

PROGRAM STUDIÓW

WYDZIAŁ: **Informatyki i Telekomunikacji**

KIERUNEK STUDIÓW: **Cyberbezpieczeństwo**

Przyporządkowany do dyscypliny: **D1 Informatyka techniczna i telekomunikacja (dyscyplina wiodąca)**

D2*

D3*

D4*

POZIOM KSZTAŁCENIA: ~~studia pierwszego stopnia (licencjackie / inżynierskie)~~ / **drugiego stopnia / jednolite magisterskie***

FORMA STUDIÓW: **stacjonarna / niestacjonarna***

PROFIL: **ogólnoakademicki / praktyczny***

JĘZYK PROWADZENIA STUDIÓW: **polski**

OBYWIAZUJE OD CYKLU KSZTAŁCENIA: **2022/2023**

Zawartość:

1. Zakładane efekty uczenia się – zał. nr 1 do programu studiów
2. Opis programu studiów – zał. nr 2 do programu studiów
3. Plan studiów – zał. nr 3 do programu studiów

*niepotrzebne skreślić

ZAKŁADANE EFEKTY UCZENIA SIĘ

Wydział: Informatyki i Telekomunikacji

Kierunek studiów: Cyberbezpieczeństwo

Poziom studiów: studia ~~pierwszego stopnia~~ / drugiego stopnia / ~~jednolite studia magisterskie~~*

Profil: ogólnoakademicki / ~~praktyczny~~*

Umiejscowienie kierunku

Dziedzina nauki: ...nauki inżynierjno-techniczne.....

Dyscyplina/dyscypliny w przypadku kilku dyscyplin proszę wskazać dyscyplinę wiodącą)

.....informatyka techniczna i telekomunikacja.....

Objaśnienie oznaczeń:

P6U – charakterystyki uniwersalne odpowiadające kształceniu na studiach pierwszego stopnia - 6 poziom PRK*

P7U – charakterystyki uniwersalne odpowiadające kształceniu na studiach drugiego stopnia - 7 poziom PRK*

P6S – charakterystyki drugiego stopnia odpowiadające kształceniu na studiach pierwszego stopnia studiów - 6 poziom PRK *

P7S – charakterystyki drugiego stopnia odpowiadające kształceniu na studiach drugiego stopnia/ jednolitych magisterskich – 7 poziom PRK*

W – kategoria „wiedza”

U – kategoria „umiejętności”

K – kategoria „kompetencje społeczne”

K(symbol kierunku)_W1, K(symbol kierunku)_W2, K(symbol kierunku)_W3, ...- efekty kierunkowe dot. kategorii „wiedza”

K(symbol kierunku)_U1, K(symbol kierunku)_U2, K(symbol kierunku)_U3, ...- efekty kierunkowe dot. kategorii „umiejętności”

K(symbol kierunku)_K1, K(symbol kierunku)_K2, K(symbol kierunku)_K3, ...- efekty kierunkowe dot. kategorii „kompetencje społeczne”

S(symbol specjalności)_W..., S(symbol specjalności)_W..., S(symbol specjalności)_W..., ...- efekty specjalnościowe dot. kategorii „wiedza”

S(symbol specjalności)_U..., S(symbol specjalności)_U..., S(symbol specjalności)_U..., ...- efekty specjalnościowe dot. kategorii „umiejętności”

S(symbol specjalności)_K..., S(symbol specjalności)_K..., S(symbol specjalności)_K..., ...- efekty specjalnościowe dot. kategorii „kompetencje społeczne”

...._inż – efekty uczenia się umożliwiające uzyskanie kompetencji inżynierskich

*niepotrzebne usunąć

Symbol kierunkowych efektów uczenia się	Opis efektów uczenia się dla kierunku studiów Cyberbezpieczeństwo Po ukończeniu kierunku studiów absolwent:	Odniesienie do charakterystyk PRK		
		Uniwersalne charakterystyki pierwszego stopnia (U)	Charakterystyki drugiego stopnia typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego (S)	
			Charakterystyki dla kwalifikacji na poziomach 6/7* PRK	Charakterystyki dla kwalifikacji na poziomach 6 i 7 PRK, umożliwiającymi uzyskanie kompetencji inżynierskich
WIEDZA (W)				
K2CBE_W01	Zna typowe zagrożenia występujące w sieciach teleinformatycznych, ma wiedzę o metodach testowania, monitorowania sieci i reagowania na zagrożenia bezpieczeństwa cybernetycznego.	P7U_W	P7S_WG	P7S_WG
K2CBE_W02	Ma poszerzoną i pogłębioną wiedzę w zakresie wybranych działów matematyki i fizyki niezbędną do rozumienia zagadnień w zakresie cyberbezpieczeństwa.	P7U_W	P7S_WG	
K2CBE_W03	Ma poszerzoną i pogłębioną wiedzę w zakresie ochrony i bezpieczeństwa infrastruktury oraz usług teleinformatycznych.	P7U_W	P7S_WG	
K2CBE_W04	Zna charakterystykę rynku teleinformatycznego i metodykę realizacji projektów teleinformatycznych.	P7U_W	P7S_WK	P7S_WK
K2CBE_W05	Ma aktualną wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w obszarze cyberbezpieczeństwa.	P7U_W	P7S_WG	P7S_WG
UMIĘTNOŚCI (U)				
K2CBE_U01	Potrafi skonfigurować i uruchomić narzędzia do monitorowania i testowania ruchu sieciowego oraz identyfikować normalny i nietypowy ruch lub oznaki włamania. Potrafi przeprowadzić testy i audyt bezpieczeństwa sieci.	P7U_U	P7S_UW P7S_UO	
K2CBE_U02	Potrafi posługiwać się metodami matematyki i fizyki do rozwiązywania szczegółowych problemów z zakresu cyberbezpieczeństwa.	P7U_U	P7S_UW	

K2CBE_U03	Potrafi projektować i implementować mechanizmy bezpieczeństwa dla infrastruktury oraz usług teleinformatycznych	P7U_U	P7S_UW P7S_UO	
K2CBE_U04	Ma umiejętności i kompetencje zgodne z wymaganiami określonymi dla poziomu dodatkowego B2+ ESOKJ w zakresie języka naukowo-technicznego związanego ze studiowaną dyscypliną i pokrewnymi zagadnieniami.	P7U_U	P7S_UK	
K2CBE_U05	Ma umiejętności i kompetencje zgodne z wymaganiami określonymi dla poziomu A1 ESOKJ; używa w elementarnym stopniu podstawowych sprawności językowych; zna podstawowe słownictwo i struktury gramatyczne w zakresie tematów życia codziennego i podstawowych zachowań interkulturowych.	P7U_U	P7S_UK	
K2CBE_U06	Potrafi przygotować biznes plan i elementy zarządzania projektem teleinformatycznym	P7U_U	P7S_UK P7S_UO	
K2CBE_U07	Potrafi referować poszczególne fazy realizacji pracy dyplomowej, przygotować prezentację zawierającą wyniki końcowe pracy, uzasadnić wnioski i konkluzje. Zna reguły kreatywnej dyskusji. Potrafi samodzielnie zrealizować dyplomową magisterską zawierającą aspekty badawcze	P7U_U	P7S_UU P7S_UW P7S_UK	
KOMPETENCJE SPOŁECZNE (K)				
K2CBE_K01	Ma świadomość społecznych skutków działalności inżynierskiej i związanej z tym odpowiedzialności za podejmowane decyzje. Rozumie potrzebę przekazywania społeczeństwu informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności absolwenta uczelni technicznej. Rozumie rolę środków masowego przekazu	P7U_K	P7S_KR P7S_KO	
K2CBE_K02	Krytycznie oceniać odbierane treści, uznawać znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych. Potrafi odpowiednio określić priorytety służące realizacji określonego zadania.	P7U_K	P7S_KK	

*niepotrzebne usunąć

PLAN STUDIÓW

WYDZIAŁ:	INFORMATYKI i TELEKOMUNIKACJI
KIERUNEK STUDIÓW:	CYBERBEZPIECZEŃSTWO
POZIOM KSZTAŁCENIA:	II stopień, studia magisterskie
FORMA STUDIÓW:	stacjonarna
PROFIL:	ogólnoakademicki
SPECJALNOŚĆ:	
JĘZYK PROWADZENIA STUDIÓW:	polski
OBOWIAZUJE OD CYKLU KSZTAŁCENIA:	2022/2023

1. Zestaw kursów i grup kursów obowiązkowych i wybieralnych w układzie semestralnym

Semestr 1

Kursy /grupy kursów obowiązkowe

liczba punktów ECTS: **27**

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ó	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1	W04CBE-SM0001G	Monitorowanie i detekcja zagrożeń (GK)	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	E(w)		DN	4	K
2	W04CBE-SM0002G	Testy penetracyjne(GK)	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	E(w)		DN	4	K
	W04CBE-SM0011G	Analiza ryzyka i reakcja na incydenty (GK)	2	0	0	4	0	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	E(w)		DN	4	K
4	W04CBE-SM0010G	Matematyka(GK)	1	1	0	0	0	K2CBE_W02 K2CBE_U02	30	90	3	0	1	T	Z	O		1	K
5	W08W04-SM0001S	Komunikacja społeczna	0	0	0	0	1	K2CBE_U06 K2CBE_K01	15	60	2	0	1	T	Z	O		1	KO
6	W04CBE-SM0009W	Fizyka	1	0	0	0	0	K2CBE_W02 K2CBE_U02	15	30	1	0	0,5	T	Z	O			KO
Razem			8	1	0	10	3	-	330	810	27	21	14,5	-	-	-		14	0

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Kursy /grupy kursów wybieralne (minimum 30 godzin w semestrze) liczba punktów ECTS: 3

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1	SJO-SM0001	Język obcy I	0	1	0	0	0	K2CBE_U05	15	30	1	0	0,5	T	Z	O			KO
2	SJO-SM0002	Język obcy II	0	3	0	0	0	K2CBE_U04	45	60	2	0	1,5	T	Z	O			KO
Razem			0	4	0	0	0		60	90	3	0	2						

Razem w semestrze

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS	Liczba punktów ECTS
w	ć	l	p	s					
8	5	0	10	3	390	900	30	21	16,5

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną działal. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Semestr 2

Kursy /grupy kursów obowiązkowe

liczba punktów ECTS: **9**

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1	W04CBE-SM0004G	Zarządzanie bezpieczeństwem informacji (GK)	1	0	0	3	1	K2CBE_W01 K2CBE_U01	75	180	6	6	3	T/Z	E(w)		DN	4	K
2	W04CBE-SM0006S	Seminarium kierunkowe	0	0	0	0	2	K2CBE_W05 K2CBE_K02	30	90	3	3	1	T	Z			2	K
Razem			1	0	0	3	3	-	105	270	9	9	4	-	-	-	0	6	-

Kursy /grupy kursów wybieralne (minimum 30 godzin w semestrze)

liczba punktów ECTS:

21

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
	CBE-SI0020BK	Blok A	6	0	0	9	3		270	630	21	21	12	T/Z	Z		DN	9	K

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

1	W04CBE-SM0200G	Ochrona systemów operacyjnych	2	0	0	3	1	K2CBE_U01	90	210	7	7	4	T/Z	Z		DN	3	K
2	W04CBE-SM0501G	Metody AI w badaniu zagrożeń w systemach komputerowych	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	Z		DN	3	K
3	W04CBE-SM0301G	Zaawansowane testy penetracyjne sieci i aplikacji (GK)	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	Z		DN	3	K
4	W04CBE-SM0203G	Informatyka śledcza (GK)	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	Z		DN	3	K
Razem			6	0	0	9	3		270	630	21	21	12					9	

Razem w semestrze

Łączna liczba godzin					Łączna liczba godzin ZZZU	Łączna liczba godzin CNBS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS	Liczba punktów ECTS
w	ć	l	p	s					
7	0	0	12	6	375	900	30	30	16

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną działalnością naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Semestr 3

Kursy /grupy kursów obowiązkowe

liczba punktów ECTS: **18**

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1	W04CBE-SM0005G	Przedsiębiorczość w ICT	2	0	0	1	0	K2CBE_W4 K2CBE_U06	45	90	3	0	2	T/Z	Z	O		1	KO
2	W04CBE-SM0008D	Praca dyplomowa						K2CBE_U07 K2CBE_K02	150	360	12		6	T	Z			12	K
3	W04CBE-SM0007S	Seminarium dyplomowe					2	K2CBE_U07 K2CBE_K02	30	90	3		2	T	Z			3	K
Razem			2	0	0	1	2		225	540	18	0	10			0	0	16	

Kursy /grupy kursów wybieralne (minimum 30 godzin w semestrze)

liczba punktów ECTS:

12

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
	CBE-SI0030BK	Blok B	2	0	0	4	0		90	360	12	12	6	T/Z	Z		DN	6	K
1	W04CBE-SM0201G	Ochrona centrów danych (GK)	1	0	0	2	0	K2CBE_W03 K2CBE_U03	45	180	6	6	3	T/Z	Z		DN	6	K
2	W04CBE-SM0401G	Audytowanie infrastruktury IT (GK)	1	0	0	2	0	K2CBE_W03 K2CBE_U03	45	180	6	6	3	T/Z	Z		DN	6	K

