

PROGRAM STUDIÓW

WYDZIAŁ: ELEKTRONIKI

KIERUNEK STUDIÓW: CYBERBEZPIECZEŃSTWO

Przyporządkowany do dyscypliny: **informatyka techniczna i telekomunikacja**

POZIOM KSZTAŁCENIA: studia drugiego stopnia (magisterskie)

FORMA STUDIÓW: stacjonarna

PROFIL: ogólnoakademicki

JĘZYK PROWADZENIA STUDIÓW: polski

Zawartość:

1. Zakładane efekty uczenia się – załącznik nr 1 do programu studiów
2. Opis programu studiów – załącznik nr 2 do programu studiów

Uchwała nr **30/03/2020-2024** Senatu PWr z dnia **19.11.2020 r.**

Obowiązuje od roku akademickiego 2020/2021

ZAKŁADANE EFEKTY UCZENIA SIĘ

Wydział: Elektroniki

Kierunek studiów: Cyberbezpieczeństwo

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

Profil: ogólnoakademicki / ~~praktyczny*~~

Umiejscowienie kierunku

Dziedzina nauki: ...nauki 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, umożliwiających 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	Zna cykl rozwoju oraz współczesne metodyki rozwoju oprogramowania, a także trendy w programowaniu, w tym algorytmy sztucznej inteligencji.	P7U_W	P7S_WG	
K2CBE_W04	Umie scharakteryzować rynek teleinformatyczny. Potrafi opisać model biznesowy działalności teleinformatycznej i objaśniać ekonomiczne podstawy działalności gospodarczej, rozpoznawać kondycję finansową firmy, określić strategię marketingową i sposób określania cen produktów i usług.	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
UMIEJĘTNOŚCI (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 tworzyć, analizować i testować oprogramowanie pod kątem bezpieczeństwa, potrafi stosować algorytmy sztucznej inteligencji.	P7U_U	P7S_UW P7S_UO	
K2CBE_U04	Ma umiejętności i kompetencje zgodne z wymaganiami dla określonego poziomu ESOKJ w zakresie języka naukowo-technicznego związanego ze studiowaną dyscypliną i pokrewnymi zagadnieniami	P7U_U	P7S_UW	
K2CBE_U05	Potrafi myśleć krytycznie i argumentować swoje stanowisko Jest w stanie interpretować trendy rynkowe, przygotować projekcje finansowe i opracować biznes plan.	P7U_U	P7S_UK P7S_UO	
K2CBE_U06	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	
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	

Kierunek studiów Cyberbezpieczeństwo
Poziom studiów studia drugiego stopnia

OPIS PROGRAMU STUDIÓW

Profil ogólnoakademicki
Forma Studiów stacjonarna

Zał. nr 3 do ZW 8/2020
Zał. nr 2 do Programu studiów

1. Opis ogólny

<p>1.1 Liczba semestrów: 3</p>	<p>1.2 Całkowita liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie: 90</p>
<p>1.3 Łączna liczba godzin zajęć: 1080</p>	<p>1.4 Wymagania wstępne (w szczególności w przypadku studiów drugiego stopnia): Kandydaci na studia magisterskie na kierunku Cyberbezpieczeństwo mogą rekrutować się po uzyskaniu co najmniej tytułu inżyniera na następujących kierunkach: Cyberbezpieczeństwo, Teleinformatyka, Telekomunikacja, Informatyka techniczna, Informatyka stosowana, Informatyka algorytmiczna. Kandydat na studia powinien mieć przede wszystkim ugruntowaną wiedzę z zakresu utrzymania sieci teleinformatycznych ze szczególnym naciskiem na aspekt bezpieczeństwa. Ponadto powinien rozumieć zagadnienia bezpieczeństwa cybernetycznego systemów operacyjnych, systemów chmurowych oraz umieć podejmować działania zmierzające do poprawy bezpieczeństwa tych systemów. Powinien również biegle programować w co najmniej jednym języku programowania wysokiego poziomu.</p>

<p>1.5 Tytuł zawodowy nadawany po zakończeniu studiów: Magister Inżynier</p>	<p>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.</p>
<p>1.7 Możliwość kontynuacji studiów: Po ukończeniu studiów drugiego stopnia na kierunku Cyberbezpieczeństwo istnieje możliwość kontynuacji kształcenia w szkole doktorskiej lub na studiach podyplomowych.</p>	<p>1.8 Wskazanie związku z misją Uczelni i strategią jej rozwoju: Program studiów kierunku Cyberbezpieczeństwo na studiach stacjonarnych drugiego stopnia jest w pełni skorelowany z misją uczelni i strategią jej rozwoju przyjętą przez Senat Politechniki Wrocławskiej dnia 21 marca 2013 roku (Uchwała nr 127/7/2012-2016) i późniejszymi zmianami (Uchwała nr 227/11/2012-2016 i Uchwała nr 759/34/2012-2016).</p>

2. Opis szczegółowy

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

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

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

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 z prowadzoną działalnością 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

Zakładane efekty kształcenia są zgodne z potrzebami rynku pracy. Takie stanowisko jest uprawomocnione wynikami analiz potrzeb rynku pracy, zawartych w następujących opracowaniach:

- „Analiza zapotrzebowania gospodarki na absolwentów kierunków kluczowych w kontekście realizacji strategii Europa 2020” – wykonana w kwietniu 2012.
- "Prognoza zapotrzebowania gospodarki regionu na siłę roboczą w układzie sektorowo-branżowym i kwalifikacyjno-zawodowym w województwie dolnośląskim", w szczególności raport pt. Analiza zapotrzebowania na kadry w branżach uznanych za strategiczne dla dolnośląskiego rynku pracy” w ramach Regionalnej Strategii Innowacji na lata 2011-2020 – opracowanie udostępnione w 2010.
- Raport końcowy „Sytuacja na dolnośląskim rynku pracy – badanie zapotrzebowania na zawody, kwalifikacje i umiejętności” oraz raporty cząstkowe pt. : „Badanie oferty dolnośląskiego rynku edukacji zawodowej” i „Analiza potencjału dolnośląskich Powiatów i Gmin w zakresie rynku pracy i edukacji” – opracowania w ramach projektu pt. „Obserwatorium Dolnośląskiego Rynku Pracy i Edukacji” realizowanego w ramach poddziałania 6.1.2 Programu Operacyjnego Kapitał Ludzki współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Społecznego - wykonane w roku 2011.
- Raport pt. „Określenie struktury zawodowej mieszkańców Dolnego Śląska oraz zdefiniowanie i opisanie kierunków rozwoju dolnośląskiego rynku pracy”, Ageron Polska opracowanie w ramach badań współfinansowanych przez Unię Europejską z Europejskiego Funduszu Społecznego w programie Kapitał Ludzki Poddziałanie 8.1.4.: Przewidywanie Zmiany Gospodarczej – wykonane w roku 2010.
- Raport pt. „Badanie ewaluacyjne ex-ante dotyczące oceny zapotrzebowania gospodarki na absolwentów szkół wyższych kierunków matematycznych, przyrodniczych i technicznych” w ramach bazy badań ewaluacyjnych Narodowej Strategii Spójności (NSS) na lata 2007-2013.

Wyniki analiz potwierdzają zwiększone zapotrzebowanie na absolwentów kierunku Cyberbezpieczeństwo, uznając cyberbezpieczeństwo za branżę strategiczną. Zakładane efekty kształcenia pozwolą na nabycie kompetencji pożądanych przez pracodawców, takich jak np. pracy grupowej. Pozwolą również na uzyskanie preferowanych przez pracodawców umiejętności praktycznych, co zapewni odbycie praktyki zawodowej oraz zaliczenie bloku kształcenia specjalistycznego w zakresie utrzymania systemów teleinformatycznych

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

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)

45,5 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	23
Liczba punktów ECTS z przedmiotów wybieralnych	37
Łączna liczba punktów ECTS	60

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 zwracany/a z prowadzoną działal. 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

2.9. Minimalna liczba punktów ECTS , którą student musi uzyskać, realizując bloki kształcenia oferowane na zajęciach ogólnouczelnianych 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)
47 ECTS

3. Opis procesu prowadzącego do uzyskania efektów uczenia się:

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 kolokwium i egzaminów.

