

WYMAGANIA EDUKACYJNE

Przedmiot: ADMINISTROWANIE SERWEROWYMI SYSTEMAMI OPERACYJNYMI (teoria)

Zawód: technik informatyk (technikum 5-letnie)

Kwalifikacja: INF.02. Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych

Jednostka efektów kształcenia z podstawy programowej: INF.02.8. Administrowanie serwerowymi systemami operacyjnymi

Źródła: *Program nauczania wydawnictwa Helion – technik informatyk* (rozdział 2.9. Administrowanie serwerowymi systemami operacyjnymi), *Podstawa programowa kształcenia w zawodach – INF.02* (Dziennik Ustaw, poz. 991).

Zasady konstrukcji wymagań

1. Przedmiot **Administrowanie serwerowymi systemami operacyjnymi** (teoria) jest oceniany wyłącznie za **wiedzę i rozumienie** – uczeń wie, zna, rozróżnia, wyjaśnia, charakteryzuje, porównuje, analizuje na podstawie opisu/schematu, zgodnie z zaleceniami programu nauczania dla zajęć teoretycznych.
 2. **Zasada kumulatywności ocen.**
Uzyskanie oceny wyższej wymaga opanowania wiadomości i umiejętności przypisanych do wszystkich ocen niższych. Np. na ocenę **dobrą (4)** uczeń musi dodatkowo spełniać wymagania na oceny **dopuszczającą (2)** i **dostateczną (3)**. Ocena **celująca (6)** oznacza pełne (100%), bezbłędne i w pełni samodzielne opanowanie wymagań przypisanych do ocen 2–5 w danym dziale.
 3. **Adaptacja do specyfiki przedmiotu.**
Program nauczania i podstawa programowa są sformułowane ogólnie. Poniższe wymagania dostosowano do realiów administrowania serwerowymi systemami operacyjnymi, w tym do współczesnych technologii (Windows Server 2016/2019/2022, Linux – Ubuntu Server, CentOS, usługi sieciowe, wirtualizacja, Active Directory, chmura).
 4. Godziny zajęć wg planu nauczania:
Administrowanie serwerowymi systemami operacyjnymi (teoria) – łącznie 90 godz.
 5. **Ocena niedostateczna.**
We wszystkich działach ocenę niedostateczną otrzymuje uczeń, który nie spełnia wymagań na ocenę dopuszczającą – nie posiada wiedzy/umiejętności koniecznych do kontynuowania nauki nawet przy pomocy nauczyciela, nie podejmuje samodzielnej pracy lub oddaje prace niesamodzielne.
-

Dział 1. Instalacja i konfiguracja sieciowych systemów operacyjnych

Zakres: rodzaje sieciowych systemów operacyjnych (Windows Server, Linux – komercyjne i open source), licencjonowanie, zgodność sprzętowa, instalacja, konfiguracja poinstalacyjna, modernizacja.

Ocena	Uczeń wie / rozumie / potrafi wyjaśnić
Dopuszczająca (2)	Wymienia znane sieciowe systemy operacyjne (Windows Server, Linux); wskazuje różnicę między systemem komercyjnym a open source; wymienia podstawowe kroki instalacji systemu serwerowego.
Dostateczna (3)	Opisuje rodzaje licencjonowania systemów komercyjnych i open source; wyjaśnia, na czym polega sprawdzenie zgodności sprzętowej na podstawie listy kompatybilności; wymienia etapy instalacji systemu Windows Server i Linux; opisuje podstawową konfigurację poinstalacyjną.
Dobra (4)	Charakteryzuje różnice między systemami Windows Server i Linux (zarządzanie, interfejs, konsola); wyjaśnia, jak zarządzać licencjami na serwerze; analizuje zgodność elementów systemu komputerowego z systemem operacyjnym; opisuje proces modernizacji systemu serwerowego.
Bardzo dobra (5)	Porównuje różne wersje Windows Server i dystrybucje Linux pod kątem zastosowań; analizuje wpływ konfiguracji sprzętowej na wydajność systemu serwerowego; uzasadnia wybór systemu operacyjnego dla konkretnego zastosowania (np. serwer plików, kontroler domeny, serwer WWW); przewiduje problemy podczas instalacji i modernizacji.
Celująca (6)	W pełni, bezbłędnie i samodzielnie opanował materiał działu: wyczerpująco analizuje wszystkie aspekty instalacji i konfiguracji systemów serwerowych; porównuje różne strategie wdrażania systemów (czysta instalacja, migracja, aktualizacja); ocenia ryzyko związane z modernizacją i proponuje procedury awaryjne; analizuje najbardziej złożone przypadki konfiguracji serwerów w środowiskach produkcyjnych.