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

3	W04CBE-SM0600G	Bezpieczeństwo aplikacji webowych	1	0	0	2	0	K2CBE_W03 K2CBE_U03	45	180	6	6	3	T/Z	Z		DN	6	K
			Razem	2	0	0	4	0		90	360	12	12	6					6

Razem w semestrze

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNBS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS	Liczba punktów ECTS
w	ć	l	p	s					
4	0	0	5	2	315	900	30	12	16

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

2. Zestaw egzaminów w układzie semestralnym

Kod kursu	Nazwy kursów kończących się egzaminem	Semestr
W04CBE-SM0001G	Monitorowanie i detekcja zagrożeń	1
W04CBE-SM0002G	Testy penetracyjne	
W04CBE-SM0011G	Analiza ryzyka i reakcja na incydenty	
W04CBE-SM0004G	Zarządzanie bezpieczeństwem informacji	2

3. Liczby dopuszczalnego deficytu punktów ECTS po poszczególnych semestrach

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

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Opinia właściwego organu Samorządu Studenckiego

.....
Data Imię, nazwisko i podpis przedstawiciela studentów

Data Podpis Dziekana

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Kierunek studiów Cyberbezpieczeństwo
Poziom studiów studia drugiego stopnia

OPIS PROGRAMU STUDIÓW
Profil ogólnoakademicki
Forma Studiów stacjonarna

Zał. nr 4 do ZW 121/2020
Zał. nr 2 do Programu studiów

1. Opis ogólny

<i>1.1 Liczba semestrów: 3</i>	<i>1.2 Całkowita liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:</i> 90
<i>1.3 Łączna liczba godzin zajęć: 1080</i>	<i>1.4 Wymagania wstępne (w szczególności w przypadku studiów drugiego stopnia):</i> REKRUTACJA wymagania corocznie określone przez Senat PWr. i Radę Wydziału Informatyki i Telekomunikacji

1.5 Tytuł zawodowy nadawany po zakończeniu studiów: Magister Inżynier

1.6 Sylwetka absolwenta, możliwości zatrudnienia: Absolwent jest przygotowany do pracy przy zabezpieczaniu systemów teleinformatycznych, obejmujących planowanie systemu zabezpieczeń, jego wdrażanie i utrzymywanie w gotowości podczas eksploatacji oraz wprowadzania niezbędnych modyfikacji dostosowujących system zabezpieczeń do występujących i ciągle ewoluujących zagrożeń. Szczególny nacisk położono na monitorowanie i reakcję na zagrożenia, a także testowanie zabezpieczeń. Kształcenie obejmuje m. in. sposoby tworzenia bezpiecznych usług, przetwarzanie dużych zbiorów informacji (Big Data) w tym metodami sztucznej inteligencji, struktury i działanie centrów przetwarzania danych, bezpieczeństwo w systemach rozproszonych, bezpieczeństwo systemów i sieci, audytowanie sieci teleinformatycznych i bezpieczne usługi internetowe oraz informatykę śledczą.

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

<p>1.7 <i>Możliwość kontynuacji studiów:</i> możliwość ubiegania się o przyjęcie do szkoły doktorskiej, studia podyplomowe</p>	<p>1.8 <i>Wskazanie związku z misją Uczelni i strategią jej rozwoju:</i> Program studiów jest zgodny z misją Politechniki Wrocławskiej i strategią jej rozwoju.</p>
--	---

2. Opis szczegółowy

2.1 Całkowita liczba efektów uczenia się w programie studiów: W (wiedza) = 5, U (umiejętności) 6, K (kompetencje) = 2, W + U + K =13

2.2 Dla kierunku studiów przyporządkowanego do więcej niż jednej dyscypliny – liczba efektów uczenia się przypisana do dyscypliny:

D1 (wiodąca) 13 (liczba ta musi być większa od połowy całkowitej liczby efektów uczenia się)

D2

D3

D4

2.3 Dla kierunku studiów przyporządkowanego do więcej niż jednej dyscypliny – procentowy udział liczby punktów ECTS dla każdej z dyscyplin:

D1 ...100.. % punktów ECTS

D2 % punktów ECTS

D3 % punktów ECTS

D4 % punktów ECTS

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną działal. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

2.4a. Dla kierunku studiów o profilu ogólnoakademickim – liczba punktów ECTS przypisana zajęciom związanym z prowadzoną w Uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów (musi być większa niż 50 % całkowitej liczby punktów ECTS z p. 1.2)

63 ECTS

2.4b. Dla kierunku studiów o profilu praktycznym - liczba punktów ECTS przypisana zajęciom kształtującym umiejętności praktyczne (musi być większa niż 50 % całkowitej liczby punktów ECTS z p. 1.2)

2.5 Zwięzła analiza zgodności zakładanych efektów uczenia się z potrzebami rynku pracy

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną działalnością naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Zakładane efekty kształcenia są zgodne z potrzebami rynku pracy. Takie stanowisko jest uprawomocnione wynikami analiz potrzeb rynku pracy, zawartych np. w Raporcie z II edycji badań: Branża IT w dobie pandemii – „Analiza sytuacji pracodawców kluczowych trendów rozwojowych i zapotrzebowania na kompetencje opracowanym w ramach Branżowego Bilansu Kapitału Ludzkiego z lat 2020-2021, czy w raporcie "Rozwój umiejętności w zakresie cyberbezpieczeństwa" - ENISA 2020

Wyniki analiz potwierdzają bardzo duże zapotrzebowanie na absolwentów kierunku cyberbezpieczeństwo. Jest to kierunek, który znajduje się na czele trendów, które w perspektywie 3-5 lat będą miały największy wpływ na zapotrzebowanie na specjalistów. Prognozuje się, że z największymi wyzwaniami będzie się wiązało zapewnienie odpowiednich kadr między innymi w obszarze Cyberbezpieczeństwa.

Dodatkowo kompetencje związane z cyberbezpieczeństwem to kluczowy zasób z perspektywy rozwoju polskich firm IT. Zakładane efekty uczenia się pozwolą na nabycie kompetencji pożądaných przez pracodawców, takich jak np. pracy grupowej. Pozwolą również na uzyskanie preferowanych przez pracodawców umiejętności praktycznych, co zapewnia odbycie praktyki zawodowej oraz zaliczenie bloku kształcenia specjalistycznego.

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

2.6. Łączna liczba punktów ECTS, którą student musi uzyskać na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia (wpisać sumę punktów ECTS dla kursów/ grup kursów oznaczonych kodem BU1, przy czym dla studiów stacjonarnych liczba ta musi być większa niż 50 % całkowitej liczby punktów ECTS z p. 1.2)

48,5 ECTS

2.7. Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć z zakresu nauk podstawowych

Liczba punktów ECTS z przedmiotów obowiązkowych	4
Liczba punktów ECTS z przedmiotów wybieralnych	0
Łączna liczba punktów ECTS	4

2.8. Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć o charakterze praktycznym, w tym zajęć projektowych (wpisać sumę punktów ECTS kursów/grup kursów oznaczonych kodem P)

Liczba punktów ECTS z przedmiotów obowiązkowych	36
Liczba punktów ECTS z przedmiotów wybieralnych	15
Łączna liczba punktów ECTS	51

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

2.9. Minimalna liczba punktów ECTS , którą student musi uzyskać, realizując bloki kształcenia oferowane na zajęciach ogólnouczeniowych lub na innym kierunku studiów (wpisać sumę punktów ECTS kursów/grup kursów oznaczonych kodem O)
12 ECTS

2.10. Łączna liczba punktów ECTS, którą student może uzyskać, realizując bloki wybieralne (min. 30 % całkowitej liczby punktów ECTS)
36 ECTS

3. Opis procesu prowadzącego do uzyskania efektów uczenia się:

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczeniowy – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną działalnością naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów częściowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

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

Do każdego efektu uczenia się przyporządkowane są kody kursów obecnych w programie studiów. Zaliczenie tych kursów (tego kursu) oznacza uzyskanie danego efektu. Kursy zaliczane są na podstawie form kontroli nabytej wiedzy, umiejętności i kompetencji społecznych, zdefiniowanych w kartach kursów. Brak osiągnięcia przez studenta efektów uczenia się, przypisanych do kursu skutkuje brakiem zaliczenia kursu i koniecznością powtórnej jego realizacji.

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

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

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

.....

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

4. Lista bloków zajęć:

4.1 Lista bloków zajęć obowiązkowych

4.1.1 Lista bloków kształcenia ogólnego

4.1.1.1 Blok *Przedmioty humanistyczno-menedżerskie (5 pkt ECTS)*

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁵	o char. prakt. ⁶	rodzaj ⁷
1	W08W04-SM0001S	Komunikacja społeczna	0	0	0	0	1	K2CBE_U06 K2CBE_K01	15	60	2	0	1	T	Z	O		1	KO
2	W04CBE-SM0005G	Przedsiębiorczość w ICT	2	0	0	1	0	K2CBE_W4 K2CBE_U06	45	90	3	0	2	T/Z	Z	O		1	KO
Razem			2	0	0	1	1	-	60	150	5	0	3	-	-	-	-	2	-

Razem dla bloków kształcenia ogólnego

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS zajęć DN ¹	Liczba punktów ECTS zajęć BU ¹
w	ć	l	p	s					
2	0	0	1	1	60	150	5	0	3

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną dział. naukową – DN

⁶Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

4.1.2 Lista bloków z zakresu nauk podstawowych

4.1.2.1 Blok *Matematyka*

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin			Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęc DN ⁵	zajęc BU ¹	ogólnouczelniany ⁴			zw. z dział. nauk. ⁵	o char. prakt. ⁶	rodzaj ⁷	
1	W04CBE-SM0010G	Matematyka(GK)	1	1	0	0	0	K2CBE_W02 K2CBE_U02	30	90	3	0	1	T	Z	O		1	K	
		Razem	1	1	0	0	0	-	30	90	3	0	1	-	-	-	0	1	-	

4.1.2.2 Blok *Fizyka*

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin			Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęc DN ⁵	zajęc BU ¹	ogólnouczelniany ⁴			zw. z dział. nauk. ⁵	o char. prakt. ⁶	rodzaj ⁷	
1	W04CBE-SM0009W	Fizyka	1	0	0	0	0	K2CBE_W02 K2CBE_U02	15	30	1	0	0,5	T	Z	O			KO	
		Razem	1	0	0	0	0	-	15	30	1	0	0,5	-	-	-	0	0	-	

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. nauką – DN

⁶Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Razem dla bloków z zakresu nauk podstawowych

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS zajęć DN ¹	Liczba punktów ECTS zajęć BU ¹
w	ć	l	p	s					
2	1	0	0	0	45	120	4	0	1,5

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

4.1.3 Lista bloków kierunkowych

4.1.3.1 Blok *Przedmioty obowiązkowe kierunkowe*

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁵	o char. prakt. ⁶	rodzaj ⁷
1	W04CBE-SM0001G	Monitorowanie i detekcja zagrożeń (GK)	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	E(w)		DN	4	K
2	W04CBE-SM0002G	Testy penetracyjne(GK)	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	E(w)		DN	4	K
3	W04CBE-SM0011G	Analiza ryzyka i reakcja na incydenty (GK)	2	0	0	4	0	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	E(w)		DN	4	K
4	W04CBE-SM0004G	Zarządzanie bezpieczeństwem informacji (GK)	1	0	0	3	1	K2CBE_W01 K2CBE_U01	75	180	6	6	3	T/Z	E(w)		DN	4	K
5	W04CBE-SM0006S	Seminarium kierunkowe	0	0	0	0	2	K2CBE_W05 K2CBE_K02	30	90	3	3	1	T	Z			2	K
6	W04CBE-SM0007S	Seminarium dyplomowe	0	0	0	0	2	K2CBE_U07 K2CBE_K02	30	90	3		2	T	Z			3	K
7	W04TAI-SM0020D	Praca dyplomowa						K2TAI_U07 K2TAI_K02		360	12		6	T	Z			12	K
Razem			7	0	0	13	7	-	405	1350	45	30	24	-	-	-		33	-

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Razem dla bloków kierunkowych

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS zajęć DN ¹	Liczba punktów ECTS zajęć BU ¹
w	ć	l	p	s					
7	0	0	13	7	405	1350	45	30	24

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

4.2 Lista bloków wybieralnych

4.2.1 Lista bloków kształcenia ogólnego

4.2.1.1 Blok *Języki obce (min 3pkt ECTS)*

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów				
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁵	o char. prakt. ⁶	rodzaj ⁷	
1	SJO-SM0001	Język obcy I	0	1	0	0	0	K2CBE_U05	15	30	1	0	0,5	T	Z	O				KO
2	SJO-SM0002	Język obcy II	0	3	0	0	0	K2CBE_U04	45	60	2	0	1,5	T	Z	O				KO
Razem			0	4	0	0	0	-	60	90	3	0	2	-	-	-			0	-

Razem dla bloków kształcenia ogólnego

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS zajęć DN ¹	Liczba punktów ECTS zajęć BU ¹
w	ć	l	p	s					
0	4	0	0	0	60	90	3	0	2