Do każdego efektu uczenia się PRK 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 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

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 (4 pkt ECTS)*

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol kierunk. efektu kształcenia	Liczba godzin		Liczba pkt. ECTS			Forma ² kursu/grupy kursów	Sposób ³ zaliczenia ^a	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	FLEU00001	Komunikacja społeczna					1	K2CBE_U05	15	60	2	0	1	T	Z	O		1	KO
2	CBEU00005	Przedsiębiorczość w ICT	2	0	0	0	1	K2CBE_W4 K2CBE_U05	45	90	3	0	2	T	Z	O			KO
Razem			2	0	0	0	2		60	150	5	0	3	-	-	-	-	1	-

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	0	2	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 związany/-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 kierunk. efektu kształcenia	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	MAEU00102	Matematyka(GK)	1	1				K2CBE_W02 K2CBE_U02	30	90	3	0	1	T	Z			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 kierunk. efektu kształcenia	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	FZEU00200	Fizyka	1					K2CBE_W02 K2CBE_U02	15	30	1	0	0,5	T	Z	O			PD
Razem			1	0	0	0	0	-	15	30	1	0	0,5	-	-	-	0	0	-

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

³ Egzamin – 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 kierunk. efektu kształcenia	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	CBEU00001	Monitorowanie i detekcja zagrożeń (GK)	2			3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	3	T	E(w)		DN	4	K
2	CBEU00002	Testy penetracyjne(GK)	2			3	1	K2CBE_W01 K2CBE_U02	90	210	7	7	3	T	E(w)		DN	4	K
3	CBEU00003	Informatyka śledcza i reakcja na incyd. (GK)	2			3	1	K2CBE_W01 K2CBE_U03	90	210	7	7	3	T	E(w)		DN	4	K
4	CBEU00004	Zarządzanie bezpieczeństwem (GK)	1			3	1	K2CBE_W01 K2CBE_U01	30	210	7	7	3	T	E(w)		DN	4	
5	CBEU00100	Seminarium kierunkowe				2		K2CBE_W05 K2CBE_K02	30	90	3	3		T	Z			2	K
6	CBEU00101	Seminarium dyplomowe					2	K2CBE_U06 K2CBE_K02 K2CBE_K02	30	90	3		2	T	Z			3	K
Razem			7	0	0	14	6	-	360	1020	34	31	14	-	-	-	-	21	-

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	14	6	360	1020	34	31	14

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

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

4.2 Lista bloków wybieralnych

4.2.1 Lista bloków kształcenia ogólnego

4.2.1.1 Blok *Języki obc (min 5pkt ECTS)*

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol kierunk. efektu kształcenia	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		Język obcy I		1				K2CBE_U04	15	30	1	0		T	Z	O		1	KO
2		Język obcy II		3				K2CBE_U04	45	60	2	0		T	Z	O		1	KO
Razem			0	4	0	0	0	-	60	90	3	0	0	-	-	-		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					
0	4	0	0	0	60	90	3	0	0

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 kierunk. efektu kształcenia	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		Blok A	2			3	1		90	210	7	7	3	T	E(w)		DN	4	K
	CBEU00200	Ochrona systemów operacyjnych (GK)						K2CBE_W01 K2CBE_U01											
	CBEU00201	Ochrona centrów danych (GK)						K2CBE_W01 K2CBE_U01											
3		Blok B	2			3	1		90	210	7	7	3	T	Z		DN	4	K
	CBEU00300	Bezpieczeństwo sieci radiowych i urządzeń mobilnych (GK)						K2CBE_W01 K2CBE_U01											

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

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

	CBEU00301	i aplikacji (GK)						K2CBE_U01											
4		Blok C	1			2	1		60	180	6	6	3	T	Z		DN	3	K
	CBEU00400	Zarządzanie projektami bezpieczeństwa IT (GK)						K2CBE_W01 K2CBE_U01											
	CBEU00401	Audytování i monitorowanie sieci i systemów (GK)						K2CBE_W01 K2CBE_U01											
5		Blok D	1	0	0	2	1		60	180	6	6	3	T	Z		DN	3	K
	CBEU00500	Metody AI w analizie wzorców zachowań						K2CBE_W03 K2CBE_U03											
	CBEU00501	Metody AI w badaniu zagrożeń w systemach komputerowych						K2CBE_W03 K2CBE_U03											
6		Blok E	1	0	0	2	1		60	180	6	6	3	T	Z		DN	3	K
	CBEU00600	Bezpieczeństwo aplikacji webowych						K2CBE_W03 K2CBE_U03											
	CBEU00601	Bezpieczne programowanie						K2CBE_W03 K2CBE_U03											
		Razem	7	0	0	12	5		360	960	32	32	15	-	-	-		17	-

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					
7	0	0	12	5	360	960	32	32	15

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

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

4.3 Blok „praca dyplomowa”

Typ pracy dyplomowej	inżynierska	
Liczba semestrów pracy dyplomowej	Liczba punktów ECTS	Kod
1	12 P(12)	CBEU00120
Charakter pracy dyplomowej		
projekt lub program komputerowy		
Liczba punktów ECTS BU ¹	6	
Liczba punktów ECTS DN ⁵	0	

5. Sposoby weryfikacji zakładanych efektów kształcenia

Typ zajęć	Sposoby weryfikacji zakładanych efektów kształcenia
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

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 związany -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

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
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

Przedmioty obowiązkowe:

1. Współczesne architektury cyberbezpieczeństwa
2. Sposoby i narzędzia do monitorowania i detekcji zagrożeń.
3. Podatności aplikacji Web – najpopularniejsze podatności, metody wykrywania
4. Dowody incydentów bezpieczeństwa – gromadzenie, metody analizy i oceny jakości
5. Metody zacierania i fałszowania dowodów cyfrowych
6. System Zarządzania Bezpieczeństwem Informacji. Organizacja bezpieczeństwa informacji.

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 Ogólnouniversyteckich – O

⁵Kurs / grupa kursów związanych z prowadzoną działalnością 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

Przedmioty wybieralne:

1. Blok A
 - 1.1. Zabezpieczenia systemów operacyjnych Windows i Linux
 - 1.2. Narzędzia monitorowania i detekcja zagrożeń w systemach chmurowych
2. Blok B
 - 2.1. Luki w bezpieczeństwie popularnych systemów bezprzewodowych, takich jak WiFi, Bluetooth, ZigBee oraz urządzeń mobilnych pracujących na systemach Android i Apple iOS
 - 2.2. Testy penetracyjne związane z technikami kryptograficznymi.
3. Blok C
 - 3.1. Metodyki inżynierii bezpieczeństwa systemu IT.
 - 3.2. Audyt infrastruktury sieciowej – etapy, sposób prowadzenia
4. Blok D
 - 4.1. Metody analizy sieci i analizy języka naturalnego w rozpoznawaniu wzorców behawioralnych
 - 4.2. Metody sztucznej inteligencji i uczenia maszynowego w modelowaniu i wykrywaniu zagrożeń systemów IT
5. Blok E
 - 5.1. Metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych
 - 5.2. Testowanie programów - testy jednostkowe, funkcjonalne, wydajnościowe, software quality assurance

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 Ogólnouczeniowy – O

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

SAMORZĄD STUDENCKI
Wydziału Elektroniki

13.11.2020

Mihael Makucsev

Data

Imię, nazwisko i podpis przedstawiciela studentów

13.11.2020

Data

Podpis Dziekana

Dziekan
Wydziału Elektroniki
prof. dr hab. inż. Czesław Smutnicki

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 Ogólnouczeniawy – O

⁵Kurs – grupa kursów związawy –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

PLAN STUDIÓW

WYDZIAŁ:	ELEKTRONIKI
KIERUNEK STUDIÓW:	CYBERBEZPIECZEŃSTWO
POZIOM KSZTAŁCENIA:	II stopień, studia magisterskie
FORMA STUDIÓW:	stacjonarna
PROFIL:	ogólnoakademicki
SPECJALNOŚĆ:	
JĘZYK PROWADZENIA STUDIÓW:	polski

