Nazwa przedmiotu						
Bezpieczeństwo i ochrona sieci komputerowych Security and safety of computer networks						
Dyscyplina					Oznaczenie przedmiotu	
Informatyka					8S_BiOSK	
Rodzaj przedmiotu	Stopień studiów	Tryb studiów	Język zajęć		Rok	Semestr
obowiązkowy	1	stacjonarne	polski		III	VI
Rodzaj zajęć		Wyk.	Ćw.	Lab.	Sem.	Proj.	Liczba punktów ECTS
Liczba godzin w semestrze		30	0	15	15	0	5
Koordynator	Dr inż. Zbigniew Weżgowiec, wezgow@el.pcz.czest.pl					
Prowadzący	Dr inż. Zbigniew Weżgowiec, wezgow@el.pcz.czest.pl					

I. KARTA PRZEDMIOTU

Cel przedmiotu

C1. Zapoznanie studentów z bezpieczeństwem sieci komputerowych
C2. Zapoznanie studentów z ochroną sieci komputerowych

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1. Znajomość podstaw sieci komputerowych

Efekty kształcenia

EK1. Student potrafi dbać o bezpieczeństwo sieci komputerowych
EK2. Student potrafi zapewnić ochronę sieci komputerowych

Treści programowe: wykłady	Liczba godzin
W1 – Wiadomości o sieciach komputerowych pod kątem ich bezpieczeństwa	2
W2 – Rola Active Directory a bezpieczeństwo systemów komputerowych	2
W3 – Chmura obliczeniowa	2
W4 – Systemy firewall	2
W5 – Systemy bankowe	2
W6 – Telefonia IP jako potencjalne zagrożenie	
W7 – Sieci komputerowe9S w handlu	2
W8 – Bezpieczeństwo fizyczne infrastruktury	2
W9 – Bezpieczeństwo stron WWW	2
W10 – Tunelowanie portów	2
W11,12 – Rola protokołów a szczególnie SSL i HTTPS	4
W13 – Sieci VPN	2
W14 – Szyfrowanie i deszyfrowanie dysków	2
W15 – Zagrożenia mobilne	2
SUMA	**30**

Treści programowe: laboratorium	Liczba godzin
L1,2 – Praca z programami antywirusowymi	2
L3,4 – Tworzenie sieci VPN	2
L5,6 – Tunelowanie portów	2
L7,8 – Bezpieczeństwo stron WWW	2
L9,10 –Programy „handlowe”	2
L11,12 Ataki na systemy sieciowe	2
L13,14 Ataki na systemy sieciowe c.d.	2
L15 – Odrabianie	1
SUMA	**15**

Treści programowe: seminarium	Liczba godzin
S1 – Klasyfikacja wirusów i zagrożeń	1
S2 – Bezpieczeństwo fizyczne infrastruktury	1
S3 – Bezpieczeństwo serwerowni	1
S4 – Awarie systemów bankowych	1
S5 – Bezpieczeństwo e-handlu ń	1

S6 – Bezpieczeństwo stron WWW	1
S7 – Telefonia IP jako potencjalne zagrożenie	1
S8 – Zagrożenia mobilne	1
S9 – Bezpieczeństwo chmury obliczeniowej	1
S10 – Active Directory a bezpieczeństwo systemów komputerowych	1
S11 – Szyfrowanie i deszyfrowanie dysków	1
S12 – Protokół SSL i HTTPS	1
S13 – Tunelowanie portów	1
S14 – Sieci VPN	1
S15 – Systemy firewall	1
SUMA	**15**

Narzędzia dydaktyczne

1. Prezentacja multimedialna
2. Specjalistyczne oprogramowanie

Sposoby oceny efektów kształcenia (F – ocena Formująca, P – ocena Podsumowująca)

F1. Ocena przygotowania do ćwiczeń laboratoryjnych
F2. Ocena poprawnego wykonania zadania postawionego w trakcie zajęć
P1. Kolokwium / test
P2. Egzamin

Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z prowadzącym	60
Zapoznanie się ze wskazaną literaturą	10
Przygotowanie do zajęć	10
Przygotowanie do testu / kolokwium / egzaminu	20
Przygotowanie sprawozdań/prezentacji	25
Sumaryczna liczba godzin/punktów ECTS dla przedmiotu	**125**

Wykaz literatury podstawowej i uzupełniającej

1. Kuczewski J., Bezpieczeństwo sieci komputerowych, Wyd. iTstart
2. Józefiok A., Bezpieczeństwo sieci Cisco. Wyd. Videopoint

Macierz realizacji efektów kształcenia

Efekt kształcenia	Odniesienie efektu do efektów kształcenia dla dyscypliny naukowej Informatyka *	Cele przedmiotu	Forma zajęć	Narzędzia dydaktyczne	Sposób oceny
EK1	KINF1_W06, KINF1_U12	1,2	Wykład, Lab.,Sem.	1.2	F1.F2.P2
EK2	KINF1_W06, KINF1_U12	1.2	Wykład, Lab.,Sem.	1,2	F1.F2.P2

* – wg załącznika

II. FORMY OCENY – SZCZEGÓŁY

Ocena	Efekty
EK1	**Efekt pierwszy**
2	Student nie potrafi dbać o bezpieczeństwo sieci komputerowych
3	Student potrafi dbać o bezpieczeństwo sieci komputerowych w ograniczonym zakresie
3.5	Student potrafi dbać o bezpieczeństwo sieci komputerowych i zna część podstawowych metod bezpieczeństwa
4	Student potrafi dbać o bezpieczeństwo sieci komputerowych i zna połowę podstawowych metod bezpieczeństwa
4.5	Student potrafi dbać o bezpieczeństwo sieci komputerowych
5	Student potrafi dbać o bezpieczeństwo sieci komputerowych i uzasadnić swoje działania
EK2	**Efekt drugi**
2	Student nie potrafi dbać o ochronę sieci komputerowych
3	Student potrafi dbać o ochronę sieci komputerowych w ograniczonym zakresie
3.5	Student potrafi dbać o ochronę sieci komputerowych i zna część podstawowych metod ochrony
4	Student potrafi dbać o ochronę sieci komputerowych i zna połowę podstawowych metod ochrony
4.5	Student potrafi dbać o ochronę sieci komputerowych
5	Student potrafi dbać o ochronę sieci komputerowych i uzasadnić swoje działania

III. INNE PRZYDATNE INFORMACJE O PRZEDMIOCIE

1. Wszelkie informacje dla studentów na temat planu zajęć dostępne są na tablicy ogłoszeń oraz na stronie el.pcz.pl.
2. Informacje na temat warunków zaliczania zajęć przekazywana jest studentom podczas pierwszych zajęć.