

(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: SECURITY OF ENVIRONMENT WITH MOBILE DEVICES		2. Kod przedmiotu: SSI_SEMD		
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:				
9. Semestr:		7		
10. Jednostka prowadząca przedmiot:		Instytut Informatyki		
11. Prowadzący przedmiot:		dr inż. Mirosław Skrzewski		
12. Przynależność do grupy przedmiotów:		przedmioty wspólne		
13. Status przedmiotu:		obieralny		
14. Język prowadzenia zajęć:		polski		
15. Przedmioty wprowadzające oraz wymagania wstępne: wiedza z zakresu działania środowiska sieci, sieci bezprzewodowych, jak również systemów mobilnych.				
16. Cel przedmiotu: Zapewnienie bezpieczeństwa środowiska IT (sieci, systemy) w instytucji umożliwiającej pracownikom korzystanie z prywatnych urządzeń do realizacji zadań (model BYOD) wymaga stosowania odmiennych od klasycznych rozwiązań monitorowania komunikacji sieciowej i wykrywania zagrożeń. Celem przedmiotu jest przedstawienie istoty tych różnic i zapoznanie studentów z metodami ochrony informacji i wykrywania zagrożeń dedykowanych do tych odmiennych warunków.				
17. Efekty kształcenia:				
Nr	Opis efektu kształcenia	Metoda sprawdzenia efektu kształcenia	Forma prowadzenia zajęć	Odniesienie do efektów dla kierunku studiów
1.	Ma podstawową wiedzę o roli kryptografii w ochronie bezpieczeństwa informacji	CL, SP	WM, L	K1A_W11, K1A_U14
2.	Zna podstawowe metody uwierzytelniania użytkowników w środowisku sieciowym	CL, SP	WM, L	K1A_W11, K1A_W12
3.	Rozumie podstawowe metody monitorowania komunikacji sieciowej	CL, SP	WM, L	K1A_W15, K1A_U22
4.	Ma podstawową wiedzę na temat metod rozprzestrzeniania się zagrożeń sieciowych i zasad im zapobiegania	CL, SP	WM, L	K1A_W13

5.	Potrafi ocenić poprawność konfiguracji urządzeń i uprawnień użytkowników w ochronie informacji	CL, SP	WM, L	K1A_U05, K1A_U18
6.	Potrafi ocenić zgodność zachowania użytkownika z polityką bezpieczeństwa	CL, SP	WM, L	K1A_U09, K1A_U15

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

W. 15 h Ćw. -- L. 15 h P. -- Sem. –

19. Treści kształcenia:

Program wykładów i ćwiczeń w laboratorium:

1. Zadania i modele rozwiązań ochrony bezpieczeństwa infrastruktury firmowej:

- a) model ochrony od zagrożeń zewnętrznych
- b) system jako niezależne chronione środowisko
- c) model ochrony bezpieczeństwa informacji

2. Systemy detekcji zagrożeń:

- a) modele detekcji i rozwiązania systemów
- b) wykorzystanie systemów pułapek

3. Monitorowanie potencjalnych kanałów infekcji:

- a) systemy scentralizowane (IDS, IPS)
- b) monitorowanie lokalne systemów

4. Monitorowanie bezpieczeństwa systemów mobilnych.

5. Ochrona informacji przed wyciekiem (systemy DLP)

20. Egzamin: nie

21. Literatura podstawowa:

Fry C., Nystrom M., *Monitoring i bezpieczeństwo sieci*, Helion, 2010

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

22. Literatura uzupełniająca:

Liderman K.: *Bezpieczeństwo Informacyjne*, PWN 2012,

E. Schetina, K. Green, J. Carlton, *Bezpieczeństwo w sieci*, Helion

23. Nakład pracy studenta potrzebny do osiągnięcia efektów kształcenia

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

24. Suma wszystkich godzin: 60

25. Liczba punktów ECTS: 2
26. Liczba punktów ECTS uzyskanych na zajęciach z bezpośrednim udziałem nauczyciela akademickiego: 1
27. Liczba punktów ECTS uzyskanych na zajęciach o charakterze praktycznym (laboratoria, projekty): 1
28. Uwagi:

Zatwierdzono:

.....
(data i podpis prowadzącego)

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