Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Inżynierii Środowiska i Energetyki

Kierunek studiów: Geoinformatyka | Profil: Ogólnoakademicki

Forma sudiów: stacjonarne | Kod kierunku: 12

Stopień studiów: I

Specjalności: bez specjalności

1 Informacje o przedmiocie

Nazwa przedmiotu	Administracja i bezpieczeństwo systemów komputerowych
Nazwa przedmiotu w języku angielskim	
Kod przedmiotu	WIŚIE GI oIS D11 21/22
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	5.00
Semestry	7

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Cwiczenia	Laboratoria	Laboratoria komputerowe	Projekt	Seminarium
7	15	0	0	30	15	0

3 Cele przedmiotu

Cel 1 Zapoznanie się z narzędziami do administracji systemów komputerowych, poznanie źródeł zagrożeń dla ich bezpieczeństwa oraz metod ochrony przed nimi. Zdobycie umiejętności administracji systemem serwera oraz bezpieczeństwem systemów komputerowych na przykładzie systemów MS Windows Server oraz Unix/Linux.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Umiejętność obsługi systemów operacyjnych typu Windows i Linux

5 Efekty kształcenia

EK1 Wiedza Zna systemy operacyjne serwerów sieciowych na poziomie administracyjnym oraz usługi serwerowe dla użytkowników sieci lokalnej i w Internecie. Zna zagadnienia ich niezawodności, zapewnienia wydajności oraz bezpieczeństwa.

EK2 Wiedza Zna metody projektowania i implementacji infrastruktury systemów informatycznych oraz procedury administrowania usługami sieciowymi oraz zapewnienia wymaganego stopnia bezpieczeństwa.

EK3 Umiejętności Potrafi zaprojektować zgodnie ze specyfikacją infrastrukturę sieciowego systemu informatycznego oraz systemu zapewnienia bezpieczeństwa.

EK4 Kompetencje społeczne Potrafi zaplanować i nadzorować zadania obsługowe dla zapewnienia niezawodnej eksploatacji systemów operacyjnych serwerów sieciowych oraz bezpieczeństwa informatycznego infrastruktury.

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Administracja systemami serwerowymi UNIX i Windows Server, administracja usługami oraz zasobami (zarządzanie użytkownikami i systemem, usługi DHCP, DNS, SMTP, kopie bezpieczeństwa)	7
W2	Problemy bezpieczeństwa w systemach i sieciach komputerowych co chronić, przed czym chronić, podstawowe typy ataków: Sning, ARP Spoong, IP Spoong, DoS. Metody przeciwdziałania atakom.	2
W3	Podstawy kryptograi: szyfry proste, szyfry komputerowe symetryczne i niesymetryczne. Algorytmy DES, IDEA, AES, RSA. Protokoły wymiany klucza, funkcje skrótu MD5, SHA. Infrastruktura klucza publicznego podpis elektroniczny w świetle przepisów, zarządzanie kluczami publicznymi uwierzytelnianie z wykorzystaniem algorytmów niesymetrycznych.	3
W4	Zarządzanie bezpieczeństwem infrastruktury zabezpieczenia stosowane w transmisji danych technologie VPN, SSL, SSH, KERBEROS. Bezpieczeństwo sieci bezprzewodowych. Metody wykrywania ataków na infrastrukturę (IDS, IPS, Firewall). Wirusy, konie trojańskie, programy szpiegujące możliwe drogi infekcji, metody przeciwdziałania.	3

Projekt		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin

Projekt		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Projekt infrastruktury serwerów usługowych dla sieci lokalnej małego i średniego przedsiębiorstwa w oparciu o rozwiązania MS Windows Server wg speckacji.	5
P2	Projekt infrastruktury serwerów usług sieciowych w Internecie z uwzględnieniem niezawodności i bezpieczeństwa wg podanej specykacji.	5
P3	Projekt systemu zapewnienia bezpieczeństwa infrastruktury i zasobów sieci wg specykacji	5

