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
Profil	Praktyczny
Stopień studiów	1-go stopnia
Forma studiów	niestacjonarne

Sylabus przedmiotu

Bezpieczeństwo systemów komputerowych

1. Dane podstawowe

Status programowy przedmiotu	Blok A: Bezpieczeństwo informacji
Rodzaj przedmiotu	Obligatoryjny
Kod przedmiotu	IZ-BSK-ZR
Rok studiów	4
Semestr	7
Osoba odpowiedzialna za przedmiot	mgr Tomasz Rutkowski
Język wykładowy	polski

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. Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

Wiedza informatyczna na temat systemów komputerowych. Podstawowa wiedza z zakresu kryptografii.

5. Efekty uczenia się

Wiedza

Kod	Student zna i rozumie:	Realizuje cel	Efekty kierunkowe
EU-W1	podstawowe metody rozwiązywania problemów bezpieczeństwa stosowane w systemach komputerowych i potrafi je stosować	CP2, CP3, CP5	IK6_W14, IK6_W17, IK6_W21
EU-W2	podstawowe zasady bezpieczeństwa przy używaniu i projektowaniu systemów informatycznych	CP1, CP2	IK6_W14, IK6_W17, IK6_W21

Kod	Student zna i rozumie:	Realizuje cel	Efekty kierunkowe
EU-W3	z konieczności zapewnienia zgodności poziomu bezpieczeństwa systemów komputerowych z wymogami prawnymi.	CP1, CP4	IK6_W14, IK6_W17, IK6_W21
EU-W4	wiedzę o narzędziach stosowanych do analizy bezpieczeństwa systemu komputerowego.	CP2, CP3, CP5	IK6_W14, IK6_W17, IK6_W21
EU-W5	rolę bezpieczeństwa danych i systemów informatycznych dla funkcjonowania współczesnego społeczeństwa.	CP1, CP2, CP4, CP5	IK6_W14, IK6_W17, IK6_W21

Umiejętności

Kod	Student potrafi:	Realizuje cel	Efekty kierunkowe
EU-U1	identyfikować zagrożenia dotyczącą bezpieczeństwa systemów komputerowych	CP2, CP3, CP4	IK6_U03, IK6_U21, IK6_U27
EU-U2	dobrać metody i narzędzia ochrony systemów komputerowych	CP1, CP3, CP5	IK6_U03, IK6_U21, IK6_U27

Kompetencje

Kod	Student jest gotów do:	Realizuje cel	Efekty kierunkowe
EU-K1	profesjonalnych działań w zakresie bezpieczeństwa informatycznego wymagają stałego pogłębiania wiedzy i umiejętności	CP1, CP2, CP3	IK6_K01, IK6_K06
EU-K2	zrozumienia konsekwencji i skutków zaniechań i podejmowanych działań z zakresu bezpieczeństwa. Jest bardziej odpowiedzialny.	CP3, CP4	IK6_K01, IK6_K06
EU-K3	chronienia swojej prywatność. Potrafi korzystać z narzędzi Tor i Truecrypt.	CP2, CP4, CP5	IK6_K01, IK6_K06

6. Treści programowe

Kod	Tematyka	wykład	laboratorium	Realizuje efekt
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	EU-K2, EU-U1, EU-W3, EU-W5
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	EU-K1, EU-U2, EU-W2, EU-W5

Kod	Tematyka	wykład	laboratorium	Realizuje efekt
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	EU-K1, EU-K2, EU-U1, EU-U2, EU-W1, EU-W2, EU-W3, EU-W4
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	EU-U2, EU-W2, EU-W3, EU-W4, EU-W5
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	EU-K2, EU-U1, EU-U2, EU-W1, EU-W2, EU-W4
TP6	Analiza prawdziwego przypadku w kontekście incydentu naruszenia Bezpieczeństwa Systemów Komputerowych.	2	0	EU-K2, EU-K3, EU-U2, EU-W2, EU-W4, EU-W5
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	EU-K2, EU-K3, EU-U1, EU-U2, EU-W1, EU-W4
TP8	Audyt Bezpieczeństwa Czynnika Ludzkiego. Czynniki zwiększające ryzyko. Schemat działania ataku socjotechnicznego. Ochrona przed atakami socjotechnicznymi. Socjotechnika w przykładach.	2	0	EU-K1, EU-K2, EU-K3, EU-U1, EU-W5
TP9	Uwierzytelnianie się w ssh przy pomocy klucza prywatnego. Konfiguracja ssh. Rejestracja zdarzeń systemowych. Szyfrowanie informacji. Podpis elektroniczny.	0	4	EU-K2, EU-K3, EU-U2
TP10	Automatyczne narzędzia badań tech. bezpieczeństwa. Kali Linux. Podstawy ochrony przed malware i oszustwami. Prywatność. Tor i Truecrypt.	0	4	EU-U1, EU-U2, EU-W1, EU-W4

Razem godzin: 24

7. Metody kształcenia

Kod	Metoda
MK1	dyskusja
MK2	kazusy
MK3	materiały dydaktyczne
MK4	rozwiązywanie zadań domowych
MK5	wykład wsparty prezentacją komputerową
MK6	wykład

8. Nakład pracy studenta

Aktywność studenta	Obciążenie
studiowanie materiałów dostępnych w literaturzu lub internecie	18
studiowanie materiałów dydaktycznych	18
przygotowanie do egzaminu	15
Praca z nauczycielem związana z: laboratorium	8
Praca z nauczycielem związana z: wykład	16
Liczba punktów ECTS (1 punkt=25h)	3
Procentowy udział pracy własnej studenta w sumarycznym obciążeniu studenta	68,00%
Sumaryczne obciążenie pracą studenta	75

9. Status zaliczenia przedmiotu

Egzamin ma formę pisemnego testu wielokrotnego wyboru. Zawiera także pytania otwarte. Przygotowane są zawsze minimum dwie grupy (A i B). Sam test egzaminacyjny zalicza min 51,0% punktów. Test egzaminacyjny stanowi 80% składnika oceny końcowej. Wynik punktowy z ćwiczeń stanowi 20% składnika oceny końcowej. Suma punktów procentowych jest przeliczana na oceny zgodnie z zakładką „kryteria".

Forma studiów	Egzamin	Praca egzaminacyjna	Zaliczenie	Praca zaliczeniowa
niestacjonarne	×			

10. Metody weryfikacji efektów uczenia się

Składowe oceny końcowej

Forma sprawdzenia	Wybrana forma	Punktacja	Realizuje efekt
Egzamin pisemny	×	80	EU-K1, EU-K2, EU-K3, EU-U1, EU-U2, EU-W1, EU-W2, EU-W3, EU-W4, EU-W5
Egzamin ustny			
Sprawdzian pisemny			
Zaliczeniowy przegląd prac			
Referat pisemny			
Referat ustny			
Kolokwium			
Praca domowa			
Miniprojekt			
Praca na zajęciach			
Projekt z dokumentacją			
Ustna prezentacja projektu			
Obecność na zajęciach	×	20	EU-K1, EU-K2, EU-K3, EU-U1, EU-U2, EU-W1, EU-W2, EU-W3, EU-W4, EU-W5
Sprawdzian ustny			
Kartkówka			
Aktywność na zajęciach			
Egzaminacyjny przegląd prac			
Sprawozdanie z praktyki zawodowej			
Prezentacja indywidualna			
Prezentacja zespołowa			

Zasady wyliczania oceny z przedmiotu

Zakres punktów	Ocena
0 – 50	2,0
51 – 60	3,0
61 – 70	3,5
71 – 80	4,0
81 – 90	4,5
91 – 100	5,0

