Załącznik Nr 5 do Zarz. Nr 33/11/12

(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: **BEZPIECZEŃSTWO SIECI KOMPUTEROWYCH**	**2. Kod przedmiotu:**
3. Karta przedmiotu ważna od roku akademickiego:	
4. Forma kształcenia: studia pierwszego stopnia	
5. Forma studiów: studia niestacjonarne (zaoczne)	
6. Kierunek studiów: INFORMATYKA (SYMBOL WYDZIAŁU) RAU	
7. Profil studiów: ogólnoakademicki	
8. Specjalność: wszystkie specjalności	
9. Semestr: 7	
10. Jednostka prowadząca przedmiot: Instytut Informatyki Pol. Śl.	
11. Prowadzący przedmiot: dr inż. Mirosław Skrzewski	
12. Przynależność do grupy przedmiotów: przedmioty wspólne	
13. Status przedmiotu: obowiązkowy	
14. Język prowadzenia zajęć: polski	
15. Przedmioty wprowadzające oraz wymagania wstępne: Systemy operacyjne, Architektura komputerów, Technologie sieciowe,	
16. Cel przedmiotu: Celem przedmiotu jest przedstawienie zagadnień związanych z bezpieczeństwem systemów komputerowych i bezpieczeństwem informacji. Studenci zapoznają się z klasyfikacją zagrożeń dla przechowywania, przesyłania i przetwarzania informacji, modelami oceny bezpieczeństwa systemów informatycznych, technikami wykrywania i monitorowania ataków oraz technicznymi i nie-technicznymi środkami ochrony przed zagrożeniami.	
17. Efekty kształcenia:	

Nr	Opis efektu kształcenia	Metoda sprawdzenia efektu kształcenia	Forma prowadzenia zajęć	Odniesienie do efektów dla kierunku studiów
1	Ma podstawową wiedzę na temat algorytmów kryptograficznych, ich właściwości i zakresu ich stosowania dla zapewnienia bezpieczeństwa przesyłu, przechowywania i weryfikacji bezpieczeństwa informacji	Kolokwium, sprawozdania z wykonania ćwiczenia	Wykład , ćwiczenia laboratoryjne	K_W14, K_W19, K_U05, K_U11, K_U14
2	Zna podstawowe metody zabezpieczania ciągłości działania systemów, kontroli integralności oprogramowania i danych w systemie komputerowym	Kolokwium, sprawozdania z wykonania ćwiczenia	Wykład , ćwiczenia laboratoryjne	K_W08, K_W14, K_U05, K_U26, K_U33
3	Ma podstawową wiedzę na temat metod uwierzytelniania i	Kolokwium	Wykład , ćwiczenia	K_W08, K_W12, K_U21, K_U26

	autoryzacji użytkowników przy dostępie do systemów.		laboratoryjne	
4	Zna podstawowe zasady bezpiecznego konfigurowania środowiska użytkownika systemów komputerowych	Kolokwium, sprawozdania z wykonania ćwiczenia	Wykład , ćwiczenia laboratoryjne	K_W08, K_W19, K_U21
5	Ma podstawową wiedzę na temat sposobów monitorowania i ograniczania możliwości dostępu do systemów w środowisku sieciowym	Kolokwium, sprawozdania z wykonania ćwiczenia	Wykład , ćwiczenia laboratoryjne	K_W08, K_W19, K_U21, K_U33
6	Zna podstawowe typy zagrożeń sieciowych, główne drogi ich rozprzestrzeniania się, podstawowe metody ich wykrywania i zapobiegania infekcjom.	Kolokwium, sprawozdania z wykonania ćwiczenia	Wykład , ćwiczenia laboratoryjne	K_W15, K_W17, K_W19, K_U05, K_U26, K_U34
7	Ma podstawową wiedzę na temat celów i metod tworzenia polityk systemowych bezpieczeństwa oraz sposobów kontroli ich przestrzegania	Kolokwium	Wykład	K_W08, K_W19, K_U05, K_U33, K_U37, K_K02

