

Nazwa zajęć: Bezpieczeństwo sieci komputerowych		IT network security	
Kierunek: Informatyka			Obowiązuje od roku ak. 2019/2020
Poziom: I st. inżynierski	Profil: praktyczny	Grupa zajęć: Specjalnościowe	
Semestr: VII	Forma zaliczenia: Z - zaliczenie na ocenę	Punkty ECTS: 5	Zajęcia do wyboru: Tak
			Język zajęć: polski

Forma zajęć i liczba godzin na studiach stacjonarnych i niestacjonarnych:

Wykład 15 / 8	Cwiczenia 45 / 24	Suma godzin: 60 / 32
-------------------------	-----------------------------	--------------------------------

Specjalność:

Nazwiska osób odpowiedzialnych za zajęcia:

mgr inż. Bogusław Kowalski

Opis zajęć:

Celem przedmiotu jest zapoznanie studentów z podstawami tworzenia Systemów Zarządzania Cyberbezpieczeństwem (SZCB) z punktu widzenia zarządzania ryzykami zagrożenia bezpieczeństwa informacji zawartych i przetwarzanych z wykorzystaniem sieci komputerowych. Student uzyskuje podstawową wiedzę z zakresu: - obowiązujących w obszarze bezpieczeństwa informacji podstawowych regulacji prawnych; - metod i narzędzi stosowanych w SZCB.

Cele dydaktyczne:

Uzyskanie przez studenta umiejętności zastosowania metod i narzędzi SZCB adekwatnych do utrzymania, na akceptowalnym poziomie, ryzyk zagrożenia bezpieczeństwa informacji w sieciach komputerowych.

Uzyskanie przez studenta podstawowej wiedzy z zakresu:- podstawowych regulacji prawnych obowiązujących w obszarze bezpieczeństwa informacji ; - metod i narzędzi stosowanych w współczesnych SZCB.

Uzyskanie umiejętności w zakresie wyszukiwania w literaturze i źródłach elektronicznych informacji na temat metod i rozwiązań stosowanych w współczesnych SZCB i kierunkach rozwoju sieci.

Umiejętność pracy w grupie oraz zapewnienia bezpieczeństwa informacji generowanej, przechowywanej i transmitowanej przez różne grupy użytkowników sieci komputerowych.

Metody dydaktyczne:

MP1	wykład informacyjny
MC1	ćwiczenie praktyczne
MS1	wykład problemowy
ME1	pokaz

Metody oceniania:

MO1	praca pisemna
MO2	egzamin ustny

Wykład

W1	Regulacje prawne, normy oraz dobre praktyki w obszarze bezpieczeństwa sieci
W2	Budowa Systemu Zarządzania Cyberbezpieczeństwem (SZCB) w praktyce
W3	Budowa i rozwój zespołów CERT/CSIRT/SOC - teoria i praktyka
W4	Przegląd typowych ataków hackerskich na zasoby sieci teleinformatyczne
W5	Techniczne aspekty zarządzania cyberbezpieczeństwem - cz1
W6	Techniczne aspekty zarządzania cyberbezpieczeństwem - cz2
W7	Testy penetracyjne zasobów IT
W8	Modelowanie zagrożeń i zarządzanie ryzykiem bezpieczeństwa informacji
W9	Zasady prowadzenia audytów informatycznych w świetle norm ISO 27001, 22301 oraz Ustawy o Krajowym Systemie Cyberbezpieczeństwa

Cwiczenia

C1	Budowa tuneli IPSEC - Cisco Packet Tracer
C2	Szyfrowanie protokołów dynamicznego routingu - Cisco Packet Tracer
C3	Szyfrowanie plików konfiguracyjnych aktywnych urządzeń sieciowych - Cisco Packet Tracer
C4	Zarządzanie incydentami bezpieczeństwa teleinformatycznego - warsztaty
C5	Analiza ryzyka bezpieczeństwa informacji firmy produkcyjnej - warsztaty
C6	Zabezpieczenie dostępu sieci z wykorzystaniem list dostępowych i firewalli sprzętowych - Cisco Packet Tracer

Literatura podstawowa

1	Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion 2014
2	IT Security Cookbook, http://www.boran.com/security/ ;

Literatura uzupełniająca

1	William Stallings, „Ochrona danych w sieci i intersieci; w teorii i praktyce”, WN-T, Warszawa 1997 r.;
2	Dyrektywa Unii Europejskiej NIS (Network Information Security)
3	Norma ISO/IEC 22301
4	Grupy norm ISO/IEC 27001;- ISO/IEC 27000;- ISO/IEC 27002;- ISO/IEC 27003;- ISO/IEC 27004;- ISO/IEC 27005;- ISO/IEC 27006, Polski Komitet Normalizacyjny;
5	Polska Norma:- PN-I-13335-1 Technika Informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych, Polski Komitet Normalizacyjny.
6	Polska Norma PN-I-02000 Technika Informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia, Polski Komitet Normalizacyjny;
7	Ustawa o Krajowym Systemie Cyberbezpieczeństwa
8	Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. nr 11 poz. 95) wraz z późniejszymi zmianami;
9	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. nr. 133. poz. 883);
10	Zbiór ogólnych i szczegółowych zaleceń Urzędu Ochrony Państwa dotyczących bezpieczeństwa teleinformatycznego.
11	Metodologia TISM firmy European Network Security Institute (ENSI); http://www.ensi.net ;

Źródła dodatkowe

1	Bruce Schneier „Kryptografia dla praktyków” – WNT, Warszawa 2002,
2	Ben Laurie, Peter Laurie "Apache. Przewodnik encyklopedyczny" – HELION, Gliwice 2003.

Warunki zaliczenia

Warunkiem zaliczenia przedmiotu jest rozwiązanie zbioru zadań i obrona pracy pisemnej na zadany temat samodzielnie przygotowanej przez studenta oraz pozytywna ocena aktywności studenta w trakcie zajęć.

Przykłady pytań zaliczeniowych

Przeprowadź analizę ryzyka cyberbezpieczeństwa wskazanej firmy produkcyjnej

Porównaj znane Ci metody szyfrowania transmisji danych w sieciach komputerowych.
 Zaprojektuj i utwórz w praktyce tunel IPSEC z wykorzystaniem platformy Cisco Packet Tracer
 Zaszzyfruj skutecznie pliki konfiguracyjne routera z wykorzystaniem platformy Cisco Packet Tracer
 Przeprowadź analizę techniczną incydentu bezpieczeństwa teleinformatycznego - malware fałszywa faktura

Obciążenie pracą studenta

Studia stacjonarne/niestacjonarne

Forma pracy studenta	Wykład		Ćwiczenia		Suma	
Zajęcia z bezpośrednim udziałem nauczyciela	15 g	8 g	45 g	24 g	60 g	32 g
Zapoznanie się z literaturą przedmiotu	8 g	15 g	7 g	10 g	15 g	25 g
Przygotowanie się do zajęć	8 g	15 g	7 g	10 g	15 g	25 g
Przygotowanie się do kolokwium			13 g	15 g	13 g	15 g
Realizacja zadanych ćwiczeń i zadań			7 g	10 g	7 g	10 g
Przygotowanie sprawozdania z ćwiczeń						
Przygotowanie projektu / pracy						
Przygotowanie się i udział w egzaminie	15 g	18 g			15 g	18 g
	46 g	56 g	79 g	69 g	125 g	125 g

Efekty uczenia się	KEK	Treści kształcenia	Metody dydaktyczne	M. oceniania
zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu praktycznych zadań inżynierskich z zakresu bezpieczeństwa sieci	K_W05	W1-W9 C1-C6	MP1, MS1, ME1, MC1	MO1,MO2
zna standardy i norm technicznych występujących w dziedzinie bezpieczeństwa systemów sieciowych	K_W06	W1-W9 C1-C6	MP1, MS1, ME1, MC1	MO1,MO2
posiada umiejętności zastosowania metod i narzędzi ochrony sieci adekwatnych do utrzymania, na akceptowalnym poziomie, ryzyk zagrożenia bezpieczeństwa informacji.	U_W1 1	W1-W9 C1-C6	MP1, MS1, ME1, MC1	MO1,MO2
ma umiejętności wyszukiwania w literaturze i źródłach elektronicznych informacji na temat metod i rozwiązań stosowanych w współczesnych CERT/CSIRT/SOC	K_U02	C1-C6	MC1	MO1
potrafi dobrać właściwe metody i narzędzia oraz umie posługiwać się technikami informacyjno-komunikacyjnymi do realizacji zadań z dziedziny bezpieczeństwa sieci komputerowych	K_U04	C1-C6	MC1	MO1
potrafi uczestniczyć w procesach projektowania, wdrażania, testowania i eksploatacji systemów zabezpieczeń	K_U13	C1-C6	MC1	MO1
gotów jest do rozwiązywania problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w dziedzinie bezpieczeństwa sieci komputerowych	K_K02	W1-W9 C1-C6	MP1, MS1, ME1, MC1	MO1,MO2