

## Zakład Systemów Informatycznych Warszawskiej Wyższej Szkoły Informatyki

### Laboratorium inżynierii bezpieczeństwa systemów informatycznych

#### **Przeznaczenie:**

Celem przedsięwzięcia było zbudowanie infrastruktury technicznej, pozwalającej studentom na zapoznanie się z wiedzą teoretyczną i praktyczną z dziedziny inżynierii bezpieczeństwa systemów teleinformatycznych.

Zrealizowane laboratorium umożliwia rozwiązywanie realnych problemów oraz oferuje cały zestaw środków i narzędzi internetowo - multimedialnych do samodzielnego zdobywania wiedzy.

#### **W skład laboratorium wchodzi zaplecze sprzętowe i programowe.**

Podstawowy cel stworzonego laboratorium to zapewnienie realizacji wszystkich zagadnień, które objęte są programem nauczania na specjalności „Inżynieria sieci teleinformatycznych” realizowanych w ramach następujących przedmiotów:

1. zarządzanie bezpieczeństwem informacji według norm ISO/IEC 27001
2. bezpieczeństwo systemów teleinformatycznych
3. bezpieczeństwo i niezawodność systemów rozproszonych
4. wykrywanie i analiza zagrożeń w sieci Internet
5. Projekt indywidualny i grupowy
6. Praca dyplomowa

#### **Zaplecze sprzętowe:**

Laboratorium zlokalizowane jest w 2 pracowniach komputerowych.

Sprzętowo realizowane jest w 2 konfiguracjach:

#### Konfiguracja 1 (sprzęt HP):

- **Sprzęt komputerowy:**
  - Komputer PC
  - Procesor Intel Core 2 Quad Q9400
  - Pamięć RAM 2 \* 2GB
  - Dysk twardy 500 GB
  - Płyta główna zawierająca 4 sloty DDR2 800MHz, zawierająca kartę graficzną, kartę muzyczną i kartę sieciową
  - Monitor LCD 19"

- Ilość – 24 stanowiska
- **Sprzęt CISCO**
  - Zestaw I (stacjonarny)**
    - Router Cisco 1700 – szt. 1
    - Router Cisco 2610 – szt. 4
    - Router Cisco 2514 – szt. 1
    - Switch Catalyst 2900 – szt. 3
    - Switch 3com 4400SE – szt. 2
    - Modem ZYDEL U – 336S Supreme – szt. 5
    - Terminale – szt. 4
    - Szafa teleinformatyczna naścienna – szt. 4
  - Zestaw II („mobilny”)**
    - Router Cisco 2801 – szt. 6
    - Switch Catalyst 2960 – szt. 3
    - Modem ZYDEL U – 336S Supreme – szt. 5
    - Szafa rakowa 42U (na kółkach) – szt. 1
- **Łącze internetowe 100Mb/s**

Konfiguracja 2 (sprzęt Lenovo):

- **Sprzęt komputerowy:**
  - Komputer PC
  - Procesor Intel Core 2 Duo E4600
  - Pamięć RAM 3 GB
  - Dysk twardy 500 GB
  - Płyta główna zawierająca 4 sloty DDR2 800MHz, zawierająca kartę graficzną, kartę muzyczną i kartę sieciową
  - Monitor 19”
  - Ilość – 24 stanowiska
- **Sprzęt CISCO**
  - Router Cisco 1700 – szt. 5
  - Switch Catalyst 2950 – szt. 3
  - Hub Ovislink FSH16D – szt. 1
  - Terminale – szt. 4
  - Szafa teleinformatyczna naścienna – szt. 4

- Łącze internetowe 100Mb/s

**W laboratorium możliwy jest do realizacji program nauczania obejmujący między innymi zagadnienia dotyczące:**

- tworzenia i eksploatacji systemów informacji,
- realizacji i weryfikacji komponentów systemów informatycznych zgodnie z ich specyfikacją,
- budowy współczesnych komputerów i urządzeń z nimi współpracujących,
- praktycznego posługiwania się narzędziami informatycznymi,
- systemów operacyjnych,
- sieci komputerowych,
- baz danych,
- programowania komputerów,
- inżynierii oprogramowania,
- podstaw sztucznej inteligencji,
- grafiki komputerowej i komunikacji człowiek-komputer,
- wykorzystywania techniki komputerowej oraz metod matematycznych i statystycznych
- w przedsiębiorstwach i instytucjach różnej wielkości,
- wykorzystywania techniki komputerowej i metod informatycznych do wspomagania nowych i eksploatacji istniejących technologii,
- samodzielnego dokształcania się w oparciu o zdobytą wiedzę umiejętność samodzielnego poszerzania wiadomości w pracy zawodowej,
- samodzielnego rozwiązywania problemów.

**Zbudowane laboratorium umożliwi przede wszystkim realizację następujących treści specjalizacyjnych:**

- praktyczne wykorzystanie wiedzy z zakresu zabezpieczeń i ochrony sieci teleinformatycznych,
- praktyczne wykorzystanie wiedzy o mechanizmach oceny sieci i jakości zabezpieczeń,
- prowadzenie symulowanych ataków na infrastrukturę teleinformatyczną,
- stosowanie systemów kryptograficznych w ochronie systemów informatycznych i informacji w tych systemach,
- stosowanie w praktyce systemów technologii bezpieczeństwa komputerowego,
- projektowanie systemów technologii bezpieczeństwa komputerowego,
- identyfikacja, modelowanie i projektowanie systemów poprawy bezpieczeństwa aplikacji w środowisku sieciowym,
- projektowanie aplikacji i systemów bezpieczeństwa komputerowego,

- konfiguracja systemów wykrywania włamań,
- zarządzanie bezpieczeństwem systemów komputerowych,
- opracowanie koncepcji zabezpieczenia fizycznego infrastruktury teleinformatycznej na podstawie wymagań normatywnych w zakresie ochrony informacji i zabezpieczenia techniczno-organizacyjnego,
- administrowanie systemami komputerowymi zgodnie z polityką bezpieczeństwa informacji,
- planowanie audytów, przygotowania dokumentacji niezbędnej do przeprowadzenia audytu, udziału w zespołach audytowych i poaudytowych, oraz przygotowania raportów.

### **Zaplecze programowe:**

Oprogramowanie, które zabezpiecza zajęcia dydaktyczne jest następujące:

- Windows 7 Pro
- Windows Server 2008 Enterprise
- Linux Debian 2.6.32-5
- Cisco Packet Tracer
- Wireless Toolkit
- MS Office 2007 Pro
- Aplikacje MSDN AA
  - Microsoft .NET
  - MS Visio
  - MS Project
  - MS Access
- Microsoft SQL Server 2012
- Oracle 11g
- Scilab
- Eclipse
- Roboguide
- AutoCad 2007
- Oprogramowanie LabVIEW Professional
- Sphinx
- Python
- Generator aplikacji Magic