4.2.2 Lista bloków kierunkowych

4.2.2.1 Blok *Przedmioty Kierunkowe*

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia	Kurs/grupa kursów			
			w	ć	l	p	s		ZZU	CNPS	łącna	zajęć DN ⁵	zajęć BU ¹			ogólnouczelniany ⁴	zw. z dział. nauk. ⁵	o char. prakt. ⁶	rodzaj ⁷
	CBE-SI0020BK	Blok A	6	0	0	9	3		270	630	21	21	12	T/Z	Z		DN	9	K

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

1	W04CBE-SM0200G	Ochrona systemów operacyjnych (GK)	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	Z		DN	3	K
2	W04CBE-SM0501G	Metody AI w badaniu zagrożeń w systemach komputerowych	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	Z		DN	3	K
3	W04CBE-SM0301G	Zaawansowane testy penetracyjne sieci i aplikacji (GK)	2	0	0	3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	4	T/Z	Z		DN	3	K
4	W04CBE-SM0203G	Informatyka śledcza (GK)	2	0	0	3	1	K2CBE_U01	90	210	7	7	4	T/Z	Z		DN	3	K
	CBE-SI0030BK	Blok B	2	0	0	4	0	K2CBE_W01 K2CBE_U01	90	360	12	12	6	T/Z	Z		DN	6	K
6	W04CBE-SM0201G	Ochrona centrów danych (GK)	1	0	0	2	0	K2CBE_W03 K2CBE_U03	45	180	6	6	3	T/Z	Z		DN	6	K
7	W04CBE-SM0401G	Audytowanie infrastruktury IT (GK)	1	0	0	2	0	K2CBE_W03 K2CBE_U03	45	180	6	6	3	T/Z	Z		DN	6	K
8	W04CBE-SM0600G	Bezpieczeństwo aplikacji webowych	1	0	0	2	0	K2CBE_W03 K2CBE_U03	45	180	6	6	3	T/Z	Z		DN	6	K
Razem			8	0	0	13	3		360	990	33	33	18					15	

Razem dla bloków specjalnościowych

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS zajęć DN ¹	Liczba punktów ECTS zajęć BU ¹
w	ć	l	p	s					
8	0	0	13	3	360	990	33	33	18

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

4.4 Blok „praca dyplomowa”

Typ pracy dyplomowej	inżynierska	
Liczba semestrów pracy dyplomo	Liczba punktów ECTS	Kod
1	12 P(12)	W04CBE-SM0008D
Charakter pracy dyplomowej		
projekt lub program komputerowy		
Liczba punktów ECTS BU ¹	6	
Liczba punktów ECTS DN ⁵	0	

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów częściowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

5. Sposoby weryfikacji zakładanych efektów uczenia się

Typ zajęć	Sposoby weryfikacji zakładanych efektów uczenia się
wykład	egzamin lub e-egzamin, praca pisemna przygotowana na podstawie wykładów i zalecanej literatury, zaliczenie ustne lub pisemne, warunkująca przystąpienie do kolokwium końcowego rozprawka rozwiązująca wybrany problem postawiony w materiale wykładów, dyskusja na wykładzie, test końcowy, ocena liczby uzyskanych poprawnych odpowiedzi, egzamin testowy, egzamin ustny, kolokwium pisemne lub w postaci e-testu, sprawdziany pisemne, pisemne zaliczenie, egzamin, konkurs kryptograficzny, kolokwium zaliczeniowe, test zaliczeniowy z wykładu, kolokwium pisemne, kolokwium, aktywność na wykładach, zaliczenie sprawdzianów pisemnych, egzamin pisemny, odpowiedź ustna, kartkówka, test pisemny, test
ćwiczenia	odpowiedzi ustne, kartkówki, kolokwia i/lub e-sprawdziany, dyskusje, sprawdziany, ćwiczenia, ocena odpowiedzi ustnych, ocena rozwiązań przykładowych zadań ćwiczeniowych, kolokwium zaliczeniowe, krótkie pisemne sprawdziany, kolokwium pisemne, sprawdziany pisemne
laboratorium	sprawność obsługi przyrządów i ich łączenia, protokoły, innowacyjność rozwiązania i prezentacji wyników, ocena pisemnych sprawozdań z realizacji kolejnych ćwiczeń laboratoryjnych, ocena przygotowania do zajęć laboratoryjnych i poprawności wykonania ćwiczeń, obserwacja wykonywania ćwiczeń laboratoryjnych, inspekcja kodu wykonanych programów z udziałem prowadzącego laboratorium, prezentacja aplikacji, 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, e-testy cząstkowe, dyskusje, pisemne sprawozdania, odpowiedzi ustne, pisemne, sprawdzenie przygotowania do laboratorium, odbiór i ocena sprawozdań, ocena końcowa z laboratorium, aktywność na zajęciach, pisemne zaliczenie – test, ocena postępów prac w ramach zajęć laboratoryjnych

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

projekt	ocena wykonanego projektu, prezentacja, dyskusja, aktywność na zajęciach projektowych, wstępna prezentacja zagadnienia projektowego, końcowa prezentacja projektu, ocena dwóch projektów (realizacja i prezentacja), wykonany (napisany) projekt, przedstawienie projektu oraz jego obrona, ocena prezentacji kolejnych etapów projektu oraz umiejętności pracy w zespole: przestrzegania harmonogramu, aktywność w zespole, umiejętność zastosowania zasad zarządzania projektem, ocena jakości wykonanego projektu oraz dokumentacji projektowej
seminarium	prezentacja udział w dyskusji
praca dyplomowa	przygotowana praca dyplomowa

6. Zakres egzaminu dyplomowego

Załącznik nr 3 do programu studiów

7. Wymagania dotyczące terminu zaliczenia określonych kursów/grup kursów lub wszystkich kursów w poszczególnych blokach

Lp.	Kod kursu	Nazwa kursu	Termin zaliczenia do.. (nr semestru)
1		<i>Wszystkie kursy/grupy kursów z planu studiów dla semestru 1 i semestru 2</i>	do końca 2 semestru

8. Plan studiów (załącznik nr 4)

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związanych/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Zaopiniowane przez właściwy organ uchwałodawczy samorządu studenckiego:

.....
Data Imię, nazwisko i podpis przedstawiciela studentów

Data Podpis Dziekana

¹BU – liczba punktów ECTS przypisanych zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia

²Tradycyjna – T, zdalna – Z

³Egzamin – E, zaliczenie na ocenę – Z. W grupie kursów po literze E lub Z wpisać w nawiasie formę kursu końcowego (w, c, l, s, p)

⁴Kurs/ grupa kursów Ogólnouczelniany – O

⁵Kurs/ grupa kursów związany/-a z prowadzoną dział. naukową – DN

⁶ Kurs / grupa kursów o charakterze praktycznym – P. W grupie kursów w nawiasie wpisać liczbę punktów ECTS dla kursów cząstkowych o charakterze praktycznym

⁷ KO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Pytania egzaminacyjne

Cyberbezpieczeństwo II st.

Przedmioty obowiązkowe:

1. Współczesne architektury cyberbezpieczeństwa
2. Sposoby i narzędzia do monitorowania i detekcji zagrożeń.
3. Podatności aplikacji Web – najpopularniejsze podatności, metody wykrywania
4. Identyfikacja zasobów IT i analiza ryzyka
5. System Zarządzania Bezpieczeństwem Informacji. Organizacja bezpieczeństwa informacji.

Przedmioty wybieralne:

Blok A

1. Zabezpieczenia systemów operacyjnych Windows i Linux
2. Testy penetracyjne związane z technikami kryptograficznymi.
3. Metody zacierania i fałszowania dowodów cyfrowych
4. Dowody incydentów bezpieczeństwa – gromadzenie, metody analizy i oceny jakości
5. Metody sztucznej inteligencji i uczenia maszynowego w modelowaniu i wykrywaniu zagrożeń systemów IT

Blok B

6. Narzędzia monitorowania i detekcja zagrożeń w systemach chmurowych
7. Metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych
8. Audyt infrastruktury sieciowej – etapy, sposób prowadzenia

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Analiza ryzyka i reakcja na incydenty	
Nazwa przedmiotu w języku angielskim Risk analysis and incident response	
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-SM0011G
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)	210	---	---	---	---
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	7				
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)	4				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH
1. Wiedza na temat systemów operacyjnych i aplikacji
2. Wiedza na temat struktur sieciowych
3. Wiedza z zakresu podstaw ochrony informacji
4. Wiedza z zakresu przetwarzania danych

CELE PRZEDMIOTU
C1. Nabycie wiedzy z zakresu praktyk bezpieczeństwa oraz ochrony informacji
C2. Poszerzenie umiejętności w zakresie obsługi procesów w cyberbezpieczeństwie
C3. Nabycie wiedzy z zakresu systemu zarządzania w oparciu o NIST cybersecurity framework

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Posiada wiedzę na zasad i praktyk w zakresie bezpieczeństwa informacji

PEU_W02 Posiada wiedzę z zakresu zarządzania, bezpieczeństwa i ochrony informacji

PEU_W02 Posiada wiedzę na temat stosowania standardów i praktyk zgodnych z międzynarodowymi standardami

Z zakresu umiejętności:

PEU_U01 Potrafi identyfikować i określać aktywa, zasoby i zagrożenia w systemach IT

PEU_U02 Potrafi określać i implementować wymagania, by zapewnić właściwy poziom ochrony informacji

PEU_U02 Potrafi wykrywać i wyceniać zagrożenia, podatności i słabości w systemach IT

PEU_U02 Potrafi odpowiednio reagować na incydenty oraz minimalizować ich skutki

PEU_U02 Potrafi zarządzać właściwym odtwarzaniem systemów po incydentach i awariach

Z zakresu kompetencji społecznych:

PEU_K01 Potrafi wykorzystywać standardy NIST w zakresie zarządzania bezpieczeństwem informacji

PEU_K02 Potrafi określać i identyfikować pracę różnych zespołów zarządzania

PEU_K03 Potrafi określić wpływy zagrożeń i odpowiednio reagować na zdarzenia

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Podstawy zarządzania systemami informatycznymi w zakresie ochrony informacji. Klasyfikacja informacji.	2
Wy2	Identyfikacja zasobów: struktura systemów, topologie sieci	2
Wy3	Identyfikacja zasobów: klasyfikacja i zarządzanie przepływem danych	2
Wy4	Identyfikacja: Analizy ryzyka, polityki, standardy i procedury	2
Wy5	Identyfikacja: opracowywanie modeli, polityk, procedur, modelowanie zagrożeń	2
Wy6	Ochrona: detekcja i skanowanie zasobów, użytkowników, narzędzi	2
Wy7	Ochrona: systemy monitorowania, analizy przypadków, reakcji na zdarzenia	2
Wy8	Wykrywanie: Wycena zagrożeń, wpływu, korelacja danych	2
Wy9	Wykrywanie: źródła danych: dzienniki, logi	2
Wy10	Reakcja: zarządzanie i koordynacja zespołów reagowania	2
Wy11	Reakcja: określanie właściwych parametrów oraz planów naprawczych	2
Wy12	Reakcja: zbieranie i charakterystyka dowodów cyfrowych	2
Wy13	Odtwarzanie: zarządzanie procesami odtwarzania	2
Wy14	Odtwarzanie: testowanie, aktualizacje planów, procesów i procedur	2
Wy15	Koordynacja pracy zespołów IT, podział zadań, repetytorium	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	Omówienie zasad realizacji zadania projektowego: zakres, temat, cele oraz formy projektu.	4
Pr2- Pr13	Realizacja projektu (przygotowanie rozwiązanie praktycznego dla postawionego projektu). Realizacja zadań cząstkowych zgodnie z harmonogramem projekt Dokumentowanie projektu (przygotowanie usystematyzowanej dokumentacji projektu).	48
Pr14- Pr15	Prezentacja rozwiązania problemu projektowego.	8
	Suma godzin	60

Forma zajęć - seminarium		Liczba godzin
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład problemowy N2. Studia literaturowe N3. Opracowanie pisemne N4. Dyskusja problemowa 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	1. Pisemne zaliczenie.

	PEU_W03	
F2	PEU_U01 PEU_U02 PEU_U03 PEU_K01 PEU_K02 PEU_K03	1. Prezentacje cząstkowe. 2. Obrona projektu, zaliczenie.
<p>$P=0,5*F1+0,5*F2$</p> <p>warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu</p>		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA	
<p><u>LITERATURA PODSTAWOWA:</u></p> <p>[1] Normy ISO rodziny 27000, PKN 2014 lub późniejsze [2] Materiały dydaktyczne kursu CSX-P www.ISACA.org [3] NIST framework oraz materiały www.nist.gov w zakresie cyberbezpieczeństwa</p> <p><u>LITERATURA UZUPEŁNIAJĄCA:</u></p> <p>[1] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych [2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [3]</p>	
OPIEKUN PRZEDMIOTU (IMIE, NAZWISKO, ADRES E-MAIL)	
Marcin Kaczmarek. CISA	
Marcin.kaczmarek@pwr.edu.pl	

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Audytowanie infrastruktury IT	
Nazwa przedmiotu w języku angielskim Auditing IT infrastructure	
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-SM0401G	
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)	210				
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)	2			1	

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Wiedza z zakresu projektowania i działania sieci komputerowych w tym: topologii, urządzeń i protokołów sieciowych
2. Umiejętności z zakresu konfiguracji urządzeń sieciowych
3. Znajomość obsługi i konfiguracji systemów Windows i Linux

CELE PRZEDMIOTU

C1 Zaznajomienie z celami i potrzebami prowadzenia audytu infrastruktury IT oraz narzędziami wspomagającymi realizację audytu sieci i systemów.

