



poziom: **Core**

wersja: **3.0**

moduł: **C : Eksploatacja**

SYLABUS

Niniejszy dokument jest sylabusem obowiązującym dla certyfikatu EUCIP ver. 3.0.
Prezentuje obszary wiedzy, których znajomość jest niezbędna do zaliczenia modułu „**Eksploatacja**”.

Zastrzeżenie:

Dokument ten został opracowany ze szczególną starannością na podstawie materiałów źródłowych pochodzących z Fundacji ECDL. Polskie Towarzystwo Informatyczne i Fundacja ECDL zastrzegają sobie prawo do zmian treści dokumentu oraz wyłączenia od odpowiedzialności za jakiegokolwiek straty i szkody powstałe na skutek wykorzystania niniejszego dokumentu i treści w nim zawartych.

Cel

Obszar wiedzy: **Eksploatacja** **Moduł C: Eksploatacja** – dotyczy sieci komputerowych i związanych z nimi usług komunikacyjnych infrastruktury IT, a także zagadnień utrzymywania i użytkowania tych usług. Moduł wymaga od kandydata znajomości komponentów sprzętowych i architektury komputerów. Niezbędna jest też wiedza dotycząca systemów operacyjnych. Kandydat powinien również rozróżniać warstwy protokołów komunikacyjnych oraz aplikacji na nich bazujących zarówno dla technologii przewodowych jak i bezprzewodowych. Istotna jest znajomość takich zagadnień jak protokół SNMP, e-mail, i serwisy internetowe, a także związanych z nimi zagadnień bezpieczeństwa. Zdający powinien rozumieć znaczenie działań zorientowanych na klienta, w odniesieniu do zagadnień IT, a także potrafić zastosować podstawowe zasady dostarczania serwisów IT.

Kategoria	Obszar wiedzy	Nr Ref.	Zakres
C.1 Komponenty i architektury systemów komputerowych	C.1.1 Sprzęt	C.1.1.1	Wskaż najważniejsze komponenty systemu komputerowego, takie jak CPU, RAM, ROM oraz opisz ich funkcje.
		C.1.1.2	Opisz wzajemne powiązania pomiędzy głównymi komponentami systemu komputerowego.
		C.1.1.3	Wskaż najważniejsze typy jednostek peryferyjnych podstawowego systemu komputerowego, takich jak ekran, klawiatura, urządzenia wskazujące, dyski, karty sieciowe, drukarki i opisz ich funkcje.
		C.1.1.4	Opisz różne rodzaje urządzeń peryferyjnych i porównaj ich cechy oraz wydajność w oparciu o odpowiednie parametry, takie jak pojemność, prędkość, rozdzielczość, standardy kompatybilności.
		C.1.1.5	Dokonaj rozróżnienia pomiędzy najważniejszymi typami pamięci, takimi jak DRAM, SRAM, EPROM, flash i porównaj ich zastosowania.
	C.1.2 Architektury komputerów	C.1.2.1	Wyjaśnij za pomocą diagramów architekturę komputera ogólnego zastosowania.
		C.1.2.2	Opisz koncepcję chipsetu i zastosowanie różnych typów magistrali w systemie komputerowym.
		C.1.2.3	Wyjaśnij koncepcję hierarchii pamięci, poziomów hierarchii, dokonaj porównania szybszych pamięci z wolniejszymi nośnikami pamięci, opisz wydajność pamięci cache oraz jej wpływ na systemy komputerowe.
		C.1.2.4	Rozpoznaj dostępne rodzaje systemów komputerowych, takie jak urządzenie naręczne, laptop, komputer stacjonarny, serwer wieloprocesorowy, komputer mainframe oraz wyjaśnij podstawowe różnice pomiędzy nimi.
	C.1.3 Procesory	C.1.3.1	Wyjaśnij koncepcję architektury listy rozkazów (ang. Instruction Set Architecture – ISA).
		C.1.3.2	Wyjaśnij dualizm koncepcji procesorów RISC oraz CISC.
		C.1.3.3	Wyjaśnij koncepcję przetwarzania potokowego i równoległego, dynamicznego planowania, wykonywania spekulatywnego.
		C.1.3.4	Wyjaśnij termin koprocesor i opisz rolę koprocesora w architekturze ISA.
		C.1.3.5	Opisz cechy mikroprocesora, takie jak liczba rdzeni, częstotliwość taktowania, stopnie potoku, system buforowania, rozmiar chipsetu, pobór mocy i straty energii.
	C.2 Systemy operacyjne	C.2.1 Założenia	C.2.1.1

	C.2.1.2	Opisz różne rodzaje systemów operacyjnych, takie jak wsadowe, z podziałem czasu, czasu rzeczywistego.
	C.2.1.3	Opisz koncepcję interfejsu programowania aplikacji (ang. Application Programming Interface – API) i wskaż przykłady API, takie jak Java API, Windows API, Google Maps API.
	C.2.1.4	Opisz w jaki sposób oprogramowanie może zarządzać zasobami komputera.
C.2.2	C.2.2.1	Wskaż powody stosowania współbieżności w systemach operacyjnych.
Procesy współbieżne i równoległe	C.2.2.2	Opisz problem wzajemnego wykluczenia.
	C.2.2.3	Opisz koncepcję przetwarzania oraz przetwarzania równoległego.
	C.2.2.4	Wyjaśnij pojęcie wątków.
	C.2.2.5	Opisz operację przełączania kontekstu.
C.2.3	C.2.3.1	Wyjaśnij cel stosowania pamięci wirtualnej.
Pamięć i zarządzanie pamięcią	C.2.3.2	Opisz w jaki sposób system operacyjny zarządza pamięcią wirtualną poprzez nośnik pamięci i pamięć sprzętową.
	C.2.3.3	Opisz koncepcję tzw. „migotania” (ang. thrashing) i jego wpływ oraz metody zapobiegania i zarządzania.
	C.2.3.4	Opisz w jaki sposób koncepcja hierarchii pamięci wpływa na programowanie.
	C.2.3.5	Opisz funkcje systemu plików.
C.2.4	C.2.4.1	Wyjaśnij potrzebę bezpieczeństwa i ochrony w systemie komputerowym w kontekście poufności, spójności i dostępności.
Bezpieczeństwo i ochrona	C.2.4.2	Opisz rodzaje mechanizmów ochrony stosowanych w systemach operacyjnych.
	C.2.4.3	Opisz zagrożenia związane ze złośliwym oprogramowaniem, takie jak luki w zabezpieczeniach, konie trojańskie, wirusy komputerowe. Opisz najważniejsze środki zapobiegawcze stosowane przeciwko takim zagrożeniom.
	C.2.4.4	Opisz różnice pomiędzy identyfikacją a uwierzytelnianiem.
	C.2.4.5	Opisz techniki uwierzytelniania i zdefiniuj „silny” mechanizm uwierzytelniający.
	C.2.4.6	Opisz założenia kontroli dostępu.
	C.2.4.7	Wyjaśnij potrzebę stosowania kopii bezpieczeństwa i przywracania systemu.

