Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2020/2021

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka Stosowana — Profil: Praktyczny

Forma sudiów: stacjonarne — Kod kierunku: MS

Stopień studiów: I

Specjalności: Matematyka z Informatyką

1 Informacje o przedmiocie

Nazwa przedmiotu	Administracja i bezpieczeństwo systemów komputerowych
Nazwa przedmiotu w języku angielskim	Computer systems administration and security
Kod przedmiotu	WIiT MS pIS D14 20/21
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	2.00
Semestry	6

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
6	15	0	0	15	0	0

3 Cele przedmiotu

Cel 1 Cel 1. Zapoznanie studentów z zagadnieniami: administrowania systemami, kontroli procesów sieciowych, instalacji i konfiguracji serwerowych usług sieciowych, serwerów takich jak DNS, FTP/SCP, HTTP, SMTP, NFS, DHCP.

Cel 2 Cel 2. Zapoznanie z zagadnieniami sieciowymi, konfiguracja sieci, domeny, serwerów, bezpieczeństwo i mo-

nitorowanie sieci, zapoznanie z narzędziami administracyjnymi, zarządzaniem zasobami, wydajnością i bezpieczeństwem systemu.

Cel 3 Cel 3. Wprowadzenie w tematykę bezpieczeństwa systemów komputerowych. Zapoznanie z tematyką zabezpieczania przesyłania informacji. Zapoznanie studentów z metodami bezpiecznego łączenia geograficznie rozproszonych lokalizacji w logiczną wirtualną sieć. Zapoznanie studentów z metodami zapewniania bezpiecznego zdalnego dostępu do zasobów sieci chronionej.

Cel 4 Cel 4. Zapoznanie studentów z technikami filtrowania ruchu sieciowego. Zapoznanie studentów ze sposobami konfigurowania filtrów pakietów oraz proxy filtrujących.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Znajomość podstaw systemów operacyjnych i sieci komputerowych

5 Efekty kształcenia

EK1 Wiedza E1. Student zapozna się z zagadnieniami administrowania systemami komputerowymi, a zwłaszcza z zagadnieniami związanymi z instalacją systemu, instalacją oprogramowania, zarządzaniem użytkownikami, kontrolą procesów sieciowych oraz instalacją i konfiguracją sieci i serwerowych usług sieciowych, pozna problemy sieciowe związane z konfiguracją: sieci, domeny, serwerów WINS, DHCP, DNS; z oraz zagadnieniami związanymi z instalacja systemu, posługiwania się wybranymi poleceniami i narzędziami administracyjnymi, zarządzaniem zasobami, wydajnością i bezpieczeństwem.

EK2 Umiejętności E2. Student potrafi przedstawić podstawowe zagrożenia systemów komputerowych.

EK3 Umiejętności E3. Student potrafi przedstawić: zasadę działania podstawowych metod zabezpieczania systemów komputerowych, podstawowe metody bezpiecznej transmisji danych, bezpieczeństwo i monitorowanie sieci, potrafi konfigurować zintegrowane sprzętowe urządzenia zabezpieczające sieć.

EK4 Kompetencje społeczne E4. Kompetencje społeczne - studenci nabiorą umiejętności pracy w zespołach.

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Znaczenie i zastosowanie dowiązań twardych i symbolicznych w Linuksie, automatyzacja rutynowych czynności poprzez tworzenie skryptów i aliasów, sposób tworzenia zleceń jednorazowych i stałych (polecenia: at i crontab) pakowanie, rozpakowywanie, kompresowanie plików i katalogów w Linuksie, aktualizowanie skompresowanych archiwów.	1
W2	Metoda instalacji, deinstalacji i aktualizacji pakietów (oprogramowania/sterowników) w ważniejszych dystrybucjach Linuksa, uzyskiwanie polskich znaków na konsoli, na wydrukach i w plikach.	1