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

Semestr 1

Kursy /grupy kursów obowiązkowe

liczba punktów ECTS: 30

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 ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1	CBEU00001	Monitorowanie i detekcja zagrożeń (GK)	2			3	1	K2CBE_W01 K2CBE_U01	90	210	7	7	3	T	E(w)		DN	4	K
2	CBEU00002	Testy penetracyjne(GK)	2			3	1	K2CBE_W01 K2CBE_U02	90	210	7	7	3	T	E(w)		DN	4	K
3	CBEU00003	Informatyka śledcza i reakcja na incyd. (GK)	2			3	1	K2CBE_W01 K2CBE_U03	90	210	7	7	3	T	E(w)		DN	4	K
4	MAEU00102	Matematyka(GK)	1	1				K2CBE_W02 K2CBE_U02	30	90	3	0	1	T	Z			1	K
5	FLEU00001	Komunikacja społeczna					1	K2CBE_U05	15	60	2	0	1	T	Z	O		1	KO
6	FZEU00200	Fizyka	1					K2CBE_W02 K2CBE_U02	15	30	1	0	0,5	T	Z	O			KO
7		Język obcy I		1				K2CBE_U04	15	30	1	0		T	Z	O		1	KO
8		Język obcy II		3				K2CBE_U04	45	60	2	0		T	Z	O		1	KO
Razem			8	5	0	9	4	-	390	900	30	21	11,5	-	-	-	-	16	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 działal. 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

Razem w semestrze

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS zajęć DN ⁵	Liczba punktów ECTS zajęć BU ¹
w	ć	l	p	s					
8	5	0	9	4	390	900	30	21	11,5

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 działalnością 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

Semestr 2

Kursy/grupy kursów obowiązkowe

liczba punktów ECTS: **10**

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 ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1	CBEU00004	Zarządzanie bezpieczeństwem (GK)	1			3	1	K2CBE_W01 K2CBE_U01	30	210	7	7	3	T	E(w)		DN	4	
2	CBEU00100	Seminarium kierunkowe				2		K2CBE_W05	30	90	3	3	1	T	Z			2	K
Razem			1	0	0	5	1	-	60	300	10	10	4	-	-	-	0	6	-

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

liczba punktów ECTS:

20

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 ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1		Blok A	2			3	1		90	210	7	7	3	T	E(w)		DN	4	K
	CBEU00200	Ochrona systemów operacyjnych (GK)						K2CBE_W01 K2CBE_U01											

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, ć, l, p, s)

⁴Kurs/grupa kursów Ogólnouczelniany – O

⁵Kurs/grupa kursów związany/a z prowadzoną działal. 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

	CBEU00...	Ochrona centrów danych (GK)						K2CBE_W01 K2CBE_U01											
2		Blok B	2			3	1		90	210	7	7	3	T	Z		DN	4	K
	CBEU00300	Bezpieczeństwo sieci radiowych i urządzeń mobilnych (GK)						K2CBE_W01 K2CBE_U01											
	CBEU00301	Zaawansowane testy penetracyjne sieci i aplikacji (GK)						K2CBE_W01 K2CBE_U01											
3		Blok C	1			2	1		60	180	6	6	3	T	Z		DN	3	K
	CBEU00400	Zarządzanie projektami bezpieczeństwa IT (GK)						K2CBE_W01 K2CBE_U01											
	CBEU00401	Audytowanie i monitorowanie sieci i systemów (GK)						K2CBE_W01 K2CBE_U01											
		Razem	5	0	0	8	3	-	240	600	20	20	9	-	-	-		11	-

Razem w semestrze

Łączna liczba godzin					Łączna liczba godzin ZUZ	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS zajęć DN ⁵	Liczba punktów ECTS zajęć BU ¹
w	ć	l	p	s					
6	0	0	13	4	300	900	30	30	13

Semestr 3

Kursy/grupy kursów obowiązkowe

liczba punktów ECTS: **18**

Tygodniowa liczba godzin	Liczba godzin	Liczba pkt. ECTS	Kurs/grupa kursów

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

²Trafficynna – 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 Ogólniuczelnianny – O

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

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

NO – kształcenia ogólnego, PD – podstawowy, K – kierunkowy, S – specjalnościowy

Lp	Kod kursu/grupy kursów	Nazwa kursu/grupy kursów (grupę kursów oznaczyć symbolem GK)	Tygodniowa liczba godzin					Symbol efektu uczenia się	Liczba godzin					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 ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1	CBEU00005	Przedsiębiorczość w ICT	2	0	0	0	1	K2CBE_W4 K2CBE_U05	45	90	3	0	2	T	Z				
2	CBEU00120	Praca dyplomowa						K2CBE_U06 K2CBE_K02 K2CBE_K02		360	12		6	T	Z			12	K
3	CBEU00101	Seminarium dyplomowe						K2CBE_U06 K2CBE_K02 K2CBE_K02	30	90	3		2	T	Z			3	K
Razem			2	0	0	0	3		75	540	18	0	10			0	0	15	

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 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 ⁶	o charakterze praktycznym ⁶	rodzaj ⁷
1		Blok D	1	0	0	2	1		60	180	6	6	3	T	Z		DN	3	K
	CBEU00500	Metody AI w analizie wzorców zachowań						K2CBE_W03 K2CBE_U03											
	CBEU00501	Metody AI w badaniu zagrożeń w systemach komputerowych						K2CBE_W03 K2CBE_U03											

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

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

2		Blok E	1	0	0	2	1		60	180	6	6	3	T	Z		DN	3	K
	CBEU00600	Bezpieczeństwo aplikacji webowych						K2CBE_W03 K2CBE_U03											
	CBEU00601	Bezpieczne programowanie						K2CBE_W03 K2CBE_U03											
		Razem	2	0	0	4	2		120	360	12	12	6	-	-	0	0	6	0

Razem w semestrze

Łączna liczba godzin					Łączna liczba godzin ZZU	Łączna liczba godzin CNPS	Łączna liczba punktów ECTS	Łączna liczba punktów ECTS zajęć DN ⁵	Liczba punktów ECTS zajęć BU ¹
w	ć	l	p	s					
4	0	0	4	5	195	900	30	12	16

2. Zestaw egzaminów w układzie semestralnym

Kod kursu	Nazwy kursów kończących się egzaminem	Semestr
CBEU00001	Monitorowanie i detekcja zagrożeń	1
CBEU00002	Testy penetracyjne	
CBEU00003	Informatyka śledcza i reakcja na incyd.	
CBEU00004	Zarządzanie bezpieczeństwem	2
	Przedmiot z bloku B wg. wyboru studenta	
CBEU00200	Ochrona systemów operacyjnych	
CBEU00...	Ochrona centrów danych	

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, ć, l, s, p)

⁴Kurs - grupa kursów Ogólnouczelniany - O

⁵Kurs - grupa kursów związany - a z prowadzoną działal. 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

3. Liczby dopuszczalnego deficytu punktów ECTS po poszczególnych semestrach

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

Opinia właściwego organu Samorządu Studenckiego

SAMORZĄD STUDENCKI

13.11.2020

Wydziału Elektroniki

Data

Mikołaj Mazurczak

Imię, nazwisko i podpis przedstawiciela studentów

Data

Podpis Dziekana

13.11.2020

Dziekan
Wydziału Elektroniki

prof. dr hab. inż. Czesław Smutnicki

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

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

WYDZIAŁ ELEKTRONIKI	
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*, stacjonarne / niestacjonarne*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	CBEU00001
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. 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	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	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)

--

WYDZIAŁ ELEKTRONIKI	
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*, stacjonarne / niestacjonarne*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	CBEU00002
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.
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	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	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 – 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: SEC560: Network Penetration Testing and Ethical Hacking
- [2] SANS: SEC542: Web App Penetration Testing and Ethical Hacking
- [3] “Professional Penetration Testing”, Thomas Wilhelm, Elsevir 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)

--

WYDZIAŁ ELEKTRONIKI	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim:	Informatyka śledcza i reakcja na incydenty
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*, stacjonarne / niestacjonarne*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	CBEU00003
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
<ol style="list-style-type: none"> 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
<ol style="list-style-type: none"> 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 częściowe. 2. Obrona projektu, zaliczenie.
F3	PEU_K01 PEU_K02 PEU_K03	1. Ocena wykonanych prezentacji, dyskusje. 2. Zaliczenie.
$P=0,5 \cdot F1 + 0,25 \cdot F2 + 0,25 \cdot F3$ <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 (IMIE, NAZWISKO, ADRES E-MAIL)

WYDZIAŁ ELEKTRONIKI	
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*, stacjonarne / niestacjonarne*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	CBEU00004
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)	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. 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>$P=0,5 \cdot F1 + 0,25 \cdot F2 + 0,25 \cdot F3$</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] 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>
<p>OPIEKUN PRZEDMIOTU (IMIE, NAZWISKO, ADRES E-MAIL)</p>

WYDZIAŁ ELEKTRONIKI	
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*, stacjonarne / niestacjonarne*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	CBEU00200
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
<ol style="list-style-type: none"> 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 (IMIE, NAZWISKO, ADRES E-MAIL)

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

WYDZIAŁ ELEKTRONIKI	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim:	Bezpieczeństwo sieci radiowych i urządzeń mobilnych
Nazwa przedmiotu w języku angielskim:	Security in radio networks and mobile devices
Kierunek studiów (jeśli dotyczy):	Cyberbezpieczeństwo
Specjalność (jeśli dotyczy):
Poziom i forma studiów:	I/ II stopień / jednolite studia magisterskie*, stacjonarne / niestacjonarne*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	CBEU00300
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	—	—	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.	Znajomość podstaw funkcjonalnych z zakresu popularnych protokołów komunikacji krótkozasięgowych (w szczególności: pasma pracy, interfejs radiowy)
2.	Znajomość notacji decybelowej oraz zjawisk propagacyjnych
3.	Znajomość podstawowych metryk oceny wydajności transmisyjnej systemów telekomunikacyjnych (przepustowość, opóźnienie, <i>jitter</i> itp.)
4.	Znajomość zagadnień związanych z sieciami komputerowymi na poziomie min. CCNA1

CELE PRZEDMIOTU

- C1. Zdobyć wiedzę z zakresu rozumienia, analizy i zabezpieczania rozmaitych krótkozasięgowych systemów bezprzewodowych, takich jak WiFi, Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC.
- C2. Zdobyć wiedzę z zakresu silnych i słabych stron urządzeń zarządzanych przez systemy Android i Apple iOS.
- C3. Zdobyć umiejętności obchodzenia standardowych zabezpieczeń stosowanych w masowych urządzeniach mobilnych, skutecznej współpracy z instytucjami pracującymi na rzecz podnoszenia bezpieczeństwa danych i sieci oraz konstruowania platform do wykonywania głębokich testów penetracyjnych.
- C4. Zdobyć doświadczenia w pracy zespołowej, w tym umiejętności planowania i harmonogramowania, komunikacji wewnątrz-zespołowej, pełnienia roli członka zespołu bądź lidera, możliwość wykazania się kreatywnością, otwartością na innowacyjne podejście do realizacji celu oraz zorientowaniem na sukces zespołu

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

- PEU_W01 Dogłębna znajomość zasad działania (w tym: używanych protokołów, interfejsów radiowych i zabezpieczeń) popularnych systemów bezprzewodowych, takich jak WiFi, Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC oraz urządzeń mobilnych pracujących na systemach Android i Apple iOS
- PEU_W02 Dogłębna znajomość luk w bezpieczeństwie popularnych systemów bezprzewodowych, takich jak WiFi, Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC oraz urządzeń mobilnych pracujących na systemach Android i Apple iOS, metod i narzędzi ich detekcji oraz oceny wysokości ryzyka.

Z zakresu umiejętności:

- PEU_U01 Umiejętność wykonywania głębokich testów penetracyjnych, celem eksploracji podatności i luk w zabezpieczeniach, w ujęciu indywidualnym i korporacyjnym, dla większości systemów bezprzewodowych – krótkozasięgowych i mobilnych, na potrzeby analiz zakresu generowanego ruchu czy treści gromadzonych w urządzeniach itp.
- PEU_U02 Umiejętność obchodzenia luk z bezpieczeństwie różnych systemów bezprzewodowych, celem odzyskania kontroli po utracie hasła, numeru PIN czy innego zabezpieczenia
- PEU_U03 Umiejętność samodzielnego studiowania wybranego zagadnienia związanego z tematyką przedmiotu, przeszukiwania i klasyfikowania aktualnej wiedzy przedmiotowej i referowania jej z uwzględnieniem reżimu czasowego i stopnia ważności prezentowanych treści.

Z zakresu kompetencji społecznych:

- PEU_K01 potrafi pracować w zespole osób o zróżnicowanych zadaniach, osobowościach i umiejętnościach interpersonalnych, ze świadomością istniejących współzależności merytorycznych i terminowych w pracy nad złożonym projektem teleinformatycznym z zakresu cyberbezpieczeństwa

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		Liczba godzin
Wy1-Wy2	Akwizycja danych z WiFi i ich analiza	3
Wy2-Wy3	Cyberataki na urządzenia konsumenckie i korporacyjne WiFi (AP i karty WLAN)	3
Wy4-Wy5	Cyberataki w sieciach korporacyjnych WiFi, DECT i ZigBee	3
Wy5-Wy6	Cyberataki na systemy: Bluetooth i Radia Programowalnego (SDR)	3
Wy7-Wy8	Łamanie zabezpieczeń się urządzeń i systemów RFID, Smart Card i NFC	3
Wy8-Wy9	Architektura urządzeń mobilnych i ich wspólne zagrożenia	3
Wy10-Wy11	Dostęp do platform mobilnych i analiza aplikacji	3
Wy11-Wy12	Inżynieria wsteczna w analizie aplikacji	3
Wy13-Wy14	Testowanie penetracyjne w urządzeniach mobilnych	4
Wy14-Wy15	Repetitorium	2
	Suma godzin	30

Forma zajęć - projekt		Liczba godzin
Pr1	Zajęcia organizacyjne: wyjaśnienie zasad liczenia oceny końcowej, przedstawienie modelu pracy studenckiej w trakcie zajęć, umówienie tematów i zagadnień projektowych, prezentacja harmonogramu zajęć	1
Pr2	Prezentacja grup projektowych, w tym: składu i pełnionych ról. Omówienie, w postaci prezentacji multimedialnej, wybranych tematów przez liderów poszczególnych zespołów oraz wykresów harmonogramów pracy (np. w postaci wykresów Gantta czy Perta)	4
Pr3	Prezentacja częściowych wyników pracy zespołów	4
Pr4	Prezentacja częściowych wyników pracy zespołów	4
Pr5	Prezentacja częściowych wyników pracy zespołów	4
Pr6	Prezentacja częściowych wyników pracy zespołów	4
Pr7	Prezentacje śródsesemestralne – omówienie dotychczasowych osiągnięć w odniesieniu do założeń wstępnych. Wystawienie ocen śródkresowych.	4
Pr8	Prezentacja częściowych wyników pracy zespołów	4
Pr9	Prezentacja częściowych wyników pracy zespołów	4
Pr10	Prezentacja częściowych wyników pracy zespołów	4
Pr11	Prezentacja częściowych wyników pracy zespołów	4
Pr12	Prezentacje końcowe efektów prac zespołów projektowych i ich ewaluacja. Wystawienie ocen końcowych	4
	Suma godzin	45

Forma zajęć - seminarium		Liczba godzin
Se1	Zajęcia organizacyjne – przedstawienie grafiku prezentacji studenckich, wyjaśnienie zasad liczenia oceny końcowej. Wyjaśnienie podstawowych zagadnień związanych z korzystaniem i cytowaniem źródeł bibliograficznych oraz prezentacją multimedialną i prezentacją wyników.	1
Se2	Wstępne prezentacje tła zagadnień będących przedmiotem indywidualnej pracy seminaryjnej, w tym określenie zakresu omówienia	2

Se3	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych. Dyskusja nad rezultatami.	2
Se1	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych. Dyskusja nad rezultatami.	2
Se2	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych. Dyskusja nad rezultatami.	2
Se3	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych. Dyskusja nad rezultatami.	2
Se7	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych. Dyskusja nad rezultatami.	2
Se7	Prezentacje wyników prac wykonanych w ramach realizacji prac własnych. Dyskusja nad rezultatami.	2
	Suma godzin	15

