Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

KARTA OPISU PRZEDMIOTU

STUDIA PODYPLOMOWE	**INFORMATYKA Z ELEMENTAMI INFORMATYKI ŚLEDCZEJ**

NAZWA PRZEDMIOTU	**KRYPTOGRAFIA I STEGANOGRAFIA**		
SUBJECT TITLE	**CRYPTOGRAPHY AND STEGANOGRAPHY**		
SEMESTR STUDIÓW	ECTS (pkt.)	TRYB ZALICZENIA PRZEDMIOTU	KOD PRZEDMIOTU
2	3	EGZAMIN	
Wymagania wstępne w zakresie przedmiotu	Nazwy przedmiotów	-	
	Wiedza	1. Podstawowa wiedza z zakresu technologii informac.	
	Umiejętności	1. Potrafi obsługiwać komputer i system operacyjny	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	

PROGRAM PRZEDMIOTU		
FORMA ZAJĘĆ	LICZBA GODZIN ZAJĘĆ W SEMESTRZE	PROWADZĄCY ZAJĘCIA (tytuł/stopień naukowy, imię i nazwisko)
WYKŁAD	10	MGR INŻ. ARTUR KALINOWSKI
ĆWICZENIA		
LABORATORIUM	10	MGR INŻ. ARTUR KALINOWSKI
PROJEKT		
SEMINARIUM		

TREŚCI KSZTAŁCENIA (PROGRAM NAUCZANIA)			
WYKŁAD	SPOSÓB REALIZACJI:	WYKŁAD Z WYKORZYSTANIEM RZUTNIKA	
Lp.	Tematyka zajęć		Liczba godzin
1.	Pojęcie kryptografii i steganografii		1
2.	Różnice między szyfrowaniem a kodowaniem informacji		1
3.	Przegląd popularnych algorytmów szyfrowania		1
4.	Jednokierunkowe funkcje skrótu jako element zwiększający bezpieczeństwo		1
5.	Kodowanie i szyfrowanie danych jako element zabezpieczeń		1
6.	Podstawowe metody kryptoanalizy		1
7.	Szyfrowanie asymetryczne i metoda ataku		1
8.	Steganografia z wykorzystaniem plików tekstowych		1
9.	Steganografia z wykorzystaniem plików binarnych		1
10.	Steganaliza (ujawnianie ukrytych danych) Zaliczenie przedmiotu.		1
		RAZEM GODZIN W SEMESTRZE	10
Sposoby sprawdzenia zamierzonych efektów kształcenia		Kolokwium pisemne	

LABORATORIUM	SPOSÓB REALIZACJI:	ZAJĘCIA PRAKTYCZNE Z KOMPUTEREM	
Lp.	Tematyka zajęć		Liczba godzin
1.	Wykorzystanie standardowych funkcji kryptograficznych systemu operacyjnego i aplikacji		1
2.	Kodowanie i dekodowanie informacji, rozpoznawanie typów funkcji skrótu oraz metod szyfrowania		1
3.	Generowanie tęczowych tablic i wykorzystywanie baz skrótów (hash)		1

4.	Łamanie haseł zaszyfrowanych archiwów z wykorzystaniem systemu Linux	1
5.	Ujawnianie treści zakodowanej strony oraz zakodowanych danych w pliku cookies celem modyfikacji i podniesienia uprawnień	1
6.	Wybrane metody szyfrowania i ataków na szyfrogramy	1
7.	Test Kasiskiego	1
8.	Ukrywanie danych tekstowych i binarnych w plikach tekstowych	1
9.	Ukrywanie danych tekstowych i binarnych w plikach binarnych	1
10.	Analiza LSB jako technika ujawniania zakamuflowanych danych	1
	RAZEM GODZIN W SEMESTRZE	10
Sposoby sprawdzenia zamierzonych efektów kształcenia:	Wykonanie zadań wyznaczonych w trakcie zajęć	

Efekty kształcenia dla przedmiotu – po zakończonym cyklu kształcenia	Wiedza	1. Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu prostych zadań inżynierskich z zakresu kryptografii, kryptoanalizy oraz steganografii 2. Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony danych
	Umiejętności	1. Ma umiejętność samokształcenia się i wyszukiwania potrzebnych informacji 2. Potrafi pozyskiwać i analizować dane, oraz interpretować otrzymane wyniki
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role. 2. Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.

ZAŁOŻENIA I CELE PRZEDMIOTU:
Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie rozpoznawania wybranych typów szyfrów i typów kodowania informacji oraz podstawowych umiejętności w zakresie kryptoanalizy i steganalizy.

METODY DYDAKTYCZNE:
Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (środki: rzutnik, komputer, prezentacje).
Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, spreparowane pliki opracowane przez prowadzącego).

FORMA I WARUNKI ZALICZENIA PRZEDMIOTU:
Wykład – zaliczenie pisemne na ocenę.
Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

LITERATURA PODSTAWOWA:
[1] Karbowski M., *Podstawy kryptografii.* ISBN: 978-83-246-1215-4, Helion, 2007
[2] Pieprzyk J., Hardjono T., Seberry J., *Teoria bezpieczeństwa systemów komputerowych.,* ISBN: 83-7361-678-0, Helion, 2005
[3] Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii.,* ISBN: 978-83-246-2986-2, 2011

LITERATURA UZUPEŁNIAJĄCA:
[1] Sklyarov I., *Hakerskie łamigłówki*, ISBN: 83-246-0422-7, Helion, 2006

*) niewłaściwe przekreślić

..... /Kierownik studiów podyplomowych/

..... /autor – osoba prowadząca wykład/

..... /Kierownik jednostki organizacyjnej: pieczęć i podpis/

..... /Dziekan Wydziału WEAiI: pieczęć i podpis/