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W3	Instalacja różnych dystrybucji systemu Linux: a)wymagania sprzętowe b) partycjonowanie i formatowanie dysków; c) tworzenie pen-driveu bootujacego; d) instalacja nowej wersji jądra Linuksa; e) Obsługa modułów jądra Linuksa, narzędzia automatycznie ładujące i wyrzucające moduły; f) Konfiguracja i kompilacja jądra Linuksa, instalacja różnych dystrybucji systemu Linux g) ładowanie systemu Linux (GRUBa); h) Konfiguracja GRUBa. Metoda łatania plików i całych katalogów.	1
W4	Zastosowanie narzędzi synchronizacji/backupu systemu plików: tar, cpio, dd, rsync, unison. Pakiet Amanda do tworzenia backupu, administracyjne znaczenie wybranych plików systemowych znajdujących się w katalogu /etc, jaknp. aliases, anacrontab, at.deny, cron.allow, cron.deny, crontab.	1
W5	Administracyjne znaczenie wybranych plików systemowych znajdujacych się w katalogu /etc (cd.): fstab, grub.conf, host.conf, hosts, hosts.allow, hosts.deny, inittab, issue, issue.net, login.defs, modprobe.conf, motd, protocols, resolv.conf, securetty, services, shells, sudoers, syslog.conf, xinetd.conf, security/limits.conf, security/console.apps/reboot /etc (cd.) sysconfig/network, oraz pliki w katalogu sysconfig/network-scripts. Rozwiązywanie prostych problemów sieciowych.	1
W6	Narzędzia konfiguracji i kontroli jakości usług (np. linuxconf, ntsysv, tc, ip). Skrypty inicjowane w momencie startu systemu Linux (katalog /etc/rc.d). Zadania i konfiguracja poszczególnych usług sieciowych w systemie Linux. Funkcjesieciowych serwerów i metoda ich konfiguracji: a) WWW (Apache); b) DNS. c) pocztowego; d) FTP; e) DHCP; oraz f) Samba.	1
W7	Tworzenie zapory sieciowej. Rejestrowanie danych w plikach dziennika i ich monitorowanie.	1
W8	Instalacja Systemu Windows Server 2008. vLite. Server Manager. Uprawnienia NTFS i Share i zarzadzanie katalogami w Windows Server 2008. Monitorowanie i optymalizacja wydajności systemu Windows. Konfiguracja sieci, Network Monitor. Konfiguracja serwera DHCP i DNS. Instalacja Active Directory i budowa struktury AD. Server Roles, replikacja i trusty w Active Directory. Zarządzanie uprawnieniami użytkowników przy pomocy GPO. Grupy, profile i login skrypty. Windows Server Update Services. Konfiguracja Windows Server 2008 R2 Core. Dokonanie backupu i przywrócenia systemu.	1
W9	Aspekty bezpieczeństwa systemów informatycznych.	1
W10	Realizacja usług zapewnienia bezpieczeństwa informacji. Podstawowe typy i własności systemów kryptograficznych.	1
W11	Infrastruktura Klucza Publicznego PKI.	1
W12	Systemy wykrywania włamań (IDS). Protokół IPSec.	1
W13	Prywatność w ruchu sieciowym. Ukrywanie ruchu steganografia sieciowa. Monitorowanie ruchu sieciowego w celu zapewnienia bezpieczeństwa.	1
W14	Bezpieczeństwo sieci bezprzewodowych.	1

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W15	Zagrożenia zewnętrzne. Przedstawienie aktualnych trendów w bezpieczeństwie i ostatnio zidentyfikowanych zagrożeń.	1

