Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2018/2019

Wydział Mechaniczny

Kierunek studiów: Inżynieria Bezpieczeństwa | Profil: Ogólnoakademicki

Forma sudiów: stacjonarne | Kod kierunku: B

Stopień studiów: I

Specjalności: Bezpieczeństwo pracy i środowiska

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo informacji w systemach komputerowych
Nazwa przedmiotu w języku angielskim	Security of Information in Computer Systems
Kod przedmiotu	B110
Kategoria przedmiotu	Przedmioty podstawowe
Liczba punktów ECTS	1.00
Semestry	1

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
1	0	0	0	15	0	0

3 Cele przedmiotu

Cel 1 Zapoznanie sie z działaniem oraz eksploatacja systemów podnoszacych bezpieczenstwo informacji. Zdobycie umiejetnosci posługiwania sie podstawowymi programami do szyfrowania dokumentów oraz szyfrowania transmisji w sieciach komputerowych tj. VPN, szyfrowanie poczty.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Brak wymagań.

5 Efekty kształcenia

EK1 Wiedza Ma podstawowa wiedzę z zakresu bezpieczeństwa przechowywania i transmisji informacji w systemach komputerowych i potrafi wykorzystywać odpowiednie oprogramowanie w tym zakresie.

EK2 Wiedza Ma podstawową wiedzę w zakresie bezpiecznych metod przetwarzania danych cyfrowych z użyciem komputera i urządzeń przetwarzających dane komputerowe.

EK3 Umiejętności Potrafi ocenić przydatność i zastosować podstawowe metody możliwe do zastosowania dla rozwiązania postawionego problemu z zakresu bezpieczeństwa informacji w systemach komputerowych z wykorzystaniem oprogramowania i dedykowanych urzadzeń.

EK4 Kompetencje społeczne Potrafi określić aspekty ekonomiczne stosowania rozwiązań w zakresie bezpieczeństwa informacji.

6 Treści programowe

Laboratorium komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K1	Problematyka bezpieczeństwa usług i zasobów w systemach komputerowych. Możliwe drogi zagrożeń, metody przeciwdziałania, kopie bezpieczeństwa. Metody przeciwdziałania włamaniom i atakom.	4
K2	Podstawy kryptografii: szyfry proste, szyfry komputerowe symetryczne i niesymetryczne. Infrastruktura klucza publicznego, podpis elektroniczny w świetle przepisów, zarządzanie kluczami publicznymi.	4
K3	Bezpieczeństwo infrastruktury teleinformatycznej, kontrola dostępu do zasobów. Metody wykrywania ataków na infrastrukturę (IDS, IPS, Firewall).	4
K4	Bezpieczeństwo w transmisji danych i technologie VPN.	2
K5	Podstawowe założenia bezpiecznych systemów komputerowych (zarządzanie ryzykiem). Audyt bezpieczeństwa i polityka bezpieczeństwa informatycznego w przedsiębiorstwie.	1

7 Narzędzia dydaktyczne

N1 Ćwiczenia laboratoryjne

N2 Konsultacje

N3 Praca w grupach

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	15
Konsultacje przedmiotowe	2
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	7
Opracowanie wyników	6
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**30**
Sumaryczna liczba punktów ECTS dla przedmiotu	1.00

9 Sposoby oceny

Ocena formująca

F1 Ćwiczenie praktyczne

F2 Sprawozdanie z ćwiczenia laboratoryjnego

F3 Test

Ocena podsumowująca

P1 Średnia ważona ocen formujących

Ocena aktywności bez udziału nauczyciela

B1 Test

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	-
Na ocenę 3.0	Potrafi dobrać i zastosować rozwiązanie w zakresie bezpieczeństwa komputera osobistego, sieci komputerowej mikroprzedsiębiorstwa i transmisji informacji w sieci publicznej.

Na ocenę 3.5	-
Na ocenę 4.0	-
Na ocenę 4.5	-
Na ocenę 5.0	-
Efekt kształcenia 2	
Na ocenę 2.0	-
Na ocenę 3.0	jw.
Na ocenę 3.5	-
Na ocenę 4.0	-
Na ocenę 4.5	-
Na ocenę 5.0	-
Efekt kształcenia 3	
Na ocenę 2.0	-
Na ocenę 3.0	jw.
Na ocenę 3.5	-
Na ocenę 4.0	-
Na ocenę 4.5	-
Na ocenę 5.0	-
Efekt kształcenia 4	
Na ocenę 2.0	-
Na ocenę 3.0	jw.
Na ocenę 3.5	-
Na ocenę 4.0	-
Na ocenę 4.5	-
Na ocenę 5.0	-

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	K1_W07	Cel 1		N1 N2 N3	F1 F2 F3 P1
EK2	K1_W11	Cel 1		N1 N2 N3	F1 F2 F3 P1
EK3	K1_UB09	Cel 1		N1 N2 N3	F1 F2 F3 P1
EK4	K1_K06	Cel 1		N1 N2 N3	F1 F2 F3 P1

11 Wykaz literatury

Literatura podstawowa

[1] Garfinkel S. i Spafford G. — *Bezpieczeństwo w Unixie i Internecie*, Warszawa, 2003, Wydawnictwo RM

[2] Stokłosa J., Bliski T., Pankowski T. — *Bezpieczeństwo danych w systemach informatycznych*, Warszawa, 2001, PWN

Literatura uzupełniająca

[1] Aeleen Frisch — *Unix. Administracja systemu.*, Warszawa, 2003, Wydawnictwo RM

[2] Cheswick W. — *Firewalle i bezpieczeństwo w sieci*, Warszawa, 2003, Helion

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr inż. Paweł, Marek Brandys (kontakt: `brandys@mech.pk.edu.pl`)

Osoby prowadzące przedmiot

1 mgr inż. Mariusz Krawczyk (kontakt: `Mariusz.Krawczyk@mech.pk.edu.pl`)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .