KARTA PRZEDMIOTU

I. Przedmiot i jego usytuowanie w systemie studiów

Jednostka prowadząca kierunek studiów	Instytut Nauk Technicznych
Nazwa kierunku studiów	Informatyka w biznesie
Forma prowadzenia studiów	stacjonarne
Profil studiów	praktyczny
Poziom kształcenia	studia I stopnia
Nazwa przedmiotu	Bezpieczeństwo systemów informatycznych
Kod przedmiotu	K 14
Poziom/kategoria przedmiotu	przedmiot: kształcenia kierunkowego
Status przedmiotu	obowiązkowy
Usytuowanie przedmiotu w planie studiów	semestr 4
Język wykładowy	polski
Liczba punktów ECTS	3
Koordynator przedmiotu	
Odpowiedzialny za realizację przedmiotu	

2. Formy zajęć dydaktycznych i ich wymiar w planie studiów.

Wykład W	Ćwiczenia C	Konwersatorium K	Laboratorium L	Projekt P	Seminarium S	Praktyka PZ
15	-	-	30	-	-	-

3. Cele przedmiotu (opcjonalnie)

C1. Zapoznanie z wiedzą wybranych zagadnień z zakresu bezpieczeństwa systemów i sieci komputerowych, w szczególności szyfrowania i kryptografii.
C2. Nabycie umiejętności technik algorytmów szyfrowania, rodzajami i typami szyfrów, uwierzytelnianiem i podpisem cyfrowym.

4. Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji.

A. Wiedza z zakresu podstawy informatyki, sieci komputerowe.

5. Efekty kształcenia dla przedmiotu, wraz z odniesieniem do kierunkowych efektów kształcenia.

Symbol efektu	Opis efektów kształcenia dla przedmiotu	odniesienie do efektów kierunkowych	odniesienie do efektów obszarowych i inżynierskich
W zakresie wiedzy:			
W_01	Demonstruje sposoby szyfrowania informacji, uwierzytelniania, haszowania.	K_W07	P6S_WG
W zakresie umiejętności:			
U_01	Projektuje i buduje systemy z kluczami publicznymi i prywatnymi.	K_U06 K_U11 K_U13	P6S_UW
W zakresie kompetencji społecznych:			
K_01	Jest świadomy z czego wynikają zasady pracy w zespole.	K_K01	P6U_KK

6. Treści kształcenia – oddzielnie dla każdej formy zajęć dydaktycznych

Treści kształcenia w zakresie wykładu

Lp.	Treści kształcenia	Liczba godz.
W 1	Zajęcia organizacyjne. Ustalenie formy zaliczenia i zakresu materiału. Podstawowe definicje bezpieczeństwa. Zarządzanie ryzykiem. Akty i normy prawne.	1
W 2	Kryptografia. Metody i kategorie łamania szyfrów. Podstawowe rodzaje szyfrów.	1
W 3	Wprowadzenie do teorii informacji. Entropia. Koincydencja znaków. Analiza częstotliwościowa szyfrów.	1
W 4	Szyfry blokowe i standard DES. Kryptografia z kluczami publicznymi, szyfr RSA.	1
W 5	Polityka bezpieczeństwa. Modele bezpieczeństwa. Tworzenie procedur bezpieczeństwa.	1
W 6	Uwierzytelnienie. Hasła. System Kerberos.	1
W 7	Systemy IDS, IPS. Aspekt prawny, rozwiązania sprzętowe i programowe.	1
W 8	Firewalle: charakterystyka firewalli, typy firewalli, implementowanie firewalli, lokalizacja i konfiguracja firewalli.	1
W 9	Metody i techniki rekonesansu w systemach i sieciach komputerowych. Techniki skanowania sieci.	1
W 10	Podpis cyfrowy. Certyfikaty bezpieczeństwa. Funkcje haszujące.	1
W 11	Bezpieczeństwo poczty elektronicznej.	1
W 12	Szkodliwe oprogramowanie: typy szkodliwego oprogramowania, wirusy, przeciwdziałanie wirusom, robaki, rozproszone ataki DoS. Programy antywirusowe.	2
W 13	Miary poufności i bezpieczeństwa systemów. Audyt systemu.	2
	Razem	15

Treści kształcenia w zakresie laboratorium

Lp.	Treści kształcenia	Liczba godz.
L 1	Kryptografia. Metody i kategorie łamania szyfrów. Podstawowe rodzaje szyfrów.	3
L 2	Wprowadzenie do teorii informacji. Entropia. Koincydencja znaków. Analiza częstotliwościowa szyfrów.	3
L 3	Szyfry blokowe i standard DES. Kryptografia z kluczami publicznymi, szyfr RSA.	3
L 4	Polityka bezpieczeństwa. Modele bezpieczeństwa. Tworzenie procedur bezpieczeństwa.	3
L 5	Uwierzytelnienie. Hasła. System Kerberos.	3
L 6	Systemy IDS, IPS. Aspekt prawny, rozwiązania sprzętowe i programowe.	3
L 7	Firewalle: charakterystyka firewalli, typy firewalli, implementowanie firewalli, lokalizacja i konfiguracja firewalli.	3
L 8	Metody i techniki rekonesansu w systemach i sieciach komputerowych. Techniki skanowania sieci.	3
L 9	Podpis cyfrowy. Certyfikaty bezpieczeństwa. Funkcje haszujące.	3
L 10	Bezpieczeństwo poczty elektronicznej.	3
	Razem	30

