(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: **BEZPIECZEŃSTWO SIECI I SYSTEMÓW KOMPUTEROWYCH**	**2. Kod przedmiotu: SSI_BSSK**
3. Karta przedmiotu ważna od roku akademickiego: 2015/2016	
4. Forma kształcenia: studia pierwszego stopnia	
5. Forma studiów: studia stacjonarne	
6. Kierunek studiów: INFORMATYKA 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: wybieralny	
14. Język prowadzenia zajęć: polski	
15. Przedmioty wprowadzające oraz wymagania wstępne: Sieci komputerowe, Systemy operacyjne	
16. Cel przedmiotu: Celem przedmiotu jest prezentacja zagadnień związanych z bezpieczeństwem sieci i systemów komputerowych. Studenci zapoznają się z rodzajami spotykanych zagrożeń oraz metodami oceny stanu 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	Zna podstawowe metody kontroli integralności systemu plików, oprogramowania i danych w systemie komputerowym	Kolokwium (SP), Sprawozdanie (RP)	Wykład (WT), laboratorium(CL)	K1A_W05, K1A_W07, K1A_U05, K1A_U09
2	Zna podstawowe zasady bezpiecznego konfigurowania środowiska użytkownika systemów komputerowych	Kolokwium (SP)	Wykład (WT),	K1A_W07, K1A_U05
3	Ma podstawową wiedzę na temat sposobów monitorowania i ograniczania możliwości dostępu do systemów w środowisku sieciowym	Kolokwium (SP), Sprawozdanie (RP)	Wykład (WT), laboratorium(CL)	K1A_W07, K1A_W15, K1A_U13

4	Zna podstawowe typy zagrożeń sieciowych, główne drogi ich rozprzestrzeniania się, metody ich wykrywania i zapobiegania infekcjom.	Kolokwium (SP), Sprawozdanie (RP)	Wykład (WT), laboratorium(CL)	K1A_W07, K1A_W11, K1A_U09
5	Ma podstawową wiedzę na temat celów i metod tworzenia polityk bezpieczeństwa oraz sposobów kontroli ich przestrzegania.	Kolokwium (SP), Sprawozdanie (RP)	Wykład (WT), laboratorium(CL)	K1A_W07, K1A_W11, K1A_W15, K1A_U23

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

W. 30 Ćw. 0 L. 30 P. 0 Sem. 0

19. Treści kształcenia:

Wykład:

Model klasyczny bezpieczeństwa, klasyfikacja zagrożeń bezpieczeństwa, kryteria bezpieczeństwa, zasady doboru metod zapobiegania zagrożeniom, analiza ryzyka. Zarządzanie bezpieczeństwem, zasady tworzenia polityk bezpieczeństwa. Protokoły komunikacyjne, bezpieczeństwo przechowywania, przetwarzania i przesyłu informacji, bezpieczeństwo fizyczne systemów.

Klasyczny model zagrożeń dla systemów IT - ataki zewnętrzne, programy autonomiczne (wormy internetowe, mailowe, wirusy, konie trojańskie), ataki skryptowe, włamania celowane. Udział czynnika ludzkiego w zagrożeniach - techniki socjotechniczne dostępu do chronionych zasobów. Metody wykrywania - analiza logów, audyt komunikacji sieciowej, wykrywanie śladów w systemach (network, system forensic), systemy IDS, IPS.

Braki modelu klasycznego. Zmiany modelu bezpieczeństwa - zanik granic fizycznych środowiska sieci, model zdalnej pracy, dostępność urządzeń mobilnych z komunikacją bezprzewodową, model BYOD.

Zmiany modelu zagrożeń - atak pośredni przez systemy użytkowników, od wewnątrz środowiska sieciowego. Nowe kanały przenikania - poprzez serwis www (ataki typu drive by download), wykorzystywanie podatności używanych aplikacji, podatności formatów danych. Nowe modele działania zagrożeń - mechanizmy polimorfizmu, metamor-fizmu, ukrywanie się programów w systemie, ataki bezplikowe. Roboty programowe (bot-y), sieci botnet, rozwój biznesowego wykorzystywania zainfekowanych komputerów.

Zmiany modelu ochrony przed zagrożeniami - system osobną twierdzą, z wielopoziomową ochroną. Technologie ochrony systemów: monitorowanie komunikacji sieciowej (audyt transakcji sieciowych, analiza przepływów w sieci, metody wizualizacji aktywności sieciowej systemów, analiza relacji komunikacji w sieci), monitorowanie obecności zagrożeń w sieci (systemy N-IDS, systemy-pułapki (honeypot), systemy rejestracji kodu zagrożeń), systemy monitorowania integralności systemów plików.

Laboratorium:

Celem laboratorium jest zapoznanie studentów z przykładowymi rozwiązaniami systemów monitorowania zagrożeń, metodami ich konfiguracji i sposobami analizowania rezultatów ich działania. Ćwiczenia prowadzone będą na maszynach wirtualnych na wydzielonej sieci.

1. System Host_IDS - monitorowanie integralności systemu plików.
2. Badanie systemu wykrywania zagrożeń sieciowych (Net_IDS).
3. Narzędzia monitorowania konfiguracji bezpieczeństwa systemu.
4. Monitorowanie przebiegu infekcji malware - system honeypot.
5. Testowanie stanu bezpieczeństwa systemu - testy penetracyjne.
6. Konfiguracja systemów ochrony przed zagrożeniami.

20. Egzamin: nie

21. Literatura podstawowa:

Liderman K.: *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN 2009
Viega J.: *Mity bezpieczeństwa IT*, Helion, 2010
Clercq J., Grillenmeier G.: *Bezpieczeństwo Microsoft Windows. Podstawy praktyczne*, PWN, 2008

22. Literatura uzupełniająca:

W. Stallings: *Kryptografia i bezpieczeństwo sieci komputerowych. Metody bezpiecznej komunikacji*, Helion 2012.
Liderman K.: *Bezpieczeństwo Informacyjne*, PWN 2012
Metasploit Przewodnik po testach penetracyjnych, Wydawnictwo: Helion, 2013

23. Nakład pracy studenta potrzebny do osiągnięcia efektów kształcenia

Lp.	Forma zajęć	Liczba godzin kontaktowych / pracy studenta
1	Wykład	30/25
2	Ćwiczenia	/
3	Laboratorium	30/25
4	Projekt	/
5	Seminarium	/
6	Inne (studiowanie dokumentacji)	/10
	Suma godzin	50/120

24. Suma wszystkich godzin: 120

25. Liczba punktów ECTS: 4

26. Liczba punktów ECTS uzyskanych na zajęciach z bezpośrednim udziałem nauczyciela akademickiego 2

27. Liczba punktów ECTS uzyskanych na zajęciach o charakterze praktycznym (laboratoria, projekty) 2

26. Uwagi:

Zatwierdzono:

…….
(data i podpis prowadzącego)

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