	Nazwa modułu. **Blok przedmiotów wybieralnych**						Kod modułu: M23
Wypełnia Zespół	Nazwa przedmiotu: **Bezpieczeństwo transmisji sygnałów**						Kod przedmiotu:
	Nazwa jednostki prowadzącej przedmiot / moduł: **INSTYTUT INFORMATYKI STOSOWANEJ**						
	Nazwa kierunku: **INFORMATYKA**						
	Forma studiów: **stacjonarne**		Profil kształcenia: **PRAKTYCZNY**				Specjalność: **Grafika komputerowa i multimedia**
	Rok / semestr: **3/6**		Status przedmiotu /modułu: **obowiązkowy**				Język przedmiotu / modułu: **polski**
	Forma zajęć	wykład	ćwiczenia	ćwiczenia laboratoryjne	konwersatorium	seminarium	inne (wpisać jakie)
	Wymiar zajęć	**15**		**30**			

Koordynator przedmiotu / modułu	**dr hab. inż. Zenon Ulman**
Prowadzący zajęcia	**dr hab. inż. Zenon Ulman, dr inż. Robert Smyk**
Cel przedmiotu / modułu	Przedstawienie problematyki jak kluczowe jest bezpieczeństwo transmitowanej informacji. Zapoznanie z podstawowymi zagrożeniami oraz możliwościami zapobiegania im. Nauczenie studenta reakcji na incydent komputerowy.
Wymagania wstępne	Umiejętności analityczne, ugruntowana arytmetyka

EFEKTY KSZTAŁCENIA		Odniesienie do efektów dla **programu**
Nr	Wiedza	
01	Ma ogólną wiedzę na temat przewodowych i bezprzewodowych technik transmisji sygnałów	K_W04, K_W02, K_W06
02	Zna bezpośrednie sposoby ochrony informacji	K_W08
03	Zna zasady zarządzania bezpieczeństwem transmisji sygnałów	K_W12, K_W17
	Umiejętności	
04	Docenia wagę ochrony informacji w systemach teleinformatycznych	K_U09
05	Stosuje podstawowe algorytmy kryptograficzne	K_U07
06	Reaguje na incydent komputerowy	K_U10
	Kompetencje społeczne	
07	Zna prawne, społeczne i gospodarcze skutki naruszenia bezpieczeństwa informacji.	K_K02, K_K03
08	Zdaje sobie sprawę, że zasady bezpieczeństwa należy aktualizować oraz co pewien czas zmieniać środki ochrony.	K_K01

TREŚCI PROGRAMOWE

Forma zajęć – WYKŁAD

Ochrona pośrednia

1. Ogólne zasady ochrony informacji
2. Ochrona w internecie i systemach informatycznych
3. Przygotowanie i sposoby reagowania na włamania do sieci
4. Zalecenia odnośnie bezpiecznego użytkowania internetu przez młodzież i dzieci
5. Sposoby fizycznego zabezpieczania węzłów sieci
6. Typowe włamania hakerów i krakerów
7. Rodzaje zakłóceń transmisji informacji

Ochrona bezpośrednia

1. Kody detekcyjne i korekcyjne, redundancja.
2. Elementy teorii liczb. Podstawy kryptografii.
3. Arytmetyka modularna.
4. Standardy kryptografii, algorytmy symetryczne i niesymetryczne
5. Algorytmy i certyfikaty podpisu elektronicznego
6. Sposoby łamania szyfrów

Przepisy i instrukcje

Dyrektywy europejskie, przepisy i kodeksy prawne, normy, cerytfikaty. Instytucje standaryzujące, certyfikujące,

wywiadowcze i wspomagające poszkodowanych przez intruzów komputerowych.
Forma zajęć – LABORATORIUM
1. Analiza wybranych algorytmów strumieniowych na przykładzie technik zabezpieczania komunikacji bezprzewodowej 2. Analiza możliwości praktycznego wykorzystania pakietu kryptograficznego OpenSSL 3. Obliczanie dużych potęg liczby modulo 4. Projektowanie algorytmu RSA 5. Realizacja podpisu cyfrowego przy użyciu RSA 6. Projektowanie algorytmu El Gamala 7. Obliczanie podpisu cyfrowego przy użyciu algorytmu El Gamala 8. Wyznaczanie złożoności obliczeniowych z użyciem notacji duże O

Metody kształcenia	Wykład, ćwiczenia audytoryjne i laboratoryjne, konsultacje, tworzenie atmosfery sprzyjającej zainteresowaniu przedmiotem i dwustronna wymiana informacji

Metody weryfikacji efektów kształcenia	Nr efektu kształcenia z sylabusa
Dialog podczas wykładów i ćwiczeń	1 - 7
Kolokwia pisemne	1 - 7
Egzamin pisemny	1 - 7

Forma i warunki zaliczenia	Kolokwia, egzamin, zaliczenie ćwiczeń laboratoryjnych
Literatura podstawowa	1. M. Kutyłkowski, W. B. Strothmann: Kryptografia – teoria i praktyka zabezpieczania systemów komputerowych, Oficyna wydawnicza ReadME, Warszawa 1999 2. R. Andersen: Inżynieria zabezpieczeń, WNT 3. M. Konkowski: Podstawy kryptografii, Helion 2006 4. D. Pipkin: Bezpieczeństwo informacji, WNT
Literatura uzupełniająca	1. K. Mundia, Ch. Prossie: Hakerom smierć, Wydawnictwo RM 2. F.L. Bauer: Sekrety kryptografii, Helion 3. F.L. Bauer, S. Lloyd: Podpis elektroniczny, klucz publiczny, Robomatic, Wrocław 2002

NAKŁAD PRACY STUDENTA:

	Liczba godzin
Udział w wykładach	15
Samodzielne studiowanie tematyki wykładów	
Udział w ćwiczeniach audytoryjnych i laboratoryjnych*	30
Samodzielne przygotowywanie się do ćwiczeń*	10
Przygotowanie projektu / eseju / itp. *	15
Przygotowanie się do egzaminu / zaliczenia	
Udział w konsultacjach	5
Inne: egzamin	2
ŁĄCZNY nakład pracy studenta w godz.	87
Liczba punktów ECTS za przedmiot	**3 ECTS**
Obciążenie studenta związane z zajęciami praktycznymi*	55 **2,2 ECTS**
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	52 **2,1 ECTS**