**Nazwa przedmiotu:**

Bezpieczeństwo systemów informatycznych

**Koordynator przedmiotu:**

dr inż. Bolesław Szomański

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Zarządzanie i Inżynieria Produkcji

**Grupa przedmiotów:**

Technologie informatyczne

**Kod przedmiotu:**

BESIN

**Semestr nominalny:**

2 / rok ak. 2010/2011

**Liczba punktów ECTS:**

2

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład: | 30h |
| Ćwiczenia: | 0h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Bezpieczeństwo informacji, zagrożenia, podatności, analiza ryzka, common criteria, ochrona Informacji Niejawnej, ochrona danych osobowych, ISO 27001

**Limit liczby studentów:**

**Cel przedmiotu:**

Przedmiot składa się z wykładu opartego na prezentacji multimedialnej oraz prezentacji niektórych rozwiązań z zakresu bezpieczeństwa. W ramach wykładów wykonywane są ćwiczenia projektowe mające na celu pokazanie praktycznych możliwości zastosowania przekazywanych informacji dotyczących bezpieczeństwa informacji.
Dodatkowym elementem nauczania jest śledzenie w internecie nowych zagrożeń, podatności oraz incydentów z zakresu bezpieczeństwa informacji.

**Treści kształcenia:**

2h - Wprowadzenie, historia rozwoju zabezpieczeń systemów informatycznych.
Początki zastosowań informatyki – problemy sprzętowe, komputery mainframe i sieci terminale – problemy z oprogramowaniem, sieci komputerowe – hasła i szyfrowanie mikrokomputery – oprogramowanie antywirusowe, „Orange Book” ocena systemów informatycznych, zabezpieczenia sieciowe, zarządzanie bezpieczeństwem informacji
2h - Zagrożenia bezpieczeństwa systemów informatycznych i informacyjnych
Zagrożenia naturalne, Zagrożenia ludzkie – przypadkowe Zagrożenia ludzkie celowe. Przykładowe zagrożenia wg ISO/IEC 27005
2h - Definicje pojęć za zakresu bezpieczeństwa informacji
Definicje podstawowych pojęć wg ISO/IEC 27000:2009, Definicje pojęć technicznych z zakresu bezpieczeństwa Przypomnienie podstawowych pojęć z zakresu sieci niezbędnych do zrozumienia bezpieczeństwa w szczególności cech protokołów sieciowych
2h - Analiza ryzyka i zarządzanie ryzykiem wg ISO/IEC 27005
podstawy zarządzania ryzykiem, proces zarządzania ryzykiem określenie zakresu, szacowanie ryzyka, postępowanie z ryzykiem, akceptowanie ryzyka, informowanie o ryzyku, monitorowanie o przegląd ryzyka
2h - Określenie bezpieczeństwa systemów informatycznych wg ISO 15048
historia oceny bezpieczeństwa, kryteria oceny bezpieczeństwa systemów bezpieczeństwa poziomy oceny zabezpieczeń
2h - Inne standardy bezpieczeństwa SSE-CMM, normy FIPS i NIST
poziomy bezpieczeństwa wg Common Criteria, omówienie różnych dostępnych powszechnie standardów, zagrożenie w systemach automatyki przemysłowej
2h – Zastosowanie Kryptografia i kryptoanalizy. i metod Identyfikacja osób
Historia kryptografii, szyfrowanie synchroniczne i asynchroniczne sposoby oceny mocy algorytmów, złamane algorytmy
2h - Podpis cyfrowy. Architektura PKI –
wprowadzenie do zagadnień , Ustawa o podpisie elektronicznych, wykorzystanie praktyczne, podpisy kwalifikowane
2h -. Oprogramowanie zabezpieczające
Firewalle, IDS i inne zastosowanie w praktyce i sposoby doboru
2h - Ustawa o Ochronie Informacji Niejawnych wydanie 2010
Rodzaje informacji niejawnych, postępowanie z informacjami niejawnymi, certyfikaty bezpieczeństwa, kancelaria tajna, bezpieczeństwo teleinformatyczne
2h - Ustawa o Ochronie danych osobowych.
Prawa osób, obowiązki administratora danych, administrator bezpieczeństwa informacji, rozporządzenie o ochronie danych osobowych
Inne tajemnice chronione – znaczenie, przypadki występowania
2h -. Zarządzanie bezpieczeństwem informacji wg ISO/IEC 27001:2005
Wprowadzenie system zarządzania bezpieczeństwem informacji, odpowiedzialność kierownictwa, audyty, przeglądy dokonywane przez kierownictwo doskonalenia, załącznik A obligatoryjny
4h - Projektowanie bezpieczeństwa informacji wg ISO/IEC 17799:2005.
Polityka bezpieczeństwa informacji, organizacja bezpieczeństwa, klasyfikacja aktywów, bezpieczeństwo osobowe i fizyczne, aspekty teleinformatyczne, zarządzanie incydentami i ciągłością działania, zgodność
2h - Audyt bezpieczeństwa informacji wg COBIT
podstawa audytu, ryzyko jako podstawa audytu, przebieg audytu, raport z audytu postępowanie poaudytowe
2h – Zaliczenie przedmiotu, podsumowanie projektów, wyjaśnienie problemów i pokazanie poprawnych rozwiązań przeprowadzenie testu komputerowego, ogłoszenie wyników testu i końcowych

**Metody oceny:**

Wykład – zaliczenie z materiału podanego na wykładzie - test oraz wykonanie krótkich ćwiczeń na wykładzie; dodatkowo punktowane prace własne z tematyki bezpieczeństwa informacji jak również przykłady zagrożeń i incydentów znalezione w Internecie lub praktyce

**Egzamin:**

**Literatura:**

PN ISO/IEC 27001:2007
PN ISO/IEC 17799:2007
ISO/IEC 15408:2008 (www.commoncriteriaportal.org)
COBIT
Ustawa o Ochronie Danych Osobowych
Ustawa o Ochronie Informacji Niejawnej
www.cert.org i inne strony www dotyczące bezpieczeństwa informacji

**Witryna www przedmiotu:**

**Uwagi:**

## Efekty przedmiotowe