

KARTA PRZEDMIOTU

1. Informacje ogólne

Nazwa przedmiotu i kod (wg planu studiów):	Bezpieczeństwo systemów informacyjnych, D1_13
Nazwa przedmiotu (j. ang.):	Information systems security
Kierunek studiów:	Informatyka
Specjalność/specjalizacja:	Informatyka praktyczna
Poziom kształcenia:	studia I stopnia
Profil kształcenia:	praktyczny (P)
Forma studiów:	studia stacjonarne/ studia niestacjonarne
Obszar kształcenia:	nauki techniczne (wg wykazu)
Dziedzina:	nauki techniczne (wg wykazu)
Dyscyplina nauki:	informatyka
Koordinator przedmiotu:	Dr inż. Agnieszka Kubacka

2. Ogólna charakterystyka przedmiotu

Przynależność do modułu:	kształcenia specjalnościowego/specjalizacyjnego do wyboru
Status przedmiotu:	do wyboru
Język wykładowy:	polski
Rok studiów, semestr:	III, 5
Forma i wymiar zajęć według planu studiów:	stacjonarne - wykład 15 h, ćw. laboratoryjne 30 h
Interesariusze i instytucje partnerskie (nieobowiązkowe)	
Wymagania wstępne:	analiza matematyczna, sieci komputerowe, podstawy inżynierii oprogramowania,

3. Bilans punktów ECTS

Całkowita liczba punktów ECTS (wg planu studiów; 1 punkt =25-30 godzin pracy studenta, w tym praca na zajęciach i poza zajęciami):	5 (A + B)	stacjonarne
A. Liczba godzin wymagających bezpośredniego udziału nauczyciela z podziałem na typy zajęć oraz całkowita liczba punktów ECTS osiągniętych na tych zajęciach	Obecność na wykładach Obecność na ćwiczeniach laboratoryjnych Udział w konsultacjach W sumie: ECTS	30 30 5 65 3
B. Poszczególne typy zadań do samokształcenia studenta (niewymagających bezpośredniego udziału nauczyciela) wraz z planowaną średnią liczbą godzin na każde i sumaryczną liczbą ECTS	przygotowanie do ćwiczeń laboratoryjnych przygotowanie do kolokwium uzupełnienie/studiowanie notatek studiowanie zalecanej literatury w sumie: ECTS	25 10 5 10 50 2
C. Liczba godzin praktycznych/laboratoryjnych w ramach przedmiotu oraz związana z tym liczba punktów ECTS	udział w ćwiczeniach laboratoryjnych praca praktyczna samodzielna w sumie: ECTS	30 30 60 3

4. Opis przedmiotu

<p>Cel przedmiotu: Celem przedmiotu jest przedstawienie istoty informacji i problematyki jej bezpieczeństwa, możliwości ochrony prawnej i fizycznej informacji oraz standardów zarządzania bezpieczeństwem informacji.</p>
<p>Metody dydaktyczne: wykład, ćwiczenia laboratoryjne</p>
<p>Treści kształcenia:</p> <p>Wykłady:</p> <ol style="list-style-type: none"> 1. Podstawowe pojęcia związane z bezpieczeństwem informacji 2. Przepisy prawne traktujące o bezpieczeństwie informacji 3. Zarządzanie informacją w IT 4. Bezpieczeństwo obiektowe 5. Elementy kryptografii 6. Testy penetracyjne <p>Ćwiczenia laboratoryjne:</p> <ol style="list-style-type: none"> 1. Systemy programowych i sprzętowych zapór sieciowych (firewall), osobiste zapory (personal firewall) 2. Systemy wykrywania włamań IDS, reakcje na włamania, dokumentowanie incydentów 3. Testowanie stanu bezpieczeństwa systemu - testy penetracyjne 4. Narzędzia monitorowania konfiguracji bezpieczeństwa systemu 5. Konstrukcja urzędów certyfikacji standardu, zarządzanie certyfikatami 6. Konfiguracja systemów ochrony przed zagrożeniami

