INSTYTUT INFORMATYKI

PWSZ w Nysie

Kierunek: INFORMATYKA

Specjalność:

BEZPIECZEŃSTWO SIECI I SYSTEMÓW INFORMATYCZNYCH

PROGRAM NAUCZANIA 2010/2011

UKŁAD SEMESTRALNY

Rok IV, semestr 7 (zimowy)

Przedmioty specjalizacyjne i specjalnościowe

Opis przedmiotu

1. Nazwa przedmiotu: Bezpieczeństwo systemów wirtualnych

2. **Kod przedmiotu: 11.3 BSS.BSW.07**

3. **Język wykładowy**: polski

4. **Kierunek**: Informatyka

5. **Specjalność**: Bezpieczeństwo sieci i systemów informatycznych

6. **Rok**: IV Semestr: 7

7. **Tytuł/stopień oraz imię i nazwisko prowadzącego przedmiot**:

Dr inż. Mariusz Gola

8. **Tytuły/stopnie oraz imiona i nazwiska pozostałych członków zespołu**:

……..

9. **Formy zajęć wchodzące w skład przedmiotu, wymiar godzinowy, forma zaliczenia**:

Forma zajęć	Wykład	Ćwiczenia/ Ćwiczenia tablicowe	Laboratorium/ Ćwiczenia praktyczne	Projekt	Seminarium
Liczba godzin w semestrze	15		15		
Forma zaliczenia	Kolokwium		Zaliczenie		

10. **Liczba punktów ECTS**: 2

11. **Poziom** : zaawansowany

12. **Wymagania wstępne**:

Znajomość materiału realizowanego w ramach kursów: *Podstawy systemów komputerowych*, *Systemy operacyjne*, *Sieci komputerowe*.

13. **Efekty kształcenia:**

Wiedza:
- Posiada podstawową wiedzę na temat zagrożeń systemów komputerowych.
- Posiada podstawową wiedzę na temat bezpieczeństwa środowisk wirtualnych.
- Posiada wiedzę na temat bezpieczeństwa przetwarzania danych w chmurze.

Umiejętności:
- Potrafi zaimplementować bezpieczny system komputerowy.
- Potrafi zaprojektować i zaimplementować bezpieczną platformę wirtualizacji.
- Potrafi zaimplementować skuteczne techniki zabezpieczeń systemów wirtualnych.
- Potrafi przygotować politykę bezpieczeństwa dla środowiska wirtualnego.

Kompetencje:
- Rozumie potrzebę ciągłego dokształcania się z zakresu bezpieczeństwa systemów wirtualnych.
- Rozumie potrzebę współdziałania przy realizacji projektów technicznych.

14. **Opis treści kształcenia w ramach poszczególnych form zajęć**:

14.1. **Wykład**:

Zagadnienia poruszane na wykładzie będą koncentrować się wokół następujących tematów:
- Bezpieczeństwo hiperviso'ra (ang. Hypervisor security)
- Bezpieczeństwo platformy gospodarza (ang Host/Platform Security)
- Bezpieczeństwo komunikacji (ang. Securing Communicatios)
- Bezpieczeństwo między systemami wirtualnymi (Security between guests systems)
- Bezpieczeństwo między systemem host / gości (ang. Security between host/guests)

Dodatkowo zostaną omówione zagadnienia związane z ogólno rozumianym bezpieczeństwem w aspekcie wykorzystania systemów wirtualnych takie jak:
- Klasyfikacja wymagań dotyczących systemu komputerowego, z punktu widzenia jakości usług świadczonych przez działające w nim oprogramowanie aplikacyjne.
- Ogólne omówienie zagrożeń systemów informatycznych z uwzględnieniem naruszeń bezpieczeństwa, zdarzeń losowych a także czynnika ludzkiego.
- Zagrożenia związane z infrastrukturą sieciową: Bezpieczeństwo DHCP, DNS, dostępu zdalnego.
- Zagrożenia związane z utratą danych i przerwaniem działania systemu. Zapewnienie nieprzerwanego działania przez implementację bezpiecznej strategii odzyskiwania sprawności po awarii, minimalizacji zagrożeń w komunikacji oraz tworzenia bezpiecznych kopii bezpieczeństwa i ich odtwarzania

14.2.Ćwiczenia/Ćwiczenia tablicowe:

14.3. Laboratorium/ Ćwiczenia praktyczne:

W ramach laboratorium studenci powinni w sposób praktyczny utrwalać i weryfikować swoją widzę nabyta podczas wykładów. Studenci będą wykonywać ćwiczenia związane z zapewnieniem bezpieczeństwa systemów wirtualnych, ich archiwizacji i nadzorowania bezpiecznej pracy.