Dział 2. Konfiguracja usług i funkcji sieciowych systemów operacyjnych

Zakres: usługi sieciowe (DHCP, DNS, IIS – WWW i FTP, Apache, serwer poczty, RRAS, WDS, usługi pulpitu zdalnego, usługi terminalowe, usługi plików, serwer wydruku, usługi zasad sieciowych i dostępu sieciowego), instalacja, konfiguracja, rekonfiguracja.

Ocena	Uczeń wie / rozumie / potrafi wyjaśnić
Dopuszczająca (2)	Wymienia podstawowe usługi sieciowe (DHCP, DNS, WWW); wskazuje, do czego służą; wymienia kroki instalacji usługi w systemie Windows Server i Linux.
Dostateczna (3)	Opisuje usługi dostępne w sieciowym systemie operacyjnym (DHCP, DNS, IIS, Apache, serwer poczty, RRAS, WDS, usługi plików, serwer wydruku); wyjaśnia, do czego służą poszczególne usługi; wymienia etapy instalacji i konfiguracji wybranej usługi.
Dobra (4)	Charakteryzuje rolę poszczególnych usług w infrastrukturze sieciowej; analizuje proces konfiguracji usług (DHCP – zakres, dzierżawa; DNS – strefy, rekordy; IIS – witryny, FTP; Apache – virtual hosty); wyjaśnia, jak dokonać rekonfiguracji usługi; opisuje zasady bezpieczeństwa usług sieciowych.
Bardzo dobra (5)	Porównuje różne usługi tego samego typu (np. IIS vs Apache, Windows DNS vs BIND); analizuje zależności między usługami (np. DHCP a DNS, AD a DNS); projektuje konfigurację usług dla konkretnego scenariusza (np. sieć biurowa, sieć szkolna); przewiduje skutki błędnej konfiguracji usług.
Celująca (6)	W pełni, bezbłędnie i samodzielnie opanował materiał działu: wyczerpująco analizuje wszystkie aspekty konfiguracji usług sieciowych; porównuje różne rozwiązania pod kątem wydajności, bezpieczeństwa i kosztów; ocenia przydatność poszczególnych usług w złożonych środowiskach; proponuje optymalne konfiguracje dla zaawansowanych scenariuszy (np. serwer terminali, serwer wydruku w dużej firmie, serwer poczty z filtrowaniem).

Dział 3. Wirtualizacja i zarządzanie centralne

Zakres: zasady działania systemów i usług wirtualizacyjnych, narzędzia do wirtualizacji (Hyper-V, VirtualBox, VMware), instalacja systemu/oprogramowania do wirtualizacji, instalacja systemów operacyjnych na maszynie wirtualnej, zarządzanie centralne stacjami roboczymi.

Ocena	Uczeń wie / rozumie / potrafi wyjaśnić
Dopuszczająca (2)	Definiuje pojęcie wirtualizacji; wymienia przykładowe narzędzia do wirtualizacji (VirtualBox, VMware, Hyper-V); wskazuje, że na maszynie wirtualnej można zainstalować system operacyjny.
Dostateczna (3)	Opisuje zasady działania systemów i usług wirtualizacyjnych; wyjaśnia różnicę między wirtualizacją a emulacją; wymienia etapy instalacji oprogramowania do wirtualizacji; opisuje proces instalacji systemu operacyjnego na maszynie wirtualnej.
Dobra (4)	Charakteryzuje różne narzędzia wirtualizacyjne (Hyper-V, VirtualBox, VMware) i ich możliwości; wyjaśnia, jakie zasoby sprzętowe są przydzielane maszynom wirtualnym; analizuje korzyści i ograniczenia wirtualizacji; opisuje, na czym polega zarządzanie centralne stacjami roboczymi.
Bardzo dobra (5)	Porównuje różne rozwiązania wirtualizacyjne pod kątem wydajności i zastosowań; analizuje scenariusze wdrożenia wirtualizacji (serwer produkcyjny, laboratorium, testy); wyjaśnia, jak zarządzać maszynami wirtualnymi w środowisku klastrowym; uzasadnia wybór narzędzia do konkretnego zadania.
Celująca (6)	W pełni, bezbłędnie i samodzielnie opanował materiał działu: wyczerpująco analizuje zaawansowane aspekty wirtualizacji (migracja maszyn, snapshoty, replikacja, chmura hybrydowa); porównuje różne platformy wirtualizacyjne pod kątem skalowalności i kosztów; ocenia ryzyko związane z wirtualizacją i proponuje rozwiązania minimalizujące przestoje; projektuje infrastrukturę wirtualną dla złożonych scenariuszy.

Dział 4. Kontroler domeny i Active Directory

Zakres: usługa domenowa Active Directory (las, drzewo, jednostki organizacyjne), promowanie serwera do roli kontrolera domeny, planowanie struktury katalogowej, tworzenie i konfiguracja kont domenowych, grup zabezpieczeń, profili użytkowników, zasad haseł, LDAP, GPO, podłączanie komputerów do domeny, zdalne zarządzanie, zabezpieczanie kontrolera.

Ocena	Uczeń wie / rozumie / potrafi wyjaśnić
Dopuszczająca (2)	Definiuje pojęcie domeny i kontrolera domeny; wymienia podstawowe pojęcia związane z Active Directory (las, drzewo, jednostka organizacyjna); wskazuje, że w domenie zarządza się użytkownikami i komputerami centralnie.
Dostateczna (3)	Opisuje usługę Active Directory i jej rolę w sieci; wyjaśnia pojęcia: las, drzewo, liść, jednostka organizacyjna; wymienia etapy promowania serwera do roli kontrolera domeny; opisuje proces tworzenia kont domenowych i grup zabezpieczeń; wyjaśnia, do czego służą zasady grup (GPO).
Dobra (4)	Charakteryzuje strukturę logiczną Active Directory; analizuje proces planowania struktury katalogowej (OU, użytkownicy, grupy); wyjaśnia zasady konfiguracji profili użytkowników (mobilny, obowiązkowy); opisuje konfigurację zasad haseł i GPO; analizuje proces podłączania komputera do domeny.
Bardzo dobra (5)	Porównuje różne modele struktury Active Directory (jednodomenowy, wielodomenowy); analizuje scenariusze wdrożenia AD w firmie (centralizacja, delegacja uprawnień); wyjaśnia zasady dziedziczenia uprawnień w AD; uzasadnia wybór strategii GPO dla konkretnych wymagań; ocenia bezpieczeństwo kontrolera domeny.
Celująca (6)	W pełni, bezbłędnie i samodzielnie opanował materiał działu: wyczerpująco analizuje zaawansowane aspekty Active Directory (zaufania między lasami, replikacja, FSMO, sites and services); porównuje różne strategie projektowania AD pod kątem skalowalności i bezpieczeństwa; ocenia ryzyko związane z awarią kontrolera domeny i proponuje rozwiązania redundancji; projektuje strukturę AD dla złożonych organizacji.

Dział 5. Protokoły sieciowe i udostępnianie zasobów

Zakres: protokoły w sieci komputerowej (TCP/IP, DHCP, DNS), konfiguracja interfejsów sieciowych (statyczna i dynamiczna), grupy robocze, architektura klient-serwer, analiza pakietów (Wireshark), udostępnianie zasobów (pliki, katalogi, drukarki), uprawnienia do zasobów lokalnych i sieciowych, polityka bezpieczeństwa współdzielenia zasobów.