5. Efekty kształcenia i sposoby weryfikacji

Efekty kształcenia		
K_W07,K_W09,K_W10,K_U09, K_U15, K_U16, K_K01, K_K03, K_K09		
Efekt przedmiotu (kod przedmiotu + kod efektu kształcenia)	Student, który zaliczył przedmiot (spełnił minimum wymagań)	Efekt kierunkowy
D1_13_W07 D1_13_W09 D1_13_W10	Wiedza: <ol style="list-style-type: none"> Ma podstawową wiedzę o cyklu życia i trendach rozwojowych systemów informatycznych sprzętowych lub programowych. Ma podstawową wiedzę nt. kodeksów etycznych dotyczących informatyki, zna zasady netykiety, rozumie zagrożenia związane z przestępczością elektroniczną, rozumie specyfikę systemów krytycznych ze względu na bezpieczeństwo. Ma podstawową wiedzę ustawy o ochronie danych osobowych oraz innych dokumentów traktujących o ochronie informacji. 	K_W07 K_W09 K_W10
D1_13_U09 D1_13_U15 D1_13_U16	Umiejętności: <ol style="list-style-type: none"> Potrafi przy formułowaniu i rozwiązywaniu zadań informatycznych dostrzegać ich aspekty społeczne, ekonomiczne i prawne. Ma umiejętność projektowania prostych sieci komputerowych oraz zapewnienia jej bezpieczeństwa. Potrafi zabezpieczyć system informatyczny, serwer, aplikację, przesyłane dane przed nieuprawnionym dostępem, a także zapewnia bezpieczeństwo działania aplikacji. 	K_U09 K_U15 K_U16
D1_13_K01 D1_13_K03 D1_13_K09	Kompetencje społeczne: <ol style="list-style-type: none"> Rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe. Zna przykłady i rozumie przyczyny wadliwie działających systemów informatycznych, które doprowadziły do poważnych strat finansowych, społecznych lub też do poważnej utraty zdrowia, a nawet życia. Rozumie potrzebę zachowań profesjonalnych i przestrzegania zasad etyki, w tym uczciwości. 	K_K01 K_K03 K_K09
Sposoby weryfikacji efektów kształcenia:		

Lp.	Efekt przedmiotu	Sposób weryfikacji	Ocena formująca – przykładowe sposoby jej wystawienia poniżej	Ocena końcowa przykładowe sposoby jej wystawienia poniżej
1	D1_13_W07 D1_13_W09 D1_13_W10	Aktywność studenta na zajęciach, sprawdziany pisemne, test zaliczeniowy	Ocena z odpowiedzi ustnych, ocena z częściowych prac pisemnych, ocena z testu	Średnia z ocen formujących, ocena z testu zaliczeniowego
2	D1_13_U09 D1_13_U15 D1_13_U16	Aktywność studenta na zajęciach, sprawdziany pisemne, test zaliczeniowy	Ocena z odpowiedzi ustnych, ocena z częściowych prac pisemnych, ocena z testu	Średnia z ocen formujących, ocena z testu zaliczeniowego
3	D1_13_K01 D1_13_K03 D1_13_K09	Aktywność studenta na zajęciach, sprawdziany pisemne, test zaliczeniowy	Ocena z odpowiedzi ustnych, ocena z częściowych prac pisemnych, ocena z testu	Średnia z ocen formujących, ocena z testu zaliczeniowego
Kryteria oceny:				
w zakresie wiedzy				Efekt kształcenia
Na ocenę 3,0	Student uzyskał minimum 50% punktów ze sprawdzianów pisemnych		D1_13_W07 D1_13_W09 D1_13_W10	
Na ocenę 5,0	Student uzyskał ponad 90% punktów ze sprawdzianów pisemnych		D1_13_W07 D1_13_W09 D1_13_W10	
w zakresie umiejętności				
Na ocenę 3,0	Student uzyskał minimum 50% punktów z realizacji ćwiczeń laboratoryjnych		D1_13_U09 D1_13_U15 D1_13_U16	
Na ocenę 5,0	Student uzyskał ponad 90% punktów z realizacji ćwiczeń laboratoryjnych		D1_13_U09 D1_13_U15 D1_13_U16	
w zakresie kompetencji społecznych				
Na ocenę 3,0	Student uzyskał minimum 50% punktów ze sprawdzianów pisemnych		D1_13_K01 D1_13_K03 D1_13_K09	
Na ocenę 5,0	Student uzyskał ponad 90% punktów ze sprawdzianów pisemnych		D1_13_K01 D1_13_K03 D1_13_K09	
<p>Kryteria oceny formującej: ocena z laboratorium: aktywność za zajęciach: 20% ocena ze sprawdzianów pisemnych: 80%</p> <p>Kryteria oceny podsumowującej: Test zaliczeniowy: 100%</p>				

Zalecana literatura:

Literatura podstawowa:

1. Zmitrowicz, K., Jakość projektów informatycznych, Helion, Gliwice, 2015
2. IT w Administracji, PRESSCOM Sp. z o.o., Wrocław
3. Ustawa o ochronie danych osobowych
4. Karbowski, M., Podstawy kryptografii, Helion , Gliwice, 2014
5. Adam Józefiok, Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco, Helion, Gliwice, 2016

Literatura uzupełniająca:

1. Rodzina norm ISO 27000
2. Józef Janczak, Andrzej Nowak, Bezpieczeństwo informacyjne: wybrane problemy, Warszawa : Wydawnictwo Akademii Obrony Narodowej , 2013

Informacje dodatkowe:

Dodatkowe obowiązki prowadzącego wraz z szacowaną całkowitą liczbą godzin:

Przygotowanie do wykładów i ćwiczeń laboratoryjnych – 30 godzin

Konsultacje – 15 godzin

Poprawa kolokwium– 40 godzin

Przygotowanie i poprawa testu – 5 godzin

W sumie: 90 godzin