Zał. nr 5 do ZW 13/2019

WYDZIAŁ INFORMATYKI I ZARZĄDZANIA

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim Bezpieczeństwo infrastruktury krytycznej
Nazwa przedmiotu w języku angielskim Critical Infrastructure Cybersecurity
Kierunek studiów (jeśli dotyczy): Inżynieria Systemów
Specjalność (jeśli dotyczy): ……..
Poziom i forma studiów: I / ~~II stopień~~ / ~~jednolite studia magisterskie~~*, stacjonarna / ~~niestacjonarna~~*
Rodzaj przedmiotu: obowiązkowy / ~~wybieralny~~ / ~~ogólnouczelniany~~ *
Kod przedmiotu INZ001846
Grupa kursów TAK / ~~NIE~~*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	30		30		
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	**1**		1		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)					
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	0,8		0,8		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

1. Wiedza z zakresu rachunku prawdopodobieństwa
2. Wiedza z zakresu matematyki dyskretnej
3. Wiedza z zakresu sieci komputerowych i transmisji danych

\

CELE PRZEDMIOTU

C1 Poznanie aktualnych problemów z zakresu bezpieczeństwa systemów informatycznych oraz infrastruktury krytycznej
C2 Poznanie metod i przykładowych rozwiązań związanych z gwarantowaniem wysokiego poziomu bezpieczeństwa.
C3 Poznanie metod projektowania rozwiązań bezpieczeństwa dla systemów infrastruktury krytycznej.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:
PEK_W01 Posiada wiedzę o zagrożeniach bezpieczeństwa
PEK_W02 Posiada wiedzę z zakresu wybranych zagadnień z kryptologii
PEK_W03 Posiada wiedzę o metodach zapewnienia bezpieczeństwa

Z zakresu umiejętności:
PEK_U01 Umie identyfikować zagrożenia dla bezpieczeństwa informatycznego
PEK_U02 Potrafi identyfikować potrzeby w zakresie ochrony systemów informatycznych
PEK_U03 Umie wybrać metody ochrony dla zapewnienia bezpieczeństwa informatycznego

Z zakresu kompetencji społecznych:
PEK_K01 Rozumie konieczność ochrony systemów infrastruktury krytycznej
PEK_K02 Rozumie wpływ zagrożeń bezpieczeństwa informatycznego dla funkcjonowania gospodarki elektronicznej

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Problemy bezpieczeństwa w systemach infrastruktury krytycznej	2
Wy2	Plan ochrony bezpieczeństwa	2
Wy3	Architektura bezpieczeństwa danych i systemów w Internecie rzeczy	2
Wy4	Kryptograficzna ochrona danych	2
Wy5	Bezpieczeństwo komunikacji	2
Wy6	Zarządzanie tożsamością i kontrola dostępu	2
Wy7	Bezpieczeństwo chmur obliczeniowych i aplikacji	2
Wy8	Utrwalenie wiadomości	1
	Suma godzin	**15**

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

Forma zajęć - laboratorium		**Liczba godzin**
La1	Techniki rekonesansu	3
La2	Rekonesans sieciowy	3
La3	Reakcja na incydenty	3
La4	Bezpieczeństwo infrastruktury korporacyjnej	3
La5	Skanowanie bezpieczeństwa systemów	3

La6	Podstawowe podatności	3
La7	Ocena konsekwencji incydentu	3
La8	Analiza powłamaniowa	3
La9	Narzędzia analizy bezpieczeństwa	3
La10	Utrwalenie materiału	3
	Suma godzin	30

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

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

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1.Wykład tradycyjny. N2. Zajęcia laboratoryjne. 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_W01, PEK_W02, PEK_W03, PEK_K01, PEK_K02.	Ocena stopnia przygotowania do realizacji ćwiczeń laboratoryjnych
F2	PEK_U01, PEK_U02, PEK_K03.	Ocena realizacji zadań laboratoryjnych
P	PEK_W01, PEK_W02, PEK_W03, PEK_K01, PEK_K02.	Test wiedzy
F1		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Ackerman, Pascal. Industrial Cybersecurity: Efficiently secure critical infrastructure systems. Packt Publishing Ltd, 2017.

[2] Stallings, William. Cryptography and network security: principles and practice. Pearson Education India, 2003.

[3] Anderson, Ross. Security engineering. John Wiley & Sons, 2008.

[4] CompTIA Cybersecurity Analyst CySA+ (CS0-001)

LITERATURA UZUPEŁNIAJĄCA:

[5] Schneier, Bruce. Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.

[6] NIST · Special Publications (NIST-SP) : http://www.nist.gov/publication-portal.cfm

[7] Giacomo Veneri, Antonio Capasso, Hands-On Industrial Internet of Things, Packt Publishing Ltd, 2018

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

Grzegorz Kołaczek, Grzegorz.Kolaczek@pwr.edu.pl