



IV. Opis programu studiów

3. KARTA PRZEDMIOTU

Kod przedmiotu	M#1-S1-IB-KiK-612
Nazwa przedmiotu	Nowoczesne Metody Kryptograficzne
Nazwa przedmiotu w języku angielskim	Modern Cryptographic Methods
Obowiązuje od roku akademickiego	2019/2020

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	INŻYNIERIA BEZPIECZEŃSTWA
Poziom kształcenia	I stopień
Profil studiów	Ogólnoakademicki
Forma i tryb prowadzenia studiów	Studia stacjonarne
Zakres	Kryminalistyka i Kryptologia
Jednostka prowadząca przedmiot	Katedra Technik Komputerowych i Uzbrojenia
Koordinator przedmiotu	dr inż. Konrad Stefański
Zatwierdził	

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	Przedmiot specjalnościowy
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	Polski
Usytuowanie modułu w planie studiów - semestr	Semestr 6
Wymagania wstępne	
Egzamin (TAK/NIE)	NIE
Liczba punktów ECTS	2

Forma prowadzenia zajęć	wykład	ćwiczenia	laboratorium	projekt	seminarium
Liczba godzin w semestrze	15		15		

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Ma podstawową wiedzę na temat współczesnych metod zapewnienia bezpieczeństwa przesyłania informacji. Posiada podstawową wiedzę na temat zagrożeń z tym związanych.	IB1_W21
	W02	Dysponuje podstawową wiedzą na szyfrowania i deszyfrowania danych i podstawowych algorytmów.	IB1_W21
Umiejętności	U01	Potrafi zastosować podstawowe algorytmy służące szyfrowaniu i deszyfrowaniu danych.	IB1_U34
Kompetencje społeczne	K01	Rozumie potrzebę dokończania się i podnoszenia swoich kompetencji zawodowych w zakresie monitorowania zagrożeń.	IB1_K01
	K02	Potrafi pracować w zespole.	IB1_K04

TREŚCI PROGRAMOWE

Forma zajęć*	Treści programowe
wykład	Kryptografia klasyczna – podstawowa terminologia. Klasyfikacja zagrożeń. Proste szyfry. Algorytmy kryptograficzne. Współczesne kryptogramy. Poufność i uwiarygodnianie.
laboratorium	Zastosowanie algorytmów służących do szyfrowania i deszyfrowania informacji. Zastosowanie mechanizmów kryptograficznych.

*) zostawić tylko realizowane formy zajęć

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia (zaznaczyć X)					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X			
W02			X			
U01					X	
K01						X
K02						X

FORMA I WARUNKI ZALICZENIA

Forma zajęć*	Forma zaliczenia	Warunki zaliczenia
wykład	Zaliczenie z oceną	Uzyskanie co najmniej połowy punktów z kolokwium zaliczeniowego.
laboratorium	Zaliczenie z oceną	Złożenie wszystkich sprawozdań z ćwiczeń laboratoryjnych. Obecność na zajęciach..

*) zostawić tylko realizowane formy zajęć

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS							
Lp.	Rodzaj aktywności	Obciążenie studenta					Jednostka
		W	C	L	P	S	
1.	Udział w zajęciach zgodnie z planem studiów	15		15			h
2.	Inne (konsultacje, egzamin)	2		2			h
3.	Razem przy bezpośrednim udziale nauczyciela akademickiego	34					h
4.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	1,4					ECTS
5.	Liczba godzin samodzielnej pracy studenta	16					h
6.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	0,6					ECTS
7.	Nakład pracy związany z zajęciami o charakterze praktycznym	25					h
8.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	1,0					ECTS
9.	Sumaryczne obciążenie pracą studenta	50					h
10.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	2					ECTS

LITERATURA

1. M. Kutyłowski i W. B. Strothmann Kryptografia: Teoria i praktyka zabezpieczania systemów komputerowych, Wyd. READ ME, Warszawa, 1999,
2. B. Schneier: Kryptografia dla praktyków, WNT, Warszawa, 2002, wydanie drugie
3. D. R. Stinson, Kryptografia, WNT, Warszawa, 2005
4. R. Wobst, Kryptologia. Budowa i łamanie zabezpieczeń, RM, Warszawa, 2002