STOSOWANE NARZĘDZIA DYDAKTYCZNE

- N1. Narzędzia programistyczne do przygotowywania prezentacji multimedialnych
 N2. Platformy sprzętowe i programowe systemów bezprzewodowych do badań penetracyjnych
 N3. Konsultacje
 N4. 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_W02	Ocena stopnia nabytej wiedzy teoretycznej na drodze przeprowadzonego kolokwium (pisemnego lub ustnego) bądź egzaminu
F2	PEU_U01, PEU_U02, PEU_K01	Ocena prezentacji kolejnych etapów projektu oraz umiejętności pracy w zespole: przestrzegania harmonogramu, aktywności w zespole, umiejętności zastosowania zasad zarządzania projektem oraz jakości: - wykonanego projektu, - dokumentacji projektowej a także – umiejętności pracy zespołowej
F3	PEU_U03	Ocena jakości prezentacji przydzielonego tematu, w tym: reprezentatywności dla zagadnienia, równomierności omówienia zagadnień składowych, czytelności i estetyki wizualnej, jakości przekazu ustnego, terminowości
$P=0,45 \cdot F1+0,35 \cdot F2+0,2 \cdot F3$		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] „Secure coding. Best practices handbook. A developer’s guide to proactive controls”, Veracode, 2018. Pozycja dostępna online:
<https://info.veracode.com/secure-coding-best-practices-hand-book-guide-resource.html>
- [2] Matthews J., „A Secure Approach to Deploying Wireless Networks”, SANS Institute, Information Security Reading Room, 2016. Pozycja dostępna online:
<https://www.sans.org/reading-room/whitepapers/wireless/paper/37342>

LITERATURA UZUPEŁNIAJĄCA:

- [1] Źródła internetowe związane z prezentowaną w trakcie seminarium tematyką bądź tematem realizowany w trakcie projektu

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

Kamil Staniec, kamil.staniec@pwr.edu.pl

WYDZIAŁ ELEKTRONIKI	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim:	Zaawansowane testy penetracyjne
Nazwa przedmiotu w języku angielskim:	Advanced pentesting
Kierunek studiów (jeśli dotyczy):	Cyberbezpieczeństwo
Specjalność (jeśli dotyczy):
Poziom i forma studiów:	I/ II stopień / jednolite studia magisterskie*, stacjonarne / niestacjonarne*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	CBEU00200
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	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	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	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 UZUPELNIAJĄCA

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, Elsevir 2010
- [4] “Penetration testing and Network Defense” – Andrew Whitaker, Daniel Newman, Cisco Press 2006

LITERATURA UZUPELNIAJACA:

- [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)

--

WYDZIAŁ ELEKTRONIKI	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim:	Zarządzanie projektami bezpieczeństwa IT
Nazwa przedmiotu w języku angielskim:	IT projects 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	CBEU00400
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15	---	---	30	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
<ol style="list-style-type: none"> 1. Wiedza z zakresu ochrony informacji 2. Poszerzona wiedza z zakresu organizacji infrastruktury informatycznej i oprogramowania 3. Podstawowa wiedza zarządzania projektami

CELE PRZEDMIOTU
<ol style="list-style-type: none"> C1. Nabycie wiedzy z zakresu organizacji projektów bezpieczeństwa C2. Poszerzenie i ugruntowanie wiedzy z zakresu kierowania projektami bezpieczeństwa IT

C3. Poszerzenie umiejętności z zakresu przeprowadzania analizy procesów biznesowych i zasobów teleinformatycznych

C4.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zna rodzaje i zastosowania projektów bezpieczeństwa IT

PEU_W02 Zna zasady funkcjonowania zespołu projektowego

PEU_W03 Poznał zasady dokumentowania wyników działań zespołu projektowego

PEU_W04 Posiada wiedzę na temat tworzenia raportów z działań audytowych

Z zakresu umiejętności:

PEU_U01 Poznał narzędzia wspomagające tworzenie raportów

PEU_U02 Poznał narzędzia pozwalające na bezpieczną komunikację z badaną infrastrukturą

PEU_U03 Potrafi posługiwać się metodami stosowanymi w inżynierii bezpieczeństwa

Z zakresu kompetencji społecznych:

PEU_K01 Potrafi współpracować w ramach zespołu bezpieczeństwa IT

PEU_K02 Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.

PEU_K02 Potrafi koordynować proces wdrażania zaleceń bezpieczeństwa powstałych w ramach projektu

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Rodzaje projektów bezpieczeństwa IT: test penetracyjny, audyt systemu, utwardzanie systemu, projektowanie zabezpieczeń.	2
Wy2	Metodyki inżynierii bezpieczeństwa systemu IT.	2
Wy3	Ocena wymaganych kompetencji i przygotowanie zespołu. Przepływ informacji i podział odpowiedzialności w zespole.	3
Wy4	Bezpieczeństwo komunikacji wewnątrz zespołu.	1
Wy5	Przygotowanie infrastruktury do testów bezpieczeństwa.	2
Wy6	Aspekty gromadzenia i przetwarzania dokumentacji projektu. Zagadnienia merytoryczne i techniczne raportowania w projektach bezpieczeństwa IT.	2
Wy7	Wdrażanie zaleceń bezpieczeństwa powstałych w ramach projektu.	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 PEU_W04	1. Pisemne zaliczenie.
F2	PEU_U01 PEU_U02	1. Prezentacje cząstkowej. 2. Obrona projektu, zaliczenie.

	PEU_U03 PEU_K01 PEU_K02 PEU_K03	
F3	PEU_U01 PEU_U02 PEU_U03	1. Ocena wykonanych prezentacji, dyskusje. 2. Zaliczenie.
$P=0,5 \cdot F1 + 0,25 \cdot F2 + 0,25 \cdot F3$ <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] Normy ISO rodziny 27000, PKN 2014 lub późniejsze
- [2] Audyt bezpieczeństwa informacji w praktyce, Romasz Polaczek, Helion ebook 2014

LITERATURA UZUPEŁNIAJĄCA:

- [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] Zarządzanie projektami IT. Wydanie III
- [4] Przewodnik audytora systemów informatycznych, Marian Molski, Małgorzata Łacheta, Helion, 2007

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

--

WYDZIAŁ ELEKTRONIKI	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim:	Audytowanie i monitorowanie sieci i systemów
Nazwa przedmiotu w języku angielskim:	Monitoring and audit of networks and system
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:	CBEU00401
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			30	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
<ol style="list-style-type: none"> 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	Repetytorium.	1
	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.	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	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] “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)

WYDZIAŁ ELEKTRONIKI	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim:	Metody AI w analizie wzorców zachowań
Nazwa przedmiotu w języku angielskim:	AI methods in the analysis of behavior patterns
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:	CBEU00500
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			30	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	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. Znajomość podstaw statystyki i rachunku prawdopodobieństwa
2. Umiejętność programowania (C++, Python, Java)
3.

CELE PRZEDMIOTU

C1 Zapoznanie słuchaczy z metodami sztucznej inteligencji(AI) i uczenia maszynowego (ML) stosowanymi w automatyzacji wykrywania zagrożeń typu fałszywe konta / botnety na portalach społecznościowych oraz spamu czy kampanii phishing mailowych.
 C2 Umiejętność doboru odpowiedniej metody AI / ML do danego problemu.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 Zapoznanie studentów z podstawowymi metodami maszynowego uczenia, w tym z uczeniem głębokim

PEU_W02 Zapoznanie studentów z metodami analizy sieci i analizy języka naturalnego w zadaniach rozpoznawania wzorców behawioralnych

Z zakresu umiejętności:

PEU_U01 Umiejętność doboru metod inteligentnych do analizy wzorców zachowań w zależności od konkretnego zadania

PEU_U02 Umiejętność oceny wyników zastosowanych metod do analizy wzorców zachowań

Z zakresu kompetencji społecznych:

PEU_K01 Umiejętność pracy zespołowej

PEU_K02 Umiejętność dyskusji w grupie, w tym argumentacji krytycznej

TREŚCI PROGRAMOWE

Forma zajęć - wykład		a. Liczba godzin
Wy1	Wprowadzenie do kursu. Omówienie tematyki i zasad prowadzenia i zaliczenia kursu. Przydział tematów	2
Wy2	Wprowadzenie do analizy sieci społecznościowych	2
Wy3	Wykrywanie fałszywych profili w sieciach społecznościowych	2
Wy4	Wprowadzenie do uczenia głębokiego, CNN, LSTM	2
Wy5	Uczenie głębokie - transformery i ich zastosowania	2
Wy6	Wprowadzenie do inżynierii języka naturalnego	2
Wy7	Przegląd metod wydobywania informacji i analizy stylometrycznej	2
Wy8	Sprawdzian nabytej wiedzy	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		b. Liczba godzin
Pr1	Zajęcia wprowadzające, omówienie formy, wymagań, potencjalnych tematów.	2
Pr2	Dyskusja tematów wybranych / proponowanych przez studentów	2
Pr3	Ustalenie tematów projektów – krótka prezentacja tematów i proponowanych metod do stosowania	2
Pr4	Realizacja projektu, konsultacje, dyskusje	2
Pr5	Realizacja projektu, konsultacje, dyskusje	2
Pr6	Realizacja projektu, konsultacje, dyskusje	2
Pr7	Realizacja projektu, konsultacje, dyskusje	2
Pr8	Prezentacja postępów i dyskusja nad dalszym etapem	2
Pr9	Prezentacja postępów i dyskusja nad dalszym etapem	2
Pr10	Uwzględnianie uwag, kontynuacja projektu, konsultacje, dyskusje	2
Pr11	Uwzględnianie uwag, kontynuacja projektu, konsultacje, dyskusje	2
Pr12	Uwzględnianie uwag, kontynuacja projektu, konsultacje, dyskusje	2
Pr13	Prezentacja końcowych wyników – analiza krytyczna wyników	2
Pr14	Prezentacja końcowych wyników – analiza krytyczna wyników	2
Pr15	Podsumowanie zajęć, dyskusja na temat osiągniętych wyników, możliwości zastosowania / kontynuacji projektów.	2
	Suma godzin	30

Forma zajęć - seminarium		Liczba godzin
Se1	Wprowadzenie do kursu. Omówienie tematyki i zasad prowadzenia i zaliczenia kursu. Przydział tematów	2
Se2	Analiza zachowań ludzi za pomocą technik uczenia maszynowego – analiza przypadków	2
Se3	Wykrywanie fałszywych profili w sieciach społecznościowych – analiza przypadków	2
Se4	Wykrywanie fałszywych profili w sieciach społecznościowych – analiza przypadków	2
Se5	Uczenie głębokie w analizie wzorców – analiza przypadków	2
Se6	Infrastruktury technologii językowych, szkieletowe systemy i potoki przetwarzania	2
Se7	Wykrywanie podobieństwa tekstu pod względem stylu, autorstwa i treści: metody i narzędzia.	2
Se8	Dyskusja: kierunki rozwoju dziedziny. Podsumowanie zajęć	1
	Suma godzin	15

STOSOWANE NARZĘDZIA DYDAKTYCZNE

- N1. Prezentacje przekazywanej wiedzy z wykorzystaniem projektora
 N2. Środki audiowizualne w przekazywaniu materiałów demonstracyjnych
 N3. Wyszukiwanie i studiowanie literatury naukowej w zasobach Biblioteki PWR i w Internecie
 N4. Udostępnione zasoby i narzędzia językowe dla języka polskiego oraz języka angielskiego.
 N5. Zasoby i narzędzia językowe oraz podstawowe architektury przetwarzania języka naturalnego dostępne na wskazanych stronach internetowych.
 N6. Materiały do wykładu i projektu udostępnione poprzez portal E-learning Wydziału Informatyki i Zarządzania.
 N7. Infrastruktura badawcza technologii językowych CLARIN (<http://www.clarin.eu>) w tym jej polska część CLARIN-PL (<http://clarin-pl.eu>).

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 (wykład)	PEU_W01 PEU_W02	Kolokwia na wykładzie.
F2 (projekt)	PEU_U01 PEU_U02 PEU_K01	Kontrola przygotowania studentów do realizacji kolejnych etapów projektu, realizacja projektu zgodnie ze wytycznymi.
F3 (seminarium)	PEU_W02 PEU_U01 PEU_K02	Ocena za wartość merytoryczną i jakość prezentacji przygotowanego i wygłoszonego referatu (60%) oraz za aktywność w trakcie zajęć (40%)
<p>P – ocena końcowa za kurs będzie średnią arytmetyczną z ocen cząstkowych (wykład, projekt i seminarium).</p> <p>Ocena końcowa z wykładu będzie wystawiana na podstawie wyników uzyskanych w kolokwiach, może zostać podniesiona o 0,5, jeżeli student wykazał się dodatkową aktywnością (w przypadku wykładu są to odpowiedzi na dodatkowe pytania i udział w dyskusji moderowanej przez wykładowcę).</p> <p>Ocena końcowa z projektu będzie wystawiana na podstawie oceny rezultatów projektu z uwzględnieniem cząstkowych ocen (punktów) otrzymanych za przygotowanie się do poszczególnych etapów projektu i ich realizację.</p> <p>Ocena końcowa za seminarium będzie w 60% oceną za wygłoszony referat (wartość merytoryczna oraz jakość prezentacji), w 40% za udział w dyskusjach w trakcie poszczególnych zajęć seminaryjnych.</p>		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

- [1] Barabási, Albert-László: "Network science." Cambridge University Press, 2016.
- [2] Kaur, Davinder, Suleyman Uslu, and Arjan Durrezi: "Trust-based security mechanism for detecting clusters of fake users in social networks." Workshops of the International Conference on Advanced Information Networking and Applications. Springer, Cham, 2019.
- [3] Ian Goodfellow and Yoshua Bengio and Aaron Courville: "Deep Learning", MIT, 2016, <http://www.deeplearningbook.org>
- [4] Thudumu, S., Branch, P., Jin, J. et al.: "A comprehensive survey of anomaly detection techniques for high dimensional big data." *J Big Data* 7, 42 (2020). <https://doi.org/10.1186/s40537-020-00320-x>
- [5] Handbook of Natural Language Processing (Second Edition). (Ed.) Nitin Indurkha i Fred J. Damerau. CRC Press, 2010.
- [6] LUDMILA I. KUNCHEVA: "COMBINING PATTERN CLASSIFIERS. Methods and Algorithms", Second Edition, John Wiley & Sons, Inc., 2014.
- [7] Savoy, Jacques: "Machine Learning Methods for Stylometry". Springer, 2020.

LITERATURA UZUPEŁNIAJĄCA:

- [2] Menczer, Filippo, Santo Fortunato, and Clayton A. Davis. A First Course in Network Science. Cambridge University Press, 2020.
- [3] Raghavendra Chalapathy, Sanjay Chawla: Deep Learning for Anomaly Detection: A Survey, proceedings of DeepLF Sydney 2019,
- [4] Shai Shalev-Shwartz and Shai Ben-David: Understanding Machine Learning: From Theory to Algorithms. Published 2014 by Cambridge University Press. <http://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning>
- [5] Daniel Bikel i Imed Zitouni. Multilingual Natural Language Processing Applications: From Theory to Practice. IBM Press, 2012.
- [6] Mikolov, T., Chen, K., Corrado, G., and Dean, J. (2013a). Efficient estimation of word representations in vector space. arXiv preprint arXiv:1301.3781
- [7] Mikolov, T., Sutskever, I., Chen, K., Corrado, G. S., and Dean, J. (2013b). Distributed representations of words and phrases and their compositionality. In Advances in Neural Information Processing Systems, pages 3111–3119.
- [8] Daniel Jurafsky, James H. Martin: "Speech and Language Processing. An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition", Third Edition draft, Stanford University, 2018. <https://web.stanford.edu/~jurafsky/slp3/ed3book.pdf>

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

Halina Kwaśnicka halina.kwasnicka@pwr.edu.pl

WYDZIAŁ Elektroniki / STUDIUM.....	
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 stopnień / jednolite studia magisterskie*, stacjonarna / niestacjonarna*
Rodzaj przedmiotu:	obowiązkowy / wybieralny/ ogólnouczelniany*
Kod kursu	CBEU00501
Grupa kursów	TAK / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			30	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	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

