Bezpieczeństwo w sieci - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo w sieci
Kod przedmiotu	15.9-WZ-BezD-BS
Wydział	Wydział Ekonomii i Zarządzania
Kierunek	Bezpieczeństwo narodowe
Profil	praktyczny
Rodzaj studiów	drugiego stopnia z tyt. magistra
Semestr rozpoczęcia	semestr zimowy 2018/2019

Informacje o przedmiocie

Semestr	3
Liczba punktów ECTS do zdobycia	2
Występuje w specjalnościach	Bezpieczeństwo biznesu i administracji
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• dr hab. inż. Sławomir Nikiel, prof. UZ

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	15	1	9	0,6	Zaliczenie na ocenę
Laboratorium	15	1	9	0,6	Zaliczenie na ocenę

Cel przedmiotu

Celem przedmiotu jest wprowadzenie studentów w tematykę nauk o bezpieczeństwie u. Wstępna analiza kwestii związanych z systemem bezpieczeństwa sieciowego

Wymagania wstępne

Wstęp do nauk o bezpieczeństwie, technologie informacyjne

Zakres tematyczny

Demografia sieci- e-business, technologie internetowe i mobilne, m-business.Sieci społecznościowe (Social networks), sieci semantyczne. Problematyka bezpieczeństwa informacji, jako istotnego czynnika bezpieczeństwa narodowego. Współczesne techniki i technologie zapewnienia bezpieczeństwa informacji chronionych. Zrozumienie zasad zarządzania ryzykiem na potrzeby bezpieczeństwa informacyjnego. Ochrona informacji a postęp technologiczny kraju. Haker i rodzaje ataków hakerskich. Bezpieczeństwo transmisji danych wrażliwych. Nieletni w cyberprzestrzeni. Anonimowość i ochrona danych w sieci.

Ochrona danych osobowych w portalach społecznościowych. Bezpieczeństwo transakcji finansowych w sieci. Zjawisko wykluczenia z cyberprzestrzeni. Trolling. Manipulowanie opinią społeczną w cyberprzestrzeni.

Metody kształcenia

Ćwiczenia w grupach projektowych: praca z dokumentem źródłowym, praca w grupach 2-4 osobowych, klasyczna metoda problemowa, dyskusja, prezentacja, ćwiczenia z analizą przykładów.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student posiada praktyczną wiedzę interdyscyplinarną, definiuje istotę zarządzania bezpieczeństwem oraz opisuje jego uwarunkowania	• K_W03	• projekt	• Laboratorium
Student ma rozszerzoną praktyczną wiedzę na temat systemów bezpieczeństwa narodowego	• K_W01	• projekt	• Laboratorium
Student rozumie potrzebę uczenia się przez całe życie. Potrafi w praktyczny sposób inspirować i organizować swój proces uczenia się.	• K_K01	• projekt	• Laboratorium
Student posiada ugruntowaną wiedzę o znaczeniu i funkcjach strategii bezpieczeństwa i budowy systemu bezpieczeństwa państwa, rozumie rolę kultury strategicznej i edukacji w praktycznym tworzeniu strategii bezpieczeństwa narodowego	• K_W02	• projekt	• Laboratorium
Student umie porównać strategie wybranych państw. Student prawidłowo interpretuje zjawiska i procesy zachodzące w różnych obszarach bezpieczeństwa	• K_U01	• projekt	• Laboratorium

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student potrafi współdziałać i pracować w grupie.	• K_K02	• projekt	• Laboratorium

Warunki zaliczenia

Efekty kształcenia będą weryfikowane trzema sposobami: poprzez systematyczną kontrolę wykonania zadań przewidzianych programem, okresowe sprawdziany (wejściówki) oraz przedstawienie prezentacji z wybranego tematu ćwiczeń projektowych.

Warunkiem zaliczenia przedmiotu jest: pozytywna ocena z ćwiczeń.

Warunkiem zaliczenia ćwiczeńjest: aktywność studentana ćwiczeniach,przygotowanie krótkiej prezentacji na wybrany temat wskazany przez prowadzącego.

Naocenękońcową z ćwiczeń składają się następujące elementy:

1. Ćwiczenia projektowe

Studenci zobowiązani są do uzyskania zaliczenia z ćwiczeń na ocenę. Warunkiem uzyskania zaliczenia jest przygotowanie i prezentacja przydzielonego tematu z wykorzystaniem technik multimedialnych. Czas prezentacji 20-30 min. Po wygłoszeniu referatu odbywa się dyskusja i oceniana jest aktywność studentów w prowadzonej dyskusji (K_U01, K_W01, K_W02, K_W03). Prezentacja stanowi 75% oceny z ćwiczeń, natomiast ocena z aktywności podczas ćwiczenia 25%. Ocenę dostateczną (3,0) otrzymuje student, który uzyska co najmniej 60-65% poprawnych odpowiedzi na pytania otwarte na ćwiczeniach (K_W01, K_W02), 66-75% na ocenę dst plus (3,5), 76-85% na ocenę dobrą (4,0), 86-94% na ocenę db plus (4,5), na ocenę bdb (5,0) 95-100%.

Literatura podstawowa

1. Kubiak M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, art. w: BEZPIECZEŃSTWO NARODOWE nr 22, II – 2012;
2. RZĄDOWY PROGRAM OCHRONY CYBERPRZESTRZENI RZECZYPOSPOLITEJ POLSKIEJ NALATA 2011-2016, MSWiA, Warszawa 2010
3. Bógdał-Brzeźińska A., Gawrycki M.F. (2003), Cyberterroryzm i problem bezpieczeństwa informacyjnego we współczesnym świecie, Wyd. ASPRA-JR, Warszawa.
4. Nowak A. Waldemar Scheffs W. , Zarządzanie bezpieczeństwem informacyjnym, AON Warszawa 2010r.

Literatura uzupełniająca

1. Pieczywok A.: Evgeny Morozov: The Net Delusion: The Dark Side of Internet Freedom, PublicAffairs, New York, 2011;
2. Innowacje w rozwoju przedsiębiorczości w procesie transformacji, pr. zb. pod red. W.

Janasza,– Difin, Warszawa 2004

Uwagi

Prowadzący zajęcia wykorzystuje także materiały własne (konferencyjne) oraz źródła internetowe.

Zmodyfikowane przez dr Paweł Szudra (ostatnia modyfikacja: 23-05-2018 16:29)

Wygenerowano automatycznie z systemu SylabUZ