Załącznik nr 7
do Zarządzenia Rektora nr 10/12
z dnia 21 lutego 2012r.

KARTA MODUŁU / KARTA PRZEDMIOTU

Kod modułu	**EiT_S_I_BST_AEwT**
Nazwa modułu	**Bezpieczeństwo systemów teleinformatycznych**
Nazwa modułu w języku angielskim	**Security of computer and communication systems**
Obowiązuje od roku akademickiego	**2012/2013**

A. USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	**Elektronika i Telekomunikacja**
Poziom kształcenia	**I stopień** *(I stopień / II stopień)*
Profil studiów	**ogólnoakademicki** *(ogólno akademicki / praktyczny)*
Forma i tryb prowadzenia studiów	**stacjonarne** *(stacjonarne / niestacjonarne)*
Specjalność	**Aparatura elektroniczna w telekomunikacji**
Jednostka prowadząca moduł	**Katedra Telekomunikacji, Fotoniki i Nanomateriałów**
Koordynator modułu	**dr inż. Agnieszka Chodorek**
Zatwierdził:	

B. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	**kierunkowy** *(podstawowy / kierunkowy / inny HES)*
Status modułu	**obowiązkowy** *(obowiązkowy / nieobowiązkowy)*
Język prowadzenia zajęć	**język polski**
Usytuowanie modułu w planie studiów - semestr	**semestr VI**
Usytuowanie realizacji przedmiotu w roku akademickim	**semestr letni** *(semestr zimowy / letni)*
Wymagania wstępne	**Systemy i sieci telekomunikacyjne, Architektura i systemy operacyjne komputerów** *(kody modułów / nazwy modułów)*
Egzamin	**nie** *(tak / nie)*
Liczba punktów ECTS	**4**

Forma prowadzenia zajęć	**wykład**	**ćwiczenia**	**laboratorium**	**Projekt**	**inne**
w semestrze	**30**		**30**		

C. EFEKTY KSZTAŁCENIA I METODY SPRAWDZANIA EFEKTÓW KSZTAŁCENIA

Cel modułu	Celem modułu jest zapoznanie studentów z podstawowymi zagadnieniami z zakresu bezpieczeństwa systemów teleinformatycznych. Szczególną uwagę zwrócono na zagadnienia kryptografii i ochrony danych oraz zrozumienie znaczenia rozwiązań wspierających bezpieczeństwo.

Symbol efektu	Efekty kształcenia	Forma prowadzenia zajęć *(w/ć/l/p/inne)*	odniesienie do efektów kierunkowych	odniesienie do efektów obszarowych
W_01	zna i rozumie typowe problemy ochrony danych	w	K_W10	T1A_W03
W_02	ma podstawową wiedzę z zakresu kryptografii	w	K_W15	T1A_W04, T1A_W07
W_03	zna metody rozwiązywania prostych problemów związanych z zapewnianiem bezpieczeństwa systemów teleinformatycznych	w/l	K_W10	T1A_W07
U_01	potrafi dobrać metodę zapewnienia bezpieczeństwa systemu teleinformatycznego	l	K_U23 K_U27	T1A_U15
U_02	potrafi dobrać typowy algorytm kryptograficzny, odpowiedni dla żądanego poziomu bezpieczeństwa, adekwatnie do zasobów i wydajności	l	K_U27	T1A_U15
K_01	jest świadomy ważności i rozumie pozatechniczne aspekty rozwiązań wspierających bezpieczeństwo.	w	K_K02	T1A_K02
K_02	ma świadomość odpowiedzialności za pracę własną i ponoszenia odpowiedzialności za realizowane zadania	w/l	K_K03	T1A_K04

Treści kształcenia:

1. Treści kształcenia w zakresie wykładu

Nr wykładu	Treści kształcenia	Odniesienie do efektów kształcenia dla modułu
1	Wprowadzenie do bezpieczeństwa systemów teleinformatycznych.	W_01
2, 3	Pojęcia związane z bezpieczeństwem. Formalno-prawne aspekty bezpieczeństwa teleinformatycznego.	W_01 K_01
4, 5	Wprowadzenie do kryptografii. Szyfry podstawieniowe i maszynowe.	W_02
6, 7	Szyfry symetryczne i asymetryczne. Szyfry strumieniowe.	W_02
8	Steganografia i cyfrowe znaki wodne	W_01 W_03
9, 10	Bezpieczeństwo stacji i bezpieczeństwo serwera.	W_01 W_03
11, 12, 13	Bezpieczeństwo sieci. IPSec. PGP. Bezpieczeństwo sieci VPN.	W_01 W_03
14	Cyberterroryzm.	W_01 K_01
15	Kolokwium	K_02

2. Treści kształcenia w zakresie ćwiczeń

Nr zajęć ćwicz.	Treści kształcenia	Odniesienie do efektów kształcenia dla modułu

3. Treści kształcenia w zakresie zadań laboratoryjnych

Nr zajęć lab.	Treści kształcenia	Odniesienie do efektów kształcenia dla modułu
1	Wprowadzenie. Wykorzystywane narzędzia.	W_03
2, 3, 4	Lokalna i zdalna kontrola dostępu	U_01
5, 6, 7, 8	Kryptografia i kryptograficzna ochrona komunikacji	U_02
9	Steganografia i cyfrowe znaki wodne	U_01
10, 11	Zabezpieczanie stacji i serwera usług	U_01 U_02
12, 13	Zapory sieciowe i wykrywanie zagrożeń	U_01
14	Wirtualne sieci prywatne	U_01 U_02
15	Kolokwium	K_02

4. Charakterystyka zadań projektowych
5. Charakterystyka zadań w ramach innych typów zajęć dydaktycznych

Metody sprawdzania efektów kształcenia

Symbol efektu	Metody sprawdzania efektów kształcenia *(sposób sprawdzenia, w tym dla umiejętności – odwołanie do konkretnych zadań projektowych, laboratoryjnych, itp.)*
W_01	kolokwium
W_02	kolokwium
W_03	kolokwium
U_01	kolokwium, sprawozdania z laboratorium
U_02	kolokwium, sprawozdania z laboratorium
K_01	kolokwium
K_02	kolokwium

D. NAKŁAD PRACY STUDENTA

Bilans punktów ECTS		
	Rodzaj aktywności	**obciążenie studenta**
1	Udział w wykładach	30
2	Udział w ćwiczeniach	
3	Udział w laboratoriach	30
4	Udział w konsultacjach (2-3 razy w semestrze)	1
5	Udział w zajęciach projektowych	
6	Konsultacje projektowe	
7	Udział w egzaminie	
8		
9	**Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela akademickiego**	**61** *(suma)*
10	**Liczba punktów ECTS, którą student uzyskuje na zajęciach wymagających bezpośredniego udziału nauczyciela akademickiego** *(1 punkt ECTS=25-30 godzin obciążenia studenta)*	**2,44**
11	Samodzielne studiowanie tematyki wykładów	4
12	Samodzielne przygotowanie się do ćwiczeń	
13	Samodzielne przygotowanie się do kolokwiów	5
14	Samodzielne przygotowanie się do laboratoriów	10
15	Wykonanie sprawozdań	15
15	Przygotowanie do kolokwium końcowego z laboratorium	5
17	Wykonanie projektu lub dokumentacji	
18	Przygotowanie do egzaminu	
19		
20	**Liczba godzin samodzielnej pracy studenta**	**39** *(suma)*
21	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy** *(1 punkt ECTS=25-30 godzin obciążenia studenta)*	**1,56**
22	**Sumaryczne obciążenie pracą studenta**	**100**
23	**Punkty ECTS za moduł** *1 punkt ECTS=25-30 godzin obciążenia studenta*	**4**
24	**Nakład pracy związany z zajęciami o charakterze praktycznym** *Suma godzin związanych z zajęciami praktycznymi*	**60**
25	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym** *1 punkt ECTS=25-30 godzin obciążenia studenta*	**2,4**

E. LITERATURA

Wykaz literatury	1. Pieprzyk J., Hardjono T., Seberry J.: „Teoria bezpieczeństwa systemów komputerowych”. Wyd. Helion, 2005 2. Cheswick W. R.: „Firewalle i bezpieczeństwo w sieci”. Wyd. Helion, 2003 3. Ferguson N., Schneier B.: „Kryptografia w praktyce”. Helion, 2004
Witryna WWW modułu/przedmiotu	