Laboratorium komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K1	Praktyczne ćwiczenia pozwalające na bliższe poznanie głównych poleceń odpowiedzialnych za dodawanie i usuwanie kont użytkowników, modyfikowanie ich własności, np. przynależności do wielu grup	1
K2	Poznanie poleceń, plików i narzędzi Linuksa pozwalających kontrolować ustawienie zegara sprzętowego i systemowego. Praktyczne ćwiczenia pozwalające na dokładniejsze poznanie poleceń montujących, formatujących, weryfikujących powierzchnie dysku oraz tworzących i sprawdzających systemy plików.	1
K3	Ćwiczenia przypominające: a) tworzenie linków twardych i symbolicznych; b) pisanie wielolinijkowych aliasów; c) tworzenia zleceń jednorazowych i stałych (polecenia: at i crontab). Ćwiczenia przypominające pakowanie, rozpakowywanie, kompresowanie plików i katalogów w Linuksie oraz aktualizowanie skompresowanych archiwów.	1
K4	Przypomnienie poleceń Linuksa omawianych na wykładach, instalujących, deinstalujących i aktualizujących pakiety (oprogramowanie/sterowniki) w ważniejszych dystrybucjach Linuksa. Praktyczne ćwiczenia pozwalające na poznanie metod łatania plików i całych katalogów.	1
K5	Praktyczne ćwiczenia pozwalające na dokładniejsze poznanie narzędzi synchronizacji/backupu systemu plików: tar, cpio, dd, rsync, unison oraz pakietu Amanda, służącego do tworzenia backupu. Obsługa modułów jądra Linuksa, narzędzia automatycznie ładujące i wyrzucające moduły.	1
K6	Konfiguracja i kompilacja jądra Linuksa. Konfiguracja GRUBa.	1
K7	Praktyczne ćwiczenia pozwalające na dokładniejsze poznanie wybranych plików systemowych znajdujących sie w katalogu /etc, jak np. aliases, anacrontab, at.deny, cron.allow, cron.deny, crontab, fstab, grub.conf, host.conf, hosts, hosts.allow, hosts.deny, inittab.	1
K8	issue, issue.net, login.defs, modprobe.conf, motd, protocols, resolv.conf, securetty, services, shells, sudoers, syslog.conf, xinetd.conf, security/limits.conf, security/console.apps/reboot, sysconfig/network, oraz pliki w katalogu sysconfig/network-scripts.	1
K9	Poznanie narzędzi konfiguracji i kontroli jakości usług (np. linuxconf, ntsysv, tc, ip) oraz skryptów inicjowanych w momencie startu systemu Linux (katalog/etc/rc.d). Konfiguracja usług sieciowych w systemie Linux.	1

Laboratorium komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K10	Rozwiązywanie prostych problemów sieciowych. Konfiguracja sieciowych serwerów linuksowych: WWW (Apache), DNS, serwera pocztowego, FTP, DHCP, Samba.	1
K11	Tworzenie zapory sieciowej. Rejestrowanie danych w plikach dziennika i ich monitorowanie.	1
K12	Konfiguracja Proxy filtrujących. Centralne zarządzanie wieloma urządzeniami.	1
K13	Autentykacja użytkowników, tworzenie polityk bezpieczeństwa bazujących na tożsamości użytkowników. Generowanie, magazynowanie, przeglądanie logów, generowanie raportów.	1
K14	Konfigurowanie tuneli VPN dla użytkowników mobilnych z wykorzystaniem PPTP, SSL i IPSec.Konfigurowanie statycznych tuneli VPN pomiędzy urządzeniami. Obsługa wielu łączy zewnętrznych MultiWAN. Klastrowanie urządzeń (Fire Cluster).	1
K15	Filtrowanie zawartości stron www (WebBlocker).Konfigurowanie modułu ochrony przed intruzami (IPS).Filtrowanie aplikacji generujących ruch sieciowy (Application control).	1

7 Narzędzia dydaktyczne

N1 wykłady

N2 prezentacje multimedialne

N3 konsultacje

N4 ćwiczenia laboratoryjne

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	30
Konsultacje przedmiotowe	6
Egzaminy i zaliczenia w sesji	4
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	12
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	8
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**60**
Sumaryczna liczba punktów ECTS dla przedmiotu	2.00