	C.2.5 Powszechnie stosowane systemy operacyjne	C.2.5.1	Opisz główne cechy systemów operacyjnych należących do rodzin Unix, Linux, Mac, takie jak sposoby instalacji, interfejsy użytkownika, bezpieczeństwo, wydajność, stabilność, popularne zastosowania.
		C.2.5.2	Opisz główne cechy systemów operacyjnych należących do rodziny Microsoft Windows, takie jak sposoby instalacji, interfejsy użytkownika, bezpieczeństwo, wydajność, stabilność, popularne zastosowania.
C.3 Komunikacja i sieci	C.3.1 Podstawowe założenia komunikacji	C.3.1.1	Wskaż różnice pomiędzy logiczną, a fizyczną funkcjonalnością sieci.
		C.3.1.2	Opisz zasady przesyłu informacji i zdefiniuj koncepcję sygnału.
		C.3.1.3	Wskaż różnice pomiędzy sygnałami ciągłymi i cyfrowymi.
		C.3.1.4	Wskaż problemy związane z konwersją sygnałów ciągłych na cyfrowe i odwrotną.
		C.3.1.5	Porównaj komutację łączy z komutacją pakietów.
		C.3.1.6	Opisz rolę jednostek standaryzacji sieci, takich jak ITU, IEEE.
	C.3.2 Komponenty i architektury sieciowe	C.3.2.1	Wymień komponenty sieciowe, takie jak host, medium i urządzenia transmisyjne oraz opisz ich funkcje.
		C.3.2.2	Dokonaj charakterystyki mediów transmisyjnych, takich jak skrętka, kabel koncentryczny, światłowód, mikrofałe.
		C.3.2.3	Opisz sposoby łączenia z sobą mediów transmisyjnych.
		C.3.2.4	Opisz funkcje urządzeń łączących, takich jak koncentrator, przełącznik, router, regeneratory sygnału.
		C.3.2.5	Wskaż cechy różniące sieci WAN i LAN.
		C.3.2.6	Opisz różne technologie i możliwości sieci WAN, takie jak system wdzwaniany (ang. dial-up), ISDN, DSL, sieć z komutacją pakietów, łącze dzierżawione.
		C.3.2.7	Opisz standardowe topologie sieci i powiąż je z odpowiednimi standardami LAN, takimi jak Ethernet, token ring, FDDI.
		C.3.2.8	Opisz różne strategie dostępu do medium transmisyjnego stosowane w różnych standardach, takie jak CSMA/CD oraz przekazywanie tokenu.
		C.3.2.9	Opisz działanie zapory sieciowej i jej znaczenie dla bezpieczeństwa sieci.
	C.3.3 Protokoły komunikacyjne	C.3.3.1	Opisz 7-warstwowy model sieciowy ISO i wymień usługi, które opisane są w każdej z warstw.
		C.3.3.2	Powiąz model TCP/IP z modelem ISO.
		C.3.3.3	Opisz w jaki sposób pakiet jest trasowany w sieci Internet.
		C.3.3.4	Porównaj strumienie i protokoły połączeniowe z komunikacją pakietową i protokołami bezpołączeniowymi.
		C.3.3.5	Wskaż różnice pomiędzy TCP i UDP pod względem niezawodności i szybkości.

C.4 Usługi sieciowe	C.4.1 Bezpieczeństwo sieci	C.4.1.1	Opisz różne rodzaje zagrożeń dla normalnego działania sieci, takich jak atak typu DoS (ang. Denial of Service), przechwytywanie danych, kradzież portów.
		C.4.1.2	Zdefiniuj koncepcje podszywania się i kradzieży tożsamości oraz związane z nimi zagrożenia bezpieczeństwa.
	C.4.2 Kryptografia	C.4.2.1	Opisz źródła kryptografii i jej zastosowania w bezpieczeństwie sieciowym.
		C.4.2.2	Wskaż różnice pomiędzy algorytmami klucza prywatnego oraz algorytmami klucza publicznego.
		C.4.2.3	Opisz w jaki sposób kryptografia jest wykorzystywana w ochronie komunikacji sieciowej poprzez poprawę poufności (IPSec, SSH, SSL), wymuszanie uwierzytelniania (podpis cyfrowy) oraz tworzenie wirtualnych sieci prywatnych (ang. Virtual Private Network – VPN).
	C.4.3 System Nazw Domenowych DNS	C.4.3.1	Opisz system DNS i jego zakres.
		C.4.3.2	Opisz system nazewnictwa hostów w sieci Internet.
		C.4.3.3	Opisz cel i zastosowanie deskryptorów zasobów.
		C.4.3.4	Opisz adresowanie IP (ang. Internet Protocol) i sposób tłumaczenia nazw domen na adresy IP.
	C.4.4 Sieć WWW	C.4.4.1	Opisz system WWW (ang. World Wide Web) jako zastosowanie architektury klient – serwer.
		C.4.4.2	Opisz rolę serwera WWW.
		C.4.4.3	Opisz rolę klienta WWW (przeglądarki).
		C.4.4.4	Opisz rolę i funkcje protokołu HTTP (ang. Hypertext Transmission Protocol).
		C.4.4.5	Opisz zastosowanie URL (ang. Uniform Resource Locator).
		C.4.4.6	Opisz cel i zastosowanie CGI (ang. Common Gateway Interface).
		C.4.4.7	Opisz koncepcję apletu.
		C.4.4.8	Wyjaśnij dynamiczne zarządzanie zawartością strony internetowej za pomocą bazy danych.
		C.4.4.9	Wymień dostępne możliwości utrzymywania strony internetowej, takie jak posiadanie własnego serwera WWW, współdzielenie serwera komercyjnego dostawcy usług, korzystanie z dedykowanego serwera komercyjnego dostawcy usług.
	C.4.5 Komunikacja elektroniczna	C.4.5.1	Porównaj systemy komunikacji elektronicznej, takie jak poczta email, SMS/MMS, komunikatory internetowe, narzędzia portali społecznościowych.
		C.4.5.2	Wskaż różnice pomiędzy zastosowaniami poczty email i webmail.
C.4.5.3		Opisz role i funkcje klientów, serwerów i bramek poczty email.	
C.4.5.4		Opisz protokoły SMTP (ang. Simple Mail Transfer Protocol), POP3 (ang. Post Office Protocol v.3), IMAP (ang. Internet Message Access Protocol).	

