I. KARTA PRZEDMIOTU

1. Nazwa przedmiotu: **BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH**
2. Kod przedmiotu: **Bsi**
3. Jednostka prowadząca: **Wydział Mechaniczno-Elektryczny**
4. Kierunek: **Automatyka i Robotyka**
5. Specjalność: **Informatyka Stosowana**
6. Moduł: **treści specjalnościowych**
7. Poziom studiów: **I stopnia**
8. Forma studiów: **stacjonarne**
9. Semestr studiów: **VII**
10. Profil: **ogólnoakademicki**
11. Prowadzący: **dr hab. inż. Tomasz Praczyk**

CEL PRZEDMIOTU

C1	Zapoznanie studentów z kryptografią symetryczną
C2	Zapoznanie studentów z kryptografią asymetryczną
C3	Zapozanie studentów z zagrożeniami płynącymi z użytkowania systemów informatycznych oraz technikami zabezpieczania systemów.
C4	Uświadomienie studentom konsekwencji prawnych związanych z użytkowaniem systemów informatycznych.

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1	Znajomość algebry Boola.
2	Podstawowa znajomość systemów operacyjnych.

EFEKTY KSZTAŁCENIA

EK1	Student zna model szyfrowania symetrycznego i zasadę działania podstawowych szyfrów symetrycznych (techniki podstawieniowe i przestawieniowe). Orientuje się w nazewnictwie, zasadach działania współczesnych szyfrów blokowych i strumieniowych.
EK2	Student zna zasadę działania kryptografii klucza publicznego, orientuje się w nazewnictwie, zagadnieniach złożoności obliczeniowej algorytmów kryptografii asymetrycznej. Zna schematy podpisów cyfrowych. Rozumie zaganienia związane z dystrybucją kluczy kryptograficznych.
EK3	Student ma świadomość konsekwencji prawnych związanych z niewłaściwym użytkowaniem systemów informatycznych. Zna podstawowe przepisy kodeksu karnego dotyczące przetwarzania informacji w systemach informatycznych.
EK4	Student potrafi w sposób praktyczny wykorzystać zdobytą wiedzę do zabezpieczania i przełamywania zabezpieczeń systemów informatycznych.

TREŚCI PROGRAMOWE

	WYKŁADY	Liczba godzin
W1	Wprowadzenie do zagadnień bezpieczeństwa informatycznego.	**1**
W2	Klasyczne techniki szyfrowania.	**1**
W3	Szyfry blokowe.	**2**
W4	Szyfry strumieniowe i generatory liczb pseudolosowych.	**2**
W5	Kryptografia klucza publicznego.	**1**
W6	Podpisy cyfrowe.	**1**
W7	Zarządzanie kluczami i dystrybucja kluczy.	**1**
W8	Aspekty prawne i etyczne.	**1**
	Razem	**10**

ĆWICZENIA

Ć1	Podstawowe zagadnienia związane z bezpieczeństwem informatycznym	**2**
	Razem	**2**

ZAJĘCIA LABORATORYJNE

L1	Laboratorium z klasycznych technik szyfrowania.	**2**
L2	Laboratorium z szyfrowania symetrycznego.	**4**
L3	Laboratorium z szyfrowania asymetrycznego.	**6**
L4	Bezpieczeństwo komputera osobistego - aktualizacje, ochrona antywirusowa, prywatność.	**4**
L5	Bezpieczeństwo komputera osobistego - kopie zapasowe, praktyczne szyfrowanie.	**2**
	Razem	**18**

NARZĘDZIA DYDAKTYCZNE

1	Notebook z projektorem
2	Tablica i kolorowe pisaki
3	Stanowiska komputerowe z oprogramowaniem dydaktycznym

SPOSOBY OCENY

FORMUJĄCA

F1	Sprawdzian	EK1-EK4
F2	Odpowiedź ustna	EK1-EK4
F3	Wykonanie zadanie obliczeniowego	EK1-EK2, EK4

PODSUMOWUJĄCA

P1	Kolokwium	EK1-EK4

OBCIĄŻENIE PRACĄ STUDENTA

Forma aktywności	**Średnia liczba godzin na zrealizowanie aktywności**	
semestr	**VII**	**razem**
udział w wykładach	10	10
udział w ćwiczeniach	2	2
udział w zajęciach laboratoryjnych	18	18
Konsultacje	4	4
Przygotowanie do wykładów i laboratoriów	16	16
SUMA GODZIN W SEMESTRZE	**50**	**50**
PUNKTY ECTS W SEMESTRZE	**2**	**2**

LITERATURA

PODSTAWOWA

1	William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Matematyka szyfrów i techniki kryptologii, Wydawnictwo Helion, 2011
2	William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Koncepcje i metody bezpiecznej komunikacji, Wydawnictwo Helion, 2012
3	Menezes A.J. , P. van Oorschot, Vanstone S.A., Kryptografia stosowana, WNT, 2005

UZUPEŁNIAJĄCA

4	Schneier B., Kryptografia dla praktyków, WNT, 2002

PROWADZĄCY PRZEDMIOT

1	dr hab. inż. Tomasz Praczyk, T.Praczyk@amw.gdynia.pl

Formy oceny

Efekt	Na ocenę 2	Na ocenę 3	Na ocenę 4	Na ocenę 5
EK1	*Student zna model szyfrowania symetrycznego i zasadę działania podstawowych szyfrów symetrycznych (techniki podstawieniowe i przestawieniowe). Orientuje się w nazewnictwie, zasadach działania współczesnych szyfrów blokowych i strumieniowych.*			
	Student nie zna modelu szyfrowania symetrycznego, ani zasad działania podstawowych szyfrów symetrycznych (techniki podstawieniowe i przestawieniowe). Nie orientuje się w nazewnictwie, zasadach działania współczesnych szyfrów blokowych i strumieniowych.	Student zna model szyfrowania symetrycznego i zasadę działania podstawowych szyfrów symetrycznych (techniki podstawieniowe i przestawieniowe). Nie orientuje się w nazewnictwie, zasadach działania współczesnych szyfrów blokowych i strumieniowych.	Student zna model szyfrowania symetrycznego, lecz nie rozumie zasady działania podstawowych szyfrów symetrycznych (techniki podstawieniowe i przestawieniowe). Przeciętnie orientuje się w nazewnictwie, zasadach działania współczesnych szyfrów blokowych i strumieniowych.	Student zna model szyfrowania symetrycznego i zasadę działania podstawowych szyfrów symetrycznych (techniki podstawieniowe i przestawieniowe). Bardzo dobrze orientuje się w nazewnictwie, zasadach działania współczesnych szyfrów blokowych i strumieniowych.
EK2	*Student zna zasadę działania kryptografii klucza publicznego, orientuje się w nazewnictwie, zagadnieniach złożoności obliczeniowej algorytmów kryptografii asymetrycznej. Zna schematy podpisów cyfrowych. Rozumie zaganienia związane z dystrybucją kluczy kryptograficznych.*			
	Student nie zna zasad działania kryptografii klucza publicznego,nie orientuje się w nazewnictwie, zagadnieniach złożoności obliczeniowej algorytmów kryptografii asymetrycznej. Nie zna schematów podpisów cyfrowych. Nie rozumie zaganienia związane z dystrybucją kluczy kryptograficznych.	Student zna zasadę działania kryptografii klucza publicznego, przeciętnie orientuje się w nazewnictwie oraz zagadnieniach złożoności obliczeniowej algorytmów kryptografii asymetrycznej. Nie zna schematów podpisów cyfrowych. Nie rozumie zaganień związanych z dystrybucją kluczy kryptograficznych.	Student zna zasadę działania kryptografii klucza publicznego, dobrze orientuje się w nazewnictwie, zagadnieniach złożoności obliczeniowej algorytmów kryptografii asymetrycznej. Zna schematy podpisów cyfrowych. Nie rozumie zaganień związanych z dystrybucją kluczy kryptograficznych.	Student zna zasadę działania kryptografii klucza publicznego, bardzo dobrze orientuje się w nazewnictwie, zagadnieniach złożoności obliczeniowej algorytmów kryptografii asymetrycznej. Zna schematy podpisów cyfrowych. Rozumie zaganienia związane z dystrybucją kluczy kryptograficznych.
EK3	*Student ma świadomość konsekwencji prawnych związanych z niewłaściwym użytkowaniem systemów informatycznych. Zna podstawowe przepisy kodeksu karnego dotyczące przetwarzania informacji w systemach informatycznych.*			
	Student nie ma świadomości konsekwencji prawnych związanych z użytkowaniem systemów informatycznych. Nie zna podstawowych przepisów kodeksu karnego dotyczące przetwarzania informacji w systemach informatycznych.	Student ma orgraniczoną świadomość konsekwencji prawnych związanych z niewłaściwym użytkowaniem systemów informatycznych. Nie zna podstawowych przepisów kodeksu karnego dotyczące przetwarzania informacji w systemach informatycznych.	Student ma świadomość konsekwencji prawnych związanych z niewłaściwym użytkowaniem systemów informatycznych.Dobrze zna podstawowe przepisy kodeksu karnego dotyczące przetwarzania informacji w systemach informatycznych.	Student ma pełną świadomość konsekwencji prawnych związanych z niewłaściwym użytkowaniem systemów informatycznych. Bardzo dobrze zna podstawowe przepisy kodeksu karnego dotyczące przetwarzania informacji w systemach informatycznych.
EK4	*Student potrafi w sposób praktyczny wykorzystać zdobytą wiedzę do zabezpieczania i przełamywania zabezpieczeń systemów informatycznych.*			
	Student nie potrafi w praktyce wykorzystać zdobytej wiedzy do zabezpieczania i przełamywania zabezpieczeń systemów informatycznych.	Student potrafi w stopniu dostatecznym praktycznie wykorzystać zdobytą wiedzę do zabezpieczania i przełamywania zabezpieczeń systemów informatycznych.	Student potrafi w stopniu dobrym praktycznie wykorzystać zdobytą wiedzę do zabezpieczania i przełamywania zabezpieczeń systemów informatycznych.	Student potrafi w stopniu bardzo dobrym praktycznie wykorzystać zdobytą wiedzę do zabezpieczania i przełamywania zabezpieczeń systemów informatycznych.