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	Zbiory i źródła danych wykorzystywane w analizie i modelowaniu zagrożeń	2
Wy3	Wybrane metody analizy danych i uczenia maszynowego (uczenie nadzorowane, redukcja wymiaru, metody grafowe)	3
Wy4	Metody modelowania szeregów czasowych	2
Wy5	Uczenie głębokie w modelowaniu i analizie zagrożeń	2
Wy6	Techniki wykrywania anomalii (nadzorowane, nienadzorowane, w oparciu o szeregi czasowe)	2
Wy7	Wybrane typy ataków / zagrożeń (np. ataki (D)DOS) – metody wykrywania	2

	Suma godzin	15
--	-------------	-----------

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

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

Forma zajęć - projekt		Liczba godzin
Pr1	Wprowadzenie do wybranego problemu / problemów analizy zagrożeń badanych w ramach projektu	2
Pr2	Wprowadzenie do wybranych narzędzi obliczeniowych	2
Pr3	Sformułowanie założeń, uszczegółowienie zadań dla poszczególnych grup projektowych	2
Pr4-13	Realizacja kolejnych etapów projektu (zebranie / preprocesiong danych / przygotowanie środowiska analizy / budowanie modeli dot. zagrożeń / badania empiryczne dot. wykrywania zagrożeń i anomalii, itd.)	20
Pr14	Dyskusja wyników, opracowanie dokumentacji projektowej	2
Pr15	Prezentacja i dyskusja wyników uzyskanych przez grupy projektowe	2
	Suma godzin	30

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 = 1/3 * (F1+F2+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.

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

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

WYDZIAŁ Elektroniki / STUDIUM.....	
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	CBEU00600
Grupa kursów	TAK/ NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			30	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)	4			1	1
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2			1	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:

- PEK_U01 – potrafi wskazać typowe błędy związane z bezpieczeństwem w konfiguracji serwerów sieciowych
 PEK_U02 – potrafi sprawdzić integralność danych w systemie komputerowym i wykorzystać techniki kryptograficzne do zwiększenia bezpieczeństwa systemu (m.in. SSL)
 PEK_U03 – potrafi skonfigurować serwer WWW
 PEK_U04 – potrafi znaleźć i wykorzystać informacje o bieżących problemach związanych z bezpieczeństwem serwerów WWW i aplikacji webowych...

Z zakresu kompetencji społecznych:

- PEK_K01 – jest świadomy znaczenia wagi przykładanej do pisania aplikacji webowych z zachowaniem reguł bezpieczeństwa
 PEK_K02 – jest świadom odpowiedzialności wynikającej z wiedzy o dziurach w bezpieczeństwie poszczególnych aplikacji lub serwerów
 PEK_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 wspomagania 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
Se1	Omówienie zasad przygotowania materiałów i ich prezentacji, uzgodnienie tematów	1
Se2	Prezentacje studenckie i dyskusja	9
Se3	Dyskusja w grupie seminaryjnej nt. stanu wiedzy literaturowej i kompletności prezentacji	5
...	Suma godzin	15

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	Kolokwium zaliczeniowe (wykład)
P2	PEK_K01, PEK_K02, PEK_K03, PEU_W01, PEU_W02, PEU_W03, PEU_W04	Ocena końcowa seminarium
P3	PEU_U01, PEU_U02, PEU_U03, PEU_U03	Ocena końcowa projektu
$P = P1 * 0.4 + P2 * 0.3 + P3 * 0.3$ <p>Warunkiem uzyskania pozytywnej oceny końcowej z przedmiotu jest wcześniejsze uzyskanie pozytywnej oceny zaliczeniowej z seminarium i projektu</p>		

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 Elektroniki / STUDIUM.....	
KARTA PRZEDMIOTU	
Nazwa przedmiotu w języku polskim:	Bezpieczne programowanie
Nazwa przedmiotu w języku angielskim:	Secure programming
Kierunek studiów (jeśli dotyczy):	Cyberbezpieczeństwo
Specjalność (jeśli dotyczy):
Poziom i forma studiów:	I/ II stopień / jednolite studia magisterskie*, stacjonarna / niestacjonarna*
Rodzaj przedmiotu:	obowiązkowy / wybieralny / ogólnouczelniany*
Kod przedmiotu	CBEU00601
Grupa kursów	TAK/ NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15			30	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)	4			1	1
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2			1	1

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Podstawowe umiejętności programowania w językach C, Python
2. Podstawowa wiedza z zakresu bezpieczeństwa systemów i sieci komputerowych, metody uwierzytelniania i autoryzacji, prawa dostępu

CELE PRZEDMIOTU

C1 – Przedstawienie studentom procesu tworzenia oprogramowania, które jest bezpieczne, niezawodne i łatwe w utrzymaniu. W ramach kursu przedstawione zostaną metody tworzenia kodu i

jego testowania, ze szczególnym naciskiem na aspekty bezpieczeństwa, jak również korzystanie z narzędzi kontroli wersji i wspomagania pracy grupowej.

C2 – Poznanie metod programowania defensywnego oraz podstaw inżynierii wstecznej (reverse engineering).

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEU_W01 – zna metody programowe i sprzętowe uwierzytelniania i autoryzacji dostępu

PEU_W02 – zna zagrożenia związane z oprogramowaniem złośliwym (malware)

PEU_W03 – zna podstawowe metody pisania programów w sposób bezpieczny

PEU_W04 – wie, co to jest nadpisanie bufora i inne typowe błędy związane z bezpieczeństwem i zna techniki wspomagające unikanie takich błędów

Z zakresu umiejętności:

PEU_U01 – potrafi ocenić poziom bezpieczeństwa różnych metod uwierzytelniania

PEU_U02 – potrafi rozpoznać typowe problemy bezpieczeństwa w programach

PEU_U03 – potrafi korzystać z narzędzi wspomagania pracy grupowej i systemów kontroli wersji

Z zakresu kompetencji społecznych:

PEK_K01 – jest świadomy znaczenia wagi przykładanej do pisania aplikacji z zachowaniem reguł bezpieczeństwa

PEK_K02 – jest świadomy odpowiedzialności wynikającej z wiedzy o dziurach w bezpieczeństwie poszczególnych aplikacji lub systemów komputerowych

PEK_K03 – rozumie konieczność samokształcenia oraz samodzielnego stosowania posiadanej wiedzy w praktyce,

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Metodologia SDLC, Programowanie defensywne i jego metody	2
Wy2	Programowanie sterowane asercjami,	2
Wy3	Dobre praktyki w programowaniu	2
Wy4	Typowe zagrożenia bezpieczeństwa – problemy programowania współbieżnego, wyścig, mechanizmy zapewniania spójności, semafony, mutexy	2
Wy5	Zagrożenia bezpieczeństwa w programowaniu – łańcuchy formatujące, nadpisanie bufora, ataki typu wstrzyknięcie kodu (Shell, SQL) i inne	2
Wy6	Testowanie programów, testy jednostkowe,	2
Wy7	Systemy kontroli wersji i wspomagania pracy grupowej.	2
Wy8	Kolokwium zaliczeniowe	1

	Suma godzin	15
--	-------------	-----------

Forma zajęć - projekt		Liczba godzin
Pr1	Konfiguracja środowiska projektowego z użyciem narzędzi zarządzania projektami i systemów kontroli wersji (git, svn, cvs) oraz portali wspomagających te procesy (github, gitlab, itp.), wypracowanie standardów pracy	4
Pr2	Praca grupowa, metodologia, funkcje członków zespołu, zarządzanie projektem	3
Pr3	Praca w grupach 3-4-osobowych nad wybranymi projektami programistycznymi z wykorzystaniem narzędzi pracy grupowej, systemów kontroli wersji oraz z zastosowaniem technik i narzędzi programowania defensywnego	18
Pr4	Restrukturyzacja i refaktoring kodu, metody testowania	5
	Suma godzin	30

Forma zajęć - seminarium		Liczba godzin
Se1	Omówienie zasad przygotowania materiałów i ich prezentacji, uzgodnienie tematów	1
Se2	Prezentacje studenckie i dyskusja	9
Se3	Dyskusja w grupie seminaryjnej nt. stanu wiedzy literaturowej i kompletności prezentacji	5
	Suma godzin	15

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

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	Kolokwium zaliczeniowe (wykład)
P2	PEK_K01, PEK_K02, PEK_K03, PEU_W01, PEU_W02, PEU_W03, PEU_W04	Ocena końcowa seminarium
P3	PEU_U01, PEU_U02, 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] Mark Dowd, The art of software security assessment : identifying and preventing software vulnerabilities, ISBN 0321444426
- [2] Ben-Ari, M. -- Podstawy programowania współbieżnego

LITERATURA UZUPEŁNIAJĄCA:

- [1] Stevens – Programowanie zastosowań sieciowych w systemie UNIX
- [2] GARFINKEL & SPAFFORD – Bezpieczeństwo w Uniksie i Internecie
- [3] Jacek Ross, Bezpieczne programowanie : aplikacje hakeroodporne, ISBN 9788324624058

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

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

WYDZIAŁ ELEKTRONIKI	
	KARTA PRZEDMIOTU
Nazwa w języku polskim:	Komunikacja społeczna
Nazwa w języku angielskim:	Social Communication
Kierunek studiów:	Automatyka i Robotyka, Elektronika, Informatyka, Telekomunikacja, Teleinformatyka, Cyberbezpieczeństwo
Stopień studiów i forma:	II stopień, stacjonarna
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	FLEU00001
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 INNYCH 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 inżynierijno-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, *Spoleczna 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 ELEKTRONIKI

KARTA PRZEDMIOTU

Nazwa w języku polskim: Fizyka
Nazwa w języku angielskim: Physics
Kierunek studiów: Teleinformatyka, Cyberbezpieczeństwo
Stopień studiów i forma: II stopień, stacjonarna
Rodzaj przedmiotu: obowiązkowy
Kod przedmiotu: FZEU00200
Grupa kursów: NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15				
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	30				
Forma zaliczenia	Zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	1				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	-				
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	0,5				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI SPOŁECZNYCH

1. Znajomość podstaw analizy matematycznej i algebry

CELE PRZEDMIOTU

- C1. Zdobyć wiedzy 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:

PEK_W01 Zna i potrafi wyjaśnić podstawowe prawa związane z podstawami mechaniki kwantowej

PEK_W02 Zna i potrafi wyjaśnić podstawowe prawa teorii względności.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wprowadzenie: zakres i metodologia fizyki; metoda naukowa.	1
Wy2	Podstawy mechaniki kwantowej.	2
Wy3	Atom wodoru, widmo absorpcji i emisji.	2
Wy4	Układy wieloatomowe, typy wiązań atomowych, struktury krystaliczne, ciekłe kryształy.	2
Wy5	Wybrane problemy mechaniki kwantowej.	2
Wy6	Elementy teorii względności.	2
Wy7	Fizyka w zastosowaniach inżynierskich.	2
Wy8	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	PEK_W01, PEK_W02	Aktywność na wykładach, zaliczenie kartkówek pisemnych
F2	PEK_W01, PEK_W02	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

LITERATURA UZUPEŁNIAJĄCA:

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

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

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

WYDZIAŁ ELEKTRONIKI	
KARTA PRZEDMIOTU	
Nazwa w języku polskim:	Matematyka
Nazwa w języku angielskim:	Mathematics
Kierunek studiów:	Teleinformatyka, Cyberbezpieczeństwo
Stopień studiów i forma:	II stopień, stacjonarna
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	MAEU00102
Grupa kursów:	TAK

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15	15			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	30				
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 INNYCH KOMPETENCJI SPOŁECZNYCH
<ol style="list-style-type: none"> 1. Znajomość rachunku różniczkowego i całkowego 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
<p>C1 Poznanie podstawowych pojęć, twierdzeń, metod i zastosowań dotyczących przestrzeni liniowych oraz przekształceń liniowych w przestrzeniach wektorowych.</p> <p>C2. Poznanie pojęcia funkcji zespolonej, jej pochodnej i całki.</p> <p>C3. Poznanie podstawowych pojęć, twierdzeń i metod dotyczących przestrzeni Banacha oraz przestrzeni Hilberta.</p> <p>C4. Poznanie pojęcia transformacji Fouriera i Laplace'a ich podstawowych własności i zastosowań.</p>

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA	
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 zadaniem 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 ELEKTRONIKI	
KARTA PRZEDMIOTU	
Nazwa w języku polskim:	Przedsiębiorczość w ICT
Nazwa w języku angielskim:	ICT Business
Kierunek studiów:	Teleinformatyka
Stopień studiów i forma:	II stopień, Ogólnoakademicki
Rodzaj przedmiotu:	obowiązkowy
Kod przedmiotu:	TLEU00116
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 kontaktu (BK)	2				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 metod analizy rynku teleinformatycznego
- C4 Nabycie umiejętności wyszukiwania, opracowania i prezentacji treści technicznych

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:

PEK_W01 Wie, jak opisać model biznesowy działalności teleinformatycznej i objaśniać ekonomiczne podstawy działalności gospodarczej, rozpoznawać kondycję finansową firm, określić strategię marketingową, określania cen produktów i usług.

Z zakresu umiejętności:

PEK_U01 Potrafi korzystać z raportów o stanie rynku teleinformatycznego. Potrafi interpretować trendy rynkowe. Umie przygotować projekcje finansowe. Potrafi opracować biznes plan.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		Liczba godzin
Wy1	Wprowadzenie	2
Wy2	Społeczeństwo informacyjne	2
Wy3	Prawo telekomunikacyjne	2
Wy4	Działalność telekomunikacyjna – uprawnienia	2
Wy5	Rynek teleinformatyczny – podstawy	2
Wy6	Analiza rynku telekomunikacyjnego	2
Wy7	Działania marketingowe – badania rynku, cena usług, zapotrzebowanie na usługi, czynniki ryzyka	2
Wy8	Planowanie sieci nakłady inwestycyjne i koszty eksploatacji	2
Wy9	Planowanie działalności telekomunikacyjnej – biznes plan	2
Wy10	Strategia ustalania cen usług – przychody, plany taryfowe	2
Wy11	Projekcje finansowe	2
Wy12	Zarządzanie projektami teleinformatycznymi	2
Wy13	Przykład działalności teleinformatycznej – analiza przypadku I	2
Wy14	Przykład działalności teleinformatycznej – analiza przypadku II	2
Wy15	Repetitorium	2
Suma godzin		30

Forma zajęć - seminarium		Liczba godzin
Se1	Wprowadzenie do seminarium, omówienie planu i warunków zaliczenia.	1
Se2	Omówienie tematów seminaryjnych, dostępnych źródeł informacji	1
Se3	Rozdanie tematów seminaryjnych, ustalenie zasad oceny prezentacji i harmonogramu prezentacji	1
Se4	Prezentacje opracowanych tematów, ocena prezentacji, dyskusja ze studentami	12
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	Aktywność na wykładach, kolokwium zaliczające
F2	PEK_W01 PEK_U01	Aktywność na zajęciach seminaryjnych, ocena prezentacji seminaryjnych przygotowanych 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] Eugeniusz W. Gaca, Krzysztof J. Heller, Paweł M. Marchelek, Budowa sieci szerokopasmowych. Projekt techniczny, budowa i eksploatacja sieci. Część II. Poradnik dla samorządowców, Fundacja Wspomagania Wsi, Warszawa 2009.
- [2] Wiesław Baług, Jarosław Józik, Robert Mierzwiński, Jacek Oko, Andrzej Sobczak, Ostatnia mila. Budowa i eksploatacja teleinformatycznej sieci dostępowej. Część III. Poradnik dla operatorów i samorządowców, Fundacja Wspomagania Wsi, Warszawa 2010.
- [3] Maciej Rogalski, Zmiany w prawie telekomunikacyjnym. Komentarz, WoltersKluwer Polska, Warszawa 2006.
- [4] Gołaczyński J. (red.), Prawne i ekonomiczne aspekty komunikacji elektronicznej, LexisNexis, Warszawa 2003.
- [5] Brigham E.F., Gapenski L.C., Zarządzanie finansami, PWE, Warszawa 2000.

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

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