	C.4.6 VoIP (ang. Voice over Internet Protocol)	C.4.6.1	Opisz koncepcję telefonii IP.
		C.4.6.2	Opisz wymagania technologii VoIP wobec sieci i użytkownika.
	C.4.7 Wymiarowanie infrastruktury systemowej	C.4.7.1	Opisz wpływ ilości i typu danych na zasoby sieciowe, jak np. wymagania dla transmisji tekstu, głosu, muzyki, obrazów, obrazów ruchomych, transmisji audiowizualnej.
		C.4.7.2	Opisz charakterystykę systemu komputera serwera pełniącego rolę hosta dla aplikacji multimedialnej.
C.5 Przetwarzanie bezprzewodowe	C.5.1 Komponenty multimedialne i bezprzewodowe	C.5.1.1	Opisz kilka elektronicznych urządzeń mobilnych, takich jak smartphone, PDA, GPS, komponenty tzw. „ubieralnej” elektroniki.
		C.5.1.2	Opisz najważniejsze multimedialne urządzenia wejścia / wyjścia, takie jak skanery, aparaty cyfrowe, mikrofony, ekrany, wyświetlacze, głośniki oraz słuchawki i wyjaśnij ich zastosowania.
		C.5.1.3	Opisz najważniejsze standardy pamięci w zastosowaniach multimedialnych, takie jak CD-ROM, DVD, dyski magnetoptyczne oraz pamięci flash i wskaż techniczne różnice pomiędzy nimi.
	C.5.2 Podstawy komunikacji bezprzewodowej	C.5.2.1	Wymień technologie stosowane w komunikacji bezprzewodowej i opisz ich funkcjonalność.
		C.5.2.2	Wskaż najważniejsze różnice pomiędzy wiodącymi standardami bezprzewodowymi, takimi jak Bluetooth, IEEE802.11, IEEE802.16(WiMax).
		C.5.2.3	Opisz ograniczenia i problemy związane z bezprzewodowym i mobilnym przetwarzaniem danych, takie jak dostępność, szybkość komunikacji, kompatybilność.
	C.5.3 Sieci i protokoły bezprzewodowe	C.5.3.1	Opisz najważniejsze komponenty bezprzewodowej sieci LAN (WLAN) i wyjaśnij ich zastosowanie.
		C.5.3.2	Dokonaj oceny kompatybilności różnych technologii WLAN.
		C.5.3.3	Opisz najważniejsze komponenty sieci satelitarnej.
		C.5.3.4	Opisz najważniejsze protokoły mobilne, takie jak mobile IP, WAP, Bluetooth, UMTS.
		C.5.3.5	Opisz zakres zastosowań każdego z protokołów dla stacji mobilnych.
		C.5.3.6	Opisz koncepcję identyfikacji radiowej (ang. Radio Frequency Identification) i jej zastosowania, takie jak identyfikacja dokumentów, śledzenie produktu, płatności w transporcie, systemy inwentaryzacyjne.
C.6 Zarządzanie sieciami	C.6.1 Podstawy zarządzania sieciami	C.6.1.1	Opisz najważniejsze funkcje systemu zarządzania siecią.

		C.6.1.2	Opisz różne parametry, którymi można zarządzać w sieci, takie jak wydajność, usterki, ustawienia konfiguracyjne.
		C.6.1.3	Porównaj różne architektury systemów zarządzania siecią.
	C.6.2 Protokół Simple Network Management Protocol	C.6.2.1	Opisz główne komponenty protokołu Simple Network Management Protocol i ich wzajemne zależności.
		C.6.2.2	Opisz najważniejsze usługi udostępniane przez protokół SNMP.
		C.6.2.3	Opisz najważniejsze ograniczenia protokołu SNMP.
	C.6.3 Narzędzia zarządzania systemami i sieciami	C.6.3.1	Wskaż różnice pomiędzy narzędziem zarządzania systemem a narzędziem zarządzania siecią.
		C.6.3.2	Wskaż kilka szeroko stosowanych narzędzi programowych do zarządzania systemami oraz sieciami, takich jak ping, traceroute, tcpdump, HP Software, Tivoli NetView, Solstice, OpenNMS.
		C.6.3.3	Opisz wymagania infrastrukturalne dla zastosowania narzędzia zarządzania siecią.
C.7 Dostarczanie usług i wsparcie	C.7.1 Relacje z klientem i ustalenia poziomu usług	C.7.1.1	Opisz proces zarządzania poziomem usług i wskaż płynące z niego korzyści.
		C.7.1.2	Wymień i opisz najważniejsze elementy dokumentu SLA (ang. Service Level Agreement), takie jak definicja usług, pomiar wydajności, zarządzanie problemami, prawa własności intelektualnej, informacje poufne, gwarancje, zakończenie usługi.
		C.7.1.3	Porównaj zastosowania i cele dokumentów SLA, kontraktów i uzgodnień poziomu wykonawczego.
	C.7.2 Planowanie pojemnościowe i awaryjne	C.7.2.1	Opisz zarządzanie pojemnością i wyjaśnij znaczenie trzech podprocesów biznesu, usług i komponentów.
		C.7.2.2	Wyjaśnij cel i główne składowe planu pojemnościowego.
		C.7.2.3	Wyjaśnij koncepcje ryzyka, zagrożenia oraz wrażliwości i wskaż przykłady każdego z nich w kontekście systemu informacyjnego, takie jak przerwanie usługi, utrata danych.
		C.7.2.4	Wymień przykłady środków ograniczających ryzyko.
		C.7.2.5	Wskaż cel i główne elementy planu awaryjnego / ciągłości usług, takie jak tolerancja błędów, procedury ponownego uruchamiania, zasoby alternatywne, przywracanie.
	C.7.3 Zarządzanie dostępnością	C.7.3.1	Wskaż cele i korzyści wynikające z zarządzania dostępnością i zdefiniuj pojęcia dostępności, niezawodności, awarii, przywracania.

	C.7.3.2	Porównaj stosowane powszechnie miary dostępności, takie jak dostępność procentowa, częstotliwość usterek, średni czas pomiędzy usterkami, wpływ usterki.
	C.7.3.3	Opisz metody i techniki zarządzania dostępnością, takie jak CFIA (ang. Component Failure Impact Analysis), FTA (ang. Fault Tree Analysis).
C.7.4 Service desk	C.7.4.1	Opisz cel istnienia jednostki service desk w organizacji wsparcia usług.
	C.7.4.2	Wskaz różne typy jednostek service desk i opisz warunki, w jakich są one odpowiednie.
	C.7.4.3	Zdefiniuj główne elementy systemu zarządzania incydentami.
C.7.5 Zarządzanie zmianami	C.7.5.1	Opisz najlepsze praktyki w zarządzaniu konfiguracją infrastruktury IT.
	C.7.5.2	Opisz najlepsze praktyki w zarządzaniu wersjami oraz zmianami w IT.
	C.7.5.3	Zdefiniuj cel żądania zmiany i najważniejsze elementy, jakie zawiera takie żądanie.