| Tytuł | Kod |
|---|---|
| **Systemy operacyjne** | **1010332411010330674** |
| Kierunek: **Informatyka** | Rok / Semestr: **1 / 1** |
| Specjalność: **-** | Przedmiot: **obowiązkowy** |
| Godziny: Wykłady: **1** Ćwiczenia: **-** Laboratoria: **1** Projekty / seminaria: **1** | Liczba punktów: **5** |
| | Język prowadzenia przedmiotu: **polski** |

## Prowadzący:

dr inż. Tomasz Bilski
Instytut Automatyki i Inżynierii Informatycznej
pl. Skłodowskiej-Curie 5
60-965 Poznań
tel. (061) 665-3714
email: tomasz.bilski@put.poznan.pl

## Wydział:

Wydział Elektryczny
ul. Piotrowo 3A
60-965 Poznań
tel. (061) 665-2539, fax. (061) 665-2548
e-mail: office_deef@put.poznan.pl

## Miejsce przedmiotu w programie studiów:

przedmiot obowiązkowy

## Założenia i cele przedmiotu:

Celem przedmiotu jest zapoznanie studentów z podstawowymi modelami, kryteriami oceny i zasadami projektowania systemów operacyjnych ze szczególnym uwzględnieniem problemów ochrony danych

## Treści programowe przedmiotu (opis przedmiotu):

Wykłady

Aspekty bezpieczeństwa danych (poufność, integralność, dostępność), ogólny model bezpieczeństwa (model Clementa). Elementy bezpieczeństwa zintegrowane z systemami operacyjnymi (uwierzytelnianie użytkowników, systemy kontroli dostępu, monitorowanie zdarzeń, ochrona procesów, mechanizmy kryptograficzne, replikacja zasobów, zapora sieciowa) - charakterystyka ogólna, przykłady. Systemy wykrywania włamań (IDS), systemy prewencyjne (IPS), metody działania. Zasady projektowania bezpiecznych systemów operacyjnych. Formalne modele systemów kontroli dostępu, klasyfikacja (uznaniowy, obowiązkowy, otwarty, zamknięty), elementy składowe modeli (podmioty, obiekty, operacje).

Model macierzowy. Model przejmij-przekaż. Model Bella-LaPaduli. Modele Diona i Biby. Standardy i kryteria oceny bezpieczeństwa (TCSEC, ITSEC, ISO 15408), etapy procesu certyfikowania systemu.

Laboratorium

Zajęcia obejmują zapoznanie się studentów z mechanizmami bezpieczeństwa zintegrowanymi z przykładowymi systemami operacyjnymi (MS Windows, Linux) oraz projektowanie i implementowanie własnych narzędzi ochrony.

1. Uwierzytelnianie, konfigurowanie i testowanie
2. Analizator bezpieczeństwa haseł, projekt, programowanie i testy własnej implementacji
3. System kontroli dostępu, konfigurowanie i testowanie
4. System monitorowania zdarzeń, konfigurowanie i testowanie
5. Analizator logów systemowych, projekt, programowanie i testy własnej implementacji
6. System wykrywania włamań (Intrusion Detection System), konfigurowanie i testowanie
7. System prewencyjny (Intrusion Prevention System), konfigurowanie i testowanie

8. Zapora sieciowa - konfigurowanie i testowanie bezpieczeństwa
9. Skaner bezpieczeństwa projekt, programowanie i testy własnej implementacji
10. Mechanizm szyfrowanie plików, konfigurowanie i testowanie

## Przedmioty wprowadzające i wymagane wiadomości wstępne:

Systemy operacyjne, ochrona danych, sieci komputerowe, umiejętność programowania w języku wysokiego poziomu.

## Forma zajęć i metody dydaktyczne:

wykład z prezentacją multimedialną, laboratorium, projekt

## Forma i warunki zaliczenia przedmiotu – wymagania i system oceniania:

egzamin pisemny
zaliczenie laboratorium
zaliczenie projektu

## Bibliografia podstawowa:

-

## Bibliografia uzupełniająca:

-