Laboratoria komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K1	Administracja systemami MS Windows oraz Linux (PAM, LDAP, rozszerzone listy ACL, usługi serwerowe, usługi katalogowe, GPO)	16
K2	Infrastruktura Klucza Publicznego, tworzenie i wykorzystanie, podpis elektroniczny dokumentów	4
K3	Narzędzia do analizy ruchu sieciowego oraz wykrywania ataków (Ethereal). Kryptograa, analiza algorytmów (Cryptool)	4
K4	Tunelowanie transmisji prywatne sieci wirtualne VPN	6

7 Narzędzia dydaktyczne

N1 Wykłady

N2 Ćwiczenia laboratoryjne

N3 Ćwiczenia projektowe

N4 Praca w grupach

N5 Konsultacje

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	5
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	30
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	55
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**150**
Sumaryczna liczba punktów ECTS dla przedmiotu	5.00

9 Sposoby oceny

Ocena formująca

F1 Sprawozdanie z ćwiczenia laboratoryjnego

F2 Projekt indywidualny

F3 Test

Ocena podsumowująca

P1 Średnia ważona ocen formujących

Ocena aktywności bez udziału nauczyciela

B1 Ćwiczenie praktyczne

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 3.0	Potra zastosować do określonych wymagań odpowiednie rozwiązanie techniczne dla infrastruktury serwerowej systemu informatycznego oraz w zakresie bezpieczeństwa pojedynczego komputera,infrastruktury sieci oraz transmisji danych w sieci publicznej.
Efekt kształcenia 2	

Na ocenę 3.0	Potra zastosować do określonych wymagań odpowiednie rozwiązanie techniczne dla infrastruktury serwerowej systemu informatycznego oraz w zakresie bezpieczeństwa pojedynczego komputera,infrastruktury sieci oraz transmisji danych w sieci publicznej.
Efekt kształcenia 3	
Na ocenę 3.0	Potra zastosować do określonych wymagań odpowiednie rozwiązanie techniczne dla infrastruktury serwerowej systemu informatycznego oraz w zakresie bezpieczeństwa pojedynczego komputera,infrastruktury sieci oraz transmisji danych w sieci publicznej.
Efekt kształcenia 4	
Na ocenę 3.0	Potra zastosować do określonych wymagań odpowiednie rozwiązanie techniczne dla infrastruktury serwerowej systemu informatycznego oraz w zakresie bezpieczeństwa pojedynczego komputera, infrastruktury sieci oraz transmisji danych w sieci publicznej.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	K_W11 K_U11	Cel 1	W1 W2 W3 W4 P1 P2 P3 K1 K2 K3 K4	N1 N2 N3 N4 N5	F1 F2 F3 P1
EK2	K_W11 K_U11	Cel 1	W1 W2 W3 W4 P1 P2 P3 K1 K2 K3 K4	N1 N2 N3 N4 N5	F1 F2 F3 P1
EK3	K_W11 K_U11	Cel 1	W1 W2 W3 W4 P1 P2 P3 K1 K2 K3 K4	N1 N2 N3 N4 N5	F1 F2 F3 P1
EK4	K_W11 K_U11	Cel 1	W1 W2 W3 W4 P1 P2 P3 K1 K2 K3 K4	N1 N2 N3 N4 N5	F1 F2 F3 P1

11 Wykaz literatury

Literatura podstawowa

[1] Janusz Zawiła-Niedźwiecki , Franciszek Wołowski — *Bezpieczeństwo systemów informacyjnych*, Warszawa, 2013, edu-Libri

[2] Sosna Łukasz — *Linux Komendy i polecenia*, Miejscowość, 2014, Wydawnictwo Helion

Literatura uzupełniająca

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

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

mgr inż. Mariusz Krawczyk (kontakt: mariusz.krawczyk@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

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