilacja i uruchomienie jądra. Konfiguracja crontab.	6
La7-8	Sieciowe systemy plików: NFS i CIFS.	6
La9-10	Uprawnienia plików i procesów. Pliki krytyczne i specjalne.	6
La11	Tworzenie kopii zapasowych danych i obrazów dysków.	3
La12-13	Konfiguracja LVM, RAID, szyfrowanie dysków o partycji.	6
La14	OpenVPN i tunele SSH.	3
La15	Wirtualizacja – konfiguracja i zarządzanie.	3
	Suma godzin	**45**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem prezentacji multimedialnych N2. Wykład problemowy N3. Ćwiczenia praktyczne na stanowisku laboratoryjnym N4. Konsultacje N5. Dyskusja N6. Praca własna – przygotowanie do wykładu i do zajęć laboratoryjnych

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 - PEU_W04	Egzamin testowy, egzamin ustny.
F2	PEU_U01 - PEU_U04	Weryfikacja praktycznych umiejętności na stanowisku komputerowym. Ocena stopnia realizacji ćwiczeń w laboratorium, sprawozdania z ćwiczeń laboratoryjnych. Odpowiedź ustna.
P =2/3 F1 + 1/3 F2, warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1 i F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

literatura PODSTAWOWA:

[1] Dennis Matotek, James Turnbull, Peter LieverdinkLinux. Linux Profesjonalne administrowanie systemem. Wydanie II. Wydawnictwo Helion, 2018

[2] Brian Ward. Jak działa Linux. Podręcznik administratora. Wydanie III. Wydawnictwo Helion, 2022

literatura UZUPEŁNIAJĄCA:

[1] Robert Love. Linux : programowanie systemowe. Gliwice: Helion, 2014.Ellen Siever. Linux in a nutshell. Sebastopol, Calif: O'Reilly Media, 2009.

[2] Łukasz Sosna. Linux : komendy i polecenia. Gliwice: Wydawnictwo Helion, 2014.

[3] Dokumentacja wybranej dystrybucji systemu operacyjnego Linux

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Marcin Głowacki (marcin.glowacki@pwr.edu.pl)
Mgr inż. Jacek Herold, mgr inż. Bartłomiej Balcerek

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ Informatyki i Telekomunikacji

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim Testy penetracyjne
Nazwa przedmiotu w języku angielskim Penetration tests
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): ……..
Poziom i forma studiów: I/~~II~~ stopień ~~/ jednolite studia magisterskie*, stacjonarna / niestacjonarna~~*
Rodzaj przedmiotu: obowiązkowy ~~/ wybieralny~~ / ~~ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0056G
Grupa kursów TAK / ~~NIE~~*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		45		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		50		
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**4**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6		1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1.
2.
3.

\

CELE PRZEDMIOTU

C1 Zaznajomienie z podstawową wiedzą, narzędziami i technikami wykonywania testów penetracyjnych w celu odnalezienia i wyeliminowania słabych punktów - elementów

podatnych na ataki, zarówno w obszarze infrastruktury teleinformatycznej jak i na poziomie aplikacji internetowych.

C2. Nabycie umiejętności planowania i przeprowadzania testów penetracyjnych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna koncepcję oraz cele testowania penetracyjnego.

PEU_W02 Posiada wiedzę o sposobach i narzędziach do prowadzania testów penetracyjnych.

Z zakresu umiejętności:

PEU_U01 Potrafi planować i przygotowywać procedury testowania penetracyjnego.

PEU_U02 Umie przeprowadzać podstawowe testy penetracyjne w obszarze infrastruktury teleinformatycznej oraz na poziomie aplikacji internetowych.

PEU_U03 Umie zaprezentować i omówić w sposób logiczny i zrozumiały opracowane koncepcje oraz dokumentację techniczną.

Z zakresu kompetencji społecznych:

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie. Potrzeba i geneza testowania penetracyjnego.	1.5
Wy2	Metodologia. Narzędzia wykorzystywane przez pentestera	1.5
Wy3	OSINT, Wykrywanie wirtualnych hostów, składnia HTTP, HTTPS, testowanie HTTPS, profilowanie celu	1.5
Wy4-5	Content Discovery, Autoryzacja/Autentykacja, testowanie sesji	3
Wy6-7	Testowanie wstrzyknięć (Command Injection, File Inclusion, Directory Traversal, SQL Injection, Insecure Deserialization)	3
Wy8-10	XSS, SSRF, XXE, Clickjacking, CSRF, Raportowanie	4.5
	Suma godzin	**15**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Przygotowanie środowiska laboratoryjnego, przedstawienie zadania projektowego,	3

	omówienie formatu raportu	
La2-La3	Open Source Intelligence (OSINT), Wprowadzenie do systemu Kali Linux	6
La4	Rekonesans oraz skany podatności	3
La5-La6	Exploitacja Web	6
La7-8	Exploitacja Serwisów	6
La9-La10	Privilege Escalation na systemie linux	6
La11-15	Przygotowanie raportu z testów penetracyjnych maszyny przydzielonej grupie projektowej	15
	Suma godzin	**45**

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3-Pr5		
Pr6-Pr8		
Pr9-Pr11		
Pr12-Pr14		
Pr15		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem transparencji i slajdów oraz narzędzi symulacyjnych N2. Materiały i instrukcje laboratoryjne on-line na stronach PWR N3. Ćwiczenia praktyczne – konfiguracja urządzeń i testy funkcjonalne N4. Konsultacje N5. Praca własna – przygotowanie projektów N6. Praca własna – samodzielne studia i przygotowanie do kolokwium

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01-02	dyskusje, kolokwium końcowe
F2	PEU_U01-03	dokumentacja projektowa, sprawozdania z laboratoriów

P=(F1+F2)/2
warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] "Web Security Testing Guide", OWASP
[2] "Bezpieczeństwo aplikacji webowych", Securitum
[3] "Ethical Hacking and Penetration Testing Guide", Baloch, Rafay

LITERATURA UZUPEŁNIAJĄCA:

[1] PortSwigger Web Academy
[2] „Black Hat Python. Język Python dla hakerów i pentesterów", Seitz Justin, Arnold Tim

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Michał Walkowski michal.walkowski@pwr.edu.pl

Studium Nauk Humanistycznych i Społecznych

KARTA PRZEDMIOTU

Nazwa w języku polskim **Własność intelektualna i prawo autorskie**
Nazwa w języku angielskim **Intellectual Property Law and Copyright**
Kierunek studiów (jeśli dotyczy): **Cyberbezpieczeństwo, Telekomunikacja, Teleinformatyka**
Specjalność (jeśli dotyczy): **……..**
Poziom i forma studiów: **I stopień / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu: **obowiązkowy / ~~wybieralny~~ / ogólnouczelniany**
Kod przedmiotu **W08W04-SI0002W**
Grupa kursów **~~TAK~~ / NIE***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25				
Forma zaliczenia	zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	1				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0				
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

1.W zakresie wiedzy – nie ma
2. W zakresie umiejętności – nie ma
3. W zakresie innych kompetencji – nie ma

\

CELE PRZEDMIOTU

1 Zaznajomienie studentów z podstawowymi wiadomościami z zakresu prawa z uwzględnieniem systemu prawnomiędzynarodowego
2 Przegląd podstawowych instytucji prawa
3 Analiza przepisów prawnych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01: Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego – umie korzystać z zasobów informacji patentowej

Z zakresu kompetencji społecznych:

PEU_K01: Rozumie prawne aspekty i skutki działalności inżynierskiej.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie	1
Wy2	Funkcje Prawa	1
Wy3	Źródła prawa	1
Wy4	Wieloaspektowość prawa	1
Wy5	Prawo precedensowe	1
Wy6	Prawo stanowione	1
Wy7	Podstawy prawa autorskiego i prawa własności intelektualnej	1
Wy8	Przedmiot i podmiot prawa własności intelektualnej	1
Wy9	Autorskie prawa majątkowe	1
Wy10	Autorskie prawa osobiste	1
Wy11	Program komputerowy jako dzieło autorskie; Rodzaje licencji	1
Wy12	Program komputerowy w systemie prawa patentowego	1
Wy13	Prawo patentowe	1
Wy14	Kolokwium	1
Wy15	Podsumowanie i zaliczenie kursu	1
	Suma godzin:	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład informacyjny N2..Prezentacja multimedialna N3. Wykład interaktywny N4. Film dokumantalny

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_K01	Aktywność w dyskusji
F2	PEU_W01 PEU_K01	Kolokwium, prezentacja
P = F1 + F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
LITERATURA PODSTAWOWA: [1] R. Golat, Prawo autorskie i prawa pokrewne, C.H.Beck, 2010 [2] M. Barczewski, Traktatowa ochrona praw autorskich i praw pokrewnych, Wolters Kluwer Polska,2007 [3] M. Byrska, Wytyczne EWG w sprawie ochrony programów komputerowych a polski projekt prawa autorskiego, ZNUJ PWiOWI 1993 [4] A. Andrzejuk Zagadnienia etyki zawodowej. NAVO. Warszawa. 1998. **LITERATURA UZUPEŁNIAJĄCA** [1] J. Barta, R. Markiewicz (red.) Prawo autorskie i prawa pokrewne. Komentarz, Warszawa 2011 [2] P. Slezak, Prawo autorskie. Wzory umów z komentarzem, Wolters Kluwer Polska - LEX, 2012
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
dr Renata Kopczyk r.kopczyk@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim Wprowadzenie do systemów komputerowych
Nazwa w języku angielskim
Kierunek studiów (jeśli dotyczy): Cyberpezpieczeństwo
Specjalność (jeśli dotyczy): Bezpieczeństwo sieci, Bezpieczeństwo danych
Poziom i forma studiów: I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna~~*
Rodzaj przedmiotu: obowiązkowy / ~~wybieralny / ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0045G
Grupa kursów TAK / ~~NIE~~*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		45		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75		50		
Forma zaliczenia	~~Egzamin~~ / zaliczenie na ocenę*		~~Egzamin~~ / zaliczenie na ocenę*		
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**5**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-		2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2		1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

\

CELE PRZEDMIOTU

C1 Nabycie wiedzy w zakresie budowy i zasad działania systemów operacyjnych.
C2 Nabycie wiedzy w zakresie współbieżność, szeregowanie zadań.
C3 Nabycie wiedzy w zakresie zarządzanie pamięcią operacyjną i masową.
C4 Nabycie wiedzy w zakresie zarządzanie urządzeniami.
C5. Nabycie wiedzy w zakresie bezpieczeństwa i ochrony,
C6. Nabycie wiedzy w zakresie budowy systemu plików.
C7 Nabycie wiedzy w zakresie działania systemów rozproszonych, ze szczególnym uwzględnieniem budowy rozproszonego systemu plików.
C8 Nabycie umiejętności pracy w systemie operacyjnym z rodziny Linux.
C9. Nabycie umiejętności pisania skryptów powłoki.
C10 Nabycie praktycznych umiejętności w zakresie prowadzenia eksperymentalnej oceny

algorytmów szeregowania i zastępowania stron.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Posiada podstawową wiedzę z zakresu budowy systemów operacyjnych.
PEU_W02 Posiada wiedzę w zakresie zasad działania podsystemów systemu operacyjnego..
PEU_W03 Zna podstawowe algorytmy szeregowania zadań.
PEU_W04 Posiada wiedzę w zakresie działania typów systemów rozproszonych i rozproszonych systemów plików.

Z zakresu umiejętności:

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

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wstęp, rys historyczny, struktura systemów operacyjnych, ich miejsce w systemach komputerowych. Przegląd struktur.	2
Wy2	Procesy - pojęcie i koordynacja. Rola planistów w systemie. Algorytmy planowania	2
Wy3	Koordynowanie procesów. Przegląd typowych problemów.	2

Wy4	Koordynowanie procesów - Semafory. Problemy synchronizacji, problem czytelników i pisarzy, problem posilających się filozofów	2
Wy5	Komunikacja międzyprocesowa	2
Wy6	Blokady, warunki ich powstawania Metody wychodzenia z blokad.	2
Wy7	Zarządzanie pamięcią operacyjną - przesłanki, ładowanie dynamiczne,łączenie dynamiczne, nakładki.	1
Wy8	Schemat ciągłego modelu pamięci oraz strategie przydziału.	1
Wy9	Model dyskretny pamięci operacyjnej - stronicowanie. Problemy ochrony.	1
Wy10	Pamięć wirtualna. Stronicowanie na żądanie. Zastępowanie stron (algorytmy). Przydział ramek (algorytmy).	2
Wy11	Zarządzanie pamięcią pomocniczą. Struktura dysku, podstawowe pojęcia. Katalog urządzenia. Zarządzanie wolnymi obszarami, metody przydziału miejsca na dysku. Planowanie dostępu do dysku.	3
Wy12	Organizacja systemu plików (Pojęcie pliku, struktura katalogowa, Operacje plikowe)	2
Wy13	Metody dostępu do informacji zawartej w pliku; semantyka spójności. Organizacja struktury katalogowej. Ochrona plików	2
Wy14	System ochrony. Powody ochrony, dokumenty ochrony; statyczne i dynamiczne. Ochrona w istniejących systemach.	2
Wy15	Wewnętrzne struktury i funkcje systemu wejścia-wyjścia.	2
Wy16	Systemy rozproszone.	2
	Razem	**30**

Forma zajęć - laboratorium		**Liczba godzin**
La1	Informacje organizacyjne, zasady pracy w laboratorium, zasady oceniania. Narzędzia wykorzystywane podczas zajęć.	3
La2	Narzędzia wykorzystywane podczas zajęć. Praca w systemie Linux - przegląd poleceń powłoki.	6
La3	Zapoznanie z programami find, talk, telnet, ftp, finger.	3
La4	Praca z urządzeniami wejścia-wyjścia.	3
La5	Wyrażenia regularne grep, sed, awk	6
La6	Ćwiczenia z pisania skryptów powłoki	6
La7	Zarządzenie procesami i komunikacja międzyprocesowa: bg, fg, nice, flock, wait	3
La8	Przeprowadzenie oceny eksperymentalnej jakości wybranych algorytmów planowania z wywłaszczeniem i bez wywłaszczenia dla otwartej i zamkniętej puli zadań	9
La9	Eksperymentalna ocena jakości wybranych algorytmów zastępowania stron	6
	Suma godzin	**45**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem prezentacji multimedialnych N2. Wykład problemowy N3. Ćwiczenia praktyczne na stanowisku laboratoryjnym N4. Konsultacje N5. Dyskusja N6. Praca własna – przygotowanie projektu oprogramowania symulacyjnego, przygotowanie do wykładu i do zajęć laboratoryjnych

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W04	Egzamin testowy, egzamin ustny.
F2	PEU_U01 PEU_U04	Weryfikacja praktycznych umiejętności na stanowisku komputerowym. Ocena stopnia realizacji ćwiczeń w laboratorium, sprawozdania z ćwiczeń laboratoryjnych. Ocena sprawozdania zawierającego projekt eksperymentu, niezbędnego oprogramowania symulacyjnego, rezultaty oraz wnioski z badań. Odpowiedź ustna.
P =2/3 F1 + 1/3 F2, warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1 i F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

literatura PODSTAWOWA:

[1] Silberschatz A., Peterson J.L., Galvin P.B., *Podstawy systemów operacyjnych*, WNT, Warszawa 2006.
[2] Bach M.J., *Budowa systemu operacyjnego UNIX*, WNT, Warszawa 1995.
[3] Stallings W., *Systemy operacyjne*, Robomatic, Wrocław 2003.
[4] Lister A.M., Eager R.D., *Wprowadzenie do systemów operacyjnych*,WNT Warszawa 1994
[5] Andrew Tanenbaum. Systemy operacyjne. Gliwice: Wydawnictwo Helion, 2016. .
[6] Stallings W., *Organizacja i architektura systemu komputerowego*, WNT, Warszawa 2004.

literatura UZUPEŁNIAJĄCA:

[1] Carl Albing. Bash : receptury. Gliwice: Helion, 2012. ISBN: 978-83-246-1378-6.
[2] Mateusz Lach. BASH : praktyczne skrypty. Gliwice: Helion, 2015. ISBN: 978-83-283-1489-4.
[3] Sarath Lakshman. Skrypty powłoki systemu Linux : receptury. Gliwice: Wydawnictwo Helion, 2012. ISBN: 978-83-246-3886-4.
[4] Robert Love. Linux : programowanie systemowe. Gliwice: Helion, 2014.Ellen Siever. Linux in a nutshell. Sebastopol, Calif: O'Reilly Media, 2009.
[5] Łukasz Sosna. Linux : komendy i polecenia. Gliwice: Wydawnictwo Helion, 2014.
[6] Dave Taylor. Genialne skrypty powłoki : ponad 100 rozwiązań dla systemów Linux, macOS i Unix. Gliwice: Helion, 2017.
[7] Dokumentacja wybranej dystrybucji systemu operacyjnego Linux

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Paweł Trajdos, pawel.trajdos@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim	**WYKRYWANIE ZAGROŻEŃ I REAKCJA NA INCYDENTY**
Nazwa przedmiotu w języku angielskim	**THREAT DETECTION SYSTEMS**
Kierunek studiów (jeśli dotyczy):	**CYBERBEZPIECZEŃSTWO**
Specjalność (jeśli dotyczy):	**BEZPIECZENSTWO SIECI**
Poziom i forma studiów:	**I / ~~II~~ stopień*, stacjonarna ~~/ niestacjonarna*~~**
Rodzaj przedmiotu:	**obowiązkowy / ~~wybieralny/ ogólnouczelniany~~ ***
Kod przedmiotu	**W04CBE-SI0028G**
Grupa kursów	**TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	---	30	---	---
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	---	50	---	---
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin / zaliczenie na ocenę*~~
Dla grupy kursów zaznaczyć kurs końcowy (X)	X	---	---	---	---
Liczba punktów ECTS	4	---			---
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0	---	3	---	---
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2	---	1,2	---	---

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Zaawansowana wiedza z zakresu systemów operacyjnych (np. kurs Bezpieczeństwo Systemów Operacyjnych), wiedza z zakresu kryptografii i kodowania (np. kurs Kryptografia i Kodowanie) oraz z zakresu ochrony informacji (np. kurs Ochrona Informacji).

\

CELE PRZEDMIOTU

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

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

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

Z zakresu umiejętności:

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

Z zakresu kompetencji społecznych:

PEU_K01 Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.
PEU_K02 Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.
PEU_K03 Ma świadomość znaczenia umiejętności wyszukiwania informacji oraz jej krytycznej analizy.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Omówienie zasad zaliczenia. Wprowadzenie do tematyki wykładu.	2
Wy2	Monitoring bezpieczeństwa systemów informatycznych – pojęcia i definicje powiązane z monitoringiem bezpieczeństwa systemów informacyjnych i informatycznych.	2
Wy3	Monitorowanie i wykrywanie zagrożeń bezpieczeństwa w systemach teleinformatycznych i sieciach komputerowych – klasyfikacja oraz metody.	2

Wy4	Monitorowanie systemów operacyjnych.	2
Wy5	Monitorowanie protokołów sieciowych.	2
Wy6	Metody ataków i narzędzia w nich wykorzystywane.	2
Wy7	Metody ochrony przed atakami.	2
Wy8	Podatności systemów teleinformatycznych	2
Wy9	Systemy monitorowania przebiegu infekcji	2
Wy10	Metody wykrywania zagrożeń (metody oparte o sygnatury, statystyki, analizy on-line, heurystykę, algorytmy genetyczne).	2
Wy11	Kompleksowy system detekcji oraz reagowania na zdarzenia w infrastrukturze sieciowej: systemy wykrywające włamania (intruzów)(IDS) oraz systemy prewencyjne (IPS). Organizacja systemów.	2
Wy12	Analiza oraz korelacja zdarzeń (systemy klasy SIEM).	2
Wy13	Strategie i tendencje w monitorowaniu i wykrywaniu zagrożeń bezpieczeństwa. Organizacja Security Operation Ceneter. Incydenty bezpieczeństwa informacji – procedury reagowania, dokumentowanie incydentów.	2
Wy14	Repetytorium	2
Wy15	Kolokwium zaliczeniowe.	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1	---	
Ćw2	---	
Ćw3	---	
Ćw4	---	
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Poznanie podstawowych narzędzi monitorowania systemu operacyjnego oraz sieci komputerowej.	2
La2-3	Poznanie narzędzi wykrywania intruzów (IDS).	4
La4-5	Poznanie narzędzi prewencyjnych (IPS).	4
La6	Monitorowanie przebiegu infekcji malware - system honeypot.	2
La7	Analiza malware z wykorzystaniem „piaskownicy” - „sandbox”.	2
La8-9	Systemy korelacji i analizy zagrożeń (np. Splunk, QRadar,).	4
La10-11	Monitorowanie i wykrywanie zagrożeń w systemach klasy SIEM.	4
La12	Monitorowanie komunikacji sieciowej (audyt transakcji sieciowych, analiza przepływów w sieci, metody wizualizacji aktywności sieciowej systemów).	2
La13	Narzędzia monitorowania parametrów oraz dostępności komponentów sieciowych oraz usług (NMS, Nagios).	2
La14	Narzędzia monitorowania konfiguracji bezpieczeństwa systemu.	2
La15	Korzystanie z baz wiedzy o zagrożeniach oraz wymiany informacji przy monitorowaniu i detekcji zagrożeń.	2

	Suma godzin	**30**

Forma zajęć - projekt		**Liczba godzin**

Forma zajęć - seminarium		**Liczba godzin**
Se1	---	
Se2	---	
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych. N2. Prezentacja syntetyczna (10 minut) zadania laboratoryjnego przez prowadzącego. N3. Realizacja zadania laboratoryjnego (wg instrukcji) na stanowisku laboratoryjnym N4. Konsultacje N5. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02 PEU_W03	1. Ocena z kolokwium (wykład)
F2	PEU_U01 PEU_U02 PEU_U03 PEU_U04 PEU_K01 PEU_K02 PEU_K03	1. Krótkie testy sprawdzające przygotowanie teoretyczne do laboratoriów 2. Proste zadania domowe dotyczące zagadnień laboratoryjnych 3. Rozwiązania zadań realizowanych w trakcie zajęć
F1 – wykład – ocena z kolokwium F2 – laboratorium – praca na zajęciach, zaliczenie praktyczne P = 0,5F1 + 0,5F2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] C. Sanders, J. Smith, *Applied Network Security Monitoring: Collection, Detection, and Analysis*, wyd. Syngress, 2013

[2] W. Stallings, L. Brown, *Computer Security. Principles and Practice*, 3th ed., Pearson, 2015.

[3] C. Fry, M. Nystrom, *Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks*, O'Reilly Media, 2009

[4] R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, 2013

[5] R. Bejtlich, *The Tao of Network Security Monitoring: Beyond Intrusion Detection*, wyd. Addison-Wesley, 2004

[6] R. Bejtlich, *Extrusion Detection: Security Monitoring for Internal Intrusions*, wyd. Addison-Wesley, 2005

LITERATURA UZUPEŁNIAJĄCA:

[1] William (Chuck) Easttom II, Computer Security Fundamentals, 3th ed., Pearson, 2016

[2] W. Stallings, Cryptography and Network Security. Principles and Practice, 5th ed., Pearson, 2011

[3] J. Luttgens, M. Pepe, K. Mandia, Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej, Helion, 2016

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

dr inż. Sławomir Kubal, slawomir.kubal@pwr.edu.pl, mgr inż. Łukasz Pajewski

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	**Zaawansowana kombinatoryka**
Nazwa w języku angielskim:	**Advanced combinatorics**
Kierunek studiów:	**Cyberbezpieczeństwo**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**obowiązkowy**
Kod przedmiotu:	**W04CBE-SI0018G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	15			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	50			
Forma zaliczenia	Zaliczenie na ocenę	Zaliczenie na ocenę			
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	4				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-	1			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2	0,7			

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Algebra liniowa z geometria analityczną
2. Analiza matematyczna 1

CELE PRZEDMIOTU

C1 Nabycie wiedzy dotyczącej elementów teorii liczb i teorii grup
C2 Nabycie wiedzy dotyczącej metod kombinatoryki
C3 Zdobycie umiejętności dotyczących użycia narzędzi kombinatoryki: indukcji matematycznej, wykorzystania własności grup i grafów
C4 Zdobycie umiejętności konstrukcji kryptosystemów opartych na grupach modulo

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 posiada wiedzę w zakresie podstawowych i zaawansowanych obiektów kombinatorycznych

PEU_W02 posiada wiedzę dotyczącą narzędzi kombinatoryki, w szczególności grup modulo, grup permutacji, oraz ich własności

Z zakresu umiejętności:

PEU_U01 potrafi stosować narzędzia kombinatoryki do rozwiązywania problemów definiowanych na zbiorach przeliczalnych

PEU_U02 potrafi poprawnie i efektywnie zastosować wiedzę z kombinatoryki do konstrukcji efektywnych algorytmów szyfrowania.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Funkcje całkowitoliczbowe, operacje sufit i podłoga, zaokrąglania liczb rzeczywistych. Asymptotyka, wprowadzenie do złożoności obliczeniowej algorytmów.	2
Wy2	Elementy logiki. Algebry Boole'a, sieci logiczne. Arytmetyka modularna. Relacje (równoważności, porządku). Diagramy Hassego.	3
Wy3	Podzielność liczb. Liczby pierwsze i względnie pierwsze. Algorytm Euklidesa oraz równania diofantyczne. Rozkład na czynniki. Funkcja Eklera, twierdzenie Eulera. Równania z kongruencją. Chińskie twierdzenie o resztach.	3
Wy4	Proste metody szyfrowania oraz kryptosystemy.	2
Wy5	Indukcja i rekurencja. Równania rekurencyjne, równanie charakterystyczne. Liczby Fibonacciego. Funkcje tworzące.	2
Wy6	Zliczanie. Zasada szufladkowa Dirichleta. Zasada włączeń i wyłączeń.	2
Wy7	Kombinatoryka: rozmieszczenia, permutacje, kombinacje, wariacje. Praktyczne zastosowania.	2
Wy8	Generatory liczb losowych. Metody generowania prostych obiektów kombinatorycznych.	1
Wy9	Wprowadzenie do teorii grafów. Grafy pełne, dwudzielne, stopień wierzchołka. Drogi i cykle. Grafy spójne. Izomorfizm. Grafy skierowane (digrafy). Topologiczne uporządkowanie wierzchołków.	3
Wy10	Komputerowa reprezentacja grafów (złożoność czasowa i pamięciowa). Drzewa - równoważność różnych definicji. Drzewa binarne (zastosowania w obliczeniach równoległych).	2
Wy11	Metody BFS i DFS przeszukiwania grafów. Grafy z obciążonymi wierzchołkami lub połączeniami. Minimalne drzewa rozpinające - algorytmy Kruskala i Prima-Dijkstry.	3
Wy12	Algorytmy wyznaczanie najkrótszych dróg w grafach..	2
Wy13	Cykle i drogi Eulera i Hamiltona (uogólnienia – problem pocztowca, komiwojażera). Kolorowanie i płaskość grafów.	3
	Suma godzin	**30**

Forma zajęć - ćwiczenia	**Liczba godzin**

Ćw1	Indukcja matematyczna	2
Ćw 2	Notacja asymptotyczna	2
Ćw 3	Rozwiązywanie równań diofantycznych	2
Ćw 4	Symbol Newtona, liczby Catalana, zależności rekurencyjne	2
Ćw 5	Kombinatoryka: permutacje; miary odległości	2
Ćw 6	Analiza kryptosystemów opartych na grupie modulo: RSA, El Gamal	2
Ćw 7	Grafy i ich własności	2
Ćw 8	Kolokwium	1
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych N2. Ćwiczenia N3. Konsultacje N4. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01,PEU_W02	Aktywność na wykładach, egzamin pisemny
F2	PEU_U01, PEU_U02	Aktywność na zajęciach ćwiczeniowych, kolokwium
P=0.5*F1+0.5*F2, warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1 i F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] M.Ch. Klin, R. Poesche, K. Rosenbaum, Algebra stosowana dla matematyków i informatyków: grupy, grafy, kombinatoryka, WNT, Warszawa 1992.
[2] R.L. Graham, D.E. Knuth, O. Patashnik, Matematyka konkretna, PWN, 1996.
[3] J.L. Kulikowski, Zarys teorii grafów, PWN, Warszawa 1986.
[4] W. Lipski, Kombinatoryka dla programistów, WNT, Warszawa 1982.
[5] K.A. Ross, Ch.B. Wright, Matematyka dyskretna, PWN, 1996.

LITERATURA UZUPEŁNIAJĄCA:

[1] M.M. Sysło, N. Deo, J. S. Kowalik, Algorytmy optymalizacji dyskretnej, PWN, Warszawa 1993.
[2] R.J. Wilson, Wprowadzenie do teorii grafów, PWN, Warszawa 1985.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr hab. Mieczysław Wodecki, prof. nadzw. PWr, mieczysław.wodecki@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ Informatyki i Telekomunikacji

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Zarządzanie projektami IT**
Nazwa w języku angielskim: **IT Project Management**
Kierunek studiów: **Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy): ……..
Poziom i forma studiów: **I stopień, stacjonarna**
Rodzaj przedmiotu: **obowiązkowy**
Kod przedmiotu: **W04CBE-SI0055G**
Grupa kursów: **TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			15	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25			25	
Forma zaliczenia	Zaliczenie na ocenę			Zaliczenie na ocenę	
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**2**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-			1	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6			0,6	

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1 Poznanie podstawowych metod zarządzania projektami
C2 Nabycie wiedzy dotyczącej różnych metodologii zarządzania projektami
C3 Nabycie umiejętności posługiwania się oprogramowaniem wspomagającym zarządzanie projektami
C4 Nabycie umiejętności wyszukiwania i dobrania metodologii zarządzania do konkretnego projektu

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Ma podstawową wiedzę na temat metod zarzadzania projektami

Z zakresu umiejętności:

PEU_U01 Potrafi dobrać i stosować metodykę zarządzania projektami, potrafi przygotować harmonogramy, zasoby i je monitorować

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie. Podstawowe pojęcia	2
Wy2	Podstawowe pojęcia i definicje	2
Wy3	Fazy zarzadzania projektem	2
Wy4	Planowanie: harmonogram, zasoby	2
Wy5	Monitorowanie postępów i zarzadzanie zmianą	2
Wy6-Wy7	Wybrane metodyki zarzadzania projektami	4
Wy8	Repetytorium	1
	Suma godzin	**15**

Forma zajęć - projekt		**Liczba godzin**
Pr1	Wprowadzenie. Omówienie zasad realizacji zadania projektowego Przydział tematów projektowych	3
Pr2-Pr6	Realizacja projektu. Dokumentowanie projektu	10
Pr7-Pr8	Prezentacja rozwiązania problemu projektowego	2
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych N2. Prezentacja syntetyczna każdego tematu, dyskusja, ocena N3. Konsultacje N4. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01	Aktywność na wykładach, kolokwium zaliczające
F2	PEU_U01	Ocena realizacji projektu
P=0,5*F1+0,5*F2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Snedaker S., Zarządzanie projektami IT w małym palcu, Helion, Gliwice 2007.
[2] Bradley K., Podstawy metodyki PRINCE2, CRM, Warszawa, 2005.
[3] Koszlajda A., Zarzadzanie projektami IT. Przewodnik po metodykach, Helion, 2021.

LITERATURA UZUPEŁNIAJĄCA:

[1] Przewodnik PMBOK. Wydanie siódme. PMI Oddział Polski.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Jarosław M. Janiszewski, jaroslaw.janiszewski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim	**ZARZĄDZANIE RYZYKIEM I POLITYKI BEZPIECZEŃSTWA**
Nazwa przedmiotu w języku angielskim	**IT RISK MANAGEMENT AND POLICIES**
Kierunek studiów (jeśli dotyczy):	**CYBERBEZPIECZEŃSTWO**
Specjalność (jeśli dotyczy):	
Poziom i forma studiów:	**I / ~~II~~ stopień*, stacjonarna ~~/ niestacjonarna~~***
Rodzaj przedmiotu:	**obowiązkowy/ ~~wybieralny~~ / ~~ogólnouczelniany~~***
Kod przedmiotu	**W04CBE-SI0058G**
Grupa kursów	**TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	---	---	---	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	---	---	---	50
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin / zaliczenie na ocenę*~~
Dla grupy kursów zaznaczyć kurs końcowy (X)	X	---	---	---	---
Liczba punktów ECTS	4	---	---	---	---
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0	---	---	---	1
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2	---	---	---	0,7

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Podstawy systemów informatycznych, systemów operacyjnych, przetwarzania danych, wiedza z zakresu bezpieczeństwa systemów operacyjnych (np. kurs Bezpieczeństwo Systemów Operacyjnych) oraz z zakresu ochrony informacji (np. kurs Ochrona Informacji).

\

CELE PRZEDMIOTU

C1. Nabycie wiedzy z zakresu zarządzania ryzykiem w systemach informatycznych. C2. Nabycie wiedzy z zakresu analizy i wyceny ryzyk. C3. Nabycie wiedzy z zakresu określania i tworzenia zasad bezpieczeństwa oraz tworzenia i analizy polityk bezpieczeństwa

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ	
Z zakresu wiedzy:	
PEU_W01	Zna ryzyka w systemach informatycznych.
PEU_W02	Zna zasady określania oraz definiowania obszarów ryzyka w systemach.
PEU_W03	Zna zasady tworzenia matryc ryzyka w oparciu o prawdopodobieństwo oraz wpływ.
PEU_W04	Rozumie i określa parametry ryzyka: istotność, wpływ, prawdopodobieństwo.
PEU_W05	Zna metodykę i zasady tworzenia i analiz polityk bezpieczeństwa.
Z zakresu umiejętności:	
PEU_U01	Potrafi zdefiniować i wskazać ryzyka związane z procesami przetwarzania informacji.
PEU_U02	Potrafi utworzyć stosowne matryce ryzyka dla procesów przetwarzania danych.
PEU_U03	Potrafi rozróżnić różne typy ryzyk oraz odnieść je do warstwy technologicznej.
PEU_U04	Potrafi rozpoznać i określić ryzyka związane z użytkowaniem systemów inf.
PEU_U05	Potrafi rozróżnić ryzyka procesowe oraz technologiczne
Z zakresu kompetencji społecznych:	
PEU_K01	Rozumie konieczność zdobywania wiedzy oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.
PEU_K02	Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		**Liczba godzin**
Wy1	Wprowadzenie do procesów przetwarzania danych oraz zagrożeń z tym związanych w obszarach Poufności, Dostępności oraz Spójności danych.	2
Wy2	Definicje ryzyk w oparciu o podejście procesowe oraz technologiczne: wzajemne relacje między nimi.	2
Wy3	Podstawowe parametry związane z ryzykiem: prawdopodobieństwo wystąpienia, zakres występowania oraz wpływ.	2
Wy4	Zasada tworzenia matryc ryzyka, podejście, analiza i wycena poszczególnych ryzyk dla wskazanych obszarów.	2
Wy5	Tworzenie raportów z analiz ryzyka dla poszczególnych obszarów oraz całościowo.	2
Wy6	Określenie i sparametryzowanie polityk bezpieczeństwa, w odniesieniu do wskazanych ryzyk.	2
Wy7	Zasady tworzenia polityk bezpieczeństwa.	2
Wy8	Omówienie obszarów definiowania polityk bezpieczeństwa, w oparciu o wymagane ustawy, rozporządzenia nadrzędne, normy ISO, NIST oraz inne.	2

Wy9	Opracowanie dokumentacji polityk bezpieczeństwa dla poszczególnych obszarów: obszary procesowe.	2
Wy10	Opracowanie dokumentacji polityk bezpieczeństwa dla poszczególnych obszarów: obszary technologiczne.	2
Wy11	Opracowanie dokumentacji polityk bezpieczeństwa dla poszczególnych obszarów: obszary zarządzania użytkownikami i dostępami.	2
Wy12	Walidacja i weryfikacja polityk bezpieczeństwa: narzędzia procesowe oraz techniczne.	2
Wy13	Analizy ryzyka, a polityki bezpieczeństwa.	2
Wy14	Zarządzanie bezpieczeństwem w oparciu o analizy ryzyk.	2
Wy15	Kolokwium.	2
	Suma godzin	**30**

Forma zajęć – ćwiczenia		**Liczba godzin**
Ćw1	---	
Ćw2	---	
Ćw3	---	
...		
	Suma godzin	

Forma zajęć – laboratorium		**Liczba godzin**
La1	---	
La2	---	
La3	---	
…		
	Suma godzin	

Forma zajęć – projekt		**Liczba godzin**
Pr1	---	
Pr2	---	
Pr3	---	
…		
	Suma godzin	

Forma zajęć – seminarium		**Liczba godzin**
Se1	Opracowanie analiz ryzyka i polityki bezpieczeństwa dla danego obszaru – dokumentacja i prezentacja. Omówienie poruszanych zagadnień i dyskusja problemowa.	14
Se2		
Se3		
Se4		
Se5		
Se6		
Se7		
Se8	Podsumowanie i ocena pracy.	1
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych. N2. Prezentacja syntetyczna (10 minut) zadania laboratoryjnego przez prowadzącego. N3. Realizacja zadania laboratoryjnego (wg instrukcji) na stanowisku laboratoryjnym. N4. Konsultacje. N5. Praca własna.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny: F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02 PEU_W03 PEU_W04 PEU_W05	1. Ocena z kolokwium (wykład). 2. Proste zadania domowe dotyczące zagadnień przetwarzania danych.
F2	PEU_U01 PEU_U02 PEU_U03 PEU_U04 PEU_U05 PEU_K01 PEU_K02	1. Krótkie prace pisemne – testy sprawdzające przygotowanie teoretyczne do seminarium. 2. Proste zadania domowe dotyczące przerabianych zagadnień. 3. Rozwiązania zadań realizowanych w trakcie zajęć. 4. Prezentacje z wykonywanych zadań i tematów.
F1 – wykład – ocena z kolokwium F2 – seminarium – średnia ważona z ocen za poszczególne zadania i prezentacje wymienione w opisie F2 P = 0,6*F1 + 0,4*F2 Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu.		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
LITERATURA PODSTAWOWA: [1] Bruce Nikkel, „Practical forensic imaging”, No Starch Press 2016 [2] Harlan Carvey, „Analiza śledcza i powłamaniowa”, Helion 2013 **LITERATURA UZUPEŁNIAJĄCA:** [1] Phil Polstra, „Linux Forensics”, Pentester Academy 2015 [2] Adam Ziaja, Praktyczna analiza powłamaniowa, Wydawnictwo Naukowe PWN 2017
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
dr inż. Robert Czechowski, robert.czechowski@pwr.edu.pl mgr inż. Marcin Kaczmarek, marcin.kaczmarek@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	**Aplikacje mobilne**
Nazwa w języku angielskim:	**Mobile Application Developement**
Kierunek studiów:	**Cyberbezpieczeństwo**
Specjalność:	**Bezpieczeństwo systemów informatycznych**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0407G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			15	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25			25	
Forma zaliczenia	Zaliczenie na ocenę			Zaliczenie na ocenę	
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**2**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-			1	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6			0,6	

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1 Zapoznanie studentów ze specyfiką systemów mobilnych

C2 Zapoznanie studentów z wybranymi technikami tworzenia aplikacji z dostępem do danych na urządzenia mobilne typu smartphone

C3 Nabycie przez studenta praktycznych umiejętności w budowie systemów informatycznych na urządzenie mobilne

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna podstawy wybranego systemu operacyjnego Android

PEU_W02 Zna podstawy programowania aplikacji na urządzenia przenośne typu smartphone

Z zakresu umiejętności:

PEU_U01 Umie zaprojektować aplikację na urządzenie mobilne typu smartphone

PEU_U02 Umie zaprogramować proste aplikacje na urządzenia przenośne z systemem Android

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do kursu - Specyfika aplikacji mobilnych	1
Wy2	Środowisko programistyczne	1
Wy3	Intencje, Zasoby, Aktywności	2
Wy4	Interfejs użytkownika - podstawy	2
Wy5	Interfejs użytkownika - część dla zaawansowanych	2
Wy6	Przechowywanie danych	2
Wy7	Praca w chmurze	2
Wy8	Dostawcy treści	2
Wy9	Test	1
	Suma godzin	**15**

Forma zajęć - projekt		**Liczba godzin**
P1	Prezentacja zasad realizacji projektów	2
P2	Rejestracja grup i tematów	2
P3	Implementacja - konsultacje	9
P4	Prezentacja - ocena	2
	Suma	15

STOSOWANE NARZĘDZIA DYDAKTYCZNE

N1 Wykład informacyjny
N2 Wykład problemowy
N3 Konsultacje
N4 Studia literaturowe
N5 Zajęcia projektowe

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P –	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się

podsumowująca (na koniec semestru)		
F1	PEU_W01 PEU_W02	Test podsumowujący zdobytą wiedzę
F2	PEU_U01 PEU_U02	Ocena zrealizowanych projektów
P = 0,5*F1+0,5*F2 Wszystkie składowe formujące (F1-F2) muszą być pozytywne aby uzyskać pozytywną ocenę podsumowującą P		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
<u>LITERATURA PODSTAWOWA:</u> 1. Joseph Annuzzi Jr., Lauren Darcey, Shane Conder. Android. Wprowadzenie do programowania aplikacji. 2. Carmen Delessio, Lauren Darcey, Shane Conder. Android Studio w 24 godziny. Wygodne programowanie dla platformy Android.
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
Dr inż. Konrad Jackowski, konrad.jackowski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim	**AUDYTOWANIE SIECI TELEINFORMATYCZNYCH**
Nazwa przedmiotu w języku angielskim	**SECURITY AUDITING OF IT NETWORKS**
Kierunek studiów (jeśli dotyczy):	**CYBERBEZPIECZEŃSTWO**
Specjalność (jeśli dotyczy):	**BEZPIECZENSTWO SYSTEMÓW INFORMATYCZNYCH**
Poziom i forma studiów:	**I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna*~~**
Rodzaj przedmiotu:	**~~obowiązkowy~~/ wybieralny/ ~~ogólnouczelniany *~~**
Kod przedmiotu	W04CBE-SI0410G
Grupa kursów	**TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15	---	30	---	---
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25	---	50	---	---
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin / zaliczenie na ocenę*~~
Dla grupy kursów zaznaczyć kurs końcowy (X)	X	---	---	---	---
Liczba punktów ECTS	3	---	---	---	---
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0	---	1	---	---
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6	---	1,5	---	---

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Zaawansowana wiedza z zakresu zagadnień sieci komputerowych (np. kurs Sieci Komputerowe III), wiedza z zakresu bezpieczeństwa systemów operacyjnych (np. kurs Bezpieczeństwo Systemów Operacyjnych) oraz z zakresu ochrony informacji (np. kurs Ochrona Informacji).

\

CELE PRZEDMIOTU

C1. Omówienie zagadnienia audytu bezpieczeństwa sieci komputerowych. Przedstawienie metodologii audytów i testów penetracyjnych.

C2. Przekazanie wiedzy umożliwiającej organizacje i prowadzenie audytów i testów penetracyjnych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Ma wiedzę na temat stosowanych metod audytu formalnego oraz technicznego a w szczególności podstawowe założenia norm ISO rodziny 27000.

PEU_W02 Ma ogólną wiedzę na temat struktury organizacji i architektury systemów wykrywania zagrożeń.

PEU_W03 Ma wiedzę na temat narzędzi i metod audytu technicznego oraz zna wybrane metody audytu technicznego oraz zastosowanie wybranych narzędzi do audytu technicznego i testów penetracyjnych.

PEU_W04 Ma wiedzę ogólną w zakresie metodyk zarządzania ryzykiem.

Z zakresu umiejętności:

PEU_U01 Potrafi używać narzędzi audytu technicznego do przetestowania bezpieczeństwo aplikacji sieciowej.

PEU_U02 Potrafi zaplanować poszczególne etapy testu penetracyjnego i określić ich kryteria.

PEU_U03 Potrafi wykonać poszczególne etapy testu penetracyjnego i przygotować raport.

PEU_U04 Potrafi dokonać mapowania potrzeb (formalnych i związanych z cechami organizacji) oraz niezbędnego poziomu organizacji usług bezpieczeństwa.

Z zakresu kompetencji społecznych:

PEU_K01 Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.

PEU_K02 Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do zagadnienia audytu teleinformatycznego. Model audytu formalnego. Model audytu merytorycznego. Uwarunkowania audytu.	3
Wy2	Standardy dotyczące audytowania systemów informatycznych ISACA (Information Systems Audit and Control Association), COBIT (Control Objectives for Information and related Technology), GTAG (Global Technology Audit Guide) oraz GAIT (Guide to the Assessment for IT Risk), normy ISO (International Organization for Standardization)	2
Wy3	Metodologie audytu technicznego i testów penetracyjnych (testy klasy blackbox/graybox: testy penetracyjne systemów	2

	informatycznych , testy penetracyjne aplikacji, testy klasy white box) omówienie najlepszych praktyk.	
Wy4	Klasyfikacja, przegląd i zastosowanie narzędzi audytorskich – dobre praktyki doboru narzedzi.	2
Wy5	Omówienie rodziny normy bezpieczeństwa ISO/IEC 27001,ISO/IEC 27002, ISO/IEC 27003.	2
Wy6	Normy bezpieczeństwa ISO/IEC 27004,ISO/IEC 27005, ISO/IEC 27006.	2
Wy7	Kolokwium zaliczeniowe.	2
	Suma godzin	**15**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1	---	
Ćw2	---	
Ćw3	---	
Ćw4	---	
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Zapoznanie się z narzędziami tzw. białego wywiadu.	2
La2	Zapoznanie się z narzędziami: nmap, hping, netcat.	2
La3	Zapoznanie się z narzędziami: OpenVAS, Nessus, OWASP ZAP.	2
La4	Testowanie podatności baz danych.	2
La5	Testowanie podatności aplikacji webowych.	2
La6,7	Zapoznanie się z platforma Metasploit Framework.	4
La8	Zastosowanie metod fuzzingu.	2
La9	Wykorzystanie podatności w językach niskiego poziomu (np. przepełnienie bufora, zastosowanie łańcuchów formatujących).	2
La10-15	Wykonanie audytu bezpieczeństwa sieci/testu penetracyjnego (testy klasy blackbox/graybox: testy penetracyjne systemów informatycznych , testy penetracyjne aplikacji, testy klasy white box)	12
	Suma godzin	**30**

Forma zajęć - projekt		**Liczba godzin**
Pr1	---	
Pr2	---	
Pr3	---	
Pr4	---	
…		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
Se1	---	
Se2	---	
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych. N2. Prezentacja syntetyczna (10 minut) zadania laboratoryjnego przez prowadzącego. N3. Realizacja zadania laboratoryjnego (wg instrukcji) na stanowisku laboratoryjnym. N4. Konsultacje. N5. Praca własna.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02 PEU_W03 PEU_W04	1. Ocena z kolokwium (wykład). 2. Proste zadania domowe dotyczące zagadnień przetwarzania danych.
F2	PEU_U01 PEU_U02 PEU_U03 PEU_U04 PEU_K01 PEU_K02	1. Krótkie prace pisemne – testy sprawdzające przygotowanie teoretyczne do laboratoriów. 2. Proste zadania domowe dotyczące przerabianych zagadnień. 3. Rozwiązania zadań realizowanych w trakcie zajęć. 4. Sprawozdania w wykonywanych ćwiczeń.
F1 – wykład – ocena z kolokwium F2 – laboratorium – średnia ważona z ocen za poszczególne zadania wymienione w opisie F2 P = 0,6F1 + 0,4F2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu.		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Eric Cole, „Bezpieczeństwo sieci : biblia” , Helion 2005

[2] Dafydd Stuttard, Marcus Pinto, :The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition, Wiley 2011

[3] Joseph Muniz, Aamir Lakhani, „Kali Linux. Testy penetracyjne” , Helion 2014

LITERATURA UZUPEŁNIAJĄCA:

[1] Patrick Henry Engebretson „Hacking i testy penetracyjne : podstawy”, Helion 2013

[2] Jon Erickson, „Hacking. The Art of Exploitation”, No Starch Press 2008

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
dr inż. Jacek Oko, Jacek.oko@pwr.edu.

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim	**Bezpieczeństwo w Sieciach Bezprzewodowych**
Nazwa w języku angielskim	**Security in Wireless Access Networks**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo Sieci**
Poziom i forma studiów:	**I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu:	**~~obowiązkowy~~ / wybieralny / ~~ogólnouczelniany~~ ***
Kod przedmiotu	**W04CBE-SI0401G**
Grupa kursów	**TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	**30**	—	**30**	—	—
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	**50**	—	**50**	—	—
Forma zaliczenia	~~Egzamin~~ / zaliczenie na ocenę*	—	~~Egzamin~~ / zaliczenie na ocenę*	—	—
Dla grupy kursów zaznaczyć kurs końcowy (X)	**X**				
Liczba punktów ECTS	**4**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	—	—	2	—	—
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	1,2	—	1,2	—	—

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1. Zdobycie podstawowej wiedzy z zakresu współczesnych radiowych sieci dostępowych o różnym zasięgu (od lokalnego do makrokomórkowego) i charakterze (tj. amatorskim i operatorskim), metod szacowania pojemności oraz przewidywania zagrożeń z zakresu kompatybilności elektromagnetycznej

C2. Zdobycie podstawowej wiedzy dotyczącej szacowania osiągów danego bezprzewodowego interfejsu dostępowego w warunkach wyjściowych (nieobciążonych) oraz z uwzględnieniem narzutu protokołowego warstw wyższych (np. MAC)

C3. Zdobycie wiedzy na temat cyberbezpieczeństwa w dostępowym segmencie systemów bezprzewodowych, w tym: metodyk detekcji ataków i ich prewencji.

C4. Zdobycie umiejętności zestawiania połączeń sieciowych dla systemów WLAN oraz Bluetooth, stosowania modeli propagacyjnych do predykcji zasięgu radiowego, praktycznej obsługi analizatora widma i analizy, interpretacji parametrów zwracanych przez terminal komórkowy dot. parametrów pracy a także konfigurowania dostępnych systemów bezprzewodowych ze szczególnym uwzględnieniem zasad cyberbezpieczeństwa

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – posiada podstawową wiedzę o metodach szacowania pojemności oraz wynikowej sprawności radiowej sieci dostępowej, w określonej technice wielodostępu (np. OFDMA, CDMA, CSMA/CA itp.)

PEU_W02 – zna systemy pracujące w pasmach nielicencjonowanych (WLAN, Bluetooth, UWB) oraz pracujące w pasmach licencjonowanych, takie jak UMTS, (DC-)HSPA(+), LTE(-Advanced)

PEU_W03 – jest w stanie podać i opisać metryki jakościowe pomocne w detekcji cyberataków oraz wskazać metody ich prewencji

PEU_W04 – jest w stanie wskazać możliwe zagrożenia związane z zagłuszaniem (intencjonalnym lub nie) i obliczyć ilościowo jego wpływ, na podstawie znajomości aspektów propagacyjnych oraz widmowych (maski promieniowania)

Z zakresu umiejętności:

PEU_U01 – potrafi skonfigurować sieć WLAN, przeprowadzać podstawową diagnostykę i nią zarządzać

PEU_U02 – potrafi skonfigurować pikosieć Bluetooth, przeprowadzać podstawową diagnostykę i nią zarządzać

PEU_U03 – potrafi stosować narzędziao testów wydajnościowych sieci WLAN oraz Bluetooth

PEU_U04 – potrafi nastawić i obsługiwać analizator widma

PEU_U05 – potrafi skonfigurować nastawy zapewniające wymagany poziom bezpieczeństwa urządzeń dostępowych systemów bezprzewodowych oraz założone parametry bezpieczeństwa transmisji

PEU_U06 – potrafi wykonać szacunkowe wyliczenia spodziewanych zakłóceń w segmencie dostępowym na podstawie znajomości charakterystyk toru odbiorczego systemu zakłócanego i charakterystyk torów nadawczych systemów zakłócających

Z zakresu kompetencji społecznych:

PEU_K01 – potrafi pracować w zespole osób realizujących dane ćwiczenie laboratoryjne a następnie przetwarzających uzyskane rezultaty i generujących końcowy raport z każdych zajęć

TREŚCI PROGRAMOWE

Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do bezprzewodowych sieci dostępowych.	**2**
Wy2	Anteny i propagacja fal radiowych.	**2**
Wy3	Wprowadzenie do pasm nielicencjonowanych. Maski promieniowania, techniki rozpraszania widma, multipleksacji oraz modulacji.	**4**
Wy4	Specyfika cyberataków w segmencie dostępowym sieci bezprzewodowych. Metody prewencji i minimalizacji ryzyka	**2**

Wy5	Bezprzewodowe sieci lokalne WLAN: rodzina systemów IEEE 802.11x – zasada działania, metody planowania sieci wielkoobszarowych.	**2**
Wy6	Charakterystyka ataków na sieci Wi-Fi. Pozyskiwanie i analiza danych. Techniki exploitacji.	**4**
Wy7	Bezprzewodowe systemy osobiste WPAN: IEEE 802.15.1 Bluetooth	**4**
Wy8	Charakterystyka ataków na sieci Bluetooth	**2**
Wy9	Charakterystyka ataków na sieci RFID, Smart Cards oraz NFC.	**4**
Wy10	Systemy komórkowe 3G, 4G i 5G. Przegląd metod zabezpieczania dostępu i szyfrowania transmisji w systemach komórkowych.	**4**
	Suma godzin:	**30**

Forma zajęć - laboratorium		**Liczba godzin**
La1	Zajęcia wprowadzające: prezentacja przepisów BHP, wstępne informacje dot. obsługi sprzętu oraz zasad raportowania ćwiczeń i zaliczeń.	**4**
La2	Badanie metod szyfrowania oraz podatności w sieciach WLAN	**6**
La2,3	Wykorzystanie analizatora widma do monitoringu środowiska elektromagnetycznego na potrzeby detekcji ewentualnych zakłóceń	**8**
La4	Analiza ramek systemów bezprzewodowych	**4**
La6	Konfiguracja, badanie wydajności, kompatybilność elektromagnetyczna, badania różnych topologii, diagnostyka i zarządzanie sieciami bezprzewodowymi WLAN	**4**
La7	Konfiguracja, diagnostyka i zarządzanie pikosieciami bezprzewodowymi Bluetooth oraz bezpieczeństwo w sieci Bluetooth	**4**
	Suma godzin:	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem tablicy i slajdów N2. Narzędzia symulacyjne N3. Konsultacje N4. Praca własna – przygotowanie do ćwiczeń laboratoryjnych N5. Praca własna – samodzielne studia i przygotowanie do zaliczenia

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu kształcenia	Sposób oceny osiągnięcia efektu kształcenia
F1	PEU_W01-04	Test zaliczeniowy z wykładu
F2	PEU_U01-06 PEU_K01	Ocena końcowa z laboratorium
P = 0,5·F1+0,5·F2 *warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu*		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
LITERATURA PODSTAWOWA: [1] D. Lund, Wireless Communications Cyber Security, Engineering & Technology Reference, 2017, 10pp. [2] Krzysztof Wesołowski, „Systemy Radiokomunikacji Ruchomej”, WKiŁ, Warszawa 1999 **LITERATURA UZUPEŁNIAJĄCA:** [1] W. Hołubowicz, M. Szwabe, „Systemy radiowe z rozpraszaniem widma, CDMA. Teoria, standardy, aplikacje”, Motorola Polska, Poznań 1998

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
Dr inż. Michał Kowal, michal.kowal@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Biometria**
Nazwa w języku angielskim:
Kierunek studiów: **Cyberbezpieczeństwo**
Specjalność: **Bezpieczeństwo systemów informatycznych**
Poziom i forma studiów: **I stopień, stacjonarna**
Rodzaj przedmiotu: **wybieralny**
Kod przedmiotu: W04CBE-SI0402G
Grupa kursów: **TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		15		15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		25		25
Forma zaliczenia	Zaliczenie na ocenę		Zaliczenie na ocenę		Zaliczenie na ocenę
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**4**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-		2		1
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2		0,6		0,7

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Wiedza z zakresu kryptografii i przetwarzania sygnałów
2. Wiedza z zakresu statystyki i rachunku prawdopodobieństwa

CELE PRZEDMIOTU

C1. Zdobycie wiedzy z zakresu biometrycznych metod identyfikacji, algorytmów i przetwarzania informacji biologicznych oraz kontekstu prawno-etycznego
C2. Wykształcenie umiejętności poprawnej prezentacji wyników studiów własnych nad opracowywanym zagadnieniem z zakresu biometrii
C3. Nabycie umiejętności samodzielnego konfigurowania prostych systemów/układów biometrycznych z funkcją ich automatycznej transmisji

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 posiada podstawową wiedzę dotyczącą metod identyfikacji oraz metryk biologicznych stosowanych w metodach biometrycznych

PEU_W02 posiada wiedzę dotyczącą budowy i zasady działania urządzeń (sond, skanerów itp.) biometrycznych

PEU_W03 zna kontekst prawny i etyczny związany z biometrią

PEU_W04 posiada wiedzę dotyczącą procesów standaryzacyjnych oraz architektury systemowej (np. modelu odniesienia FIDO UAF)

Z zakresu umiejętności:

PEU_U01 potrafi dobrać odpowiednią metodę biometryczną do konkretnych potrzeb identyfikacyjnych

PEU_U02 wyspecyfikować parametry niezbędne do dokonania poprawnej identyfikacji biometrycznej oraz wskazać odpowiednią metodę, aparaturę i oprogramowanie

PEU_U03 potrafi opracować praktyczny układ identyfikacyjny w oparciu o wybraną platformę mikroprocesorową (np. Arduino) dysponując dostępnymi czytnikami (np. linii papilarnych)

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do systemów biometrycznych: cel, sens i rola we współczesnych społeczeństwach, bezpieczeństwie i gospodarkach (w tym aspekty ekonomiczne), omówienie trendów rozwojowych	2
Wy2	Podstawowe pojęcia z zakresu biometrii. Biometria w kryminalistyce, handlu, administracji, bankowości, medycynie i innych zastosowaniach	2
Wy3	Metryki statystyczne oraz podstawowe algorytmy matematyczne stosowane w biometrii (np. korelacja, rozpoznawanie wzorców itp.)	4
Wy4	Metody identyfikacji na podstawie linii papilarnych, pozyskiwanie obrazu, poziomy szczegółowości, budowa deskryptorów i modeli	4
Wy5	Metody identyfikacji na podstawie charakterystyki twarzowej, przetwarzanie, segmentacja, modele i algorytmy	4
Wy6	Metody identyfikacji akustycznej (rozpoznawanie po głosie)	2
Wy7	Metody identyfikacji na podstawie charakterystyki tęczówki, segmentacja, kodowanie i właściwości modelu	2
Wy8	Biometria behawioralna (keystroking, podpis odręczny, wzorce zachowań w światach wirtualnych)	2
Wy9	Bezpieczeństwo sensorów i systemów biometrycznych, standaryzacja	3
Wy10	Biometria w kontekście prawnym i etyka w biometrii	3
Wy11	Powtórka materiału	2
	Suma godzin	**30**

Forma zajęć - laboratorium		**Liczba godzin**
La1	Zajęcia wprowadzającej: zasady BHP, prezentacja aparatury biometrycznej wykorzystywanej na zajęciach laboratoryjnych, wytyczne dotyczące protokołowania i raportowania wyników	1
La2	Konfiguracja i testowanie działania biometrycznego układu identyfikacji na podstawie linii papilarnych	2

La3	Konfiguracja i testowanie działania biometrycznego układu identyfikacji na podstawie głosu	2
La4	Konfiguracja i testowanie działania biometrycznego układu identyfikacji na podstawie wzorca twarzy	2
La5	Konfiguracja i testowanie działania biometrycznego układu identyfikacji na podstawie charakterystyki oka bądź ucha	2
La6	Konfigurowanie i testowanie działania biometrycznego układu identyfikacji na podstawie charakterystyk behawioralnych sposobu pisania na interfejsie wejścia (keystroking)	2
La7	Konfigurowanie krótko-zasięgowego układu transmisji danych z układu biometrycznego	2
La8	Konfigurowanie dalekosiężnego układu transmisji danych z układu biometrycznego (z wykorzystaniem systemów komórkowych bądź LPWAN)	2
	Suma godzin:	**15**

Forma zajęć - seminarium		**Liczba godzin**
Se1	Zajęcia organizacyjne – przedstawienie grafiku prezentacji studenckich, wyjaśnienie zasad liczenia oceny końcowej. Wyjaśnienie podstawowych zagadnień związanych z korzystaniem i cytowaniem źródeł bibliograficznych oraz prezentacją multimedialną i prezentacją wyników.	1
Se2	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych – część I	2
Se3	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych – część I	2
Se4	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych – część I	2
Se5	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se6	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se7	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se8	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem tablicy i slajdów N2. Narzędzia programistyczne do przygotowywania prezentacji multimedialnych N3. Konsultacje N4. Praca własna – przygotowanie multimedialnej prezentacji wyników pracy własnej N5. Praca własna – samodzielne studia i przygotowanie do zaliczenia

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w	Numer efektu uczenia	Sposób oceny osiągnięcia efektu uczenia się

trakcie semestru), P – podsumowująca (na koniec semestru)	się	
F1	PEU_W01, PEU_W02, PEU_W03, PEU_W04	Aktywność na wykładach, zaliczenie sprawdzianów pisemnych, egzamin pisemny
F2	PEU_W02, PEU_U02, PEU_U03	Aktywność na zajęciach laboratoryjnych, ocena sprawozdań z zadań laboratoryjnych
F3	PEU_U01, PEU_U02	Jakość obu prezentacji wygłoszonych w trakcie zajęć seminaryjnych
P = 0,4*F1 + 0,4*F2 + 0,2*F3 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1, F2 i F3		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Bolle R. M., Connell J. H., Pankanti S., Ratha N. K., Senior, "Biometria", Wydawnictwa Naukowo-Techniczne PWN-WNT, 2008

[2] Anil Jain, Patrick Flynn, Arun A. Ross, "Handbook of Biometrics", Springer-Verlag US, 2008

[3] P.Viola and M.Jones "Rapid Object Detection using a Boosted Cascade of Simple Features", https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf (dostęp: 16.01.2023)

[4] M.Turk and A.Pentland, "Eignefaces for Recognition", https://www.face-rec.org/algorithms/PCA/jcn.pdf (dostęp: 16.01.2023)

LITERATURA UZUPEŁNIAJĄCA:

[1] Krzysztof Ślot, Rozpoznawanie biometryczne. Nowe metody ilościowej reprezentacji obiektów, Wydawnictwa Komunikacji i Łączności, 2011

[2] Krzysztof Ślot, Wybrane zagadnienia biometrii, Wydawnictwa Komunikacji i Łączności, 2008

[3] Literatura, w tym artykuły naukowe, związana z przydzielonym tematem seminaryjnym

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Wojciech Wodo, wojciech.wodo@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim	**BEZPIECZEŃSTWO SERWERÓW I APLIKACJI WEB**
Nazwa przedmiotu w języku angielskim	**SECURITY OF SERVERS AND WEB APPLICATIONS**
Kierunek studiów (jeśli dotyczy):	**CYBERBEZPIECZEŃSTWO**
Specjalność (jeśli dotyczy):	**BEZPIECZENSTWO SYST. INFROM.**
Poziom i forma studiów:	**I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu:	**~~obowiązkowy~~/ wybieralny /~~ogólnouczelniany *~~**
Kod przedmiotu	W04CBE-SI0403G
Grupa kursów	**TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15	---	45	---	---
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	---	100	---	---
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X	---	---	---	---
Liczba punktów ECTS	6	---	---	---	---
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0	---	3	---	---
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6	---	1,8	---	---

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Zaawansowana wiedza z zakresu systemów w operacyjnych (np. kurs Systemy Operacyjne), wiedza z zakresu kryptografii i kodowania (np. kurs Kryptografia i Kodowanie) oraz z zakresu ochrony informacji (np. kurs Ochrona Informacji).
2. Podstawowe umiejętności programowania w językach C, Perl, Python

\

CELE PRZEDMIOTU

C1. Nabycie wiedzy i podniesienie kompetencji z zakresu bezpiecznego programowania w różnych środowiskach, ze szczególnym uwzględnieniem programowania web (skrypty, muddleware, aplikacje klienckie), a także pozisnie metodologii wspomagających tworzenie bezpiecznych programów, takich jak programowanie defensywne i programowanie sterowane testowaniem.

C2. Poznanie typowych ataków na serwery WWW i aplikacje webowe

C3. Poznanie metod zapobiegania atakom na aplikacje webowe oraz minimalizowania zagrożeń z nich wynikających.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy: (K1CBE_W26)

PEU_W01 Zna podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych.

PEU_W02 Zna metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych

PEU_W03 Wie co to są certyfikaty SSL i jak działają protokoły SSL/TLS

PEU_W04 Zna metody ataków typu XSS, CSRF, ,,code injection'', w szczególności SQL-injection i problemy z przekazywaniem parametrów pomiędzy programami

Z zakresu umiejętności:

PEU_U01 Potrafi wskazać typowe błędy związane z bezpieczeństwem w konfiguracji serwerów sieciowych, potrafi skonfigurować serwer WWW

PEU_U02 Potrafi sprawdzić integralność danych w systemie komputerowym i wykorzystać techniki kryptograficzne do do zwiększenia bezpieczeństwa systemu.

Z zakresu kompetencji społecznych:

PEU_K01 Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.

PEU_K02 Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.

PEU_K03 Jest świadomy znaczenia wagi przykładanej do pisania aplikacji webowych z zachowaniem reguł bezpieczeństwa.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Bezpieczeństwo infrastruktury, konfiguracja serwerów, SSL, TLS	2
Wy2	Mechanizmy uwierzytelniania i podtrzymania sesji w aplikacjach webowych	2
Wy3	Omijanie mechanizmów uwierzytelniania i autoryzacji dostępu	2
Wy4	Błędy programistyczne: XSS< CSRF, SQL-Injection	2
Wy5	Błędy charakterystyczne dla poszczególnych języków programowania (C, PHP, Perl, Python, .NET, CGI, aplikacje web, Javascript)	2
Wy6	Typowe błędy programistyczne, metody ataków na aplikacje sieciowe klient-serwer I aplikacje webowe.	2
Wy7	Metody wspomagania programistów w pisaniu bezpiecznych programów (defensive programming, test-driven development, CD/CI, systemy kontroli wersji, zarządzanie projektami)	2
Wy8	Kolokwium zaliczeniowe	1
	Suma godzin	15

Forma zajęć - ćwiczenia		Liczba godzin
Ćw1	---	
Ćw2	---	
Ćw3	---	
Ćw4	---	
..		
	Suma godzin	

Forma zajęć - laboratorium		Liczba godzin
La1 - 4	Implementacja ataków z wykorzystaniem technik XSS, CSRF, SQL-injection	12
La5-6	Tworzemie certyfikatów SSL z użyciem własnego Certificate Authority, konfigurowanie serwerów WWW z użyciem TLS i autoryzacji za pomocą certyfikatów	6
La7	Implementacja metod uwierzytelniania w sesjach webowych	3
La8	Symulowanie ataków i obrona przed nimi.	3
La9	Wykorzystanie systemów kontroli wersji: CVS, SVN, Git, GitHub	3
La10-15	Zadania projektowe związane z bezpiecznym programowaniem aplikacji sieciowych	18
	Suma godzin	**45**

Forma zajęć - projekt		Liczba godzin
Pr1	---	
Pr2	---	
Pr3	---	
Pr4	---	
…		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1	---	
Se2	---	
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem prezentacji multimedialnych. N2. Prezentacja syntetyczna (10 minut) zadania laboratoryjnego przez prowadzącego. N3. Realizacja zadania laboratoryjnego (wg instrukcji) na stanowisku laboratoryjnym. N4. Konsultacje. N5. Praca własna.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02 PEU_W03 PEU_W04 PEU_K01	1. Ocena z kolokwium (wykład)
F2	PEU_U01 PEU_U02 PEU_K01 PEU_K02 PEU_K03	1. Zadania domowe dotyczące zagadnień laboratoryjnych 2. Rozwiązania zadań realizowanych w trakcie zajęć 3. Ocena projektu sieciowego 4. Sprawozdania w wykonywanych ćwiczeń
F1 – wykład – ocena z kolokwium F2 – laboratorium – średnia ważona z ocen za poszczególne zadania labpratoryjne P = 0,5F1 + 0,5F2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWCBEK00027-OCHRONASYSTEMOWOPERACYJNYCH_F.DOCXA:

[1] W. Stallings, L. Brown, *Computer Security. Principles and Practice*, 3th ed., Pearson, 2015.
[2] S. Garfinkel, G. Spafford, „Bezpieczeństwo w Unixie i Internecie”
[3] W. Stallings, *Cryptography and Network Security. Principles and Practice*, 5th ed., Pearson, 2011.
[4] J. Forristal; J. Traxler: Hack proofing your web applications
[5] Dan Cederholm: Kuloodporne strony internetowe

LITERATURA UZUPEŁNIAJĄCA:

[1] C. P. Pfleeger, S. L. Pfleeger - *Analyzing Computer Security. A threat/Vulnerabiliity/ Countermeasure Approach* , Pearson, 2012

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
dr inż. Tomasz Surmacz, Tomasz.Surmacz@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim Bezpieczeństwo chmur obliczeniowych
Nazwa przedmiotu w języku angielskim Cloud Security
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): Bezpieczeństwo Systemów Informatycznych
Poziom i forma studiów: I / ~~II stopień / jednolite studia magisterskie*,~~ stacjonarna / ~~niestacjonarna~~*
Rodzaj przedmiotu: ~~obowiązkowy~~ / wybieralny / ~~ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0404G
Grupa kursów TAK / ~~NIE~~*

	Wykład	**Ćwiczenia**	**Laboratorium**	**Projekt**	**Seminarium**
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15	---	45	---	---
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	35	---	90	---	---
Forma zaliczenia	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin / zaliczenie na ocenę*~~	~~Egzamin /~~ zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**5**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			4		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0,6		1,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1.

CELE PRZEDMIOTU

C1. Nabycie wiedzy z zakresu zabezpieczania chmur obliczeniowych - polityki, kontrakty i zarządzanie na wszystkich warstwach.
C2. Poszerzenie umiejętności z zakresu zabezpieczania chmur obliczeniowych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna typowe zagrożenia dla środowisk wirtualnych oraz chmur obliczeniowych w centrach danych, w tym sposoby wykrywania włamań sieciowych i kontroli dostępu.

Z zakresu umiejętności:

PEU_U01 Potrafi planować oraz implementować mechanizmy zabezpieczające w środowisku chmur obliczeniowych.

Z zakresu kompetencji społecznych:

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie. Centra danych i chmury obliczeniowe – zagrożenia.	1
Wy2	Standardy bezpieczeństwa dla środowisk chmur obliczeniowych.	2
Wy3	Bezpieczeństwo infrastruktury w chmurach obliczeniowych.	2
Wy4	Koncepcja Software Defined Networks (SDN) – ochrona sieci wirtualnych.	2
Wy5	Ochrona w chmurach publicznych na przykładzie Amazon AWS IAM i AWS VPC. Kontrola dostępu.	2
Wy6,7	Bezpieczeństwo danych w chmurach obliczeniowych. Metody kryptograficzne, zarządzanie kluczami i certyfikatami.	4
Wy8	Zarządzanie dostępem uprzywilejowanym.	2
	Suma godzin	15

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1	---	---
Ćw2	---	---
Ćw3	---	---
Ćw4	---	---
..		
	Suma godzin	---

Forma zajęć - laboratorium		**Liczba godzin**
La1	Omówienie zasad realizacji laboratorium: zakres, tematyka, cele oraz narzędzia.	3
La2-8	Zabezpieczanie infrastruktury w chmurach obliczeniowych.	21
La9-12	Bezpieczeństwo danych w chmurach obliczeniowych. Metody kryptograficzne, zarządzanie kluczami i certyfikatami.	12
La13,14	Zarządzanie dostępem uprzywilejowanym.	6
Lab15	Repetytorium	3

	Suma godzin	45

Forma zajęć - projekt		Liczba godzin
Pr1		
Pr2		
Pr3		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład problemowy N2. Studia literaturowe N3. Opracowanie pisemne N4. Dyskusja problemowa N5. Weryfikacja rozwiązań N6. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01	1. Pisemne zaliczenie.
F2	PEU_U01	1. Realizacja ćwiczeń laboratoryjnych
P=0,40*F1+0,60*F2 warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Cloud Computing introduction, https://oze.pwr.edu.pl//kursy/introcloud/introcloud.html
[2] CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0
[3] Cisco Academy Course: Cloud Security
[4] Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) (v. 1.00 – luty 2020)
[5] Software-Defined Perimeter (SDP) Specification v2.0 (https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter-and-zero-trust/)

LITERATURA UZUPEŁNIAJĄCA:

[1] Wprowadzenie do bezpieczeństwa w chmurze (https://www.intel.pl/content/www/pl/pl/cloud-computing/cloud-security.html)
[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
[3] ISO/IEC 27017, ISO/IEC 27018
[4] „Jak migrować do chmury zgodnie z prawem?" (https://www.traple.pl/2021/12/21/jak-migrowac-do-chmury-zgodnie-z-prawem/)

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr inż. Marcin Głowacki (Marcin.Glowacki@pwr.edu.pl)

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim	**Cyberbezpieczeństwo w Internecie Rzeczy**
Nazwa w języku angielskim	**Internet of Things**
Kierunek studiów:	**Cyberbezpieczeństwo**
Specjalność:	**Bezpieczeństwo systemów informatycznych**
Poziom i forma studiów:	**I / ~~II~~ stopień*, stacjonarna / ~~niestacjonarna~~***
Rodzaj przedmiotu:	**~~obowiązkowy~~ / wybieralny / ~~ogólnouczelniany~~ ***
Kod przedmiotu	**W04CBE-SI0405G**
Grupa kursów	**TAK / ~~NIE~~***

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	**15**	—	**30**	—	—
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	**50**	—	**50**	—	—
Forma zaliczenia	~~Egzamin~~ / zaliczenie na ocenę*	—	~~Egzamin~~ / zaliczenie na ocenę*	—	—
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**4**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	—	—	2	—	—
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	0,6	—	1,2	—	—

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Znajomość podstawowych protokołów wielodostępu
2. Znajomość zjawisk towarzyszących rozchodzeniu się fal radiowych oraz podstawowych modeli propagacyjnych

CELE PRZEDMIOTU

C1. Zdobycie podstawowej wiedzy na temat istoty i roli Internetu Rzeczy (IoT) we współczesnych realiach gospodarczych i technologicznych

C2. Zdobycie podstawowej wiedzy z zakresu: - zastosowań, - specyfiki i zasad działania systemów stosowanych w Internecie Rzeczy, - wiodących standardów transmisyjnych IoT

C3. Zdobycie podstawowej wiedzy o zagrożeniach dla prywatności, urządzeń i sieci IoT oraz metodach przeciwdziałania im

C4. Zdobycie umiejętności instalowania i zarządzania bezpieczną siecią sensorową dostosowaną do określonych potrzeb, z zastosowaniem dostępnych i optymalnych technik transmisyjnych Internetu Rzeczy

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – posiada podstawową wiedzę z zakresu: genezy, zastosowań, stanu badań i perspektyw rozwoju, architektury oraz warstwy fizycznej i protokołów wielodostępu stosowanych w systemach IoT

PEU_W02 – zna podstawowe systemy telekomunikacyjne IoT: - z grupy 3GPP (NB-IoT, LTE-M/TC), - rozwiązań firmowych (LoRa, Weightless, SigFox itp.)

PEU_W03 – zna zagrożenia wynikające ze stosowania systemów i podejścia IoT, zarówno pod kątem sprzętowym jak i programowym, oraz metody przeciwdziałania zagrożeniom w tych zakresach

Z zakresu umiejętności:

PEU_U01 – potrafi odpowiednio skonfigurować układ mikroprocesorowy (np. Arduino, Raspberry Pi) do rejestracji odczytów rozmaitych czujników analogowych i cyfrowych

PEU_U02 – umie dobrać oraz skonfigurować sieć sensorową w segmencie lokalnym z wykorzystaniem jednej z dostępnych technik transmisyjnych (tj. ZigBee, WLAN, Bluetooth, UWB, NRF24L01, 315/433/434 MHz) uwzględniając określone wymagania pomiarowe oraz implementując techniki zapewniające założony poziom cyberbezpieczeństwa

PEU_U03 – umie dobrać oraz skonfigurować sieć IoT w segmencie dostępowym bądź dalekosiężnym (LPWAN) z zastosowaniem jednej z dostępnych technik transmisyjnych (np. LoRa, NB-IoT) oraz implementując techniki zapewniające założony poziom cyberbezpieczeństwa

Z zakresu kompetencji społecznych:

PEU_K01 – potrafi pracować w zespole osób o zróżnicowanych zadaniach, ze świadomością istniejących współzależności merytorycznych i terminowych w pracy nad złożonym projektem teleinformatycznym

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Specyfika sieci systemów IoT, zastosowania, stan badań, perspektywy, architektura systemów	**2**
Wy2	Geneza Internetu Rzeczy (techniki LPWAN), przegląd najważniejszych standardów telekomunikacyjnych IoT w zakresie krótko- i dalekosiężnym	**4**
Wy3	Ochrona prywatności oraz etyka w dobie IoT, przegląd zagrożeń. Metody przeciwdziałania zagrożeniom w tym zakresie	**2**
Wy4	Bezpieczeństwo urządzeń IoT i sieci. Metody przeciwdziałania zagrożeniom w tym zakresie	**3**
Wy5	Bezpieczeństwo danych i oprogramowania w systemach IoT. Metody przeciwdziałania zagrożeniom w tym zakresie	**2**
	Repetytorium	**2**
	Suma godzin:	**15**

Forma zajęć - laboratorium		Liczba godzin
La1	Zajęcia organizacyjne – zaznajomienie z zasadami BHP, przedstawienie grafiku zajęć, prezentacja tematów ćwiczeń laboratoryjnych i narzędzi dydaktycznych, podział na grupy.	3
La2-La9	Realizacja ćwiczeń laboratoryjnych	27
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z użyciem prezentacji multimedialnych N2. Platformy mikrokontrolerów oraz układy programowalne systemów IoT N3. Narzędzia symulacyjne N4. Konsultacje N5. Praca własna – przygotowanie do ćwiczeń laboratoryjnych

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu kształcenia	Sposób oceny osiągnięcia efektu kształcenia
F1	PEU_W01-03	Test zaliczeniowy z wykładu
F2	PEU_U01-03 PEL_K01	Ocena końcowa z laboratorium
P = 0,76·F1+0,24·F2 *warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu*		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] J. Schlienz, D. Raddino, „Narrowband Internet of Things. Whitepaper”, Rhide-Schwarz, 1MA266_0e

[2] N. Sornin (Semtech), M. Luis (Semtech), T. Eirich (IBM), T. Kramp (IBM), O.Hersent (Actility), „LoRaWAN™ Specification. Version: v1.0.2”, July 2016, status: Final

LITERATURA UZUPEŁNIAJĄCA:

[3] „LoRaWAN™ Regional Parameters”, LoRa Alliance Technical committee, Version: v1.0, July 2016, status: Final

[4] McNamara D.A., Pistotius C.W.I., Malherbe J.A.G., „Wireless Sensor Networks. Technology, protocols, and applications”, Wiley & Sons Wiley, 2007

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Dr hab. inż. Kamil Staniec, prof. PWr, kamil.staniec@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ **Informatyki i Telekomunikacji**

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim: Praca dyplomowa
Nazwa przedmiotu w języku angielskim Diploma thesis
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): Bezpieczeństwo systemów informatycznych
Poziom i forma studiów: I / ~~II stopień / jednolite studia magisterskie*,~~ stacjonarna / ~~niestacjonarna*~~
Rodzaj przedmiotu: ~~obowiązkowy~~ / wybieralny ~~/ ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0400P
Grupa kursów ~~TAK~~ / NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)				180	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)				300	
Forma zaliczenia	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS				12	
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)				12	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)				7,2	

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Umiejętność przygotowania przeglądu literatury i precyzowania problemu badawczego.
2. Podstawowa wiedza dotycząca właściwości, struktur i sposobów działania systemów i sieci teleinformatycznych.
3. Umiejętność przygotowania dokumentacji.

CELE PRZEDMIOTU

C1 Zapoznanie z wytycznymi formalnymi odnośnie przygotowania pracy pisemnej, opisu literatury i struktury pracy dyplomowej.
C2 Nabycie poszerzonej wiedzy dotyczącej tematyki pracy dyplomowej.
C3 Nabycie umiejętności przygotowania badań, weryfikacji, opracowania i prezentacji wyników.
C4 Nabycie umiejętności terminowej i systematycznej pracy.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

Z zakresu umiejętności:
PEU_U01 – Potrafi wyszukać informacje z różnych źródeł, umie dokonać ich krytycznej analizy, syntezy, twórczej interpretacji oraz potrafi je zaprezentować.
PEU _U02 – Potrafi formułować i testować hipotezy dotyczące prostych problemów badawczych.
PEU _U04 – Potrafi — zgodnie z zadaną specyfikacją — zaprojektować, analizować lub zrealizować (przynajmniej w części) złożony system teleinformatyczny mający na celu realizację szeroko rozumianych usług transmisyjnych i przetwarzania danych, używając właściwych metod, technik i narzędzi.

Z zakresu kompetencji społecznych:
PEU _K01 – Jest gotów do krytycznej oceny odbieranych treści, ma świadomość znaczenia wiedzy w rozwiązywaniu problemów i ochronie środowiska.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
	Suma godzin	**0**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**

Forma zajęć - projekt		**Liczba godzin**
Pr1	Opracowanie metod(y) rozwiązywania problemu; implementacja	60
Pr2	Przeprowadzenie analiz i badań oraz opracowanie wyników	60
Pr3	Opracowanie dokumentacji (pracy pisemnej) pracy	60
…		
	Suma godzin	**180**

Forma zajęć - seminarium	**Liczba godzin**

Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Środowisko eksperymentalne (w tym platformy symulacyjne np.: Matlab, MathCad, Piast) wedle wyboru studenta. N2. Edytor tekstu. N3. Edytor grafik (tabel/rysunków) niezbędnych do realizacji pracy dyplomowej.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
P (projekt)	PEU _U01 PEU _U02 PEU _U04 PEU _K01	Ocena końcowa związaną z oceną przygotowanej pracy dyplomowej. Ocenie podlegać umiejętność zdefiniowania problemu, przeglądu stanu wiedzy i techniki, zaproponowania poprawnej metody, zaprojektowanie i przeprowadzenie eksperymentu lub analizy, krytyczna analiza wyników.

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA

[1] Regulamin procesu dyplomowania na Wydziale Informatyki i Telekomunikacji Politechniki Wrocławskiej

[2] Formatka pracy dyplomowej przygotowania przez WIT PWr

[3] Dokumentacja programu Plagiat.pl

LITERATURA UZUPEŁNIAJĄCA:

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Prof. dr hab. inż. Tadeusz Więckowski (Tadeusz.wieckowski@pwr.edu.pl)

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	**Projekt zespołowy**
Nazwa w języku angielskim:	**Team Project**
Kierunek studiów:	**Cyberbezpieczeństwo**
Specjalność:	**Bezpieczeństwo systemów informatycznych**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**obowiązkowy**
Kod przedmiotu:	**W04CBE-SI0408P**
Grupa kursów:	**NIE**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)				45	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)				125	
Forma zaliczenia				Zaliczenie na ocenę	
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS				**5**	
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-			5	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)				1,8	

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1 Nabycie umiejętności wykonania przydzielonych zadań inżynierskich w ramach realizacji złożonego zadania inżynierskiego

C2 Zdobycie doświadczeń w pracy zespołowej, w tym umiejętności planowania i harmonogramowania, komunikacji wewnątrz-zespołowej, pełnienia roli członka zespołu bądź lidera, możliwość wykazania się kreatywnością, otwartością na innowacyjne podejście do realizacji celu oraz zorientowaniem na sukces zespołu

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu umiejętności:

PEU_U01 potrafi wykonać zadania w ramach realizacji złożonego projektu informatycznego

PEU_U02 umie zastosować zasady zarządzania projektem do realizacji złożonego projektu informatycznego

PEU_U03 umie opracować dokumentację projektu

Z zakresu kompetencji:

PEU_K01 jest świadomy konieczności należytej współpracy z zespołem, wykazuje się świadomością swojej roli w projekcie oraz dbałością o terminową realizację powierzonych zadań

TREŚCI PROGRAMOWE		
Forma zajęć – projekt		**Liczba godzin**
Pr1	Ustalenie tematyki projektu (np. informacyjny system internetowy, złożony internetowy system bazodanowy, kompleksowy projekt sieci teleinformatycznej z uwzględnieniem technik bezprzewodowej transmisji, projekt informatyzacji firmy, system eksperymentowania, system diagnostyki sieci teleinformatycznej) i celu projektu. Przydział ról w projekcie, wstępny przydział zadań do wykonania, wybór lidera zespołu	4
Pr2	Zapoznanie się z obszarem problemowym projektu. Przegląd rozwiązań w obszarze problemu – analiza metod i stosowanych środków informatycznych.	4
Pr3	Analiza wymagań użytkownika, łącznie z analizą ekonomiczną skutków implementacji projektu. Opracowanie założeń projektowych. Ustalenie wstępnego harmonogramu działań (w formie wykresu Gantt'a) oraz zasad komunikacji wewnątrz-zespołowej i z prowadzącym.	4
Pr4	Zaplanowanie zasad zarządzania jakością w projekcie, opracowanie procedur kontrolowania jakości, analiza ryzyka. Ustalenie zasad odbioru wyników poszczególnych etapów projektu oraz zasad dokumentowania etapów	4
Pr5	Realizacja indywidualnych zadań projektowych wg harmonogramu realizacji I etapu projektu	8
Pr6	Realizacja spotkań zespołu z prowadzącym - zgodnie z ustalonym harmonogramem (kamień milowy)	4
Pr7	Realizacja indywidualnych zadań projektowych wg harmonogramu realizacji II etapu projektu	8
Pr8	Prezentacja efektów wykonanego projektu, dyskusja problemowa, ocena elementów wykonanego projektu przez prowadzącego. Weryfikacja projektu. Ustalenie ewentualnych zmian	5
Pr9	Przedstawienie ostatecznej dokumentacji projektu w formie pisemnej	4
	Suma godzin	**45**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Prezentacja multimedialna
N2. Dyskusja problemowa
N3. Konsultacje
N4. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01, PEU_U02, PEU_K01	Ocena prezentacji kolejnych etapów projektu oraz umiejętności pracy w zespole: przestrzegania harmonogramu, aktywność w zespole, umiejętność zastosowania zasad zarządzania projektem
F2	PEU_U03	Ocena jakość wykonanego projektu oraz dokumentacji projektowej
P=0.4*F1+0.6*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Praca zbiorowa, A Guide to the Project Management Body of Knowledge (PMBOK Guide), wydanie polskie, 2009
[2] Praca zbiorowa, Zarządzanie projektem informatycznym - model najlepszych praktyk, IFC Press, Kraków 2003
[3] Robertson J., Robertson S., (1999), Pełna analiza systemowa, WNT Warszawa, 2003
[4] Dennis A., Wixam B.H., System Analysis, Design, John Wiley & Sons, 2003
[5] Bentley C. (2002), Managing Projects the Prince 2 Way, Colin Bentley 2002.
[6] Anderson H.R.: Fixed Broadband Wireless System Design, John Wiley & Sons, 2003.

LITERATURA UZUPEŁNIAJĄCA:

[7] Pozycje literaturowe dotyczące wybranych technologii i środowisk programistycznych

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ Informatyki i Telekomunikacji

KARTA PRZEDMIOTU

Nazwa w języku polskim	**Przetwarzanie dużych zbiorów danych**
Nazwa w języku angielskim	**Big Data**
Kierunek studiów:	**Cyberbezpieczeństwo**
Specjalność:	**Bezpieczeństwo danych**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu	**W04CBE-SI0406G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30			15	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50			50	
Forma zaliczenia	Zaliczenie na ocenę		Zaliczenie na ocenę	Zaliczenie na ocenę	
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	**4**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-			2	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2			0,6	

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1 Nabycie wiedzy dotyczącej tworzenia sieciowych pamięci masowych
C2 Nabycie wiedzy dotyczącej tworzenia systemów przetwarzania dużej ilości danych (big data).
C3 Zdobycie umiejętności związanych z projektowaniem, konfigurowaniem oraz zarządzaniem sieciowymi pamięciami masowymi.
C4 Zdobycie umiejętności związanych z projektowaniem i tworzeniem analitycznych baz danych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – zna fizyczne i logiczne składowe infrastruktury pamięci masowych oraz technologie sieciowe pamięci masowych
PEU_W02 – zna wymagania i rozwiązania zapewnienia ciągłości biznesowej i bezpieczeństwa informacji oraz wie jak zidentyfikować parametry zarządzania i monitorowania infrastruktury pamięci masowych
PEU_W03 – zna etapy procesu przetwarzania dużej ilości danych oraz algorytmy stosowane w przetwarzaniu dużych zbiorów danych
PEU_W04 – zna modele i warstwy logiczne hurtowni danych

Z zakresu umiejętności:

PEU_U01 – potrafi zaprojektować, skonfigurować i zarządzać wybranymi rozwiązaniami sieciowych pamięci masowych
PEU_U02 – umie wykorzystywać mechanizmy zapewnienia ciągłości biznesowej
PEU_U03 – potrafi zaprojektować strukturę logiczną systemu do przetwarzania dużej ilości danych
PEU_U04 – potrafi zaprojektować proces ETL

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Sprawy organizacyjne	1
Wy2	Technologie Trzeciej Platformy	1
Wy3	Infrastruktura centrum danych	1
Wy4	Inteligentne systemy pamięci masowych	1
Wy5	Blokowe systemy pamięci masowych	1
Wy6	Plikowe systemy pamięci masowych	1
Wy7	Obiektowe i zunifikowane pamięci masowe	1
Wy8	Pamięci masowe sterowane programowo (SDS)	1
Wy9	Sieci Fibre Channel SAN (FC SAN)	1
Wy10	Sieci IP SAN i FCoE	1
Wy11	Wprowadzenie do ciągłości biznesowej	1
Wy12	Backup i archiwizacja	1
Wy13	Replikacja	1
Wy14	Zabezpieczanie infrastruktury pamięci masowych	1
Wy15	Zarządzanie infrastrukturą pamięci masowych	1
Wy16	Rozwój systemów baz danych i potrzeby przetwarzania dużej ilości danych	1
Wy17	Model logiczny systemów przetwarzania dużych wolumenów danych	2
Wy18	Potrzeby tworzenia systemów analityki biznesowej oraz ich umiejscowienie w strukturze informatycznej firmy	2
Wy19	Potrzeby tworzenia systemów hurtowni danych	2
Wy20	Modele logiczne hurtowni danych	2
Wy21	Proces ekstrakcji, transformacji i ładowania danych	2
Wy22	Raportowanie analityczne w wybranym środowisku	2

Wy23	Zaliczenie	2
	Suma godzin	**30**

Forma zajęć – projekt		**Liczba godzin**
Pr1	Sprawy organizacyjne. Omówienie treści projektu.	2
Pr2	Opracowanie wymagań użytkownika dotyczących analizy dużej ilości danych i sieciowych pamięci masowych.	4
Pr3	Sformułowanie wymagań dotyczących usługi raportowania	2
Pr4	Zaprojektowanie modelu logicznego systemu przetwarzającego dużą ilość danych	3
Pr5	Zaprojektowanie etapów procesu ETL i konfiguracji usług sieciowych pamięci masowych	2
Pr6	Wybór środowiska do implementacji projektu	2
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład informacyjny z wykorzystaniem prezentacji multimedialnej. N2. Wykład problemowy z wykorzystaniem prezentacji multimedialnej. N3. Konsultacje. N4. Praca własna – przygotowanie do projektu. N5. Praca własna – samodzielne studia i przygotowanie do zaliczenia wykładu. N6. Prezentacja projektu.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01-W04	Odpowiedzi ustne, sprawdzian pisemny w formie testu
F2	PEU_U01-U04	Ocena przygotowania projektu, obrona projektu, udział w dyskusjach problemowych.
P = 1/2*F1 + 1/2*F2 Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1, F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Pelikant A., Hurtownie danych. Od przetwarzania analitycznego do raportowania, Helion, Gliwice, 2011

[2] Todman C., Projektowanie hurtowni danych. Wspomaganie zarządzania relacjami z klientam, Helion, Gliwice 2011

[3] Zikopoulos P., Eaton C. Understanding big data: Analytics for enterprise class hadoop and streaming data. McGraw-Hill Osborne Media, 2011.

[4] Information Storage and Management – Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments 2nd Edition, John Wiley & Sons, Inc.

LITERATURA UZUPEŁNIAJĄCA:

[1] Chen H., Chiang R., Storey V.,. Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly 36 vol 4 (2012).

[2] Nigel Poulton, Data Storage Networking: Real World Skills for the CompTIA Storage+ Certification and Beyond, Sybex 2014

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Robert Burduk, robert.burduk@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁINFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Seminarium dyplomowe**
Nazwa w języku angielskim: **Diploma Seminar**
Kierunek studiów: **Cyberbezpieczeństwo**
Specjalność: **Bezpieczeństwo systemów informatycznych**
Poziom i forma studiów: **I stopień, stacjonarna**
Rodzaj przedmiotu: **wybieralny**
Kod przedmiotu: **W04CBE-SI0409S**
Grupa kursów: **NIE**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)					30
Liczba godzin całkowitego nakładu pracy studenta (CNPS)					50
Forma zaliczenia					Zaliczenie na ocenę
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS					**2**
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)					2
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)					1,3

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1 Nabycie umiejętności poszukiwania selektywnej wiedzy niezbędnej do tworzenia własnych oryginalnych rozwiązań.
C2 Zdobycie umiejętności przygotowania prezentacji pozwalającej w sposób komunikatywny przekazać słuchaczom swoje oryginalne pomysły, koncepcje i rozwiązania.
C3 Nabycie umiejętności kreatywnej dyskusji, w której w sposób rzeczowy i merytoryczny można uzasadnić i obronić swoje stanowisko.
C4 Nabycie umiejętności pisania dzieła prezentującego własne osiągnięcia, w tym prezentacji własnych osiągnięć na tle rozwoju myśli światowej.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ
Z zakresu umiejętności: PEU_U01 potrafi przygotować prezentację zawierającą wyniki rozwiązań PEU_U02 potrafi w dyskusji rzeczowo uzasadnić swoje oryginalne pomysły i rozwiązania PEU_U03 potrafi krytycznie ocenić rozwiązania naukowo-techniczne innych osób

TREŚCI PROGRAMOWE		
Forma zajęć - seminarium		**Liczba godzin**
Se1	Omówienie zasad przygotowania i pisania pracy dyplomowej, a w szczególności przedstawienie zasad edytorskich	2
Se2	Prezentacje indywidualne dotyczące omówienia aktualnego stanu wiedzy związanego z problematyką realizowanej pracy dyplomowej oraz odniesienia przewidywanego, oryginalnego własnego wkładu do osiągnięć literaturowych	8
Se3	Dyskusja w grupie seminaryjnej nt. stanu wiedzy literaturowej i założonej koncepcji rozwiązania stawianych sobie problemów, składających się na pracę dyplomową	6
Se4	Prezentacje indywidualne dotyczące zrealizowanej pracy dyplomowej z uwypukleniem własnego oryginalnego dorobku autora wraz z dyskusją w grupie seminaryjnej	14
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. prezentacja multimedialna N2. dyskusja problemowa N3. praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny: F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01	prezentacja
F2	PEU_U02, PEU_U03	dyskusja
P= 0.5*F1+0.5*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
Literatura związana z problematyką pracy dyplomowej
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
Dr hab. inż. Ryszard Zieliński, ryszard.zielinski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim Bezpieczeństwo sieci i systemów teleinformatycznych w elektroenergetyce

Nazwa przedmiotu w języku angielskim Security of ICT systems and networks in power engineering

Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo

Specjalność (jeśli dotyczy): Bezpieczeństwo infrastruktury krytycznej

Poziom i forma studiów: I stopień / stacjonarna

Rodzaj przedmiotu: wybieralny

Kod przedmiotu: W04CBE-SI0309W

Grupa kursów: NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25				
Forma zaliczenia	zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	1				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)					
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału (BU)	0,6				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. podstawowa wiedza nt. przetwarzania sygnałów cyfrowych
2. znajomość zasad projektowania i eksploatacji sieci teleinformatycznych
3. znajomość komunikacji sieciowej na podstawie modelu ISO/OSI oraz TCP/IP

\

CELE PRZEDMIOTU

Nabycie podstawowej wiedzy z zakresu:

C1.1 projektowania i eksploatacji przemysłowych sieci teleinformatycznych

C1.1 budowy i zastosowania protokołów telekomunikacyjnych automatyki przemysłowej

C1.1 zagrożeń cybernetycznych i rozwiązań pozwalających wzrost bezpieczeństwa cyfrowego

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Posiada wiedzę w zakresie projektowania i funkcjonowania inteligentnych sieci elektroenergetycznych wykorzystujących technologię ICT

PEU_W02 Student zna rozwiązania techniczne i rozumie zasady funkcjonowania mechanizmów pozwalających na wzrost cyberbezpieczeństwa i poprawę niezawodności systemów i sieci teleinformatycznych

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie w tematykę przedmiotu. Podstawowa koncepcja i terminologia. Kwestie organizacyjne.	1
Wy2	Polityka bezpieczeństwa, klasyfikacja zagrożeń, architektura logiczna i zarządzanie bezpieczeństwem ISE	2
Wy3	Bezpieczeństwo sieci i inteligentnych urządzeń automatyki domowej	2
Wy4	Dedykowane protokoły komunikacyjne stosowane w przemyśle	2
Wy5	Algorytmy i mechanizmy rekonfiguracji sieci i systemu Replikacja baz danych i synchronizacja czasu w urządzeniach IED	2
Wy6	Informatyka śledcza w przemyśle 4.0	2
Wy7	Rozwiązania techniczne dedykowane cyfrowej ochronie ISE	2
Wy8	Kolokwium zaliczeniowe	2
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny z prezentacjami i dyskusją

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 – W02	Kolokwium zaliczeniowe
P = F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] T. Flick, J. Morehouse, Securing the Smart Grid. Next Generation Power Grid Security, Elsevier Inc. 2011
[2] F. Skopik, P. Smith, Smart Grid Security Innovative Solutions for a Modernized Grid, 2015
[3] J. Stoustrup, A. Annaswamy, A. Chakrabortty, Z. Qu, Smart Grid Control, 2018

LITERATURA UZUPEŁNIAJĄCA:

[1] CCNA Exploration, Semestr 1 – Podstawy sieci, Akademia Cisco, 2008
[2] CCNA Exploration, Semestr 2 – Protokoły i koncepcje routingu, Akademia Cisco, 2008
[3] R. Anderson, Inżynieria zabezpieczeń, Wydawnictwo: Wydawnictwa Naukowo-Techniczne, 2005

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

dr inż. Robert Czechowski, robert.czechowski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Bezpieczeństwo systemów sterowania i nadzoru w elektroenergetyce**
Nazwa przedmiotu w języku angielskim:	**Security of control and supervision systems in power engineering**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0307G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	35		65		
Forma zaliczenia	zaliczenie na ocenę		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**4**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału (BU)	0,6		1,2		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Ma wiedzę w zakresie zasad i technik realizacji zabezpieczeń elementów systemu elektroenergetycznego.
2. Ma wiedzę w zakresie podstawowych zasad i technik regulacji i sterowania pracą systemu elektroenergetycznego w stanach normalnych i awaryjnych.
3. Potrafi łączyć, eksploatować i koordynować przekaźniki pomiarowe jednowejściowe i wielowejściowe oraz zabezpieczenia elektroenergetyczne.
4. Potrafi zainstalować, nastawić i wykonać badania eksploatacyjne podstawowych układów sterowania i kontroli stosowanych w elektroenergetyce

CELE PRZEDMIOTU

C1 Zapoznanie studenta z nowoczesnymi zabezpieczeniami elektroenergetycznymi sieci elektroenergetycznych, koncentratorami oraz stanowiskiem dyspozytorskim.

C2	Nabycie praktycznej wiedzy i umiejętności nastawiania wielkości rozruchowych wybranych kryteriów zabezpieczeń linii w zależności od układu pracy sieci elektroenergetycznej.
C3	Wyrobienie umiejętności zastosowania nowoczesnych metod, technik i narzędzi do badania zabezpieczeń elektroenergetycznych.
C4	Rozwój kompetencji związanych z szeroko rozumianymi aplikacjami SCADA (protokoły komunikacyjne, koncentratory, stanowisko dyspozytorskie).

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01	Zna sposoby realizacji łączności pomiędzy zabezpieczeniami elektroenergetycznymi, układami sterowania i regulacji oraz stanowiskiem dyspozytorskim.
PEU_W02	Zna środki stosowane w systemach elektroenergetycznych w celu zapewnienia bezpieczeństwa ich pracy.

Z zakresu umiejętności:

PEU_U01	Potrafi dobrać i dokonać nastaw wartości rozruchowych wielkości kryterialnych zabezpieczeń oraz wyznaczyć charakterystyki podstawowych kryteriów zabezpieczeń elektroenergetycznych.
PEU_U02:	Ma umiejętności związane z nawiązywaniem komunikacji cyfrowej między zabezpieczeniem elektroenergetycznym a sterownikiem polowym (koncentratorem), jako elementem Systemu Sterowania i Nadzoru.

Z zakresu kompetencji społecznych:

PEU_K01	Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie - cele przedmiotu, organizacja zajęć, literatura, ustalenie zasad zaliczenia. Klasyfikacja i zadania automatyki zabezpieczeniowej. Podstawowe pojęcia i wymagania.	1
Wy2	Zabezpieczenia i automatyki stosowane w sieciach średniego napięcia.	2
Wy3	Zabezpieczenia i automatyki stosowane w sieciach wysokiego i najwyższych napięć.	2
Wy4	Protokoły komunikacyjne wykorzystywane w elektroenergetyce.	2
Wy5	Systemy typu SCADA.	2
Wy6	Cyfrowa stacja elektroenergetyczna.	2
Wy7	Cyberbezpieczeństwo krytycznej infrastruktury elektroenergetycznej.	2
Wy8	Kolokwium zaliczeniowe.	2
	Suma godzin	**15**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
...		
	Suma godzin	

Forma zajęć - laboratorium		Liczba godzin
La1	Prezentacja regulaminu BHP i regulaminu wewnętrznego laboratorium. Ustalenie zasad zaliczenia przedmiotu. Ogólne zapoznanie się ze stanowiskiem laboratoryjnym, fizycznymi modelami zabezpieczeń i kryteriami zabezpieczeniowymi	2
La2	Zapoznanie się z zasadą działania i funkcjonalnością cyfrowego testera zabezpieczeń.	2
La3	Zapoznanie się z budową (obwody wejścia/wyjścia) i zasadą działania (kryteria zabezpieczeń) zabezpieczenia cyfrowego.	4
La4	Programowanie zabezpieczeń	2
La5	Badanie wybranego, cyfrowego zabezpieczenia elektroenergetycznego	8
La6	Komunikacja miedzy urządzeniami po protokole MODBUS.	2
La7	Lokalne Stanowisko Dyspozytorskie – lokalne stanowisko Systemu Sterowania i Nadzoru	2
La8	Komunikacja GOOSE – wstęp do komunikacji zgodnej ze standardem IEC61850	2
La9	Komunikacja MMS – wstęp do komunikacji zgodnej ze standardem IEC61850	2
La10	Brama dostępowa – komunikacja (po protokole DNP3) ze zdalnym Stanowiskiem Dyspozytorskim	2
La11	Zaliczenie i uzupełnienie zaległości laboratoryjnych	2
	Suma godzin	30

Forma zajęć - projekt		Liczba godzin
Pr1		
Pr2		
Pr3		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
N1	Wykład problemowy.
N2	Wykład z użyciem technik audiowizualnych, prezentacje multimedialne.
N3	Laboratorium pomiarowe prowadzone w sposób tradycyjny w ćwiczeniowych grupach studenckich
N4	Sprawdzenie wiadomości w formie ustnej lub pisemnej.
N5	Przygotowanie sprawozdania z przeprowadzonych pomiarów.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1(W)	PEU_W01 PEU_W02	Kolokwium w formie pisemnej
P(W)	P(W)=F1	
F1(L)	PEU_U01 PEU_K01	Sprawdzenie przygotowania do ćwiczeń laboratoryjnych i aktywność na zajęciach laboratoryjnych
F2(L)	PEU_U02 PEU_K01	Ocena sprawozdań z wykonanych badań
P(L)	P(L)=0,2F1+0,8F2	
P = 0,5P(W) + 0,5P(L) **Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu**		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Synal B. Rojewski W. Dzierżanowski W.: Elektroenergetyczna automatyka zabezpieczeniowa – podstawy, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2003

[2] Winkler W., Wiszniewski A., Automatyka zabezpieczeniowa w systemach elektroenergetycznych, WNT, Warszawa 2004.

[3] Praca zbiorowa pod redakcją Dejmaniuk D. „Technika cyfrowa w automatyce elektroenergetycznej", Komitet Automatyki Elektroenergetycznej SEP, Bielsko-Biała, 24-26 kwietnia 2013.

LITERATURA UZUPEŁNIAJĄCA:

[1] Synal B., Rojewski W., Zabezpieczenia elektroenergetyczne – Podstawy, Podręcznik INPE dla elektryków, Zeszyt 19, 2008.

[2] Instrukcje do ćwiczeń laboratoryjnych.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Marcin Habrych, marcin.habrych@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Cyberbezpieczeństwo inteligentnych sieci elektroenergetycznych**
Nazwa przedmiotu w języku angielskim:	**Cybersecurity of Smart Power Grids**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0308G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			15	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	35			40	
Forma zaliczenia	zaliczenie na ocenę			zaliczenie na ocenę	
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**3**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)				1	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału (BU)	0,6			0,6	

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Ma uporządkowaną i podbudowaną teoretycznie wiedzę niezbędną do rozumienia celu oraz zakresu działania technologii inteligentnych sieci elektroenergetycznych (Smart Power Grids).
Ma podstawową wiedzę z zakresu bezpieczeństwa informatycznego, w tym szeroko pojętego bezpieczeństwa informacji przetwarzanych w systemach elektronicznych oraz bezpieczeństwa systemów informatycznych.
Potrafi poprawnie i efektywnie wykonać testy eksploatacyjne cyfrowych elementów zabezpieczeń sieci komputerowych.

CELE PRZEDMIOTU

C1	Zaznajomienie studenta z powszechnie uznanymi dobrymi praktykami zarządzania cyberbezpieczeństwem przemysłowych systemów infrastruktury krytycznej (OT), do których zalicza się inteligentne sieci elektroenergetyczne.
C2	Zapoznanie studenta ze standardami w stosowaniu zabezpieczeń informatycznych elementów infrastruktury inteligentnych sieci elektroenergetycznych.
C3	Wyrobienie umiejętności identyfikacji, przeciwdziałania i reagowania na zaistniałe zagrożenia cyberprzestępstwami oraz cyberterroryzmem ukierunkowanymi na inteligentne sieci elektroenergetyczne
C4	Nabycie praktycznej wiedzy i umiejętności w zakresie opracowywania procedur wspierających bezpieczeństwo informatyczne przemysłowych systemów OT oraz monitorowania znanych podatności na cyberatak.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01	Zna i rozumie przyczyny i skutki zagrożeń informatycznych dla infrastruktury inteligentnych sieci elektroenergetycznych.
PEU_W02	Ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie identyfikacji i reagowania na incydenty cybernetyczne w inteligentnych sieciach elektroenergetycznych.

Z zakresu umiejętności:

PEU_U01	Potrafi opracowywać procedury wspierające bezpieczeństwo informatyczne przemysłowych systemów OT
PEU_U02	Potrafi podejmować działania związane z naruszeniem poufności informacji przetwarzanych w ISE

Z zakresu kompetencji społecznych:

PEU_K01	Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole

TREŚCI PROGRAMOWE

Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie - cele przedmiotu, organizacja zajęć, literatura, ustalenie zasad zaliczenia. Cele, zadania oraz zagrożenia dot. inteligentnych sieci elektroenergetycznych (ISE), jako podsystemu infrastruktury krytycznej.	1
Wy2	Podstawy prawne, podstawowe definicje i klasyfikacja systemów informacyjnych. Cel i strategia bezpieczeństwa informacji.	2
Wy3	Wybrane zagadnienia z teorii bezpieczeństwa informacji przetwarzanych w systemach elektronicznych ISE.	2
Wy4	Bezpieczeństwo informacji w inteligentnych sieciach domowych (HAN - Home Area Network).	2
Wy5	Zarządzanie bezpieczeństwem informacji w systemach zdalnego odczytu liczników (AMI – Advanced Metering Infrastructure)	2
Wy6	Wybrane zagadnienia z zakresu zarządzania rozproszonymi źródłami energii.	2
Wy7	Utrzymanie ciągłości działania systemów informacyjnych ISE oraz procesy wznowienia działania systemów informacyjnych po przerwie spowodowanej czynnikami naturalnymi lub wywołanej przez człowieka.	2
Wy8	Kolokwium zaliczeniowe	2
	Suma godzin	**15**

Forma zajęć - ćwiczenia		Liczba godzin
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		Liczba godzin
La1		
La2		
La3		
La4		
La5		
…		
	Suma godzin	

Forma zajęć - projekt		Liczba godzin
Pr1	Wprowadzenie - organizacja zajęć, literatura, ustalenie zasad zaliczenia, prezentacja regulaminu BHP. Zapoznanie się ze strukturą dokumentów Polityki Bezpieczeństwa Informacji.	1
Pr2	Opis chronionej infrastruktury systemu informacyjnego.	2
Pr3	Rozkład odpowiedzialności za bezpieczeństwo informacji.	2
Pr4	Kontrola dostępu do informacji.	2
Pr5	Procedury wznowienia działania systemów informacyjnych po przerwie spowodowanej czynnikami naturalnymi lub wywołanej przez człowieka.	2
Pr6	Opis działań, które powinny zostać podjęte w przypadku naruszenia bezpieczeństwa informacji.	2
Pr7	Zakres stosowania i rozpowszechniania Polityki bezpieczeństwa informacji.	2
Pr8	Termin wyrównawczy	2
	Suma godzin	**15**

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład problemowy. N2. Wykład z użyciem technik audiowizualnych, prezentacje multimedialne. N3. Przygotowanie sprawozdania z wykonanych projektów. N4. Sprawdzenie wiadomości w formie ustnej lub pisemnej.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1(W)	PEU_W01 PEU_W02	Kolokwium w formie pisemnej
P(W)	P(W)=F1	
F1(P)	PEU_U01 PEU_U02 PEU_K01	Ocena sprawozdań z wykonanych projektów
P(P)	P(L)=F1	
P = 0,6 P(W) + 0,4 P(L) **Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu**		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] William Stallings, Lawrie Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Wydawnictwo Helion

[2] Liderman Krzysztof, Analiza ryzyka i ochrona informacji w systemach komputerowych, Wydawnictwo Naukowe PWN, 2009

[3] Liderman Krzysztof, Bezpieczeństwo informacyjne. Nowe wyzwania, Wydawnictwo Naukowe PWN, 2017

[4] Kowalewski Marian, Kowalewski Jakub, Polityka bezpieczeństwa informacji w praktyce, Wydawnictwo PRESSCOM

[5] Kifner Tadeusz, Polityka bezpieczeństwa i ochrony informacji, Wydawnictwo Helion, 1999

LITERATURA UZUPEŁNIAJĄCA:

[1] Janczewski Lech, Kutyłowski Mirosław [Red.], ICT systems security and privacy protection: 33rd IFIP TC 11 International Conference WCC 2018, Poznań;

[2] Tarnowski Ireneusz, Bezpieczeństwo systemów IT: Reagowanie na incydenty - procedury operacyjne obsługi incydentu. IT Professional (Wrocław). 2016, nr 12, s. 51-55

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Marek Wąsowski, marek.wasowski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Bezpieczeństwo w wytwarzaniu i przesyle energii elektrycznej**
Nazwa przedmiotu w języku angielskim:	**Security of supply in generation and transmission of electricity**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0303W**
Grupa kursów:	**NIE**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75				
Forma zaliczenia	zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**3**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)					
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału (BU)	1,2				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Zna podstawowe zasady funkcjonowania systemów technicznych.
2. Ma wiedzę w zakresie budowy elementów systemów elektroenergetycznych i maszyn elektrycznych prądu przemiennego.
3. Zna ogólne zasady pracy i metody rozwiązywania obwodów prądu przemiennego. Zna i rozumie wybrane metody obliczeniowe tj. metoda iteracyjna, metoda składowych symetrycznych.

CELE PRZEDMIOTU

C1. Zapoznanie studenta z wiedzą związaną z przesyłaniem i dystrybucją energii elektrycznej.
C2. Nabycie wiedzy z zakresu wymagań stawianych systemom elektroenergetycznym oraz zasad bezpiecznej ich eksploatacji w różnych okresach czasowych.

C3. Zapoznanie z aktualnymi przepisami prawnymi w zakresie eksploatacji i bezpieczeństwa Krajowego Systemu Energetycznego.
C4. Zna problemy systemów sterowania i nadzoru w elektroenergetyce.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna budowę systemu elektroenergetycznego i zasady bezpieczeństwa elektroenergetycznego.

PEU_W02 Rozumie i potrafi opisać podstawowe skutki utraty bezpieczeństwa w różnych horyzontach czasowych.

PEU_W03 Zna mechanizmy zabezpieczeń systemów informatycznych wchodzących w skład infrastruktury krytycznej wytwarzania i przesyłu energii elektrycznej.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie - cele przedmiotu, organizacja zajęć, literatura, zasady zaliczenia. Energetyka jako gałąź przemysłu.	2
Wy2	Polityka energetyczna – zakres, cele i instrumenty.	2
Wy3	Definicje związane z bezpieczeństwem w odniesieniu do elementów systemu i jego struktury. Krajowy System Elektroenergetyczny.	2
Wy4	Skutki ekonomiczne i społeczne utraty bezpieczeństwa elektroenergetycznego.	2
Wy5	Bezpieczeństwo strategiczne – w horyzoncie wieloletnim.	2
Wy6	Bezpieczeństwo średniookresowe – w horyzoncie rocznym – związane z eksploatacją.	2
Wy7	Bezpieczeństwo krótkookresowe – w horyzoncie sezonowym – związane z przygotowaniem ruchu.	2
Wy8	Bezpieczeństwo bieżące – w horyzoncie operatorskim – w stanach normalnych i nienormalnych – pozom przesyłowy/systemowy.	2
Wy9	Bezpieczeństwo bieżące – w horyzoncie operatorskim – w stanach normalnych i nienormalnych – pozom dystrybucyjny/lokalny.	2
Wy10	Bezpieczeństwo w stanach awaryjnych lokalnych i totalnych – horyzonty sekundowe i minutowe.	2
Wy11	Perspektywiczne technologie wytwarzania i ich wpływ na bezpieczeństwo systemu.	2
Wy12	Organizacja łączności służącej do zarządzania i sterowania w KSE.	
Wy13	Systemy sterownia i nadzoru. Bezpieczeństwo systemów informatycznych wchodzących w skład infrastruktury krytycznej wytwarzania i przesyłu energii elektrycznej.	2
Wy14	Systemy i mechanizmy zabezpieczenia urządzeń i systemów komputerowych przed nieupoważnionym dostępem.	2
Wy15	Kolokwium zaliczeniowe.	2
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład problemowy. N2. Wykład z użyciem technik audiowizualnych, prezentacje multimedialne.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02 PEU_W03	Kolokwium w formie pisemnej
P	P=F1	

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Kremens Z., Sobierajski M.: Analiza systemów elektroenergetycznych. WNT, Warszawa, 1996

[2] Paska J.: Niezawodność systemów elektroenergetycznych. Oficyna Wydawnicza Politechniki Warszawskiej. Warszawa 2005.

[3] Machowski J., Lubośny Z.: Stabilność systemu elektroenergetycznego, Wydawnictwo Naukowe PWN, WNT, 2018

[4] Toczyłowski E.: Optymalizacja procesów rynkowych przy ograniczeniach. Wydawnictwo EXIT, Warszawa, 2004

LITERATURA UZUPEŁNIAJĄCA:

[1] Instrukcja Ruchu i Eksploatacji Sieci Przesyłowej

[2] Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne. Stan prawny na dzień 7 kwietnia 2007 r. Tekst ujednolicony w Biurze Prawnym URE.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Robert Lis, robert.lis@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Elektroenergetyczna automatyka zabezpieczeniowa**
Nazwa przedmiotu w języku angielskim:	**Power System Protection**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0301G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75		25		
Forma zaliczenia	Egzamin		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**4**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału (BU)	1,4		0,6		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Zna zasady funkcjonowania systemu elektroenergetycznego i stacji elektroenergetycznych.
2. Ma wiedzę w zakresie budowy transformatorów i maszyn elektrycznych prądu przemiennego.
3. Zna ogólne zasady i techniki opisu pracy obwodów elektrycznych. Zna i rozumie wybrane przekształcenia, jak np. metoda składowych symetrycznych.
4. Potrafi planować i bezpiecznie wykonywać pomiary oraz opracowywać wyniki pomiarów.

CELE PRZEDMIOTU

C1. Zapoznanie studenta z rodzajami elektroenergetycznej automatyki zabezpieczeniowej w powiązaniu z rodzajem zakłócenia w pracy stanem systemu elektroenergetycznego

C2. Zapoznanie studenta z budową i zasadą działania przetworników wielkości pomiarowych zabezpieczeń.

C3. Zapoznanie studenta z budową i zasadami działania elektroenergetycznych przekaźników pomiarowych jedno i wielowejściowych.

C4. Zapoznanie studenta z zasadami i technikami realizacji zabezpieczeń elementów systemu elektroenergetycznego.
C5. Nabycie praktycznej umiejętności wykonywania badań elementów elektroenergetycznej automatyki zabezpieczeniowej – przetworników i przekaźników pomiarowych oraz zabezpieczeń elektroenergetycznych.
C6. Nabycie praktycznej umiejętności doboru rodzaju i obliczania nastaw zabezpieczeń elektroenergetycznych
C7. Nabycie umiejętności pracy w zespole

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01: Zna budowę i zasadę działania przekładników prądowych, napięciowych i filtrów składowych symetrycznych oraz analogowych i cyfrowych przekaźników elektroenergetycznych

PEU_W02 Rozumie i potrafi opisać podstawowe kryteria działania zabezpieczeń elektroenergetycznych oraz przedstawić podstawowe charakterystyki jednowejściowych i wielowejściowych przekaźników elektroenergetycznych

PEU_W03 Zna zasady wyposażania elementów systemu elektroenergetycznego w automatykę zabezpieczeniową i rozumie zasady doboru nastaw tej automatyki.

Z zakresu umiejętności:

PEU_U01 Potrafi zaprojektować układ pomiarowy, dobrać przyrządy pomiarowe oraz połączyć układ do badania przetworników i przekaźników pomiarowych jedno i wielowejściowych.

PEU_U02 Potrafi wykonać pomiary charakterystyk, opracować wyniki i sformułować wnioski.

Z zakresu kompetencji społecznych:

PEU_K01 Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wprowadzenie - cele przedmiotu, organizacja zajęć, literatura, ustalenie zasad zaliczenia. Klasyfikacja i zadania automatyki zabezpieczeniowej. Podstawowe pojęcia i wymagania.	2
Wy2	Charakterystyka zakłóceń w pracy systemu elektroenergetycznego. Przetworniki wielkości pomiarowych – przekładniki prądowe, napięciowe i filtry składowych symetrycznych	2
Wy3	Przetworniki wielkości pomiarowych – przekładniki prądowe, napięciowe i filtry składowych symetrycznych	2
Wy4	Przekaźniki i zespoły zabezpieczeniowe. Cechy charakterystyczne kolejnych generacji zabezpieczeń i tendencje rozwojowe	2
Wy5	Przekaźniki pomiarowe jednowejściowe zależne i niezależne.	2
Wy6	Kształtowanie charakterystyk przekaźników wielowejściowych. Przekaźniki kierunkowe i impedancyjne	2
Wy7	Przekaźniki różnicowe i porównawczo-fazowe	2
Wy8	Przekaźniki odległościowe	2
Wy9	Zabezpieczenia generatorów synchronicznych.	2
Wy10	Zabezpieczenia transformatorów	2

Wy11	Zabezpieczenia silników wysokiego napięcia.	2
Wy12	Zabezpieczenia sieci rozdzielczych średniego napięcia.	2
Wy13	Zabezpieczenia sieci przesyłowych i przesyłowo-rozdzielczych	2
Wy14	Zabezpieczenia szyn zbiorczych.	2
Wy15	Kolokwium zaliczeniowe.	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Prezentacja regulaminu BHP i regulaminu wewnętrznego laboratorium. Ustalenie zasad zaliczenia przedmiotu. Ogólne zapoznanie się ze stanowiskami laboratoryjnymi	1
La2	Badanie przekaźników i przetworników sygnałów prądowych i napięciowych	2
La3	Badanie przekaźników jedno- i wielowejściowych o charakterystyce niezależnej	2
La4	Badanie zabezpieczeń różnicowych transformatora.	2
La5	Badanie zabezpieczeń kierunkowych linii	2
La6	Badanie zabezpieczeń silnikowych	2
La7	Badanie filtrów składowej zerowej prądu	2
La8	Zajęcia odróbkowe. Wystawienie ocen	2
	Suma godzin	**15**

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład problemowy. N2. Wykład z użyciem technik audiowizualnych, prezentacje multimedialne.

N3. Laboratorium pomiarowe prowadzone w sposób tradycyjny w ćwiczeniowych grupach studenckich N4. Sprawdzenie wiadomości w formie ustnej lub pisemnej. N5. Przygotowanie sprawozdania z przeprowadzonych pomiarów.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1(W)	PEU_W01 PEU_W02 PEU_W03	Kolokwium w formie pisemnej
P(W)	P(W)=F1	
F1(L)	PEU_U01 PEU_K01	Sprawdzenie przygotowania do ćwiczeń laboratoryjnych i aktywność na zajęciach laboratoryjnych
F2(L)	PEU_U02 PEU_K01	Ocena sprawozdań z wykonanych badań
P(L)	P(L)=0,2F1+0,8F2	
P = 0,7P(W) + 0,3P(L) **Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu**		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Synal B. Rojewski W. Dzierżanowski W.: Elektroenergetyczna automatyka zabezpieczeniowa – podstawy, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2003

[2] Winkler W., Wiszniewski A., Automatyka zabezpieczeniowa w systemach elektroenergetycznych, WNT, Warszawa 2004.

[3] Praca zbiorowa pod red. B. Synala, Automatyka elektroenergetyczna, ćwiczenia laboratoryjne, część I: Przetworniki sygnałów pomiarowych i przekaźniki automatyki zabezpieczeniowej, część II: Układy automatyki zabezpieczeniowej i regulacyjnej skrypt Politechniki Wrocławskiej, Wrocław 1991.

[4] Praca zbiorowa pod red. B. Synala, Automatyka elektroenergetyczna, ćwiczenia laboratoryjne. Cz. II, Układy automatyki zabezpieczeniowej i regulacyjnej, Wyd. PWr., Wrocław 1991.

LITERATURA UZUPEŁNIAJĄCA:

[1] Synal B., Rojewski W., Zabezpieczenia elektroenergetyczne – Podstawy, Podręcznik INPE dla elektryków, Zeszyt 19, 2008.

[2] Instrukcje do ćwiczeń laboratoryjnych.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Marcin Habrych, marcin.habrych@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Komunikacja w inteligentnych systemach pomiarowych**
Nazwa przedmiotu w języku angielskim:	**Communication in intelligent measurement systems**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0305G**
Grupa kursów**:**	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		25		
Forma zaliczenia	zaliczenie na ocenę		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**3**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			1		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1,2		0,6		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Ma podstawową wiedzę niezbędną do zrozumienia zjawisk towarzyszących przewodowemu i bezprzewodowemu przetwarzaniu i przesyłowi sygnałów.
2. Ma podstawową wiedzę w zakresie teorii pola elektromagnetycznego.

CELE PRZEDMIOTU

C1. Zapoznanie studenta z podstawową wiedzą niezbędną do zrozumienia zjawisk fizycznych towarzyszących przewodowemu i bezprzewodowemu przesyłowi sygnałów analogowych i cyfrowych.

C2. Zapoznanie studenta z możliwością połączenia czujników w wybraną sieć do zdalnego pomiaru wielkości.

C3. Wyrobienie umiejętności teoretycznego i praktycznego wykorzystania przewodowej w tym techniki PLC i bezprzewodowej komunikacji do monitoringu i pomiarów zdalnych w systemach elektroenergetycznych.
C4. Nabycie wiedzy odnośnie do aktualnych trendów w technice przesyłania sygnałów w odniesieniu do zastosowań przemysłowych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01: Ma poszerzoną wiedzę z zakresu technik sterowania i komunikacji wykorzystywanych w układach automatyki elektroenergetycznej.

PEU_W02: Ma wiedzę na temat fizycznych podstaw działania, realizacji i sposobu aplikacji urządzeń pomiarowych.

Z zakresu umiejętności:

PEU_U01: Potrafi projektować i przetestować eksperymentalnie złożone układy sterowania, pomiaru i automatyki elektroenergetycznej

PEU_U02: Potrafi opracować wyniki pomiarów i sformułować wnioski

Z zakresu kompetencji społecznych:

PEU_K01: Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Zapoznanie z przedmiotem, wymaganiami i sposobem zaliczenia. Zadania przewodowej w tym PLC oraz bezprzewodowej komunikacji, podstawowe definicje	2
Wy2	Normalizacja komunikacji przewodowej w tym PLC, wady i zalety	2
Wy3	Architektura sieci elektrycznej, modelowanie urządzeń elektrycznych, architektura warstwowa OSI	2
Wy4	Funkcjonalność kanału transmisyjnego, synchronizacja, sterowanie ramkami, priorytety zarządzania ramką	2
Wy5	Przegląd sposobów zabezpieczania sieci PLC. Funkcjonalność trybów transmisji w sieci: master – slave, p2p, centralizowana	2
Wy6	Główny obszar zastosowań: telefonia, przesyłanie obrazu, multimedia, urządzenia dla różnych trybów transmisji	2
Wy7	Wybór kabla transmisyjnego, sposoby sprzęgania, transformatory i mierniki.	2
Wy8	Problemy aplikacji wybranych czujników/urządzeń pomiarowych	2
Wy9	Monitorowanie wielkości elektrycznych i nieelektrycznych oraz zdalny pomiar	2
Wy10	Architektura bezprzewodowych sieci HAN, LAN, zalety i wady	2
Wy11	Architektura przewodowych sieci HAN, LAN, zalety i wady	2
Wy12	Komunikacja GOOSE, jako część komunikacji zgodnej ze standardem IEC61850	2
Wy13	Komunikacja MMS, jako część komunikacji zgodnej ze standardem IEC61850, Komunikacja między urządzeniami po protokole MODBUS (RS485)	2
Wy14	Komunikacja po protokole DNP3 ze zdalnym Centrum Nadzoru, lokalne stanowisko Systemu Sterowania i Nadzoru (SCADA)	2

Wy15	Podsumowanie. Zaliczenie przedmiotu	2
	Suma godzin	**30**

Forma zajęć - laboratorium		**Liczba godzin**
La1	Prezentacja regulaminu BHP i regulaminu wewnętrznego laboratorium. Ustalenie zasad zaliczenia przedmiotu. Ogólne zapoznanie się ze stanowiskami laboratoryjnymi, fizycznymi modelami elementów	1
La2	Analiza wpływu zakłóceń na skuteczność transmisji PLC	2
La3	Komunikacja PLC w technologii DCSK	2
La4	Komunikacja PLC w technologii PRIME	2
La5	Wpływ metody sprzężenia układu pomiarowego z medium transmisyjnym, na jakość pomiaru	2
La6	Komunikacja z zastosowaniem BPL, jako smart meters model TCP/IP	2
La7	Badanie wpływu elementów otaczającego środowiska, na jakość bezprzewodowej transmisji danych pomiarowych	2
La8	Podsumowanie. Zaliczenie przedmiotu	2
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE

N1. Wykład z użyciem technik audiowizualnych, prezentacje multimedialne
N2. Laboratorium pomiarowe na fizycznych modelach elementów EAZ, prowadzone w sposób tradycyjny w ćwiczeniowych grupach studenckich

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1(w)	PEU_W01 PEU_W02	Zaliczenie w formie pisemnej i/lub ustnej
P(w)=F1(w)		
F1(l)	PEU_U01, PEU_K01	Sprawdzenie i ocena przygotowania do ćwiczeń laboratoryjnych
F2(l)	PEU_U02, PEU_K01	Ocena sprawozdań z wykonanych badań
P(l) P=0,3F1(l) +0,7F2(l)		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Xavier Carcelle, Power Line Communication in Practice, Artec House, Boston London 2006
[2] Yang Xiao, Yi Pan, Emerging Wireless LANs, Wireless PANs, Wireless MANs, Willey&Sons, Inc. Pub. 2009

LITERATURA UZUPEŁNIAJĄCA:

[1] Wybrane artykuły publikowane w renomowanych czasopismach światowych

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Marek Wąsowski, marek.wasowski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ **Informatyki i Telekomunikacji**

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim: Praca dyplomowa
Nazwa przedmiotu w języku angielskim Diploma thesis
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo
Specjalność (jeśli dotyczy): Bezpieczeństwo infrastruktury krytycznej
Poziom i forma studiów: I / ~~II stopień / jednolite studia magisterskie*,~~ stacjonarna / ~~niestacjonarna*~~
Rodzaj przedmiotu: ~~obowiązkowy~~ / wybieralny / ~~ogólnouczelniany~~ *
Kod przedmiotu W04CBE-SI0100D
Grupa kursów ~~TAK~~ / NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)				180	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)				300	
Forma zaliczenia	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*	~~Egzamin /~~ zaliczenie na ocenę*	Egzamin / zaliczenie na ocenę*
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS				12	
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)				12	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)				7,2	

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Umiejętność przygotowania przeglądu literatury i precyzowania problemu badawczego.
2. Podstawowa wiedza dotycząca właściwości, struktur i sposobów działania systemów i sieci teleinformatycznych.
3. Umiejętność przygotowania dokumentacji.

CELE PRZEDMIOTU

C1 Zapoznanie z wytycznymi formalnymi odnośnie przygotowania pracy pisemnej, opisu literatury i struktury pracy dyplomowej.
C2 Nabycie poszerzonej wiedzy dotyczącej tematyki pracy dyplomowej.
C3 Nabycie umiejętności przygotowania badań, weryfikacji, opracowania i prezentacji wyników.
C4 Nabycie umiejętności terminowej i systematycznej pracy.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

Z zakresu umiejętności:
PEU_U01 – Potrafi wyszukać informacje z różnych źródeł, umie dokonać ich krytycznej analizy, syntezy, twórczej interpretacji oraz potrafi je zaprezentować.
PEU _U02 – Potrafi formułować i testować hipotezy dotyczące prostych problemów badawczych.
PEU _U04 – Potrafi — zgodnie z zadaną specyfikacją — zaprojektować, analizować lub zrealizować (przynajmniej w części) złożony system teleinformatyczny mający na celu realizację szeroko rozumianych usług transmisyjnych i przetwarzania danych, używając właściwych metod, technik i narzędzi.

Z zakresu kompetencji społecznych:
PEU _K01 – Jest gotów do krytycznej oceny odbieranych treści, ma świadomość znaczenia wiedzy w rozwiązywaniu problemów i ochronie środowiska.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
	Suma godzin	**0**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**

Forma zajęć - projekt		**Liczba godzin**
Pr1	Opracowanie metod(y) rozwiązywania problemu; implementacja	60
Pr2	Przeprowadzenie analiz i badań oraz opracowanie wyników	60
Pr3	Opracowanie dokumentacji (pracy pisemnej) pracy	60
…		
	Suma godzin	**180**

Forma zajęć - seminarium	**Liczba godzin**

Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Środowisko eksperymentalne (w tym platformy symulacyjne np.: Matlab, MathCad, Piast) wedle wyboru studenta. N2. Edytor tekstu. N3. Edytor grafik (tabel/rysunków) niezbędnych do realizacji pracy dyplomowej.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
P (projekt)	PEU _U01 PEU _U02 PEU _U04 PEU _K01	Ocena końcowa związaną z oceną przygotowanej pracy dyplomowej. Ocenie podlegać umiejętność zdefiniowania problemu, przeglądu stanu wiedzy i techniki, zaproponowania poprawnej metody, zaprojektowanie i przeprowadzenie eksperymentu lub analizy, krytyczna analiza wyników.

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA

[1] Regulamin procesu dyplomowania na Wydziale Informatyki i Telekomunikacji Politechniki Wrocławskiej

[2] Formatka pracy dyplomowej przygotowania przez WIT PWr

[3] Dokumentacja programu Plagiat.pl

LITERATURA UZUPEŁNIAJĄCA:

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Prof. dr hab. inż. Tadeusz Więckowski (Tadeusz.wieckowski@pwr.edu.pl)

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Programowanie bezpiecznych internetowych transmisji danych**
Nazwa przedmiotu w języku angielskim:	**Programming of secure data transmission over the Internet**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0304G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			15	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25			25	
Forma zaliczenia	zaliczenie na ocenę			zaliczenie na ocenę	
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**2**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)				1	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	0.6			0,6	

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Z zakresu wiedzy:

1. Ma podstawową wiedzę z zakresu projektowania sieci teleinformatycznych
2. Ma ogólną wiedzę z zarządzania infrastrukturą teleinformatyczną
3. Ma wiedzę z zakresu programowania w językach ANSI C, Javascript, Lazarus , Python

Z zakresu umiejętności:

1. Potrafi opracować algorytm rozwiązujący problem z zakresu analizy i przetwarzania danych
2. Potrafi napisać program komputerowy na podstawie zadanego algorytmu
3. Potrafi opracować dokumentację z wykonanych zadań

CELE PRZEDMIOTU

C1. Zapoznanie z technologią przygotowywania bezpiecznych transmisji oraz przetwarzania danych teleinformatycznych na potrzeby elektroenergetyki

C2. Nabycie praktycznych umiejętności programowania aplikacji internetowych klient-serwer

C3. Przygotowanie do rozwiązywania problemów w zespole projektowym

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Ma ogólną wiedzę z zakresu ochrony systemu elektroenergetycznego przed jego destabilizacją wskutek nieuprawnionej ingerencji i zakłócaniem transmisji danych

PEU_W02 Ma wiedzę w zakresie analizowania i modelowania wybranych zdarzeń występujących podczas teletransmisji danych

PEU_W03 Zna podstawowe zasady projektowania aplikacji sieciowych klient-serwer wspomagających działania kontrolno-regulacyjne w elektroenergetyce

Z zakresu umiejętności:

PEU_U01 Potrafi określić i ocenić wybrane zagrożenia lokalnej destabilizacji podsystemu elektroenergetycznego

PEU_U02 Potrafi opracować algorytm i zaprogramować aplikację internetową klient-serwer w zakresie monitorowania i sterowania wybranymi obiektami symulatora podsystemu elektroenergetycznego CMAD-SEE

TREŚCI PROGRAMOWE

Forma zajęć – wykład		Liczba godzin
Wy1	Przedstawienie przedmiotowych efektów uczenia się. Omówienie formy udostępniania materiałów dydaktycznych (konspektów) oraz warunków zaliczenia kursu. Cele i zadania sieci teleinformatycznych w działaniach inżynierskich. Wielozadaniowość i współbieżność procesów w nowoczesnych systemach komputerowych. Zasady bezpiecznego współdzielenia zasobów informacyjnych w SEE.	2
Wy2	Wybrane elementy stabilności systemu elektroenergetycznego (SEE). Podstawowe metody sterowania SEE–regulacja mocy, częstotliwości i napięcia. Rozproszone źródła energii – farmy wiatrowe i fotowoltaiczne. Możliwe zagrożenia stabilności SEE. Ataki typu „BlackIoT" (Internet of Things).	2
Wy3	Zasady programowania zadań sieciowych w językach kompilowanych oraz skryptowych. Elementy programowania strukturalnego oraz obiektowego. Kryteria wyboru odpowiedniej technologii programowania w kontekście działań kontrolno-regulacyjnych SEE. Przykłady realizacji dydaktycznych i komercyjnych. Centrum Monitorowania i Akwizycji Danych (CMAD.pwr.edu.pl)	2
Wy4	Prezentacja dedykowanego internetowego symulatora podsystemu CMAD-SEE. Zasady dostępu, monitorowania i regulacji wybranych obiektów systemu elektroenergetycznego. Projektowanie i programowanie aplikacji internetowej KLIENT-SEE podsystemu CMAD-SEE. Dokumentacja pakietu dydaktycznego SISTLAB-SEE.	2
Wy5	Aspekty akwizycji oraz enkapsulacji i dekapsulacji pakietów danych pozyskiwanych z systemów diagnostyki i monitorowania SEE. Problemy synchronizacji pomiarów w SEE. Pieczątki czasowe. Serwery NTP.	2

	Standardy GPS i DCF77. Zagrożenie utraty integralności danych	
Wy6	Elementy analizy danych w SEE. Algorytmy wyznaczania i porównywania wskaźników wartości niemianowanych. Zastosowanie dyskretnej transformaty Fouriera DFT w algorytmach analizy współzależności cech. Przegląd wybranych algorytmów statystyki kwalitatywnej.	2
Wy7	Znaczenie kodowania i dekodowania transmisji teleinformatycznych z elementami kryptografii w kontekście monitorowania i regulacji SEE. Algorytm RSA. Programowanie prostych generatorów liczb pseudolosowych w ANSI C.	2
Wy8	Godzina przeznaczone na pracę własną i przygotowanie do komputerowego testu zaliczeniowego przeprowadzanego w laboratorium.	1
	Suma godzin	**15**

Forma zajęć – ćwiczenia		**Liczba godzin**
Ćw1		
	Suma godzin	

Forma zajęć – laboratorium		**Liczba godzin**
La1		
	Suma godzin	

Forma zajęć - projekt		**Liczba godzin**
Pr1	Studenci w dwu lub jednoosobowych grupach laboratoryjnych realizują po zakończeniu cyklu wykładów w drugiej połowie semestru projekt aplikacji internetowej KLIENT-SEE w zakresie monitorowania i regulacji wybranych obiektów symulatora podsystemu elektroenergetycznego CMAD-SEE. Tematy projektów związane z prezentacjami wykładowymi są proponowane przez studentów i po uzgodnieniu szczegółów realizacji, zatwierdzane przez prowadzącego zajęcia. Każdy projekt obejmuje etapy wykonawcze: sformułowanie problemu, opracowanie algorytmu działania aplikacji, odpowiedni dobór języka lub języków programowania, uruchomienie i testowanie aplikacji, sporządzenie dokumentacji. Wszystkie elementy projektu: kody źródłowe aplikacji oraz wersja elektroniczna dokumentacji są wprowadzane do repozytorium plików projektu na stronie kursu portalu kształcenia na odległość: http://eportal.eny.pwr.edu.pl	15
	Suma godzin	**15**

Forma zajęć – seminarium		**Liczba godzin**
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z prezentacją multimedialną i elementami kształcenia na odległość
N2. Studenci opracowują dokumentację projektu: http://eportal.eny.pwr.edu.pl
N3. Samokształcenie na odległość – http://eportal.eny.pwr.edu.pl: materiały pomocnicze

N4. Samokształcenie na odległość – http://eportal.eny.pwr.edu.pl: testy kontrolne N5. Praca własna (m.in. przygotowanie do testu zaliczeniowego (kolokwium)) N6. Konsultacje tradycyjne

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
Wykład		
F1	PEU_W01, PEU_W02, PEU_W03	Samokształcenie na odległość - test kontrolny Platforma edukacyjna: http://eportal.eny.pwr.edu.pl
F2	PEU_W01, PEU_W02, PEU_W03	Test zaliczeniowy (kolokwium) przy obecności prowadzących zajęcia w pracowni komputerowej. Platforma edukacyjna: http://eportal.eny.pwr.edu.pl
P1=0.15*F1+0.85*F2		
Projekt		
F1	PEU_U01, PEU_U02	Ocena opracowanego projektu problemowego oraz dokumentacji w formie elektronicznej Platforma edukacyjna: http://eportal.eny.pwr.edu.pl
P2=F1		
P=0.4*P1+0.6*P2 **Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu**		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Douglas E. Comer, David L. Stevens, Sieci komputerowe TCP/IP – Projektowanie w trybie klient-serwer. Wersja BSD, Warszawa: WNT, 1997 i późniejsze
[2] Jaworski, R.Morawski,J.Olędzki J., Nowoczesne sieci miejskie, WNT (w. dowolne)
[3] Kernighan B.W, Ritchie D.M, Język C, WNT (wydanie dowolne)
[4] Machowski J., Lubośny Z., Stabilność systemu elektroenergetycznego, WNT, 2018
[5] Rochkind M.J., Programowanie w systemie UNIX dla zaawansowanych, WNT (w .d.)

LITERATURA UZUPEŁNIAJĄCA:

[1] Bernas S., Systemy elektroenergetyczne (SEE), WNT (wydanie dowolne)
[2] Kulikowski R., Sterowanie w wielkich systemach, WNT (wydanie dowolne)
[3] Welschenbach M., Kryptografia w C i C++, MIKOM, 2002

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Jarosław Szymańda, jaroslaw.szymanda@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	**Projekt zespołowy**
Nazwa w języku angielskim:	**Team Project**
Kierunek studiów:	**Cyberbezpieczeństwo**
Specjalność:	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**obowiązkowy**
Kod przedmiotu:	**W04CBE-SI0313P**
Grupa kursów:	**NIE**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)				45	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)				125	
Forma zaliczenia				Zaliczenie na ocenę	
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS				**5**	
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-			5	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)				1,8	

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1 Nabycie umiejętności wykonania przydzielonych zadań inżynierskich w ramach realizacji złożonego zadania inżynierskiego

C2 Zdobycie doświadczeń w pracy zespołowej, w tym umiejętności planowania i harmonogramowania, komunikacji wewnątrz-zespołowej, pełnienia roli członka zespołu bądź lidera, możliwość wykazania się kreatywnością, otwartością na innowacyjne podejście do realizacji celu oraz zorientowaniem na sukces zespołu

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu umiejętności:

PEU_U01 potrafi wykonać zadania w ramach realizacji złożonego projektu informatycznego

PEU_U02 umie zastosować zasady zarządzania projektem do realizacji złożonego projektu informatycznego

PEU_U03 umie opracować dokumentację projektu

Z zakresu kompetencji:

PEU_K01 jest świadomy konieczności należytej współpracy z zespołem, wykazuje się świadomością swojej roli w projekcie oraz dbałością o terminową realizację powierzonych zadań

TREŚCI PROGRAMOWE		
Forma zajęć – projekt		**Liczba godzin**
Pr1	Ustalenie tematyki projektu (np. informacyjny system internetowy, złożony internetowy system bazodanowy, kompleksowy projekt sieci teleinformatycznej z uwzględnieniem technik bezprzewodowej transmisji, projekt informatyzacji firmy, system eksperymentowania, system diagnostyki sieci teleinformatycznej) i celu projektu. Przydział ról w projekcie, wstępny przydział zadań do wykonania, wybór lidera zespołu	4
Pr2	Zapoznanie się z obszarem problemowym projektu. Przegląd rozwiązań w obszarze problemu – analiza metod i stosowanych środków informatycznych.	4
Pr3	Analiza wymagań użytkownika, łącznie z analizą ekonomiczną skutków implementacji projektu. Opracowanie założeń projektowych. Ustalenie wstępnego harmonogramu działań (w formie wykresu Gantt'a) oraz zasad komunikacji wewnątrz-zespołowej i z prowadzącym.	4
Pr4	Zaplanowanie zasad zarządzania jakością w projekcie, opracowanie procedur kontrolowania jakości, analiza ryzyka. Ustalenie zasad odbioru wyników poszczególnych etapów projektu oraz zasad dokumentowania etapów	4
Pr5	Realizacja indywidualnych zadań projektowych wg harmonogramu realizacji I etapu projektu	8
Pr6	Realizacja spotkań zespołu z prowadzącym - zgodnie z ustalonym harmonogramem (kamień milowy)	4
Pr7	Realizacja indywidualnych zadań projektowych wg harmonogramu realizacji II etapu projektu	8
Pr8	Prezentacja efektów wykonanego projektu, dyskusja problemowa, ocena elementów wykonanego projektu przez prowadzącego. Weryfikacja projektu. Ustalenie ewentualnych zmian	5
Pr9	Przedstawienie ostatecznej dokumentacji projektu w formie pisemnej	4
	Suma godzin	**45**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Prezentacja multimedialna
N2. Dyskusja problemowa
N3. Konsultacje
N4. Praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01, PEU_U02, PEU_K01	Ocena prezentacji kolejnych etapów projektu oraz umiejętności pracy w zespole: przestrzegania harmonogramu, aktywność w zespole, umiejętność zastosowania zasad zarządzania projektem
F2	PEU_U03	Ocena jakość wykonanego projektu oraz dokumentacji projektowej
P=0.4*F1+0.6*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Praca zbiorowa, A Guide to the Project Management Body of Knowledge (PMBOK Guide), wydanie polskie, 2009
[2] Praca zbiorowa, Zarządzanie projektem informatycznym - model najlepszych praktyk, IFC Press, Kraków 2003
[3] Robertson J., Robertson S., (1999), Pełna analiza systemowa, WNT Warszawa, 2003
[4] Dennis A., Wixam B.H., System Analysis, Design, John Wiley & Sons, 2003
[5] Bentley C. (2002), Managing Projects the Prince 2 Way, Colin Bentley 2002.
[6] Anderson H.R.: Fixed Broadband Wireless System Design, John Wiley & Sons, 2003.

LITERATURA UZUPEŁNIAJĄCA:

[7] Pozycje literaturowe dotyczące wybranych technologii i środowisk programistycznych

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Rozproszone systemy automatyki**
Nazwa przedmiotu w języku angielskim:	**Distributed automation systems**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień/stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0311G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25		50		
Forma zaliczenia	zaliczenie na ocenę		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**3**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udział (BU)	0.6		1,2		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Ma podstawową wiedzę o sterownikach programowalnych
2. Ma podstawową wiedzę o przemysłowych systemach automatyki i sieciach komunikacyjnych
3. Potrafi praktycznie wykorzystać wiedzę o sterownikach programowalnych i ich komponentach

CELE PRZEDMIOTU

C1. Zapoznanie z podstawową wiedzą dotyczącą rozproszonych systemów automatyki.
C2. Zapoznanie z wybranymi rodzajami przemysłowych sieci komunikacyjnych wykorzystywanymi w rozproszonych systemach automatyki.
C3. Praktyczne zapoznanie z urządzeniami wykorzystywanymi w rozproszonych systemach automatyki.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Ma wiedzę w zakresie stosowania sterowników PLC oraz sieci komunikacyjnych w rozproszonych systemach automatyki.

PEU_W02 Wie, jakie są charakterystyczne cechy rozproszonego systemu automatyki.

Z zakresu umiejętności:

PEU_U01 Potrafi zastosować sterowniki PLC w rozproszonych systemach automatyki.

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

Z zakresu kompetencji społecznych:

PEU_K01 Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane działania.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		**Liczba godzin**
Wy1	Wykład wprowadzający. Podstawowe definicje i pojęcia	2
Wy2	Budowa i programowanie sterowników PLC oraz modułów rozproszonych	3
Wy3	Systemy czasu rzeczywistego w rozproszonych systemach automatyki. Elementy składowe rozproszonego systemu automatyki	2
Wy4	Komunikacja w rozproszonych systemach automatyki. Przykłady przemysłowych sieci komunikacyjnych	3
Wy5	Systemy SCADA i DCS w rozproszonych systemach automatyki	2
Wy6	Wymiana danych za pomocą protokołów DDE i OPC	2
Wy7	Kolokwium zaliczeniowe	1
	Suma godzin	**15**

Forma zajęć - laboratorium		**Liczba godzin**
La1	Zajęcia wprowadzające. Zapoznanie się z regulaminem BHP. Zapoznanie się ze stanowiskiem laboratoryjnym.	2
La2	Realizacja wybranego, podstawowego układu sterowania z wykorzystaniem sterownika PLC	2
La3	Realizacja zaawansowanych funkcji sterowania w wybranym układzie sterowania z wykorzystaniem sterownika PLC i wybranego modelu procesu przemysłowego	4
La4	Zajęcia wprowadzające do wykorzystania sieci komunikacyjnych i modułów rozproszonych	2
La5	Realizacja wybranego procesu przemysłowego z wykorzystaniem modułów rozproszonych i sieci komunikacyjnej	8
La6	Programowanie współpracy sterowników PLC z wybranym systemem DCS	2
La7	Programowanie systemu wizualizacji z wykorzystaniem paneli operatorskich	4
La8	Programowanie systemu wizualizacji z wykorzystaniem oprogramowania typu SCADA	4
La9	Zajęcia zaliczeniowe	2
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład prowadzony w sposób tradycyjny N2. Prezentacja multimedialna N3. Konsultacje N4. Tradycyjnie prowadzone laboratorium N5. Kolokwium zaliczeniowe

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_W01 PEU_W02	Kolokwium zaliczeniowe
F2	PEU_U01 PEU_U02 PEU_K01	Aktywność na zajęciach
F3	PEU_U01 PEU_U02	Ocena napisanych programów, ocena sprawozdania
P=0.2*F1+0.2*F2+0.6*F3		
Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Flaga S., Programowanie sterowników PLC w języku drabinkowym, Wyd. BTC, Legionowo, 2010.
[2] Grega W., Sterowanie cyfrowe w czasie rzeczywistym, Wyd. Wydz. AAIiE AGH, Kraków 1999.
[3] Kasprzyk J., Programowanie sterowników przemysłowych, WNT, Warszawa 2006.
[4] Werewka J., Systemy rozproszone sterowania i akwizycji danych, CCATIE vol. 9, Kraków 1998.

LITERATURA UZUPEŁNIAJĄCA:

[1] Notatki z wykładu.
[2] Dokumentacje techniczne producentów sterowników PLC.
[3] Dokumentacje techniczne producentów systemów SCADA i DCS.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Krzysztof Dyrcz, krzysztof.dyrcz@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	**Seminarium dyplomowe**
Nazwa w języku angielskim:	**Diploma Seminar**
Kierunek studiów:	**Cyberbezpieczeństwo**
Specjalność:	Bezpieczeństwo infrastruktury krytycznej
Stopień studiów i forma:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0312S**
Grupa kursów:	**NIE**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)					30
Liczba godzin całkowitego nakładu pracy studenta (CNPS)					50
Forma zaliczenia					Zaliczenie na ocenę
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS					**2**
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)					2
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)					1,3

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1 Nabycie umiejętności poszukiwania selektywnej wiedzy niezbędnej do tworzenia własnych oryginalnych rozwiązań.

C2 Zdobycie umiejętności przygotowania prezentacji pozwalającej w sposób komunikatywny przekazać słuchaczom swoje oryginalne pomysły, koncepcje i rozwiązania.

C3 Nabycie umiejętności kreatywnej dyskusji, w której w sposób rzeczowy i merytoryczny można uzasadnić i obronić swoje stanowisko.

C4 Nabycie umiejętności pisania dzieła prezentującego własne osiągnięcia, w tym prezentacji własnych osiągnięć na tle rozwoju myśli światowej.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ
Z zakresu umiejętności: PEU_U01 potrafi przygotować prezentację zawierającą wyniki rozwiązań PEU_U02 potrafi w dyskusji rzeczowo uzasadnić swoje oryginalne pomysły i rozwiązania PEU_U03 potrafi krytycznie ocenić rozwiązania naukowo-techniczne innych osób

TREŚCI PROGRAMOWE		
Forma zajęć - seminarium		**Liczba godzin**
Se1	Omówienie zasad przygotowania i pisania pracy dyplomowej, a w szczególności przedstawienie zasad edytorskich	2
Se2	Prezentacje indywidualne dotyczące omówienia aktualnego stanu wiedzy związanego z problematyką realizowanej pracy dyplomowej oraz odniesienia przewidywanego, oryginalnego własnego wkładu do osiągnięć literaturowych	8
Se3	Dyskusja w grupie seminaryjnej nt. stanu wiedzy literaturowej i założonej koncepcji rozwiązania stawianych sobie problemów, składających się na pracę dyplomową	6
Se4	Prezentacje indywidualne dotyczące zrealizowanej pracy dyplomowej z uwypukleniem własnego oryginalnego dorobku autora wraz z dyskusją w grupie seminaryjnej	14
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. prezentacja multimedialna N2. dyskusja problemowa N3. praca własna

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny: F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	PEU_U01	prezentacja
F2	PEU_U02, PEU_U03	dyskusja
P= 0.5*F1+0.5*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
Literatura związana z problematyką pracy dyplomowej
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
Dr hab. inż. Ryszard Zieliński, ryszard.zielinski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Systemy zasilania gwarantowanego**
Nazwa przedmiotu w języku angielskim:	**Guaranteed power supply systems**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0310G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	25		25		
Forma zaliczenia	zaliczenie na ocenę		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**2**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			1		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału (BU)	0,6		0,6		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Brak wymagań wstępnych.

CELE PRZEDMIOTU

C1. Zaznajomienie z zasadami i technikami realizacji zabezpieczeń instalacji elektrycznych zasilających urządzenia lokalnych sieci komputerowych

C2. Nabycie praktycznej umiejętności wykonywania badań elementów zabezpieczeniowych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Ma wiedzę dotyczącą mechanizmu rozwoju wyładowań piorunowych oraz rodzajów wyładowań doziemnych; zna zasady ochrony przepięciowej w instalacjach elektroenergetycznych i sygnałowych; ma podstawową wiedzę z zakresu ekranowania pola elektromagnetycznego.

Z zakresu umiejętności:

PEU_U01 Posiada umiejętności praktyczne potrzebne do wykonywania prób i badań urządzeń wysokimi napięciami udarowymi, symulującymi przepięcia piorunowe i łączeniowe.

Z zakresu kompetencji społecznych:

PEU_K01 Zdolność do samodzielnego myślenia, wyszukiwania i analizowania informacji

PEU_K02 Ma świadomość działania zespołowego i odpowiedzialności wszystkich członków zespołu za wykonanie powierzonego zadania

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wiadomości wstępne, wprowadzenie w problematykę przedmiotu	2
Wy2	Zakłócenia impulsowe. Wyładowania piorunowe	2
Wy3	Przebiegi falowe	2
Wy4	Urządzenia ochrony przeciwprzepięciowej	2
Wy5	Zasady ochrony przeciwprzepięciowej	2
Wy6	Ekranowanie pola elektromagnetycznego	2
Wy7	Wytwarzanie i pomiary wysokich napięć i prądów udarowych	2
Wy8	Kolokwium/zaliczenie	1
	Suma godzin	**15**

Forma zajęć - ćwiczenia		Liczba godzin
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		Liczba godzin
La1	Wstęp, zapoznanie się z zasadami pracy w laboratorium, szkolenie BHP. Zapoznanie się z lokalizacją rozdzielnic zasilających, dróg ewakuacyjnych, sprzętu gaśniczego. Ustalenie zasad zaliczenia przedmiotu	3
La2	Wytwarzanie i pomiary napięć udarowych	3
La3	Elementy ochrony przeciwprzepięciowej – charakterystyki statyczne	3
La4	Elementy ochrony przeciwprzepięciowej – charakterystyki dynamiczne	3
La5	Odrobienie zaległych ćwiczeń, zaliczenie laboratorium	3
	Suma godzin	**15**

Forma zajęć - projekt		Liczba godzin
Pr1		
Pr2		
Pr3		
Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
Se3		
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny. N2. Laboratorium prowadzone w sposób tradycyjny. N3. Sprawdzenie przygotowania do zajęć. N4. Sprawozdania z ćwiczeń laboratoryjnych. N5. Praca własna.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1 (W)	PEU_W01 PEU_K01	F1 - kolokwium
P (W)	P = F1	
F2 (L)	PEU_U01 PEU_K02	Sprawdzenie i ocena przygotowania do ćwiczeń laboratoryjnych
F3 (L)	PEU_U01 PEU_K02	Ocena sprawozdań z wykonanych badań
P (L)	P = 0.5 F1+ 0.5 F2	

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
LITERATURA PODSTAWOWA: [1] Sowa A., Kompleksowa ochrona odgromowa i przepięciowa. Biblioteka COSiW SEP, Warszawa 2005. [2] Juchniewicz J., Lisiecki J., Wysokonapięciowe układy izolacyjne, skrypt PWr, 1980 r. **LITERATURA UZUPEŁNIAJĄCA:** [1] Praca zbiorowa pod red. J. Fleszyńskiego, Laboratorium wysokonapięciowe w dydaktyce i elektroenergetyce, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 1999 r.
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Maciej Jaroszewski, maciej.jaroszewski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Zaburzenia jakości energii elektrycznej**
Nazwa przedmiotu w języku angielskim:	**Power quality disturbances**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0306G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75		25		
Forma zaliczenia	zaliczenie na ocenę		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**4**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			1		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału (BU)	1,2		0,6		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Z zakresu wiedzy:

1. Zna podstawowe prawa elektrotechniki i ma podstawową wiedzę w zakresie metrologii i jednostek miar.

Z zakresu umiejętności:

1. Potrafi wykonać pomiary podstawowych wielkości elektrycznych z wykorzystaniem przyrządów analogowych, cyfrowych i oscyloskopu.

Z zakresu kompetencji społecznych:

1. Rozumie potrzebę i zna możliwości ciągłego dokształcania się, podnoszenia kompetencji zawodowych, osobistych i społecznych.

CELE PRZEDMIOTU

C1 Zdobycie wiedzy na temat parametrów definiujących jakość energii oraz norm i przepisów dedykowanych poziomom dopuszczalnym i metodom oceny jakości energii.

C2	Poznanie zjawisk dotyczących zaburzeń jakości energii, źródeł i skutków zaburzeń jakości energii oraz sposobów ich eliminacji.
C3	Nabycie umiejętności zastosowania analizatorów jakości energii oraz metodyki oceny i wykonywania raportów.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01	Ma ogólną wiedzę na temat zagadnień związanych z zaburzeniami jakości energii elektrycznej, zna dokumenty legislacyjne i regulacje dotyczące wymogów w tym zakresie
PEU_W02	Posiada wiedzę w zakresie potencjalnych źródeł zaburzeń jakości energii oraz ich wpływu na pracę urządzeń elektrycznych oraz zna wybrane sposoby poprawy jakość energii elektrycznej
PEU_W03	Orientuje się w obecnym stanie rozwoju urządzeń i systemów monitorowania jakości energii elektrycznej, zna zasady tworzenia raportów oceny jakości energii elektrycznej

Z zakresu umiejętności:

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

Z zakresu kompetencji społecznych:

PEU_K01	Dba o wykonanie powierzonych zadań, wykazuje aktywną postawę i potrafi współpracować z zespołem

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wprowadzenie. Podstawowe zagadnienia, definicje, jakość dostaw energii elektrycznej, jakość napięcia zasilającego, jakość energii. Umiejscowienie jakości energii elektrycznej w klasyfikacji zaburzeń kompatybilności elektromagnetycznej. Przegląd i klasyfikacja zaburzeń jakości energii.	2
Wy2	Definicje zaburzeń jakości energii oraz algorytmy pomiaru parametrów jakości energii – zaburzenia wolnozmienne	2
Wy3	Definicje zaburzeń jakości energii oraz algorytmy pomiaru parametrów jakości energii – zaburzenia szybkozmienne	2
Wy4	Jakość energii elektrycznej w świetle norm i przepisów prawnych	2
Wy5	Kompatybilność elektromagnetyczna w zakresie niskich i wysokich częstotliwości	2
Wy6	Źródła i parametry zewnętrznych zakłóceń elektromagnetycznych, wyładowania atmosferyczne jako źródła zakłóceń, elementy ochrony przed wyładowaniami atmosferycznymi, ekranowanie, efektywność ekranowania przed zakłóceniami elektromagnetycznymi i elektrycznymi, ekranowanie pól magnetycznych niskiej częstotliwości	2
Wy7	Przegląd źródeł zaburzeń jakości energii w sieciach elektroenergetycznych	2
Wy8	Wybrane badania emisji zaburzeń jakości energii elektrycznej wprowadzane do sieci elektroenergetycznej przez odbiorniki elektryczne	2

Wy9	Przegląd skutków oddziaływania zaburzeń jakości energii na odbiorniki elektryczne i elementy sieć elektroenergetycznych	2
Wy10	Wybrane badania odporności odbiorników elektrycznych na zaburzenia jakości energii elektrycznej	2
Wy11	Przegląd metod i urządzeń ograniczających emisję zaburzeń jakości energii elektrycznej	2
Wy12	Przegląd metod i urządzeń zwiększających odporność urządzeń elektrycznych na zaburzenia jakości energii elektrycznej	2
Wy13	Metodyka wykonywania pomiarów i oceny jakości energii w sieciach elektroenergetycznych, przegląd analizatorów jakości energii elektrycznej, układy pomiarowe, omówienie wymagań dla raportu jakości energii elektrycznej.	2
Wy14	Systemy monitoringu jakości energii, elementy systemów rozproszonych, stacyjne układy pomiarowe, zagadnienia synchronizacji pomiarów i zdalnego dostępu, funkcjonalności oprogramowania nadrzędnego.	2
Wy15	Kolokwium	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		**Liczba godzin**
…		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1	Przedstawienie regulaminu BHP i zasad zaliczenia laboratorium, prezentacja stanowisk laboratoryjnych	1
La2	Układ pomiarowy i konfiguracja analizatora jakości energii elektrycznej oraz wykorzystanie do obserwacji wybranych zaburzeń jakości energii na stanowisku laboratoryjnym, tryb oscyloskopu, tryb analizatora, tryb rejestratora	2
La3	Badanie wybranych zaburzeń jakości napięcia zasilającego – wyznaczanie parametrów wahań napięcia, asymetrii, zapadów	2
La4	Analiza przebiegów prądowych i napięciowych – wyznaczanie zawartości harmonicznych i interahrmonicznych	2
La5	Analizator widma niskich i wysokich częstotliwości	2
La6	Badanie emisji wyższych harmonicznych przez odbiorniki energii	2
La7	Badanie odporności odbiorników energii elektrycznej na zapady i krótkie przerwy napięcia zasilającego	2
La8	Badania skuteczności stosowania wybranych urządzeń do poprawy jakości napięcia zasilającego	2
	Suma godzin	**15**

Forma zajęć - projekt		**Liczba godzin**
…		
	Suma godzin	

Forma zajęć - seminarium		**Liczba godzin**
…		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
N1	Wykład tradycyjny z użyciem technik audiowizualnych
N2	Laboratorium pomiarowe prowadzone w sposób tradycyjny w ćwiczeniowych grupach studenckich, przygotowanie sprawozdania

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
P	PEU_W01 PEU_W02 PEU_W03	Zaliczenie w formie pisemnej
P	PEU_U01 PEU_U02 PEU_U03 PEU_K01	Ocena sprawozdań z wykonywanych zajęć laboratoryjnych

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Hanzelka Z., Jakość dostaw energii elektrycznej. Zaburzenia wartości skutecznej napięcia, Wydawnictwo AGH, 2013.
[2] Kowalski Z., Jakość energii elektrycznej, Wydawnictwo Politechniki Łódzkiej, Łódź 2007.
[3] Bollen M. H. J.: Understanding Power Quality Problems Voltage Sags and Interruptions, IEEE Press, New York, USA, 2000.
[4] Baggini A., Handbook of Power Quality, John Wiley&Sons, Ltd, 2008
[5] PN-EN 50160:2010, 2015, Parametry napięcia zasilającego w publicznych sieciach rozdzielczych.
[6] Rozporządzenie Ministra Gospodarki w sprawie szczegółowych warunków funkcjonowania systemu elektroenergetycznego. Dz. U. Nr 93 z dn. 04.05.2007 r.
[7] Henry W. Ott, Electromagnetic Compatibility Engineering, John Wiley & Sons, Inc., Hoboken, New Jersey 2009.

LITERATURA UZUPEŁNIAJĄCA:

[1] IEEE Std 1159-2009: IEEE Recommended Practice for Monitoring Electric Power Quality.
[2] Dugan R.C., Mc Gramaghan M.F., Beaty H. W., Santoso S: Electrical Power System Quality, Wyd 2. MC Graw-Hill 2002.
[3] Clayton R. P.: Introduction to electromagnetic compatibility John Wiley & Sons, New York, 1992.
[4] Arrillaga J. Watson N. R.: Power System Quality Assessment, John Wiley & Sons, New York, 2000.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Tomasz Sikorski, tomasz.sikorski@pwr.edu.pl

Załącznik nr 6 do ZW 121/2020

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Zagrożenia w funkcjonowaniu infrastruktury elektroenergetycznej**
Nazwa przedmiotu w języku angielskim:	**Threats in operation of electric power infrastructure**
Kierunek studiów (jeśli dotyczy):	**Cyberbezpieczeństwo**
Specjalność (jeśli dotyczy):	**Bezpieczeństwo infrastruktury krytycznej**
Poziom i forma studiów:	**I, stacjonarna**
Rodzaj przedmiotu:	**wybieralny**
Kod przedmiotu:	**W04CBE-SI0302G**
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50		25		
Forma zaliczenia	zaliczenie na ocenę		zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	**3**				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału (BU)	1,2		0,6		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Ma podstawową wiedzę z zakresu elektrotechniki.
2. Rozumie potrzebę dokształcania się, podnoszenia kompetencji zawodowych, osobistych i społecznych.

CELE PRZEDMIOTU

C1. Nabycie wiedzy dotyczącej roli, funkcjonowania i wyposażenia stacji elektroenergetycznych.

C2. Nabycie wiedzy o narażeniach klimatycznych, środowiskowych i eksploatacyjnych występujących w stacjach elektroenergetycznych.

C3. Nabycie wiedzy o urządzeniach prowadzenia ruchu stacji oraz rozwiązaniach automatyki stacyjnej i systemów sterowania i nadzoru (SSiN) w kontekście bezpieczeństwa pracy i jego zagrożeń.
C4. Nabycie umiejętności rozróżniania narażeń klimatycznych, środowiskowych i eksploatacyjnych występujących w stacjach elektroenergetycznych i ich przeciwdziałaniu.
C5. Nabycie umiejętności oceny poziomu bezpieczeństwa pracy dla urządzeń prowadzenia ruchu stacji, automatyki stacyjnej i systemów sterowania i nadzoru (SSiN).
C6.Nabycie umiejętności identyfikacji zagrożenia bezpieczeństwa pracy stacji elektroenergetycznej i zastosowania adekwatnych środków w celu jego ograniczenia.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:
PEU_W01: Ma wiedzę z zakresu roli, funkcjonowania i wyposażenia stacji elektroenergetycznych.
PEU_W02: Zna narażenia klimatyczne, środowiskowe i eksploatacyjne występujące w stacjach elektroenergetycznych.
PEU_W03: Zna urządzenia prowadzenia ruchu stacji oraz rozwiązania automatyki stacyjnej i systemy sterowania i nadzoru (SSiN) w kontekście bezpieczeństwa pracy i jego zagrożeń.
Z zakresu umiejętności:
PEU_U01: Potrafi określić narażenia klimatyczne, środowiskowe i eksploatacyjne występujące w stacjach elektroenergetycznych i im przeciwdziałać.
PEU_U02: Potrafi zidentyfikować zagrożenia bezpieczeństwa pracy stacji elektroenergetycznej i zastosować adekwatne środki w celu jego ograniczenia.
Z zakresu kompetencji społecznych:
PEU_K01: Rozumie potrzebę i zna możliwości dokształcania się (studia drugiego i trzeciego stopnia, studia podyplomowe, kursy), podnoszenia kompetencji zawodowych, osobistych i społecznych.
PEU_K02: Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane działania.
PEU_K03: Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role oraz potrafi myśleć krytycznie i argumentować swoje stanowisko, dzięki czemu może odpowiednio dobrać priorytety i środki służące realizacji określonego przez siebie lub innych zadania.

TREŚCI PROGRAMOWE

Forma zajęć – wykład		Liczba godzin
Wy1	Funkcjonowanie, rola i znaczenie stacji elektroenergetycznych w Krajowym Systemie Elektroenergetycznym (KSE).	2
Wy2	Rozwiązania i wyposażenie stacji elektroenergetycznych.	2
Wy3	Narażenia klimatyczne i środowiskowe występujące w stacjach elektroenergetycznych.	2
Wy4	Eksploatacja stacji elektroenergetycznych.	2
Wy5	Identyfikacja narażeń klimatycznych, środowiskowych i eksploatacyjnych występujących w stacjach elektroenergetycznych.	2
Wy6	Sposoby i środki przeciwdziałania lub ograniczania narażeń.	2
Wy7	Urządzenia prowadzenia ruchu stacji i automatyka stacyjna.	2

Wy8	Systemy sterowania i nadzoru (SSiN) stacji elektroenergetycznych.	2
Wy9	Komputerowe systemy wspomagania, nadzorowania i kierowania pracą stacji stosowane w stacjach energetyki zawodowej.	2
Wy10	Zawansowane systemy sterowania i nadzoru stacji elektroenergetycznych (Smart Operations) w ramach Smart Grid.	2
Wy11	Ocena poziomu bezpieczeństwa pracy stacji elektroenergetycznych.	2
Wy12	Identyfikacja zagrożeń bezpieczeństwa pracy stacji elektroenergetycznej.	2
Wy13	Sposoby i środki przeciwdziałania lub ograniczania zagrożeń bezpieczeństwa pracy stacji elektroenergetycznej.	2
Wy14	Uwarunkowania prawne, techniczne, ekonomiczne i społeczne związane z bezpieczeństwem pracy infrastruktury elektroenergetycznej.	2
Wy15	Kolokwium zaliczeniowe	2
	Suma godzin	**30**

Forma zajęć – laboratorium		**Liczba godzin**
La1	Zajęcia wprowadzające. Przedstawienie zasad bezpiecznej pracy przy urządzeniach elektrycznych w laboratorium. Zapoznanie studentów ze stanowiskami laboratoryjnymi, programem ćwiczeń, zasadami przeprowadzania pomiarów oraz opracowywania sprawozdań z wykonanych pomiarów.	2
La2	Identyfikacja narażeń klimatycznych, środowiskowych i eksploatacyjnych aparatury łączeniowej.	2
La3	Bezpieczeństwo pracy rozdzielnic średniego i niskiego napięcia.	2
La4	Bezpieczeństwo pracy inteligentnych instalacji.	2
La5	Systemy sterowania i nadzoru (SSiN) stacji elektroenergetycznych.	2
La6	Ocena zagrożeń bezpieczeństwa pracy stacji elektroenergetycznej i jej elementów.	2
La7	Ocena poziomu bezpieczeństwa pracy stacji elektroenergetycznej.	2
La8	Zaliczenie	1
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z użyciem technik audiowizualnych, prezentacje multimedialne. N2. Dyskusja problemowa. N3. Laboratorium prowadzone w ćwiczeniowych grupach studenckich. N4. Konsultacje. N5. Opracowanie sprawozdań z wykonanych ćwiczeń.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ		
Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1 (W)	PEU_W01 PEU_W02 PEU_W03 PEU_K01	Kolokwium pisemne.
P (W) P=F1		

F1 (L)	PEU_U01 PEU_U02 PEU_K01	Pytania ustne (sprawdzenie przygotowania do zajęć).
F2 (L)	PEU_U01 PEU_U02 PEU_K01 PEU_K02 PEU_K03	Aktywność na zajęciach.
F3 (L)	PEU_U01 PEU_U02 PEU_K01 PEU_K02 PEU_K03	Sprawozdania z wykonanych ćwiczeń.
P (L) P=0,4F1+0,3F2+0,3F3		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Dołęga W., Stacje elektroenergetyczne, Wydawnictwo Politechniki Wrocławskiej, Wrocław 2007.
[2] Markiewicz H., Urządzenia elektroenergetyczne, WNT, Warszawa 2016.
[3] Praca zbiorowa, Poradnik inżyniera elektryka, Tom 3, WNT Warszawa, 2011.

LITERATURA UZUPEŁNIAJĄCA:

[1] Praca zbiorowa pod redakcją Adama Rynkowskiego i W. Jabłońskiego, Sieci, instalacje i urządzenia elektroenergetyczne o napięciu powyżej 1kV. Poradnik inżyniera elektryka, projektanta i inwestora. Warszawa , Wydawnictwo Verlag Dashofer Sp.z.o.o., 2011.
[2] Artykuły w czasopismach: Elektro-Info, Napędy i Sterowanie, Wiadomości Elektrotechniczne, Przegląd Elektrotechniczny, Rynek Energii.
[3] Strony internetowe rekomendowane przez Prowadzącego.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Waldemar Dołęga, waldemar.dolega@pwr.edu.pl