

Cyberbezpieczeństwo - opis przedmiotu

Informacje ogólne	
Nazwa przedmiotu	Cyberbezpieczeństwo
Kod przedmiotu	14.1-WH-PolitD-Cyb-S18
Wydział	Wydział Nauk Społecznych
Kierunek	Politologia
Profil	ogólnoakademicki
Rodzaj studiów	drugiego stopnia z tyt. magistra
Semestr rozpoczęcia	semestr zimowy 2018/2019

Informacje o przedmiocie	
Semestr	4
Liczba punktów ECTS do zdobycia	3
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	dr hab. inż. Piotr Kwiatkiewicz, 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	30	2	-	-	Egzamin

Cel przedmiotu

Celem przedmiotu jest zagadnienie systemu bezpieczeństwa jako zjawiska związanego z procesem informatyzacji i technologizacji życia społecznego.

Wymagania wstępne

brak

Zakres tematyczny

1. Bezpieczeństwo sieci informatycznych.
2. Bezpieczeństwo systemów elektronicznych.
- 3 Bezpieczeństwo użytkowników sieci informatycznych.
4. Patologie systemów teleinformatycznych.
5. Problem wykorzystania i pozyskiwania energii dla celów teleinformatycznych.
6. Cyberbezpieczeństwo jako element polityki publicznej.
7. Cyberobrona

Metody kształcenia

Prezentacja multimedialna, praca w sieci internetowej, wykład konwersatoryjny

Efekty uczenia się i metody weryfikacji osiągnięcia efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
potrafi ocenić poziom bezpieczeństwa systemu lub sieci w aspektach prawnych, etycznych i organizacyjnych w świetle obowiązującego prawa;	• KP2_W02	• aktywność w trakcie zajęć • egzamin - ustny, opisowy, testowy i inne • przygotowanie projektu	• Wykład
potrafi stosować właściwe techniki i metody bezpieczeństwa	• KP2_U04	• aktywność w trakcie zajęć • dyskusja • egzamin - ustny, opisowy, testowy i inne	• Wykład
potrafi oceniać stopień zagrożeń środowiskowych, naturalnych i celowych	• KP2_K02	• aktywność w trakcie zajęć • egzamin - ustny, opisowy, testowy i inne	• Wykład

Warunki zaliczenia

Przygotowanie prezentacji (70%) i jej obrona w formie egzaminu; aktywne uczestnictwo w zajęciach (30%)

Literatura podstawowa

1. Orędzie o stanie Unii w 2017 r. – Komisja zwiększa zdolności reagowania UE na ataki cybernetyczne
2. M. Szmit, D. Lisiak-Felicka, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, Kraków 2016.
- 3.. Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, red. M. Górka, Warszawa 2014.

Literatura uzupełniająca

Uwagi

brak

Zmodyfikowane przez dr hab. Łukasz Młyńczyk, prof. UZ (ostatnia modyfikacja: 27-09-2018 15:58)

Wygenerowano automatycznie z systemu SylabUZ