Ocena	Uczeń wie / rozumie / potrafi wyjaśnić
Dopuszczająca (2)	Wymienia podstawowe protokoły sieciowe (TCP/IP, DHCP, DNS); wskazuje, że zasoby sieciowe można udostępniać; wymienia rodzaje uprawnień do plików i katalogów.
Dostateczna (3)	Opisuje protokoły sieciowe i ich role; wyjaśnia, jak skonfigurować interfejs sieciowy (statyczny, DHCP); wymienia rodzaje zasobów sieciowych (pliki, drukarki); opisuje zasady udostępniania i ochrony zasobów; wyjaśnia, na czym polega polityka bezpieczeństwa w aspekcie współdzielenia zasobów.
Dobra (4)	Charakteryzuje architekturę klient-serwer i grupy robocze; analizuje proces konfiguracji statycznej i dynamicznej adresacji IP; wyjaśnia, jak działają uprawnienia do zasobów lokalnych i sieciowych (NTFS, udziały); opisuje, jak publikować zasoby sieciowe z wykorzystaniem usług katalogowych; analizuje pakiety sieciowe w Wireshark.
Bardzo dobra (5)	Analizuje ruch sieciowy i identyfikuje protokoły oraz usługi; porównuje różne metody udostępniania zasobów; wyjaśnia mechanizmy dziedziczenia uprawnień; uzasadnia wybór polityki bezpieczeństwa dla konkretnego scenariusza; ocenia skuteczność zabezpieczeń zasobów sieciowych.
Celująca (6)	W pełni, bezbłędnie i samodzielnie opanował materiał działu: wyczerpująco analizuje złożone scenariusze udostępniania zasobów (np. macierze dyskowe, serwery plików z kontrolą wersji, serwery wydruku); porównuje różne modele uprawnień i polityk bezpieczeństwa; ocenia ryzyko związane z błędną konfiguracją uprawnień; projektuje politykę bezpieczeństwa współdzielenia zasobów dla dużej organizacji.

Dział 6. Zarządzanie stacjami roboczymi

Zakres: narzędzia do zarządzania stacjami roboczymi, zdalne zarządzanie, monitorowanie działań użytkowników, zdalne usuwanie usterek systemu, zasady bezpieczeństwa zarządzania zdalnego.

Ocena	Uczeń wie / rozumie / potrafi wyjaśnić
Dopuszczająca (2)	Wymienia narzędzia do zarządzania stacjami roboczymi (pulpit zdalny, zdalna asystencja); wskazuje, że można monitorować działania użytkowników.

Ocena	Uczeń wie / rozumie / potrafi wyjaśnić
Dostateczna (3)	Opisuje narzędzia służące do zarządzania stacjami roboczymi; rozróżnia sposoby zarządzania (lokalne, zdalne); wyjaśnia, na czym polega monitorowanie działań użytkowników; opisuje proces zdalnego usuwania usterek systemu.
Dobra (4)	Charakteryzuje różne narzędzia do zdalnego zarządzania (RDP, VNC, PowerShell Remoting, RSAT); analizuje proces monitorowania działań użytkowników z poziomu systemu operacyjnego; wyjaśnia, jak zabezpieczyć zdalny dostęp do stacji roboczych.
Bardzo dobra (5)	Porównuje różne metody zdalnego zarządzania pod kątem bezpieczeństwa i wydajności; analizuje scenariusze zdalnego rozwiązywania problemów; uzasadnia wybór narzędzia w zależności od sytuacji; ocenia ryzyko związane z zarządzaniem zdalnym.
Celująca (6)	W pełni, bezbłędnie i samodzielnie opanował materiał działu: wyczerpująco analizuje zaawansowane scenariusze zarządzania stacjami roboczymi (zarządzanie flotą komputerów, automatyzacja, skrypty); porównuje różne strategie zarządzania w dużych organizacjach; projektuje politykę zdalnego zarządzania z uwzględnieniem bezpieczeństwa; ocenia skuteczność różnych narzędzi w złożonych środowiskach.