15. **Literatura podstawowa**:

1. Archiwizacja i odzyskiwanie danych, W. Curtis Preston, Helion 2008
2. Bezpieczeństwo protokołu TCP/IP, Libor Dostalek , PWN 2006
3. 125 sposobów na bezpieczeństwo sieci. Wydanie II, Autor: Andrew Lockhart, Helion 2007
4. The Best Damn Server Virtualization Book Period, Rogier Dittner, David Rule, Syngres 2007
5. VMware ESX Server in the Enterprise: Planning and Securing Virtualization Servers, Edward L. Haletky, Prentice Hall 2007

16. **Literatura towarzysząca**:

Dokumentacja oprogramowania:
- www.citrix.com/xenserver
- www.microsoft.com
- www.vmware.com
- www.openvz.org
- www.openqrm.org
- www.centos.org

Opis przedmiotu

1. Nazwa przedmiotu: Zarządzanie bezpieczeństwem informacji

2. **Kod przedmiotu: 11.3 BSS.ZBI.07**

3. **Język wykładowy**: polski

4. **Kierunek**: Informatyka

5. **Specjalność: Bezpieczeństwo sieci i systemów informatycznych**

6. **Rok**: IV Semestr: 7

7. **Tytuł/stopień oraz imię i nazwisko prowadzącego przedmiot**:

Dr inż. Mariusz Gola

8. **Tytuły/stopnie oraz imiona i nazwiska pozostałych członków zespołu**:

……..

9. **Formy zajęć wchodzące w skład przedmiotu, wymiar godzinowy, forma zaliczenia**:

Forma zajęć	Wykład	Ćwiczenia/ Ćwiczenia tablicowe	Laboratorium/ Ćwiczenia praktyczne	Projekt	Seminarium
Liczba godzin w semestrze	30		15		
Forma zaliczenia	Kolokwium		Zaliczenie		

10. **Liczba punktów ECTS**: 2

11. **Poziom** : zaawansowany

12. **Wymagania wstępne**:

Ogólna znajomość systemów operacyjnych i sieci komputerowych i zagadnień związanych z ochrona informacji w systemach i sieciach komputerowych.

13. **Efekty kształcenia:**

Wiedza:
- Posiada podstawową wiedzę na temat zagrożeń systemów i sieci komputerowych.
- Posiada wiedzę na temat podstawowych zabezpieczeń systemów i sieci komputerowych.
- Posiada wiedzę na temat zarządzania bezpieczeństwem informacji w przedsiębiorstwie.

Umiejętności:
- Potrafi zaimplementować bezpieczny system komputerowy.
- Potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie; posługuje się narzędziami kompresji i szyfrowania danych.
- Potrafi wykonać prostą analizę sposobu funkcjonowania systemu informatycznego i ocenić istniejące rozwiązania informatyczne w zakresie bezpieczeństwa.
- Potrafi przeanalizować i wdrożyć procedury związane z zarządzaniem bezpieczeństwem informacji w skali przedsiębiorstwa.

Kompetencje:
- Rozumie potrzebę ciągłego dokształcania się z zakresu zarządzania bezpieczeństwem informacji.
- Rozumie potrzebę współdziałania przy realizacji projektów technicznych.

14. **Opis treści kształcenia w ramach poszczególnych form zajęć**:

14.1. **Wykład**:

W ramach wykładu poruszane będą treści związane z następującymi zagadnieniami:
- Informacja w działalności organizacji - zagrożenia dla ciągłości działalności.
- Klasyfikacja zagrożeń i ich źródło.
- Normy zarządzania bezpieczeństwem informacji.
- Podstawowe pojęcia i definicje zawarte w normie ISO/IEC 27001:2005.
- System zarządzania bezpieczeństwem informacji, model zarządzania i wymagania
- Polityka bezpieczeństwa, organizacja i zarządzanie bezpieczeństwem informacji, zarządzanie aktywami bezpieczeństwo osobowe, fizyczne i środowiskowe, bezpieczeństwo aplikacji i systemów, zarządzanie systemami i sieciami, kontrola dostępu do systemów, rozwój i utrzymanie systemów, zarządzanie incydentami i ciągłością działania, zgodność z regulacjami prawnymi, niezależne przeglądy i kontrola wewnętrzna.
- Analiza ryzyka i definiowanie potrzeb dla systemów przetwarzających informacje.
- Nadzór i odpowiedzialność.
- Dokumentacja systemu zarządzania bezpieczeństwem informacji.
- Przeprowadzanie audytu teleinformatycznego. Cele i powody przeprowadzania audytów, skład zespołu audytowego, poszczególne etapy audytu, najlepsze praktyki audytowi, przedstawienie norm, metodologia audytu, obszary prac audytowych , prace wykonywane na poszczególnych etapach audytu

14.4.Ćwiczenia teoretyczne:

14.5.Laboratorium/ Ćwiczenia praktyczne

W ramach laboratorium studenci powinni w sposób praktyczny utrwalać i weryfikować swoją widzę nabyta podczas wykładów. Ćwiczenia laboratoryjne będą prowadzone w następujących formach.,

Analiza przypadku: Na podstawie opracowań przygotowanych przez prowadzącego studenci będą analizować bezpieczeństwo wybranej firmy, zgodność zastosowanych rozwiązań z istniejącymi normami. Będą proponować własne rozwiązania. Studenci będą także przygotowywać dokumentacje niezbędną do przeprowadzania audytu teleinformatycznego.