18. Formy zajęć dydaktycznych i ich wymiar (liczba godzin)

W. 10 Ćw. L. 15 P. Sem.

19. Treści kształcenia:

Wykład:

Określenie bezpieczeństwa, modele bezpieczeństwa systemów komputerowych, bezpieczeństwo informacji, model C-I-A (*confidentiality, integrity, availability*) atrybutów informacji, atrybuty rozszerzone. Klasyfikacja zagrożeń, metody oceny bezpieczeństwa.
Kryptografia, przegląd ważniejszych metod szyfrowania, algorytmy symetryczne (DES, AES), asymetryczne (RSA, El Gamal), jednokierunkowe (MD5, SHA-1). Zastosowania kryptografii do ochrony integralności, weryfikacji źródła (autorstwa) informacji – podpis elektroniczny, certyfikaty cyfrowe, infrastruktura PKI.
Bezpieczeństwo systemu komputerowego, kontrola dostępu, metody uwierzytelniania, protokół Kerberos.
Integralność systemu plików, bezpieczeństwo danych, metody ochrony. Bezpieczeństwo oprogramowania systemu, dziury bezpieczeństwa, zasady tworzenia bezpiecznego oprogramowania, instalacja poprawek bezpieczeństwa oprogramowania. Procedury odtwarzania systemu po awarii.
Bezpieczeństwo sieci, granice bezpieczeństwa, kontrola dostępu do systemu, bezpieczne protokoły komunikacyjne, zasada minimum udostępnianych usług. Przegląd zagrożeń sieciowych – wirusy, wormy, ataki skryptowe, programy szpiegowskie, roboty programowe (botnet), spam, ataki DoS, DDoS. Ataki typu social engineering.
Metody wykrywania zagrożeń sieciowych, zasady detekcji anomalii i detekcji wzorców zagrożeń (sygnatur), błędy metod wykrywania. Systemy monitorowania zagrożeń, przykłady (IDS, IPS)
Konfiguracja środowiska użytkownika, zasada minimalnych uprawnień. Ograniczenia administracyjne działania użytkownika – polityki bezpieczeństwa, incydenty bezpieczeństwa. Zasady tworzenia polityki bezpieczeństwa, przykłady polityk, zarządzanie bezpieczeństwem.

Laboratorium:

- Ochrona bezpieczeństwa przesyłu informacji - certyfikaty, podpis cyfrowy
- Bezpieczeństwo przechowywania informacji - system plików EFS
- Monitorowanie integralności systemu plików
- Wykrywanie zagrożeń i kontrola komunikacji sieciowej
- Monitorowanie i testowanie bezpieczeństwa systemu
- Konfigurowanie systemów ochrony przed zagrożeniami.

20. Egzamin: nie

21. Literatura podstawowa:

- William Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji*, Helion 2012

22. Literatura uzupełniająca:

- Fry C., Nystrom M., *Monitoring i bezpieczeństwo sieci*, Helion, 2010
- Ross J., *Bezpieczne programowanie. Aplikacje hakeroodporne*, Helion, 2009
- Viega J., Mity *bezpieczeństwa IT. Czy na pewno nie masz się czego bać?*, Helion 2010.

23. Nakład pracy studenta potrzebny do osiągnięcia efektów kształcenia

Lp.	Forma zajęć	Liczba godzin kontaktowych / pracy studenta
1	Wykład	10/50
2	Ćwiczenia	/
3	Laboratorium	15/30
4	Projekt	/
5	Seminarium	/
6	Inne	/
	Suma godzin	25/80

24. Suma wszystkich godzin: 105

25. Liczba punktów ECTS: 4

26. Liczba punktów ECTS uzyskanych na zajęciach z bezpośrednim udziałem nauczyciela akademickiego

27. Liczba punktów ECTS uzyskanych na zajęciach o charakterze praktycznym (laboratoria, projekty)

26. Uwagi:

Zatwierdzono:

…….
(data i podpis prowadzącego)

……
(*data i podpis dyrektora instytutu/kierownika katedry/ Dyrektora Kolegium Języków Obcych/kierownika lub dyrektora jednostki międzywydziałowej)*