9 Sposoby oceny

Ocena formująca

F1 Komputerowe ćwiczenia laboratoryjne

F2 Sprawdzian

Ocena podsumowująca

P1 Średnia ocen formujących

Warunki zaliczenia przedmiotu

W1 zaliczenie wszystkich ćwiczeń

W2 zaliczenie sprawdzianu

Ocena aktywności bez udziału nauczyciela

B1 Przygotowanie sprawozdań do wykonanych ćwiczeń

Kryteria oceny

Efekt kształcenia 1

Na ocenę 3.0	Student potrafi opisać działania związane z administrowaniem systemu linuksowego, ważniejsze polecenia wspomagające tworzenie backupu, zdalne administrowanie, bezpieczna współprace sieciowa systemu z innymi komputerami; oraz potrafi opisać wszystkie procesy konfiguracji usług sieciowych, spośród usług takich jak: DNS, FTP/SCP, HTTP/HTTPs, SMTP/SMTPs, POP/POPs, NFS, NIS, Samba czy DHCP.
Efekt kształcenia 2	
Na ocenę 3.0	Student potrafi zastosować działania związane z omawianymi na wykładach i ćwiczonymi na laboratoriach poleceniami linuksowymi, związanymi z administrowaniem systemu linuksowego, aktualizacją oprogramowania, zarządzaniem użytkownikami, istniejącym w systemie sprzętem, instalowaniem i aktualizacją sterowników w systemie, kontrolą procesów sieciowych oraz potrafi zastosować polecenia wspomagające tworzenie backupu, zdalne administrowanie i bezpieczną współpracę sieciową systemu z innymi komputerami.
Efekt kształcenia 3	
Na ocenę 3.0	Student potrafi wymienić podstawowe metody zabezpieczania systemów komputerowych, a na oceny wyższe potrafi opisać zasady działania zapory sieciowej, ochrony przed intruzami, ochrony antyspamowej i/lub Proxy filtrujących. Potrafi przedstawić typy (być może tylko dla niektórych) tych ochron.
Efekt kształcenia 4	
Na ocenę 3.0	Student potrafi wymienić podstawowe metody bezpiecznej transmisji danych, porównać ich zalety. Współpracuje w grupie, a na wyższe oceny potrafi przyjąć w grupie różne role.

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_W17 K_W23 K_U09 K_U17 K_K01 K_K02	Cel 1	W1 W2 W3 W4 W5 W6 W8 K1 K2 K3 K4 K10	N1 N2	F1 F2
EK2	K_W17 K_U09 K_U17 K_U23 K_U24 K_K01 K_K02	Cel 2 Cel 3	W5 W9 W10 W11 W12 W14 W15 K11 K12 K13 K14 K15	N1 N2	F1

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK3	K_W17 K_U23 K_U24 K_U30 K_K02 K_K06	Cel 2 Cel 3 Cel 4	W7 W9 W10 W11 W12 W13 W14 W15 K8 K11 K13 K14	N1 N2	F1 F2
EK4	K_U33 K_U34 K_K06	Cel 4	W13 W14 W15 K12 K13 K14	N3	F1 P1

11 Wykaz literatury

Literatura podstawowa

[1] M. Pelc — *Linux praktyka administracji*, Poznań, 2005, Nakom

[2] William R. Stanek — *Microsoft Windows Server 2008 R2 Vademecum Administratora*, Warszawa, 2010, Microsoft Press

Literatura uzupełniająca

[1] WatchGuard — *http://www.watchguard.com/help/docs/wsm/11/en-US/index.html*, WWW, 2011, WatchGuard

[2] Carlisle Adams, Steve Lloyd — *PKI podstawy i zasady działania : koncepcje, standardy i wdrażanie infrastruktury kluczy publicznych*, Warszawa, 2007, PWN

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr inż. Jerzy Białas (kontakt: jerzy.bialas@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

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