Bezpieczeństwo technologiczne informacji - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo technologiczne informacji
Kod przedmiotu	14.1-WZ-BezD-BTI-S16
Wydział	Wydział Ekonomii i Zarządzania
Kierunek	Bezpieczeństwo narodowe / Bezpieczeństwo biznesu i administracji
Profil	praktyczny
Rodzaj studiów	drugiego stopnia z tyt. magistra
Semestr rozpoczęcia	semestr zimowy 2016/2017

Informacje o przedmiocie

Semestr	1
Liczba punktów ECTS do zdobycia	3
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
Laboratorium	15	1	9	0,6	Zaliczenie na ocenę

Cel przedmiotu

Celem prowadzącego jest przekazanie wiedzy z zakresu wykorzystania technologii dla zapewnienia bezpieczeństwa informacji. Wstępna analiza kwestii związanych z systemem bezpieczeństwa technologicznego. Definicyjne ujęcie, związanych z technologiami terminów i zagadnień przygotowujących do wykorzystania nabytej wiedzy w pracy zawodowej.

Wymagania wstępne

Wstęp do nauk o bezpieczeństwie

Zakres tematyczny

Wprowadzenie do zagadnień technologicznych związanych z bezpieczeństwem. Zadania służb cywilnych oraz sił zbrojnych w dziedzinie bezpieczeństwa publicznego. Wybrane aspekty technologii dla bezpieczeństwa: Technologie sieciowe i mobilne, zagrożenia oraz sposoby zwalczania cyberprzestępczości, technologie przechowywania i zabezpieczenia informacji, biometryka, technologie wojskowe ISR (Intelligence Surveillance Reconaissance), problematyka ochrony prywatności oraz danych osobowych.

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 ma rozszerzoną praktyczną wiedzę na temat systemów bezpieczeństwa narodowego	• K_W01	• 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 zna metody i praktyczne narzędzia badawczewykorzystywane w badaniach nad bezpieczeństwem	• K_W09	• projekt	• Laboratorium
Student umie porównać strategie wybranych państw. Student prawidłowo interpretuje zjawiska i procesy zachodzące w różnych obszarach bezpieczeństwa	• K_U01	• projekt	• Laboratorium
Student odpowiednio potrafi określić priorytety służące realizacji określonego przez siebie lub innych zadania.	• K_K03	• projekt	• Laboratorium
Student potrafi w praktyce samodzielnie i krytycznie uzupełniać wiedzę i umiejętności, rozszerzone o wymiar interdyscyplinarny.	• K_K06	• projekt	• Laboratorium

Warunki zaliczenia

Literatura podstawowa

1. Ruszczyk L.; Instrukcja ochrony informacji niejawnych; Gdańsk 2000
2. **Pokruszyński W.: Teoretyczne aspekty bezpieczeństwa: podręcznik akademicki,** Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi, Józefów 2010.
3. Cisowski Z., Organizacja i funkcjonowanie służb ochrony osób i mienia, Szczytno 2002;
4. Nowak A., Scheffs W., Zarządzanie bezpieczeństwem informacyjnym, AON Warszawa 2010r.
5. Białas A., Ochrona informacji i usług we współczesnej firmie lub instytucji, WNT, Warszawa 2006r.

Literatura uzupełniająca

1. Ustawa o ochronie danych osobowych.

2. Ustawa o dostępie do informacji publicznych.

3. Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej;

4. Bógdał-Brzeźińska A., Gawrycki M.F. (2003), Cyberterroryzm i problem bezpieczeństwa informacyjnego we współczesnym świecie, Wyd. ASPRA-JR, Warszawa 2003 r.

5. Zamiar Z., Wełyczko L.: Zarządzanie kryzysowe, Wyższa Szkoła Oficerska Wojsk Lądowych imienia generała Tadeusza Kościuszki, Wrocław 2012.

6. RozporządzeniePrezesa Rady Ministrów z dnia 25.01.1999r. w sprawie podstawowych wymagań bezpieczeństwa da systemów teleinformatycznych przetwarzających informacje niejawne.

7. Polska Norma PN-ISO/IEC 17799:2007. Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, Polski komitet Normalizacyjny, Warszawa 2007r .

Uwagi

Zmodyfikowane przez dr hab. inż. Sławomir Nikiel, prof. UZ (ostatnia modyfikacja: 19-07-2016 11:44)