WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ I ZARZĄDZANIA WIT
POD AUSPICJAMI POLSKIEJ AKADEMII NAUK
01-447 Warszawa \ ul. Newelska 6 \ www.WIT.edu.pl

WYDZIAŁ INFORMATYKI

Kierunek studiów	Informatyka
Stopień studiów	1-go stopnia
Forma studiów	niestacjonarne

Sylabus przedmiotu

Bezpieczeństwo systemów komputerowych

1. Dane podstawowe

Kod przedmiotu	IZ-BSK-ZR
Rok studiów	4
Semestr	7

2. Wymiar godzin i forma zajęć

Rodzaj	Liczba godzin
Wykład	16
Laboratorium	8
Razem godzin	24

3. Cele przedmiotu

Kod	Cel
CP1	Zapoznanie się z podstawami bezpieczeństwa systemów komputerowych, obowiązującymi w tym zakresie przepisami i normami ISO oraz problematyką tworzenia Polityk, Zasad i Procedur Bezpieczeństwa systemów komputerowych.
CP2	Zapoznanie się z najczęściej spotykanymi zagrożeniami, błędami prowadzącymi do powstania luk w bezpieczeństwie systemów oraz technikami ich unikania.
CP3	Nabycie umiejętności korzystania z: narzędzi do analizy zabezpieczeń, narzędzi do monitoringu, systemami wykrywania ataków i sposobami ochrony przed atakami - uzupełnieniem jest omówienie zagadnień z zakresu informatyki śledczej.
CP4	Zapoznanie z modelami bezpieczeństwa i klasami bezpieczeństwa systemów. Uzyskanie wiedzy o podstawowych modelach uwierzytelniania, strategiach kontroli dostępu w tym także w kontekście bezpieczeństwa protokołów komunikacyjnych i usług aplikacyjnych.
CP5	Studium przypadku - poznanie praktycznych metod wyboru i zastosowania odpowiednich zabezpieczeń na podstawie prawdziwego wydarzenia - studenci zapoznają się z przyczynami wystąpienia incydentów, sposobami ich wykrywania i analizą.

4. Treści programowe

Kod	Tematyka	wykład	laboratorium
TP1	Podstawowe zagadnienia i definicje z zakresu bezpieczeństwa systemów komputerowych. Znaczenie bezpieczeństwa systemów komputerowych. Zagrożenia mające wpływ na bezpieczeństwo systemów komputerowych. Odpowiedzialność karna wynikająca z naruszenia przepisów z zakresu bezpieczeństwa systemów komputerowych. Ogólne problemy konstrukcji zabezpieczeń. Określenie zasobów wymagających ochrony. Identyfikacja zagrożeń. Analiza pochodzenia zagrożenia.	2	0
TP2	Polityka Bezpieczeństwa. Przygotowanie do opracowania polityki bezpieczeństwa systemu. Analiza ryzyka czyli analiza zasobów, oraz zagrożeń i podatności zasobów. Sformułowanie polityki i opracowanie na tej podstawie dokumentu „Polityki bezpieczeństwa systemu". Podstawowe zasady polityki bezpieczeństwa. Ogólne zasady polityki bezpieczeństwa. Środki realizacji polityki bezpieczeństwa. Podstawowe modele bezpieczeństwa. Sposoby realizacji polityki bezpieczeństwa. Normy techniczne i przepisy prawa regulujące bezpieczeństwo systemów informatycznych.	2	0

Kod	Tematyka	wykład	laboratorium
TP3	Projektowanie bezpiecznych metod ochrony systemów komputerowych. Optymalny plan wdrożenia zabezpieczeń. Wybór odpowiednich zabezpieczeń. Wdrożenie bezpiecznych metod ochrony systemów komputerowych. Zasady wdrożenia przyjętych zabezpieczeń. Szkolenia związane z bezpieczeństwem. Poprawa świadomości pracowników. Proces utrzymania zabezpieczeń. Audyty bezpieczeństwa systemu. Automatyczne monitorowanie zabezpieczeń systemu. Zasady postępowania w przypadku wystąpienia incydentu bezpieczeństwa. Zasady zarządzania zmianami.	2	0
TP4	Zarządzanie bezpieczeństwem systemów. Zasady zarządzania bezpieczeństwem systemów. Zarządzanie bezpieczeństwem systemów w kontekście ograniczeń występujących przy jego realizacji. Zarządzanie bezpieczeństwem systemów – koszty czy zyski? Poziom osiągniętego bezpieczeństwa w odniesieniu do struktury wydatków na bezpieczeństwo systemów. Czy wydatki na bezpieczeństwo systemów się zwracają? Analiza stanu bezpieczeństwa systemów w świetle raportów firm: PricewaterhouseCoopers oraz Ernst&Young.	2	0
TP5	Atak na bezpieczeństwo systemu komputerowego. Podstawowe pojęcia i definicje. Klasy ataków. Formy ataku elektronicznego. Fazy ataku elektronicznego. Sposoby zmniejszenia podatności na atak. Problemy związane z zabezpieczeniem przed atakiem. Podstawowe reguły ochrony przed atakiem. Proces przydziału praw dostępu. Kontrola dostępu do danych. Klasy bezpieczeństwa systemów komputerowych.	2	0
TP6	Analiza prawdziwego przypadku w kontekście incydentu naruszenia Bezpieczeństwa Systemów Komputerowych.	2	0
TP7	Wybrane zagadnienia informatyki śledczej. Definicja informatyki śledczej. Cel dla którego powstała informatyka śledcza. Rola informatyki śledczej. Zadania informatyki śledczej. Narzędzia stosowane w informatyce śledczej. Dane ulotne. Dowody cyfrowe.	2	0
TP8	Audyt Bezpieczeństwa Czynnika Ludzkiego. Czynniki zwiększające ryzyko. Schemat działania ataku socjotechnicznego. Ochrona przed atakami socjotechnicznymi. Socjotechnika w przykładach.	2	0
TP9	Uwierzytelnianie się w ssh przy pomocy klucza prywatnego. Konfiguracja ssh. Rejestracja zdarzeń systemowych. Szyfrowanie informacji. Podpis elektroniczny.	0	4
TP10	Automatyczne narzędzia badań tech. bezpieczeństwa. Kali Linux. Podstawy ochrony przed malware i oszustwami. Prywatność. Tor i Truecrypt.	0	4

Razem godzin: 24