***Projekt*:** Na podstawie wytycznych podanych przez prowadzącego (potrzeby klienta) studenci będą opracowywać politykę bezpieczeństwa dla firmy. Rozwiązania te będą dyskutowane podczas zajęć z prowadzącym i pozostałymi studentami.

Ćwiczeni praktyczne: Studenci będą wykonywać ćwiczenia praktyczne związane wykorzystaniem testów penetracyjnych, analizą ruchu sieciowego, badaniem bezpieczeństwa systemów.

15. **Literatura podstawowa**:

1. Polityka bezpieczeństwa i ochrony informacji, Tadeusz Kifner, Helion 1999
2. Przewodnik audytora systemów informatycznych, Marian Molski, Małgorzata Łacheta Helion 2006
3. Audyt bezpieczeństwa informacji w praktyce, Tomasz Polaczek Helion 2006

16. **Literatura towarzysząca**:

1. Hacking. Sztuka penetracji. Wydanie II, Jon Erickson Helion 2008
2. 125 sposobów na bezpieczeństwo sieci. Wydanie II, Autor: Andrew Lockhart, Helion 2007
3. PKI. Podstawy i zasady działania, Carlisle Adams, PWN 2007

Opis przedmiotu

1. Nazwa przedmiotu: Seminarium dyplomowe II

2. **Kod przedmiotu: 11.3 INF.SEM.07**

3. **Język wykładowy**: polski

4. **Kierunek**: Informatyka

5. **Specjalność**: -

6. **Rok**: IV Semestr: 7

7. **Tytuł/stopień oraz imię i nazwisko prowadzącego przedmiot**:

prof. Leszek Borzemski, prof. Ngoc Thanh Nguyen, prof. Włodzimierz Stanisławski

8. **Tytuły/stopnie oraz imiona i nazwiska pozostałych członków zespołu**:

9. **Formy zajęć wchodzące w skład przedmiotu, wymiar godzinowy, forma zaliczenia**:

Forma zajęć	Wykład	Ćwiczenia/ Ćwiczenia tablicowe	Laboratorium/ Ćwiczenia praktyczne	Projekt	Seminarium
Liczba godzin w semestrze					30
Forma zaliczenia					Ocena wystąpienia od strony merytorycznej oraz technicznej. Ocena udziału w dyskusjach.

10. **Liczba punktów ECTS**: 10

11. **Poziom** : podstawowy

12. **Wymagania wstępne**:

brak

13. **Efekty kształcenia:**

Wiedza: - Posiada rozszerzoną i głęboką wiedzę z zakresu prezentacji wyników prac rozwojowych i technicznych. - Posiada ogólna wiedzę na temat praw autorskich. Umiejętności: - Potrafi używać narzędzi służących do prezentacji. - Potrafi używać narzędzi służących do edytowania tekstów naukowych i technicznych. - Potrafi zwięźle i jasno przedstawić wyniki swoich prac.

Kompetencje:
- Potrafi umiejscowić wyniki swoich prac rozwojowych i technicznych w potencjalnych zastosowaniach praktycznych.

14. **Opis treści kształcenia w ramach poszczególnych form zajęć**:

14.1. **Wykład**:

14.2. **Ćwiczenia/Ćwiczenia tablicowe**:

14.3. **Laboratorium/ Ćwiczenia praktyczne**:

14.4. **Projekt**:

14.5. **Seminarium**:

Prezentowane są wymagania i wzorce prac inżynierskich oraz zasady merytoryczne oraz organizacyjne związane z pisaniem prac inżynierskich obowiązujące studentów Instytutu Informatyki w PWSZ w Nysie. Studenci przygotowują samodzielne prezentacje poszczególnych etapów realizacji pracy, począwszy od definiowania tematu, określania zakresu pracy, a skończywszy na wybranych rezultatach. Seminarium służy samodzielnemu przedstawieniu przez studenta wybranych problemów, metod i algorytmów projektowania systemów informatycznych będących przedmiotem ich prac inżynierskich.

15. **Literatura podstawowa**:

Literatura zgodna z bieżącymi potrzebami pracy inżynierskiej

16. **Literatura towarzysząca**: