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. **Cele kształcenia**:

Zapoznanie z powszechnie dostępnymi, otwartymi rozwiązaniami mającymi charakter specjalizowanych systemów operacyjnych i oprogramowania uzupełniającego, realizującego dodatkowe właściwości tych systemów oraz ich kluczowymi obszarami zastosowań, ze szczególnym uwzględnieniem zagadnień bezpieczeństwa przepływu danych, aplikacji i systemów.

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