7. Metody weryfikacji efektów kształcenia / w odniesieniu do poszczególnych efektów/

Symbol efektu kształcenia	Forma weryfikacji						
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawdzian wejściowy	Sprawozdanie	Inne
W_01			X				
U_01						X	
K_01							X

8. Narzędzia dydaktyczne

Symbol	Rodzaj zajęć
N1	wykład
N2	laboratorium

9. Ocena osiągniętych efektów kształcenia

9.1. Sposoby oceny

Ocena formująca

F1	Kolokwium
F2	Ćwiczenia laboratoryjne

Ocena podsumowująca

P1	Zaliczenie wykładów na podstawie kolokwium F1
P2	Zaliczenie zajęć laboratoryjnych na podstawie średniej F2
P3	Zaliczenie przedmiotu na podstawie średniej ważonej F1+F2

9.2. Kryteria oceny

Student, który osiągnął zakładany poziom wiedzy, posiadł wymagane umiejętności, cechuje się określonymi kompetencjami społecznymi, które są zdefiniowane w efektach kształcenia dla modułu, zalicza moduł kształcenia. Student, który nie osiągnął zakładanych efektów kształcenia, nie zalicza modułu kształcenia. Student, który zaliczył moduł:

Symbol efektu kształcenia	**na ocenę 3**	**na ocenę 3,5**	**na ocenę 4**	**na ocenę 4,5**	**na ocenę 5**
W_01	Demonstruje sposoby szyfrowania informacji, uwierzytelniania, haszowania.	nie tylko osiągnął poziom wiedzy i umiejętności wymagany na ocenę 3, ale również co najmniej 50% dodatkowych wymagań na ocenę 4	nie tylko osiągnął poziom wiedzy i umiejętności wymagany na ocenę 3, ale również stosuje poprawne metody i algorytmy szyfrowania, uwierzytelniania i haszowania.	nie tylko osiągnął poziom wiedzy i umiejętności wymagany na ocenę 4, ale również co najmniej 50% dodatkowych wymagań na ocenę 5	nie tylko osiągnął poziom wiedzy i umiejętności wymagany na ocenę 4, ale również stosuje zaawansowane implementacje algorytmów szyfrujących informacje, algotymów uwierzytelniających i haszujących.
U_01	Projektuje i buduje systemy z kluczami publicznymi i prywatnymi	nie tylko osiągnął poziom wiedzy i umiejętności wymagany na ocenę 3, ale również co najmniej 50% dodatkowych wymagań na ocenę 4	nie tylko osiągnął poziom wiedzy i umiejętności wymagany na ocenę 3, ale również używa je we właściwy sposób	nie tylko osiągnął poziom wiedzy i umiejętności wymagany na ocenę 4, ale również co najmniej 50% dodatkowych wymagań na ocenę 5	nie tylko osiągnął poziom wiedzy i umiejętności wymagany na ocenę 4, ale również modyfikuje je w dowolny sposób zwiększając złożoność i bezpieczeństwo systemu
K_01	Jest świadomy z czego wynikają zasady pracy w zespole na poziomie podstawowym	Jest świadomy z czego wynikają zasady pracy w zespole na poziomie dostatecznym	Jest świadomy z czego wynikają zasady pracy w zespole na poziomie dobrym	Jest świadomy z czego wynikają zasady pracy w zespole na poziomie wyróżniającym	Jest świadomy z czego wynikają zasady pracy w zespole na poziomie bardzo dobrym

10. Literatura podstawowa i uzupełniająca

Literatura podstawowa:

1. Schneier Bruce, Kryptografia dla praktyków, Wydawnictwo Naukowo Techniczne., 2002
2. Stallings William, Ochrona danych w sieci i intersieci, Wydawnictwo Naukowo Techniczne., 1997
3. Seberry J., Pierzyk J, Cryptogaphy: An Introduction to Computer Security, Englewood Cliffs, NJ: Prentice-Hall., 1989
4. W. Stallings , "Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptografii" , Helion., 2011

Literatura uzupełniająca:

1. D. J. Barnett, R. E. Silverman, R. G. Byrnes , Linux Security Cookbook , O'Reilly Media., 2003

11. Macierz realizacji przedmiotu

Symbol efektu kształcenia	Odniesienie efektu do efektów zdefiniowanych dla programu	Cele Przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
W_01	P6S_WG-K_W07	C1	W 1-13	N1	F1
U_01	P6S_UW- K_U06 P6S_U - K_U11 P6S_UW- K_U13	C2	L 1-10	N2	F2
K_01	P6U_KK- K_K01	C1, C2	W 1-13 L 1-10	N1, N2	F1, F2

12. Obciążenie pracą studenta

Forma aktywności	**Średnia liczba godzin na zrealizowanie aktywności**
Udział w wykładach	15
Udział w ćwiczeniach	-
Udział w konwersatoriach/laboratoriach	30
Udział nauczyciela akademickiego w egzaminie	-
Udział w konsultacjach	5
Suma godzin kontaktowych	50
Samodzielne studiowanie treści wykładów	10
Samodzielne przygotowanie do ćwiczeń	20
Przygotowanie do egzaminu i kolokwiów	10
Suma godzin pracy własnej studenta	40
Sumaryczne obciążenie studenta	90
Liczba punktów ECTS za przedmiot	3
Obciążenie studenta zajęciami praktycznymi	50
Liczba punktów ECTS za zajęcia praktyczne	2

13. Zatwierdzenie karty przedmiotu do realizacji.

14. Odpowiedzialny za przedmiot: **Dyrektor Instytutu:**

Przemyśl, dnia …… .