C2. Nabycie umiejętności przeprowadzenia audytu infrastruktury IT

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna koncepcję oraz cele prowadzenie audytu.

PEU_W02 Posiada poszerzoną wiedzę o sposobach i narzędziach do prowadzenia monitorowania i audytu.

Z zakresu umiejętności:

PEU_U01 Potrafi planować i przygotowywać narzędzia do audytu .

PEU_U02 Umie analizować dane pozyskane dzięki przeprowadzonemu audytowi i reagować na wykryte zagrożenia.

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. Cele i potrzeba audytowania i monitorowania infrastruktury i systemów	2
Wy2	Analiza ryzyka na potrzeby monitorowania i audytu	2
Wy3	Audyt infrastruktury sieciowej	2
Wy4	Monitorowanie i audytowanie usług chmurowych i kontenerowych	2
Wy5	Audyt aplikacji web	2
Wy6-7	Audyt systemów operacyjnych	4
Wy8	Repetitorium.	1
	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	Omówienie zasad realizacji zadania projektowego: zakres, temat, cele oraz formy projektu.	2
Pr2- Pr13	Realizacja projektu (przygotowanie rozwiązanie praktycznego dla postawionego projektu). Realizacja zadań cząstkowych zgodnie z harmonogramem projekt Dokumentowanie projektu (przygotowanie usystematyzowanej dokumentacji projektu).	24
Pr14- Pr15	Prezentacja rozwiązania problemu projektowego.	4
	Suma godzin	30

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
Se3		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem slajdów oraz narzędzi symulacyjnych 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, wygłoszone prezentacje
$P=(F1+F2)/2$ warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] “IT Auditing Using Controls to Protect Information Assets”, Mike Schiller, McGraw-Hill Education
- [2] “Auditing IT Infrastructures for Compliance”, Martin Weiss, Michael G. Solomon Jones & Bartlett Learning 2015
- [3] Network Forensics: Tracking Hackers through Cyberspace, Sherri Davidoff Jonathan Ham, Prentice Hall 2012

LITERATURA UZUPEŁNIAJĄCA:

- [1] “Security Strategies in Linux Platforms and Applications”, Michael Jang, Ric Messier, Jones & Bartlett Learning
- [2] “Security Strategies in Windows Platforms and Applications”, Michael G. Solomon, Jones & Bartlett Learning
- [3] Dokumentacja do: Burp
- [4] Dokumentacja do: Zeek
- [5] Dokumentacja do: Snort

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

mgr inż. Damian Stygar, Damian.stygar@pwr.edu.pl

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Bezpieczeństwo aplikacji webowych	
Nazwa przedmiotu w języku angielskim ... Web application security.....	
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-SM0600G
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)	180				
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)	2			1	

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. 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, middleware, client-apps), a także poznania metodologii wspomagających tworzenie bezpiecznych programów, takie jak programowanie defensywne i programowanie sterowane testowaniem.

C2 W części praktycznej -- zapoznanie się z typowymi atakami i metodom ich przeciwdziałania, jak również poznanie narzędzi wspomagających tworzenie bezpiecznych rozwiązań webowych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

- PEU_W01 – zna metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych
- PEU_W02 – wie, co to są certyfikaty SSL i jak działają protokoły SSL/TLS
- PEU_W03 – zna metody ataków typu XSS i CSRF
- PEU_W04 – zna metody ataków typu „code injection”, w szczególności SQL-Injection oraz problemy z przekazywaniem parametrów pomiędzy programami

...

Z zakresu umiejętności:

- PEU_U01 – potrafi wskazać typowe błędy związane z bezpieczeństwem w konfiguracji serwerów sieciowych
- PEU_U02 – potrafi sprawdzić integralność danych w systemie komputerowym i wykorzystać techniki kryptograficzne do zwiększenia bezpieczeństwa systemu (m.in. SSL)
- PEU_U03 – potrafi skonfigurować serwer WWW
- PEU_U04 – potrafi znaleźć i wykorzystać informacje o bieżących problemach związanych z bezpieczeństwem serwerów WWW i aplikacji webowych...

Z zakresu kompetencji społecznych:

- PEU_K01 – jest świadomy znaczenia wagi przykładanej do pisania aplikacji webowych z zachowaniem reguł bezpieczeństwa
- PEU_K02 – jest świadom odpowiedzialności wynikającej z wiedzy o dziurach w bezpieczeństwie poszczególnych aplikacji lub serwerów
- PEU_K03 – rozumie konieczność samokształcenia oraz samodzielnego stosowania posiadanej wiedzy w praktyce,

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 (SQL/shell injections, cross-site scripting)	2
Wy5	Błędy specyficzne w poszczególnych językach i systemach programowania (C, PHP, Perl, Python, .NET, CGI, aplikacje web, Javascript)	2
Wy6	Typowe błędy programistyczne i metody ataków na aplikacje sieciowe typu klient-serwer, a także aplikacje WWW.	2
Wy7	Metody wspomaganie programistów w pisaniu bezpiecznego kodu (defensive programming, test-driven development, systemy kontroli wersji, zarządzanie projektami)	2
Wy8	Kolokwium zaliczeniowe	1
	Suma godzin	

Forma zajęć - projekt		Liczba godzin
Pr1	Implementacja prostych ataków z wykorzystaniem technik XSS i CSRF	5
Pr2	Indywidualne projekty realizowane w grupach 2-3-osobowych dotyczące implementacji exploitów i zabezpieczeń usług oferowanych przez aplikacje webowe	25
	Suma godzin	30

Forma zajęć - seminarium		Liczba godzin
...	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
<p>N1. Wykłady</p> <p>N2. Praca własna - Zadania projektowe do wykonania w wolnym czasie</p> <p>N3. Prezentacje projektów i dyskusja z prowadzącym zajęcia</p> <p>N4. Praca własna – przygotowanie prezentacji wystąpienia na wybrany temat, realizowane w grupach 2-3 osobowych.</p> <p>N5. Kilkunastominutowe prezentacje seminaryjne na wybrany temat realizowane w grupach 2-3 osobowych.</p>

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
P1	PEU_W01, PEU_W02, PEU_W03, PEU_W04, PEU_K01, PEU_K02, PEU_K03	Kolokwium zaliczeniowe (wykład)
P2	PEU_U01, PEU_U02, PEU_U03, PEU_U03	Ocena końcowa projektu

$$P = P1 * 0.4 + P2 * 0.3 + P3 * 0.3$$

Warunkiem uzyskania pozytywnej oceny końcowej z przedmiotu jest wcześniejsze uzyskanie pozytywnej oceny zaliczeniowej z seminarium i projektu

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] Dafydd Stuttard; Marcus Pinto, The Web application hacker's handbook : finding and exploiting security flaws
- [2] Jeff Forristal ; Julie Traxler; Hack proofing : your Web applications : edycja polska

LITERATURA UZUPEŁNIAJĄCA:

- [1] Paweł Frankowski WordPress i Joomla! : zabezpieczanie i ratowanie stron www
- [2] Dan Cederholm ; Kuloodporne strony internetowe

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

Dr inż. Tomasz Surmacz, tomasz.surmacz@pwr.edu.pl, tel. 2752

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim	Fizyka
Nazwa przedmiotu w języku angielskim	Physics
Kierunek studiów (jeśli dotyczy):	Teleinformatyka, Cyberbezpieczeństwo, Informatyka Techniczna
Specjalność (jeśli dotyczy):	
Poziom i forma studiów:	II stopień / jednolite studia magisterskie* , stacjonarna / niestacjonarna*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	W04CBE-SM0009W
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	30				
Forma zaliczenia	Egzamin / 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)	0,5				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Kurs podstawowy z fizyki i matematyki

CELE PRZEDMIOTU

- C1. Zdobyć wiedzę w zakresie wybranych, fundamentalnych praw fizyki współczesnej koniecznej do zrozumienia zjawisk fizycznych w obrębie studiowanej dyscypliny naukowej.
- C2. Zrozumienie potrzeby samokształcenia.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna i potrafi wyjaśnić podstawowe prawa związane z podstawami mechaniki kwantowej.

PEU_W02 Zna i potrafi wyjaśnić podstawowe prawa teorii względności.

PEU_W03 Zna i potrafi wyjaśnić podstawowe zagadnienia fizyki współczesnej i zna przykłady ich zastosowań.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wprowadzenie: zakres i metodologia fizyki; metoda naukowa	1
Wy2	Podstawy mechaniki kwantowej	4
Wy3	Elementy teorii względności	2
Wy4	Czas - podstawa wczesnych modeli fizycznych, jego rola w przesyłaniu informacji. Współczesne poglądy na czas.	2
Wy5	Fizyka w zastosowaniach - od kodowania informacji (rodzaje nośników informacji) przez jej przesyłanie do komputera kwantowego.	4
Wy6	Podsumowanie	2
Suma godzin		15

STOSOWANE NARZĘDZIA DYDAKTYCZNE

N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych

N2. Konsultacje

N3. Praca własna – wskazana lektura dodatkowa

N4. Praca własna – przygotowanie do testu

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	Aktywność na wykładach, zaliczenie kartkówek pisemnych lub prac zespołowych
F2	PEU_U01, PEU_U02, PEU_U03	Test końcowy
$P = (1/3)*F1 + (2/3)*F2$		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] D. Halliday, R. Resnick, 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] Materiały publikowane przez wykładowcę

LITERATURA UZUPEŁNIAJĄCA:

- [5] H.D. Young, R.A. Freedman, University Physics, Pearson-Addison Wesley 2014

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

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Informatyka śledcza	
Nazwa przedmiotu w języku angielskim Cybersecurity forensics	
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-SM0203G
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	---	---	45	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	210	---	---	---	---
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	7				
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)	3				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Poszerzona wiedza z zakresu kodowania i szyfrowania,
2. Wiedza z zakresu bezpieczeństwa systemów operacyjnych
3. Wiedza z zakresu ochrony informacji
4. Podstawowa wiedza z zakresu informatyki śledczej

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 zagadnienia związane z gromadzeniem i oceną jakości danych jako dowodów

PEU_W02 Zna aspekty obsługi incydentów i funkcjonowania SOC

PEU_W03 Posiada wiedzę na temat metod zacierania i fałszowania dowodów cyfrowych

PEU_W04 Posiada wiedzę z zakresu zabezpieczenia systemu IT przed efektami incydentu

Z zakresu umiejętności:

PEU_U01 Potrafi pozyskiwać dowody z cyfrowych źródeł danych

PEU_U02 Opanował narzędzia służące do analizy i przetwarzania danych cyfrowych pod kątem dowodowym

PEU_U03 Opanował narzędzia służące weryfikacji integralności danych cyfrowych

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 Potrafi efektywnie współpracować z organami działającymi w zakresie informatyki śledczej

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Zagadnienia związane z gromadzeniem dowodów dyskowych i sieciowych.	2
Wy2	Zagadnienia związane z analizą dowodów, ocena jakości dowodów.	2
Wy3	Ocena integralności danych pod kątem dowodowym.	2
Wy4	Metody i narzędzia pozyskiwania dowodów ze zbiorów i nośników danych.	2
Wy5	Możliwości źródeł danych pod kątem pozyskiwania dowodów.	2
Wy6	Możliwości pozyskiwania dowodów z danych zaszyfrowanych.	2
Wy7	Metody obchodzenia zabezpieczeń dostępu do nośników.	2
Wy8	Aspekty zacierania i fałszowania dowodów cyfrowych.	2
Wy9	Aspekty komunikacji ze służbami państwowymi.	2
Wy10	Gromadzenie i ochrona dzienników zdarzeń pod kątem wykorzystania w celach dowodowych.	2
Wy11	Zabezpieczenie systemu przed efektami incydentu. Zabezpieczenie sieci przez rozprzestrzenianiem się incydentu.	2
Wy12	Metody i procedury obsługi incydentów.	2
Wy13	Aspekty funkcjonowania SOC.	2
Wy14	Uwarunkowania prawne dotyczące dokumentowania i raportowania incydentów.	2
Wy15	Kolokwium zaliczeniowe	2
	Suma godzin	

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	Omówienie zasad realizacji zadania projektowego: zakres, temat, cele oraz formy projektu.	3
Pr2- Pr13	Realizacja projektu (przygotowanie rozwiązanie praktycznego dla postawionego projektu). Realizacja zadań cząstkowych zgodnie z harmonogramem projekt Dokumentowanie projektu (przygotowanie usystematyzowanej dokumentacji projektu).	36
Pr14- Pr15	Prezentacja rozwiązania problemu projektowego.	6
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1	Omówienie tematyki seminarium oraz zalecanych pozycji literaturowych.	1
Se2 – Se7	Prezentacje studentów dotyczące przedmiotowych zagadnień (cząstkowych/całkowitych). Dyskusja w grupie seminaryjnej.	12
Se8	Prezentacja końcowa problemu seminaryjnego Dyskusja w grupie seminaryjnej.	2
	Suma godzin	15

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
N1.	Wykład problemowy
N2.	Studia literaturowe
N3.	Opracowanie pisemne
N4.	Dyskusja problemowa
N5.	Prezentacje multimedialne
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 PEU_W02 PEU_W03 PEU_W04	1. Pisemne zaliczenie.
F2	PEU_U01 PEU_U02 PEU_U03	1. Prezentacje częściowej. 2. Obrona projektu, zaliczenie.
F3	PEU_K01 PEU_K02 PEU_K03	1. Ocena wykonanych prezentacji, dyskusje. 2. Zaliczenie.
$P=0,5*F1+0,25*F2+0,25*F3$ <p>Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu</p>		

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] Altheide Cory, Harlan Carvey, „Informatyka śledcza. Przewodnik po narzędziach open source”, Helion 2014

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

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

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa w języku polskim:	Matematyka
Nazwa w języku angielskim:	Mathematics
Kierunek studiów:	Teleinformatyka, Cyberbezpieczeństwo
Poziom i forma studiów:	II stopień, stacjonarna
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	W04CBE-SM0010G
Grupa kursów:	TAK

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15	15			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	90				
Forma zaliczenia	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)		1			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	1				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Znajomość rachunku różniczkowego i całkowitego funkcji jednej zmiennej.
2. Znajomość własności i zastosowań liczb zespolonych oraz rachunku macierzy.
3. Znajomość podstawowych metod rozwiązywania układów równań liniowych.
4. Znajomość teorii i zastosowań szeregów liczbowych oraz szeregów potęgowych.

CELE PRZEDMIOTU

- C1 Poznanie podstawowych pojęć, twierdzeń, metod i zastosowań dotyczących przestrzeni liniowych oraz przekształceń liniowych w przestrzeniach wektorowych.
- C2. Poznanie pojęcia funkcji zespolonej, jej pochodnej i całki.
- C3. Poznanie podstawowych pojęć, twierdzeń i metod dotyczących przestrzeni Banacha oraz przestrzeni Hilberta.
- C4. Poznanie pojęcia transformacji Fouriera i Laplace'a ich odstawowych własności i zastosowań.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy student:

PEK_W01 zna podstawowe pojęcia i własności przestrzeni liniowych i przekształceń liniowych.

PEK_W02 zna pojęcie funkcji zespolonej.

PEK_W03 zna podstawowe pojęcia i własności iloczynu skalarnego, przestrzeni Banacha i Hilberta.

PEK_W04 zna pojęcie transformacji Fouriea i Laplace'a oraz ich zastosowań.

Z zakresu umiejętności:

PEK_U01 potrafi wyznaczyć bazę i wymiar przestrzeni liniowej o skończonym wymiarze oraz współrzędne wektora w zadanej bazie.

PEK_U02 potrafi wyznaczyć macierz przekształcenia liniowego w zadanych bazach, potrafi wykorzystać własności przekształceń liniowych do wyznaczania potęg macierzy.

PEK_U03 potrafi skonstruować układ ortogonalny w przestrzeni Hilberta oraz rozwinąć w szereg ortogonalny wektor z przestrzeni Hilberta z zadany układem ortogonalnym.

PEK_U04 potrafi rozwiązywać zadania z użyciem transformacji Fouriera i Laplace'a.

Z zakresu kompetencji społecznych:

PEK_K01 zna podstawowe dziedziny zastosowań abstrakcyjnej algebry liniowej oraz rachunku różniczkowego i całkowego w teleinformatyce.

PEK_K02 rozumie konieczność samodzielnej pracy

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Przestrzenie liniowe. Podprzestrzenie liniowe. Liniowa niezależność wektorów. Baza i wymiar przestrzeni liniowej.	2
Wy2	Odwzorowanie liniowe. Reprezentacja macierzowa odwzorowań liniowych.	1
Wy3	Przestrzenie unormowane. Przestrzenie Banacha. Przestrzenie unitarne. Przestrzenie Hilberta.	2
Wy4	Układy ortogonalne. Baza ortogonalna w przestrzeni Hilberta. Rzut ortogonalny. Funkcjonał liniowy. Twierdzenie Riesz o postaci funkcyjonału liniowego w przestrzeni Hilberta.	2
Wy5	Podstawowe własności funkcji zmiennej zespolonej. Pochodna i całka funkcji zespolonej.	2
Wy6	Transformacja Laplace'a. Podstawowe własności i zastosowania.	2
Wy7	Transformacja Fouriera. Podstawowe własności i zastosowania.	2
Wy8	Kolokwium	2
Suma godzin		15

Forma zajęć - ćwiczenia		Liczba godzin
Ćw1	Wektory, działania na wektorach, badanie niezależności wektorów. Wyznaczanie bazy, współrzędne wektora w bazie oraz obliczanie wymiaru przestrzeni.	2

Ćw2	Sprawdzanie warunków definicji przestrzeni liniowej. Wyznaczanie podprzestrzeni. Przekształcenia odwrotne oraz izomorfizm przestrzeni. Wyznaczanie macierzy odwzorowań liniowych.	2
Ćw3	Badanie unitarności macierzy oraz przestrzeni unitarnych. Klasyczne przykłady przestrzeni Hilberta oraz Banacha.	2
Ćw4	Sprawdzanie ortogonalności macierzy, wektorów – wyznaczanie bazy ortogonalnej. Przykładowe funkcjonały liniowe, konstrukcje przestrzeni funkcjonałów. Przestrzenie sprzężone.	2
Ćw5	Powtórzenie (zadania): funkcje wielu zmiennych, pochodne, całki i ekstrema funkcji wielu zmiennych. Liczby zespolone, działania. Przykłady funkcji zespolonych, badanie i własności	2
Ćw 6	Zadania na obliczanie pochodnej i funkcji zmiennej zespolonej.	2
Ćw7	Przykłady zastosowania w technice transformaty Laplace'a oraz Fouriera.	2
Ćw8	Kolokwium zaliczeniowe.	1
	Suma godzin	15

STOSOWANE NARZĘDZIA DYDAKTYCZNE

- N1. Wykład – metoda tradycyjna i z wykorzystaniem narzędzi multimedialnych
N2. Praca w grupach i indywidualna – samodzielne rozwiązywanie zadań
N3. Praca własna studenta – samodzielne rozwiązywanie list zadań
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	PEK_W01, PEK_W02, PEK_W03, PEK_W04.	Aktywność na wykładach, zaliczenie prac pisemnych (typu praca w grupach).
F2	PEK_U01, PEK_U02, PEK_U03, PEK_U04.	Zaliczenie prac pisemnych (kolokwia).
P=0.3*F1+0.7*F2, warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen F1 i F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] A. Białynicki-Birula, Algebra liniowa z geometrią, PWN Warszawa 1979.
[2] J. Długosz, Funkcje zespolone. Teoria, przykłady, zadania, GiS 2005.
[3] J. Musielak, Wstęp do analizy funkcjonalnej, PWN, 1976.
[4] S. Prus, A. Stachura, Analiza funkcjonalna w zadaniach, PWN 2009.
[5] J. Rusinek, Zadania z analizy funkcjonalnej, Wydawnictwo UKSW, Warszawa 2004.
[6] J. Rutkowski, Algebra liniowa w zadaniach, PWN 2008.

LITERATURA UZUPEŁNIAJĄCA:

- [1] M. Gewert, Z. Skoczylas, Algebra liniowa 2, Definicje, twierdzenia, wzory. Oficyna Wydawnicza GiS, Wrocław 2005.
[2] M. Gewert, Z. Skoczylas, Algebra liniowa 2, Przykłady i zadania. Oficyna Wydawnicza GiS, Wrocław 2005.

- [3] J. Górniak, T. Pytlik, Analiza funkcjonalna w zadaniach, Wydawnictwo Politechniki Wrocławskiej, Wrocław 1992.
- [4] R. Grzymkowski, R. Wituła, Wybrane zagadnienia z funkcji zespolonych i transformaty Laplace'a, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, 2001.
- [5] E. Kącki, L. Siewierski, Wybrane działy matematyki wyższej z ćwiczeniami. Wydawnictwo Wyższej Szkoły Informatyki w Łodzi, Łódź 2002.
- [6] F. Leja, Funkcje zespolone, PWN 1973.
- [7] W. Rudin, Analiza funkcjonalna, PWN 2016.
- [8] W. Rudin, Analiza rzeczywista i zespolona, PWN, Warszawa 1986.

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

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

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa w języku polskim:	Komunikacja społeczna
Nazwa w języku angielskim:	Social Communication
Kierunek studiów:	Automatyka i Robotyka, Elektronika, Informatyka, Telekomunikacja, Teleinformatyka, Cyberbezpieczeństwo
Poziom i forma studiów:	II stopień, stacjonarna
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	W08W04-SM0001S
Grupa kursów:	NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)					15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)					60
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)					1
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)					1

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

- C1 Student poznaje problematykę interdyscyplinarną z zakresu teorii kultury, teorii organizacji i zarządzania i teorii mediów oraz zagadnienia transdyscyplinarne z zakresu nauk humanistycznych i społecznych oraz inżyneryjno-technicznych ze szczególnym uwzględnieniem specyfiki kierunku studiów
- C2 Poprzez indywidualne opracowanie tematów Student poznaje główne narzędzia metodologiczne oraz wiedzę z zakresu komunikacji społecznej, teorii mediów, kultury i społeczeństwa jako podstawa orientacji we współczesnym procesie globalizacji ze wskazaniem głównych obszarów zastosowania w kontekście praktyki zawodowej inżyniera
- C3 Student poznaje główne teorie organizacji i zarządzania przy podkreśleniu uwarunkowań kulturowych systemów organizacyjnych oraz przy zastosowaniu metody porównawczej

C4 Poprzez prezentację wyników badań student poprawia kompetencje w zakresie pracy indywidualnej i grupowej w oparciu o wykorzystanie narzędzi komunikacji interpersonalnej

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu kompetencji:

PEK_U01	potrafi przygotować prezentację
PEK_U02	Student potrafi wykazać się wiedzą niezbędną od rozumienia społecznych, ekonomicznych, politycznych i prawnych uwarunkowań działalności inżynierskiej
PEK_U03	Student zna metody funkcjonowania instytucji i mechanizmów na gruncie polskimi międzynarodowym w przestrzeni politycznej, prawnej, gospodarczej i społecznej oraz ich uwzględnienia w praktyce inżynierskiej

TREŚCI PROGRAMOWE

Forma zajęć - seminarium		Liczba godzin
Sem1	Świat człowieka jako przestrzeń komunikacji. Orientacja transdyscyplinarna w kontekście cywilizacji, organizacji i mediów na styku nauk humanistycznych i społecznych oraz nauk inżynieryjno – technicznych.	3
Sem2	Cywilizacje jako przestrzeń rozwoju człowieczeństwa (humanitas). Czym jest cywilizacja i jak ją wyjaśniać? Definicje, dziedziny i teorie cywilizacji.	2
Sem3	Synergia czy zderzenie? Konsekwencje afirmacji wielości cywilizacji na kanwie porównawczej nauki o cywilizacjach.	2
Sem4	Proces organizacji społeczeństwa a wielość cywilizacji: indywidualizm a kolektywizm, organiczności a technokratyzm w kontekście porównawczej analizy kultur organizacyjnych.	2
Sem5	Główne teorie i praktyka zarządzania organizacjami	2
Sem6	Media jako główna przestrzeń i zasadniczy element komunikacji społecznej z typologią mediów przy uwzględnieniu uwarunkowań cywilizacyjnych i technologicznych na przykładzie koncepcji IoT, Przemysłu 4.0 i Społeczeństwa 5.0	2
Sem7	Pedagogika mediów, kompetencje społeczno-medialne i fenomeny: czyja odpowiedzialność za media? Fake-news i Post-prawda	2
Suma godzin		15

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	PEK_U01	prezentacja
F2	PEK_U02, PEK_U03	dyskusja

$P = 0.5 * F1 + 0.5 * F2$, gdzie $F1 > 2.0$ i $F2 > 2.0$

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] McQuail, Denis, *Teoria komunikowania masowego*, PWN, Warszawa 2007
- [2] Konersmann, Ralf, *Filozofia kultury*, Oficyna Naukowa, Warszawa 2009
- [3] Huntington, Samuel P., *Zderzenie cywilizacji*, Muza SA, Warszawa 2003
- [4] Kaliszewski, Andrzej, *Główne nurty w kulturze XX i XXI wieku*, Poltext, Warszawa 2012
- [5] Hofstede, Geert/ Hofstede, Geert Jan, *Kultury i organizacje*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2007
- [6] Griffin, Ricky W., *Podstawy zarządzania organizacjami*, PWN, Warszawa 2004
- [7] Levinson, Paul, *Nowe nowe media*, WAM, Kraków 2010
- [8] Briggs, Asa/ Burke Peter, *Společna historia mediów. Od Gutenberga do Internetu*, PWN, Warszawa 2010

LITERATURA UZUPEŁNIAJĄCA:

- [1] Koźmiński, A.K., Piotrowski, W., *Zarządzanie. Teoria i praktyka*, PWN, Warszawa 2000
- [2] Lepa, Adam, *Pedagogika mass-mediów*, Archidiecezjalne Wydawnictwo Łódzkie, Łódź 2000
- [3] Dusek, Val, *Wprowadzenie do filozofii techniki*, Wydawnictwo WAM, Kraków 2011
- [4] Stępień Tomasz, *Kultura, cywilizacja i historia. Geneza pojęć i teorii na kanwie sporu realizm vs. Antyrealizm*, [w:] Sikora, Marek (red.), *Realizm wobec wyzwań antyrealizmu. Multidyscyplinarny przegląd stanowisk*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2011

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

Dr Tomasz Stępień, Tomasz.stepien@pwr.edu.pl

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-SM0501G
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30			45	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	180				
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	7				
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)	3				

*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		
La2		
La3		
La4		
La5		
...		
	Suma godzin	

Forma zajęć - projekt		Liczba godzin
Pr1	Wprowadzenie do wybranego problemu / problemów analizy zagrożeń badanych w ramach projektu	2
Pr2	Wprowadzenie do Pythona	4
Pr3	Wprowadzenie do wybranych narzędzi obliczeniowych	3
Pr4	Omówienie przykładowych zagadnień projektowych	6
Pr5	Sformułowanie założeń, uszczegółowienie zadań dla poszczególnych grup projektowych	3
Pr6-13	Realizacja kolejnych etapów projektu (zebranie / preprocesiong danych / przygotowanie środowiska analizy / budowanie modeli dot. zagrożeń / badania empiryczne dot. wykrywania zagrożeń i anomalii, itd.)	21
Pr14	Dyskusja wyników, opracowanie dokumentacji projektowej	3
Pr15	Prezentacja i dyskusja wyników uzyskanych przez grupy projektowe	3
	Suma godzin	45

Forma zajęć - seminarium		Liczba godzin
Se1-7	Prezentacja wybranych szczegółowych zagadnień dot. wykorzystania metod AI w zadaniach związanych z cyberbezpieczeństwem – wybranych przykładów, metod, narzędzi. Prezentacje te mogą być związane ze specyfiką tematów / zadań realizowanych w części projektowej kursu.	15
	Suma godzin	15

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	Ocena wykonanych zadań projektowych,
F2	PEU_K01	Ocena prezentacji seminaryjnych
F3	PEU_W01-03	Kolokwium pisemne
P = 0.45*F1+0.4*F2+0.15*F3, o ile F1>2 i F2>2 i F3>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 (IMIE, NAZWISKO, ADRES E-MAIL)

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

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Monitorowanie i detekcja zagrożeń	
Nazwa przedmiotu w języku angielskim Monitoring and detection of cyberthreats	
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-SM0001G	
Grupa kursów TAK / NIE*	

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30			45	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	210				
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	7				
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)	4				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Wiedza z zakresu projektowania i działanie sieci komputerowych w tym: topologii, urządzeń i protokołów sieciowych
2. Umiejętności z zakresu konfiguracji urządzeń sieciowych

CELE PRZEDMIOTU

C1 Zaznajomienie z celami i potrzebami prowadzenia monitorowania infrastruktury IT oraz narzędziami wspomagającymi realizację monitorowania i detekcji zagrożeń.

C2. Nabycie umiejętności wdrażania monitorowania i detekcji zagrożeń w sieciach teleinformatycznych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna koncepcję oraz cele monitorowania i detekcji zagrożeń.

PEU_W02 Posiada wiedzę o sposobach i narzędziach do prowadzenia monitorowania i detekcji zagrożeń.

Z zakresu umiejętności:

PEU_U01 Potrafi planować i przygotowywać narzędzia do monitorowania i detekcji zagrożeń.

PEU_U02 Umie analizować dane pozyskane dzięki monitorowaniu i reagować na wykryte zagrożenia.

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. Cele i potrzeba monitorowania zagrożeń w sieciach teleinformatycznych.	2
Wy2-3	Współczesne architektury cyberbezpieczeństwa	4
Wy4	Monitorowanie bezpieczeństwa sieci	2
Wy5	Bezpieczeństwo urządzeń końcowych sieci	2
Wy6-7	Analiza ruchu sieciowego	4
Wy8-9	Narzędzia do analizy ruchu w sieci	4
Wy10	Wykrywanie incydentów	2
Wy11	Automatyzacja i ciągłe monitorowanie	2
Wy12-13	Narzędzia do monitorowania bezpieczeństwa	4
Wy14	Trendy i przyszłość	2
Wy15	Repetytorium.	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	Omówienie zasad realizacji zadania projektowego: zakres, temat, cele oraz formy projektu.	3
Pr2- Pr13	Realizacja projektu (przygotowanie rozwiązanie praktycznego dla postawionego projektu). Realizacja zadań cząstkowych zgodnie z harmonogramem projekt Dokumentowanie projektu (przygotowanie usystematyzowanej dokumentacji projektu).	36
Pr14- Pr15	Prezentacja rozwiązania problemu projektowego.	6
	Suma godzin	45

Forma zajęć - seminarium		Liczba godzin
Se1	Omówienie tematyki seminarium oraz zalecanych pozycji literaturowych.	1
Se2 – Se7	Prezentacje studentów dotyczące przedmiotowych zagadnień (cząstkowych/całkowitych). Dyskusja w grupie seminaryjnej.	12
Se8	Prezentacja końcowa problemu seminaryjnego Dyskusja w grupie seminaryjnej.	2
	Suma godzin	15

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład z wykorzystaniem slajdów oraz narzędzi symulacyjnych 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_U01-02	dokumentacja projektowa, wygłoszone prezentacje
F3	PEU_U03	prezentacja, omówienie tematu i dyskusja
$P=(F1+F2+F3)/3$		

warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] “The Practice of Network Security Monitoring: Understanding Incident Detection and Response”, Richard Bejtlich, No Starch Press 2013
- [2] “Applied Network Security Monitoring: Collection, Detection, and Analysis”, Chris Sanders, Syngress 2012
- [3] Network Forensics: Tracking Hackers through Cyberspace, Sherri Davidoff Jonathan Ham, Prentice Hall 2012

LITERATURA UZUPEŁNIAJĄCA:

- [1] “Zero Trust Networks: Building Secure Systems in Untrusted Networks”, Evan Gilman Doug Barth, O'Reilly Media 2017
- [2] “Defensive Security Handbook: Best Practices for Securing Infrastructure”, Lee Brotherston, O'Reilly Media 2017
- [3] Dokumentacja do: Wireshark
- [4] Dokumentacja do: Zeek
- [5] Dokumentacja do: Snort

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

Dr inż. Marcin Głowacki, marcin.glowacki@pwr.edu.pl

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Ochrona centrów danych	
Nazwa przedmiotu w języku angielskim Data center protection	
Kierunek studiów (jeśli dotyczy): Cyberbezpieczeństwo	
Specjalność (jeśli dotyczy): ...CBEU00201...	
Poziom i forma studiów:	I/ II stopień /jednolite studia magisterskie*, stacjonarna / niestacjonarna*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	W04CBE-SM0201G
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)	180	---	---	---	---
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)	3				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1.

CELE PRZEDMIOTU

- C1. Nabycie wiedzy z zakresu zabezpieczania wirtualnych i konwergentnych centrów danych - polityki, kontrakty i zarządzanie na wszystkich warstwach.
- C2. Poszerzenie umiejętności z zakresu zabezpieczania wirtualnych i konwergentnych centrów danych.

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 przeprowadzać oceny podatności w środowisku wirtualnym, audyty techniczne oraz analizę incydentów w wirtualnych i hybrydowych centrach danych.

Z zakresu kompetencji społecznych:

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Centra danych i chmury obliczeniowe – wprowadzenie.	1
Wy2	Cechy charakterystyczne chmur obliczeniowych – skalowalność zasobów. Model realizacji usług XaaS w chmurach obliczeniowych.	2
Wy3	Chmury publiczne, prywatne i hybrydowe. Standardy bezpieczeństwa dla środowisk chmurowych.	2
Wy4	Bezpieczeństwo infrastruktury w chmurach obliczeniowych. Koncepcja Software Defined Networks (SDN) – ochrona sieci wirtualnych.	2
Wy5	Ochrona w chmurach publicznych na przykładzie Amazon AWS IAM i AWS VPC	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	---	---
La2	---	---
La3	---	---
La4	---	---
La5	---	---

...		
	Suma godzin	---

Forma zajęć - projekt		Liczba godzin
Pr1	Omówienie zasad realizacji zadania projektowego: zakres, temat, cele oraz formy projektu.	2
Pr2-Pr13	Realizacja projektu (przygotowanie rozwiązanie praktycznego dla postawionego zadania). Realizacja zadań cząstkowych zgodnie z harmonogramem projektu Dokumentowanie projektu (przygotowanie usystematyzowanej dokumentacji projektu).	24
Pr14-Pr15	Prezentacja rozwiązania problemu projektowego.	4
	Suma godzin	30

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. Prezentacje multimedialne 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. Prezentacje cząstkowej. 2. Obrona projektu, zaliczenie.
$P=0,5 \cdot F1 + 0,5 \cdot F2$ <p>warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu</p>		

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)

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Ochrona systemów operacyjnych	
Nazwa przedmiotu w języku angielskim Operating Systems Protection	
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-SM0200G	
Grupa kursów TAK / NIE*	

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30			45	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	210				
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	7				
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)	3				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Ogólna znajomość budowy systemów operacyjnych
2. Praktyczna znajomość środowiska programowego Systemów Operacyjnych.
3. Podstawowa umiejętność programowania w języku C

CELE PRZEDMIOTU

- C1 Poznanie zbioru zagadnień związanych z aktywną ochroną Systemów Operacyjnych
 C2 Poznanie narzędzi i metod weryfikacji bezpieczeństwa i ochrony Systemów Operacyjnych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01. Znajomość zbioru zagadnień składających się na bezpieczeństwo popularnych systemów operacyjnych. Znajomość metod ataków i zagrożeń, znajomość metod wykrywania zagrożeń. Znajomość metod i narzędzi służących weryfikacji poziomu bezpieczeństwa systemów Microsoft i Unix i poprawy bezpieczeństwa tych systemów.

PEU_W02

...

Z zakresu umiejętności:

PEU_U01 Praktyczna znajomość systemów i narzędzi służących weryfikacji bezpieczeństwa systemów operacyjnych, oraz metod poprawy ochrony tych systemów.

PEU_U02

...

Z zakresu kompetencji społecznych:

PEU_K01 Zrozumienie zasad etyki wymaganej podczas wykonywania prac związanych z uzyskaniem dostępu do systemów i poufnych danych instytucji i osób trzecich.

PEU_K02

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Ochrona a bezpieczeństwo – zbiór zagadnień, cele i tematyka wykładu, wymagania, literatura.	2
Wy2	PowerShell – informacje, podstawy programowania, zastosowanie.	2
Wy3	Eksploity. Platforma Metasploit.	2
Wy4	Wykorzystywanie exploitów do ataków.	2
Wy5	Architektura bezpiecznych sieci – metody i narzędzia do testowania.	2
Wy6	Podatności systemów na ataki – testy penetracyjne	2
Wy7	Działania w zakresie zwiększania bezpieczeństwa systemów – monitorowanie, detekcja ataków	2
Wy8	Analiza szkodliwego oprogramowania malware – metody, narzędzia.	2
Wy9	Ochrona sieci bezprzewodowych, narzędzia testujące.	2
Wy10	Architektura i ochrona aplikacji WWW.	2
Wy11	Łamanie haseł – narzędzia, metody	2
Wy12	Zabezpieczanie systemów Windows z użyciem PowerShell	2
Wy13	Zabezpieczanie systemów Linux/Unix/iOS	2
Wy14	Zbieranie dowodów ataków, reakcja na incydenty.	2
Wy15	Opracowywanie wyników, raportowanie o zagrożeniach	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- Pr5	Praktyczne poznanie programowania w języku PowerShell. Opracowanie i napisanie programu zabezpieczającego wskazaną przez prowadzącego podatność w systemie Windows.	15
Pr6 – Pr10	Praktyczne poznanie platformy Metasploit. Opracowanie i przeprowadzenie ataku na wskazany system testowy z użyciem exploitów.	15
Pr11 - Pr14	Opracowanie metody wybór narzędzi i przeprowadzenie procesu łamania haseł w środowisku testowego systemu Unix.	12
Pr15	Podsumowanie efektów i wyników oraz ocena wykonanych projektów.	3
...		
	Suma godzin	45

Forma zajęć - seminarium		Liczba godzin
Se1	Prowadzący - Wprowadzenie do zajęć, ustalenie zasad prezentacji i zasad oceny.	1
Se2 – Se 14	Studenci - Prezentacje z postępów prac w ramach projektu.	13
Se15	Podsumowanie, dyskusja i ustalenie ocen z prezentacji.	1
...		
	Suma godzin	15

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład – prezentacja z wykorzystaniem przykładów z użyciem omawianych systemów i narzędzi.
N2. System operacyjny Kali Linux – dostępny podczas zajęć projektowych, pożądana instalacja na komputerach studentów.
N3. Testowe systemy operacyjne Windows i Linux, oraz testowa sieć lokalna z wybranymi urządzeniami sieciowymi dostępna dla studentów.
N4. Konsultacje i dyskusje podczas zajęć projektowych.

