# EITC/IS/OS

## Bezpieczeństwo systemów operacyjnych

Szczegółowa zawartość programowa kursu (15 godz.):

- Wprowadzenie do systemów operacyjnych
    - Miejsce, rola i zadania systemu operacyjnego w oprogramowaniu komputera
    - Klasyfikacja systemów operacyjnych
        - Klasyfikacja ze względu na sposób przetwarzania
        - Klasyfikacja ze względu na liczbę wykonywanych programów
        - Klasyfikacja ze względu na liczbę użytkowników
        - Inne rodzaje systemów operacyjnych
    - Zasada działania systemu operacyjnego
        - Cykl rozkazowy
        - Przerwania w systemie komputerowym
        - Zasady ochrony pamięci
        - Przerwanie zegarowe
- Procesy, zasoby, wątki
    - Obsługa procesów i zasobów
        - Podział operacji jądra systemu w zarządzaniu procesami i zasobami
        - Zarządcy
        - Cykl zmian stanów procesów i zasobów
        - Klasyfikacja zasobów
        - Kolejki procesów
        - Przełączanie kontekstu
        - Elementarne operacje na procesach
        - Elementarne operacje na zasobach
    - Wątki
        - Realizacja wątków
        - Przełączanie kontekstu wątków
        - Elementarne operacje na wątkach
    - Realizacja procesów/wątków w systemach Linux i Windows
        - Procesy/wątki w systemie Linux
        - Procesy/wątki w systemie Windows 2000/XP
- System plików – warstwa logiczna
    - Pliki w systemie operacyjnym
        - Zadania systemu operacyjnego
        - Atrybuty pliku
        - Typy plików
        - Struktura pliku
        - Metody dostępu do plików
        - Podstawowe operacje na plikach
    - Interfejs dostępu do pliku w systemie uniksopodobnym
    - Organizacja logiczna systemu plików
        - Podział na strefy
        - Operacje na katalogu
        - Struktura logiczna katalogów
- System plików – warstwa fizyczna
    - Przydział miejsca na dysku
        - Przydział ciągły
        - Przydział listowy (łańcuchowy)
        - Przydział indeksowy
    - Zarządzanie wolną przestrzenią

- Implementacja katalogu
- Przechowywanie podręczne w systemie plików
- Integralność systemu plików
- Synchronizacja dostępu do plików

- System plików – przegląd wybranych implementacji
  - CP/M
  - MS DOS i Windows 9x (FAT12/16/32)
  - ISO 9660
  - UNIX
  - NTFS
- Wprowadzenie do bezpieczeństwa systemów operacyjnych
  - Co to jest bezpieczny system?
  - Czynniki decydujące o znaczeniu bezpieczeństwa
  - Zagrożenia bezpieczeństwa
  - Ogólne problemy konstrukcji zabezpieczeń
  - Strategia bezpieczeństwa
  - Polityka bezpieczeństwa
  - Normy i zalecenia zarządzania bezpieczeństwem
- Podstawowe problemy bezpieczeństwa systemów operacyjnych
  - Wprowadzenie
  - Naruszenia bezpieczeństwa systemu operacyjnego
  - Rozpoznawanie systemu operacyjnego komputera ofiary
  - Uwierzytelnianie
  - Prawa dostępu do zasobów
    - Standard POSIX (Portable Operating System Interface) 1003.1
    - Standard POSIX 1003.1e/1003.2c
    - Listy dostępu ACL
  - Uprawnienia specjalne w systemie Unix
  - Malware
    - Wirusy i inne robactwo
  - Zamaskowane kanały komunikacji
- Uwierzytelnianie i kontrola dostępu
  - Ogólne założenie uwierzytelniania w systemie Linux
  - Prawa dostępu do plików w systemach uniksopodobnych
  - Mechanizm POSIX ACL w systemie Linux i Windows
    - Lokalna kontrola dostępu w systemie Linux
    - Lokalna kontrola dostępu w systemie Windows XP
  - Modularne systemy uwierzytelniania i kontroli dostępu
    - Mechanizm PAM
- Ograniczenia i delegacja uprawnień, domeny zaufania, kontrola dostępu zdalnego
  - Ograniczone środowiska wykonywania aplikacji, ograniczone powłoki systemu operacyjnego środowisk serwerowych, delegacja uprawnień
    - Mechanizm limitów
    - Mechanizm SUDO
    - Mechanizm SUID i SGID
  - Domeny zaufania, mechanizmy kontroli zdalnego dostępu
    - Zastosowanie domen zaufania
    - Polecenie rlogin w systemie Linux
    - Zabezpieczanie usług sieciowych programem tcpd
- Umacnianie ochrony systemu operacyjnego serwerowych środowisk MS Windows
  - Konta użytkowników
  - System plików
  - Szyfrowanie danych
    - Szyfrowanie na poziomie systemu plików
    - Archiwa z ochroną kryptograficzną

- Kryptograficzna ochrony poczty elektronicznej
- Środowisko sieciowe
  - Otoczenie sieciowe i udziały sieciowe
  - Ukrycie komputera w otoczeniu sieciowym
  - Połączenia sieciowe
  - Zapory sieciowe
- Podsumowanie