11. Macierz realizacji przedmiotu

Efekt uczenia się	Cel przedmiotu	Treści programowe	Metody kształcenia
EU-W1	CP2, CP3, CP5	TP3, TP5, TP7, TP10	MK1, MK2, MK3, MK4, MK5, MK6
EU-W2	CP1, CP2	TP2, TP3, TP4, TP5, TP6	MK1, MK2, MK3, MK4, MK5, MK6
EU-W3	CP1, CP4	TP1, TP3, TP4	MK1, MK2, MK3, MK4, MK5, MK6
EU-W4	CP2, CP3, CP5	TP3, TP4, TP5, TP6, TP7, TP10	MK1, MK2, MK3, MK4, MK5, MK6
EU-W5	CP1, CP2, CP4, CP5	TP1, TP2, TP4, TP6, TP8	MK1, MK2, MK3, MK4, MK5, MK6
EU-U1	CP2, CP3, CP4	TP1, TP3, TP5, TP7, TP8, TP10	MK1, MK2, MK3, MK4, MK5, MK6
EU-U2	CP1, CP3, CP5	TP2, TP3, TP4, TP5, TP6, TP7, TP9, TP10	MK1, MK2, MK3, MK4, MK5, MK6
EU-K1	CP1, CP2, CP3	TP2, TP3, TP8	MK1, MK2, MK3, MK4, MK5, MK6
EU-K2	CP3, CP4	TP1, TP3, TP5, TP6, TP7, TP8, TP9	MK1, MK2, MK3, MK4, MK5, MK6
EU-K3	CP2, CP4, CP5	TP6, TP7, TP8, TP9	MK1, MK2, MK3, MK4, MK5, MK6

12. Odniesienie efektów uczenia się

Efekt uczenia się	Efekty kształcenia dla kierunku studiów	Charakterystyki drugiego stopnia w obszarze kształcenia
EU-W1	IK6_W21, IK6_W17, IK6_W14	P6S_WG, P6S_WK
EU-W2	IK6_W21, IK6_W17, IK6_W14	P6S_WG, P6S_WK
EU-W3	IK6_W21, IK6_W17, IK6_W14	P6S_WG, P6S_WK
EU-W4	IK6_W21, IK6_W17, IK6_W14	P6S_WG, P6S_WK
EU-W5	IK6_W21, IK6_W17, IK6_W14	P6S_WG, P6S_WK
EU-U1	IK6_U27, IK6_U21, IK6_U03	P6S_UU, P6S_UW
EU-U2	IK6_U27, IK6_U21, IK6_U03	P6S_UU, P6S_UW
EU-K1	IK6_K06, IK6_K01	P6S_KK, P6S_KR
EU-K2	IK6_K06, IK6_K01	P6S_KK, P6S_KR
EU-K3	IK6_K06, IK6_K01	P6S_KK, P6S_KR

13. Literatura

Literatura podstawowa

1. Cory Altheide, Harlan Carvey, Informatyka śledcza. Przewodnik po narzędziach open source., Helion
2. Kevin D. Mitnick, William L. Simon, Sztuka podstępu. Łamałem ludzi, nie hasła.
3. Radosław Sokół, Jak pozostać anonimowym w sieci, Helion
4. Thomas Wilhelm, Profesjonalne testy penetracyjne. Zbuduj własne środowisko do testów, Helion

Literatura uzupełniająca

1. Marek Serafin, Sieci VPN. Zdalna praca i bezpieczeństwo danych.

Strony WWW

1. Wiedza z zakresu bezpieczeństwa IT podana w sposób prosty, łatwy a często i przyjemny., niebezpiecznik.pl

14. Informacje o nauczycielach akademickich

Osoby odpowiedzialne za przedmiot

1. mgr Tomasz Rutkowski

Osoby prowądzace przedmiot

1. mgr Bartłomiej Solarz-Niesłuchowski
2. mgr Tomasz Rutkowski