- N5. Praca własna – przygotowanie do projektu
 N6. Praca własna – opracowanie prezentacji i przedstawienie wyników wykonanych projektów
 N7. 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		Test końcowy z wykładu
F2		Średnia ocen z wykonanych projektów
F3		Ocena z seminarium na podstawie referatów
P = 40% test końcowy wykład + 50% ocena z projektu + 10% ocena z seminarium Test końcowy zaliczony jeśli wynik $\geq 55\%$. Ocena z projektu $\geq 3,0$. Ocena z seminarium $\geq 3,0$		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] Stallings William , Brown Lawrie , Computer Security: Principles and Practice, Global Edition. 2018r.
- [2] Stallings William , Brown Lawrie , Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Tom 1 i Tom 2, Wydawnictwo Helion (tłumaczenie pozycji 1) 2019r.
- [3] Lee Brotherston, Amanda Berlin, Bezpieczeństwo defensywne. Podstawy i najlepsze praktyki. Wydawnictwo Helion. 2018r.

LITERATURA UZUPEŁNIAJĄCA:

- [1] Ric Messier, Kali Linux. Testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie. Wydawnictwo Helion S.A. 2019r.
- [2] Krzysztof Liderman, Bezpieczeństwo informacyjne. Wydawnictwo Naukowe PWN, 2017r.
- [3] Internet: www.offensive-security.com

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

Dr inż. Zbigniew Soltys, zbigniew.soltys@pwr.edu.pl

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	
Poziom i forma studiów: I/ II stopień /jednolite studia magisterskie*, stacjonarna / niestacjonarna*	
Rodzaj przedmiotu: obowiązkowy / wybieralny /ogólnouczelniany *	
Kod przedmiotu W04CBE-SM0008D	
Grupa kursów TAK / NIE	

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)				150	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)				360	
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)				6	

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Umiejętność przygotowania przeglądu literatury i precyzowania problemu badawczego
2. Podstawowe wiedza dotycząca struktur danych i algorytmów oraz programowania
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 z zakresu wiedzy dotyczącej tematyki pracy dyplomowej
- C3 Nabycie umiejętności przygotowania eksperymentów, weryfikacji i opracowania wyników przeprowadzonych badań
- 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_U03 – Potrafi — zgodnie z zadaną specyfikacją — zaprojektować i zrealizować (przynajmniej w części) złożony system informatyczny mający na celu ekstrakcję wiedzy z 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.

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	50
Pr2	Przeprowadzenie badań i opracowanie wyników	50
Pr3	Opracowanie dokumentacji (pracy pisemnej) pracy	50
...		
	Suma godzin	150

Forma zajęć - seminarium		Liczba godzin
Se1		
Se2		
Se3		

...		
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Środowisko eksperymentalne 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_U03 PEU_K01	Ocena końcowa związana z oceną przygotowanej pracy dyplomowej. Ocenie podlegać umiejętność zdefiniowania problemu, przeglądu stanu wiedzy i techniki, zaproponowania poprawnej metody, zaprojektowanie i przeprowadzenie eksperymentu, krytyczna analiza wyników.

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
<u>LITERATURA PODSTAWOWA</u>
[1] Regulamin procesu dyplomowania na Wydziale Informatyki i Telekomunikacji Politechniki Wrocławskiej
[2] Formatka pracy dyplomowej przygotowania przez WIT PWr
[3] Dokumentacja programu Plagiat.pl
<u>LITERATURA UZUPEŁNIAJĄCA:</u>
OPIEKUN PRZEDMIOTU (IMIE, NAZWISKO, ADRES E-MAIL)
Prof. dr hab. inż. Tadeusz Więckowski, Tadeusz.wieckowski@pwr.edu.pl

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa w języku polskim:	Przedsiębiorczość w ICT
Nazwa w języku angielskim:	ICT Business
Kierunek studiów:	Cyberbezpieczeństwo
Poziom i forma studiów:	II stopień, Ogólnoakademicki
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	W04CBE-SM0005G
Grupa kursów:	TAK

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30			15	
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	60			30	
Forma zaliczenia	Zaliczenie na ocenę			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)	-			1	
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	1			1	

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

- C1 Poznanie rynku teleinformatycznego
- C2 Nabycie wiedzy dotyczącej parametrów ekonomicznych i zasad działalności biznesowej
- C3 Nabycie wiedzy dotyczącej metodyk zarządzania projektami teleinformatycznymi
- C4 Nabycie umiejętności definiowania elementów zarządzania projektem

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEK_W01 Zna charakterystykę rynku teleinformatycznego i metodykę realizacji projektów teleinformatycznych.

Z zakresu umiejętności:

PEK_U01 Potrafi korzystać z raportów o stanie rynku teleinformatycznego Umie przygotować projekcje finansowe. Potrafi opracować biznes plan. Umie zdefiniować elementy zarządzania projektem

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wprowadzenie	2
Wy2	Formy prowadzenia działalności gospodarczej	2
Wy3	Prawo telekomunikacyjne - uprawnienia do prowadzenia działalności	2
Wy4	Rynek teleinformatyczny – podstawy	2
Wy5	Analiza rynku telekomunikacyjnego	2
Wy6	Elementy planowania działalności – rynek, marketing, ceny	2
Wy7	Elementy planowania działalności – nakłady i koszty, finansowanie	2
Wy8	Planowanie działalności telekomunikacyjnej – elementy biznes planu	2
Wy9	Projekcje finansowe – sprawozdania finansowe	2
Wy10	Przykład działalności teleinformatycznej – analiza przypadku	2
Wy11	Metodyki zarządzania projektami teleinformatycznymi – główne zasady	2
Wy12	Fazy zarządzania projektem teleinformatycznym	2
Wy13	Definiowanie projektu i tworzenie zespołu projektowego	2
Wy14	Harmonogram realizacji i komunikacja w projekcie	2
Wy15	Repetytorium	2
Suma godzin		30

Forma zajęć - projekt		Liczba godzin
Pr1	Omówienie zasad realizacji zadania projektowego: zakres, temat, cele oraz formy projektu.	2
Pr2 – Pr13	Realizacja projektu (przygotowanie rozwiązania praktycznego dla postawionego zadania). Realizacja zadań cząstkowych zgodnie z harmonogramem projektu. Dokumentowanie projektu (przygotowanie usystematyzowanej dokumentacji projektu).	11
Pr14- Pr15	Prezentacja rozwiązań problemu projektowego.	2
Suma godzin		15

STOSOWANE NARZĘDZIA DYDAKTYCZNE

- N1. Wykład tradycyjny z wykorzystaniem prezentacji multimedialnych
- N2. Prezentacja syntetyczna każdego tematu
- N3. Prezentacja studenta, dyskusja oraz ocena prezentacji
- N4. Elektroniczna wersja prezentacji
- N5. Konsultacje
- 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	PEK_W01	Kolokwium zaliczające
F2	PEK_W01 PEK_U01	Ocena realizacji zadania projektowego przygotowanego przez studenta
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] Piątek S., Prawo telekomunikacyjne - Komentarz”, Wydanie 2, C.H.Beck, Warszawa 2005.
- [2] Hawawini G., Viallet, Finanse menedżerskie, PWE, Warszawa 2007.
- [3] Fiore F.F., Jak szybko przygotować biznesplan, Wolters Kluwer, Kraków 2006.
- [4] Janiszewski J.M. (red.), Budowa sieci szerokopasmowych. Planowanie i przygotowanie koncepcji. Poradnik dla samorządowców, Fundacja Wspierania Wsi, Warszawa 2008.
- [5] Snedaker S., Zarządzanie projektami IT w małym palcu, Helion, Gliwice 2007.

LITERATURA UZUPEŁNIAJĄCA:

- [1] Brigham E.F., Gapenski L.C., Zarządzanie finansami, PWE, Warszawa 2000.
- [2] Yoffie D.B., Cusano M.A., Zasady strategii. Bill Gates, Andy Grove i Steve Jobs. Pięć ponadczasowych lekcji. Dom Wydawniczy Rebis, Poznań 2016.
- [3] Isaacson W., Steve Jobs, Insignis Media, Kraków 2013.
- [4] Bradley K., Podstawy metodyki PRINCE2, Centrum rozwiązań menedżerskich, Warszawa 2002.

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

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

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	Seminarium dyplomowe
Nazwa w języku angielskim:	Graduate Seminar
Kierunek studiów:	Cyberbezpieczeństwo
Poziom i forma studiów:	II stopień, stacjonarna
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	W04CBE-SM0007S
Grupa kursów:	NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)					30
Liczba godzin całkowitego nakładu pracy studenta (CNPS)					90
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)					3
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)					2

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

- C1 Nabycie umiejętności poszukiwania selektywnej wiedzy niezbędnej do tworzenia własnych oryginalnych rozwiązań.
- C2 Zdobywanie 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.
- C5. Nabycie świadomości odpowiedzialnego pełnienia ról zawodowych w obszarze cyberbezpieczeństwa z uwzględnieniem zmieniających się potrzeb społecznych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 posiada wiedzę o zasadach przygotowania i napisania dzieła prezentującego własne rozwiązania naukowo-techniczne

PEU_W02 posiada wiedzę o aktualnym stanie rozwoju systemów cyberbezpieczeństwa

Z zakresu umiejętności:

PEU_U01 potrafi przygotować prezentację zawierającą wyniki własnych oryginalnych badań

PEU_U02 potrafi w dyskusji rzeczowo uzasadnić swoje oryginalne pomysły i rozwiązania

PEU_U03 potrafi krytycznie ocenić rozwiązania naukowo-techniczne innych osób

Z zakresu kompetencji:

PEU_K01 ma świadomość odpowiedzialnego pełnienia ról zawodowych w obszarze

cyberbezpieczeństwa z uwzględnieniem zmieniających się potrzeb społecznych

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_W02, PEU_U01	prezentacja
F2	PEU_W01, PEU_U02, PEU_U03	dyskusja
P= 0.5 F1+0.5 F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
Literatura związana z problematyką pracy dyplomowej
OPIEKUN PRZEDMIOTU (IMIE, NAZWISKO, ADRES E-MAIL)
dr inż. Jarosław Janiszewski, prof. uczelni, jaroslaw.janiszewski@pwr.edu.pl

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	Seminarium kierunkowe
Nazwa w języku angielskim:	Cybersecurity Maintenance Seminar
Kierunek studiów:	Cyberbezpieczeństwo
Profil:	ogólnouczelniany / praktyczny*
Poziom i forma studiów:	II stopień, stacjonarna
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	W04CBE-SM0006S
Grupa kursów:	NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	—	—	—	—	30
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	—	—	—	—	90
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

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

- C1. Wykształcenie umiejętności poprawnego wykorzystywania dostępnych źródeł bibliograficznych, wnioskowania oraz prezentacji wyników
- C2. Wykształcenie umiejętności poprawnej prezentacji wyników studiów własnych nad opracowywanym zagadnieniem z zakresu cyberbezpieczeństwa

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu umiejętności:

PEU_W01 – posiada aktualną wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w obszarze cyberbezpieczeństwa

Z zakresu umiejętności:

PEU_U01 – potrafi odpowiednio wykorzystywać, cytować i opisywać źródła bibliograficzne

PEU_U02 – potrafi biegłe wykorzystywać dostępne narzędzia multimedialne pomocne podczas przygotowywania prezentacji multimedialnych

PEU_U03 – potrafi odpowiednio prezentować wyniki wykonanych prac z uwzględnieniem: rygorów czasowych, poziomu wiedzy odbiorców oraz przyjętych standardów z zakresu umiejętności komunikacji

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.	2
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 – część I	2
Se6	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych – część I	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
Se9	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se10	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se11	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se12	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se13	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se14	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia –	2

	część II	
Se15	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
	Suma godzin	30

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
N1. Narzędzia programistyczne do przygotowywania prezentacji multimedialnych	
N2. Konsultacje	
N3. Praca własna – przygotowanie multimedialnej prezentacji wyników pracy własnej	

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_U01-03	Prezentacja wstępna wyników (część I)
F2	PEU_W01 PEU_U01-03	Prezentacja końcowa wyników (część II)
P=0,3·F1+0,7·F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
<u>LITERATURA PODSTAWOWA:</u> Literatura, w tym artykuły naukowe, związana z przydzielonym tematem.

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

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa w języku polskim:	Seminarium Specjalnościowe
Nazwa w języku angielskim:	Teleinformatic Networks Maintenance Seminar
Kierunek studiów:	Teleinformatyka
Specjalność:	Utrzymanie Sieci Teleinformatycznych
Profil:	ogólnouczelniany / praktyczny*
Poziom i forma studiów:	II stopień, stacjonarna
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	W04TIN-SM0205S
Grupa kursów:	NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	—	—	—	—	30
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	—	—	—	—	60
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

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

- C1. Wykształcenie umiejętności poprawnego wykorzystywania dostępnych źródeł bibliograficznych, wnioskowania oraz prezentacji wyników
- C2. Wykształcenie umiejętności poprawnej prezentacji wyników studiów własnych nad opracowywanym zagadnieniem z zakresu teleinformatyki

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu umiejętności:

PEU_W01 – posiada aktualną wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w obszarze teleinformatyki

Z zakresu umiejętności:

PEU_U01 – potrafi odpowiednio wykorzystywać, cytować i opisywać źródła bibliograficzne

PEU_U02 – potrafi biegłe wykorzystywać dostępne narzędzia multimedialne pomocne podczas przygotowywania prezentacji multimedialnych

PEU_U03 – potrafi odpowiednio prezentować wyniki wykonanych prac z uwzględnieniem: rygorów czasowych, poziomu wiedzy odbiorców oraz przyjętych standardów z zakresu umiejętności komunikacji

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.	2
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 – część I	2
Se6	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych – część I	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
Se9	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se10	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se11	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se12	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se13	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
Se14	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia –	2

	część II	
Se15	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych, ocena zawartości merytorycznej oraz jakości wystąpienia – część II	2
	Suma godzin	30

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
N1. Narzędzia programistyczne do przygotowywania prezentacji multimedialnych	
N2. Konsultacje	
N3. Praca własna – przygotowanie multimedialnej prezentacji wyników pracy własnej	

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_U01-03	Prezentacja wstępna wyników (część I)
F2	PEU_W01 PEU_U01-03	Prezentacja końcowa wyników (część II)
P=0,3·F1+0,7·F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
<u>LITERATURA PODSTAWOWA:</u> Literatura, w tym artykuły naukowe, związana z przydzielonym tematem.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)
dr inż. Robert Czechowski, Robert.czechowski@pwr.edu.pl

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-SM0002G	
Grupa kursów TAK / NIE*	

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30			45	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	210				
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	7				
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)	4				

*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 prowadzenia 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.	2
Wy2	Metodologia. Planowanie i określanie celów i zakresu testów penetracyjnych.	2
Wy3	Ataki na infrastrukturę sieciową. Rekonesans – odkrywanie i mapowanie.	2
Wy4-5	Głębokie skanowanie i wykrywanie celów. Szukanie podatności i luk bezpieczeństwa.	4
Wy6-7	Wykorzystywanie exploitów w celu naruszenia bezpieczeństwa po stronie klienta i po stronie usługi. Eskalacja lokalnych uprawnień na komputerach.	4
Wy8-10	Testowanie konfiguracji i mechanizmów uwierzytelniania. Nieatoryzowany dostęp i łamanie haseł.	6
Wy11-12	Manipulowanie aplikacjami internetowymi. Testy prowadzone metodą wstrzykiwania komend, plików i zapytań SQL.	4
Wy13-14	Metody wykrywania podatności aplikacji Web, tj. Cross-Site Scripting (XSS) i Cross-Site Request Forgery (CSRF/XSRF).	4
Wy15	Repetitorium.	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	Podział na grupy i rozdział tematów projektów.	3
Pr2	Uszczegółowienie tematów oraz zakresu prac projektowych.	3
Pr3-Pr5	Praca koncepcyjna w zakresie planowania testów penetracyjnych.	9
Pr6-Pr8	Przygotowanie procedur testowych.	9
Pr9-Pr11	Przygotowanie infrastruktury do przeprowadzenia wybranych testów penetracyjnych.	9
Pr12-Pr14	Przeprowadzenie wybranych testów penetracyjnych i analiza wyników.	9
Pr15	Przygotowanie dokumentacji projektowej	3
	Suma godzin	45

Forma zajęć - seminarium		Liczba godzin
Se1	Podział na grupy i rozdział tematów	1
Se2-Se4	Wstępne prezentacje założeń dla scenariuszy oraz metod przeprowadzania testów penetracyjnych.	6
Se5-Se8	Finałowe prezentacje scenariuszy oraz metod przeprowadzania testów penetracyjnych.	8
	Suma godzin	15

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	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
---	---------------------------------	--

– podsumowująca (na koniec semestru)		
F1	PEU_W01-02	dyskusje, kolokwium końcowe
F2	PEU_U01-02	dokumentacja projektowa, wygłoszone prezentacje
F3	PEU_U03	prezentacja, omówienie tematu i dyskusja
$P=(F1+F2+F3)/3$ warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] SANS: SEC560: Network Penetration Testing and Ethical Hacking
- [2] SANS: SEC542: Web App Penetration Testing and Ethical Hacking
- [3] “Professional Penetration Testing”, Thomas Wilhelm, Elsevier 2010
- [4] “Penetration testing and Network Defense” – Andrew Whitaker, Daniel Newman, Cisco Press 2006

LITERATURA UZUPEŁNIAJĄCA:

- [1] Dokumentacja do: Dynamic Application Security Testing (DAST)
- [2] Dokumentacja do: Nessus
- [3] Dokumentacja do: OWASP ZAP (Zed Attack Proxy Project)
- [4] Dokumentacja do: Static Application Security Testing (SAST)
- [5] Dokumentacja do: Checkmarx
- [6] Dokumentacja do: SonarQube

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

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

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Zaawansowane testy penetracyjne sieci i aplikacji Web	
Nazwa przedmiotu w języku angielskim Advanced pentesting of networks and web applications	
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-SM0301G
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30			45	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	210				
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	7				
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)	4				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

- 1.
- 2.
- 3.

CELE PRZEDMIOTU

C1 Zaznajomienie z wiedzą, narzędziami i technikami wykonywania zaawansowanych 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 zaawansowanych testów penetracyjnych.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna koncepcję oraz cele zaawansowanego testowania penetracyjnego.

PEU_W02 Posiada wiedzę o sposobach i narzędziach do prowadzenia zaawansowanych testów penetracyjnych.

Z zakresu umiejętności:

PEU_U01 Potrafi planować i przygotowywać procedury zaawansowanego testowania penetracyjnego.

PEU_U02 Umie przeprowadzać zaawansowane 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
Wy1-2	Zaawansowane ataki sieciowe.	4
Wy3-4	Testy penetracyjne związane z technikami kryptograficznymi.	4
Wy5-6	Użycie skryptowych języków programowania w testowaniu penetracyjnym.	4
Wy7-8	Badanie podatności aplikacji na ataki w systemach Linux.	4
Wy9-10	Badanie podatności aplikacji na ataki w systemach MS Windows.	4
Wy11-12	Ataki na aplikacje serwerowe z użyciem LFI / RFI i SQLi. Kombinacje ataków XSS i XSRF.	4
Wy13	Zaawansowane ataki na aplikacje Webowe.	2
Wy14	Omijanie filtrów pakietowych dla usług Webowych	2
Wy15	Repetitorium.	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	Podział na grupy i rozdział tematów projektów.	3
Pr2	Uszczegółowienie tematów oraz zakresu prac projektowych.	3
Pr3- Pr5	Praca koncepcyjna w zakresie planowania testów penetracyjnych.	9
Pr6- Pr8	Przygotowanie procedur testowych.	9
Pr9- Pr11	Przygotowanie infrastruktury do przeprowadzenia wybranych zaawansowanych testów penetracyjnych.	9
Pr12- Pr14	Przeprowadzenie wybranych zaawansowanych testów penetracyjnych i analiza wyników.	9
Pr15	Przygotowanie dokumentacji projektowej	3
	Suma godzin	45

Forma zajęć - seminarium		Liczba godzin
Se1	Podział na grupy i rozdział tematów	1
Se2- Se4	Wstępne prezentacje założeń dla scenariuszy oraz metod przeprowadzania testów penetracyjnych.	6
Se5- Se8	Finałowe prezentacje scenariuszy oraz metod przeprowadzania testów penetracyjnych.	8
	Suma godzin	15

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_U01-02	dokumentacja projektowa, wygłoszone prezentacje
F3	PEU_U03	prezentacja, omówienie tematu i dyskusja
$P=(F1+F2+F3)/3$ warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] SANS: SEC660: Network Penetration Testing and Ethical Hacking
- [2] SANS: SEC642: Web App Penetration Testing and Ethical Hacking
- [3] “Professional Penetration Testing”, Thomas Wilhelm, Elsevier 2010
- [4] “Penetration testing and Network Defense” – Andrew Whitaker, Daniel Newman, Cisco Press 2006

LITERATURA UZUPEŁNIAJĄCA:

- [1] Dokumentacja do: Dynamic Application Security Testing (DAST)
- [2] Dokumentacja do: Nessus
- [3] Dokumentacja do: OWASP ZAP (Zed Attack Proxy Project)
- [4] Dokumentacja do: Static Application Security Testing (SAST)
- [5] Dokumentacja do: Checkmarx
- [6] Dokumentacja do: SonarQube

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

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

WYDZIAŁ Informatyki i Telekomunikacji	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim Zarządzanie bezpieczeństwem informacji	
Nazwa przedmiotu w języku angielskim Information security management	
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-SM0004G
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15	---	---	45	15
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	180	---	---	---	---
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)	3				

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Wiedza z zakresu kodowania i szyfrowania,
2. Wiedza z zakresu ochrony informacji
3. Poszerzona wiedza z zakresu organizacji infrastruktury informatycznej i oprogramowania

CELE PRZEDMIOTU

- C1. Nabycie wiedzy z zakresu organizacji systemu ochrony informacji
- C2. Poszerzenie 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:

PEU_W01 Posiada wiedzę na temat norm i regulacji w zakresie bezpieczeństwa informacji

PEU_W02 Posiada wiedzę z zakresu zarządzania, bezpieczeństwa i ochrony informacji

PEU_W02 Posiada wiedzę z zakresu metod kryptograficznych stosowanych w ochronie informacji

Z zakresu umiejętności:

PEU_U01 Potrafi zastosować normy bezpieczeństwa do chronionych systemów

PEU_U02 Potrafi wdrożyć Systemu Zarządzania Bezpieczeństwem Informacji.

PEU_U02 Potrafi wdrożyć adekwatne rozwiązania kryptograficzne do ochrony informacji

Z zakresu kompetencji społecznych:

PEU_K01 Potrafi wykorzystywać zewnętrzne źródła wiedzy w zakresie bezpieczeństwa informacji

PEU_K02 Posiada umiejętności do współpracy z właścicielami aktywów informatycznych

PEU_K03 Potrafi określić wpływ wykształcenia kadry informatycznej na bezpieczeństwo systemu

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Uwarunkowania normatywne ochrony informacji, normy ISO.	2
Wy2	Pojęcie Systemu Zarządzania Bezpieczeństwem Informacji. Organizacja bezpieczeństwa informacji.	2
Wy3	Zarządzanie aktywami informacyjnymi i informatycznymi.	2
Wy4	Ochrona informacji w procesie prowadzenia projektu IT.	2
Wy5	Kontrola dostępu. Bezpieczeństwo zasobów ludzkich.	2
Wy6	Polityki bezpieczeństwa informacji.	2
Wy7	Zastosowanie kryptografii.	2
Wy8	Kolokwium zaliczeniowe	1
	Suma godzin	

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	Omówienie zasad realizacji zadania projektowego: zakres, temat, cele oraz formy projektu.	3
Pr2- Pr13	Realizacja projektu (przygotowanie rozwiązanie praktycznego dla postawionego projektu). Realizacja zadań cząstkowych zgodnie z harmonogramem projekt Dokumentowanie projektu (przygotowanie usystematyzowanej dokumentacji projektu).	36
Pr14- Pr15	Prezentacja rozwiązania problemu projektowego.	6
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1	Omówienie tematyki seminarium oraz zalecanych pozycji literaturowych.	1
Se2 – Se7	Prezentacje studentów dotyczące przedmiotowych zagadnień (cząstkowych/całkowitych). Dyskusja w grupie seminaryjnej.	12
Se8	Prezentacja końcowa problemu seminaryjnego Dyskusja w grupie seminaryjnej.	2
	Suma godzin	

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład problemowy N2. Studia literaturowe N3. Opracowanie pisemne N4. Dyskusja problemowa N5. Prezentacje multimedialne 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 PEU_W02 PEU_W03	1. Pisemne zaliczenie.
F2	PEU_U01 PEU_U02 PEU_U03 PEU_K01	1. Prezentacje cząstkowej. 2. Obrona projektu, zaliczenie.

F3	PEU_K01 PEU_K02 PEU_K03 PEU_W01 PEU_W02 PEU_W03	1. Ocena wykonanych prezentacji, dyskusje. 2. Zaliczenie.
$P=0,5*F1+0,25*F2+0,25*F3$ warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnych ocen z wszystkich form zajęć prowadzonych w ramach kursu		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
<p><u>LITERATURA PODSTAWOWA:</u></p> <p>[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 2014</p> <p><u>LITERATURA UZUPEŁNIAJĄCA:</u></p> <p>[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.</p>
OPIEKUN PRZEDMIOTU (IMIE, NAZWISKO, ADRES E-MAIL)
Mgr inż. Marcin Kaczmarek, marcin.kaczmarek@pwr.edu.pl