KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Monitorowanie i ochrona infrastruktury krytycznej [S2IBiJ1-BiZK>MiOIK]

Przedmiot

Kierunek studiów
Inżynieria bezpieczeństwa i jakości

Rok/Semestr
2/3

Studia w zakresie (specjalność)
Bezpieczeństwo i zarządzanie kryzysowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
0

Laboratorium
15

Inne
0

Ćwiczenia
0

Projekty/seminaria
15

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Grzegorz Dahlke
grzegorz.dahlke@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający nauczanie powinien znać podstawową terminologię z zakresu zarządzania kryzysowego oraz klasyfikację infrastruktury krytycznej.

Cel przedmiotu

Celem przedmiotu jest przekazanie wiedzy z zakresu metod, technik i uwarunkowań ochrony infrastruktury krytycznej (europejskiej, krajowej, wojewódzkiej, powiatowej, gminnej oraz istotnej na poziomie przedsiębiorstw) oraz identyfikacji i oceny poziomów zagrożeń, które mogą wpłynąć na jej funkcjonowanie.

Przedmiotowe efekty uczenia się

Wiedza:
1. Student zna metody, narzędzia i kryteria identyfikacji infrastruktury krytycznej [K2_W01].
2. Student zna metody identyfikacji i analizy poziomu zagrożeń infrastruktury krytycznej [K2_W03].
3. Student posiada wiedzę specjalistyczną w zakresie modelowania awarii w obszarze infrastruktury krytycznej oraz w zakresie doboru i projektowania sposobów ochrony infrastruktury krytycznej [K2_W06].

Umiejętności:
1. Student potrafi ocenić skuteczność wybranych form ochrony infrastruktury krytycznej [K2_U02].
2. Student potrafi opracować hierarchię ważności infrastruktury krytycznej [K2_U03].
3. Student umie dobrać i ocenić oraz zaprojektować wybrane sposoby ochrony infrastruktury krytycznej [K2_U05].

Kompetencje społeczne:
1. Student ma świadomość zależności przyczynowo skutkowych w projektowaniu ochrony infrastruktury krytycznej [K2_K02].
2. Student ma świadomość konieczności ciągłego rozwoju i poznawania nowych metod i narzędzi badania i ochrony infrastruktury krytycznej [K2_K05].

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Ocena formująca:
a) w zakresie zajęć projektowych: na podstawie realizacji projektów wykonywanych przez podgrupy;
b) w zakresie ćwiczeń laboratoryjnych: na podstawie kolokwium realizowanego na ostatnich zajęciach oraz oceny realizacji zdań podczas ćwiczeń laboratoryjnych.
Ocena podsumowująca:
a) w zakresie zajęć projektowych: na podstawie średniej arytmetycznej ocen cząstkowych za zadania/podrozdziały projektu;
b) w zakresie zajęć laboratoryjnych: na podstawie średniej arytmetycznej z ocen z kolokwium oraz realizacji zadań podczas ćwiczeń laboratoryjnych.
Zakres zaliczenia 51% punktów.
Skala ocen:
0 - 50 niedostateczny
51 - 59 dostateczny
60 - 69 dostateczny plus
70 - 79 dobry
80 - 89 dobry plus
90 - 100 bardzo dobry

Treści programowe

Treści programowe obejmują przekazanie wiedzy z zakresu metod, technik i uwarunkowań ochrony infrastruktury krytycznej (europejskiej, krajowej, wojewódzkiej, powiatowej, gminnej oraz istotnej na poziomie przedsiębiorstw) oraz identyfikacji i oceny poziomów zagrożeń, które mogą wpłynąć na jej funkcjonowanie.

Tematyka zajęć

Fazy funkcjonowania infrastruktury krytycznej. Identyfikowanie zagrożeń dla infrastruktury krytycznej. Normalizacja w ocenie zagrożeń infrastruktury krytycznej. Metody, narzędzia i techniki monitorowania zagrożeń dla infrastruktury krytycznej. Smart Critical Infrastructure (SCI). Wskaźniki podatności, wrażliwości i odporności IK na zakłócenia. Fazy przebiegu zakłócenia infrastruktury krytycznej. Analiza poziomów skuteczności ochrony (fizycznej, technicznej, osobowej, teleinformatycznej i prawnej) infrastruktury krytycznej. Metody oceny ważności infrastruktury krytycznej w aspekcie ryzyka, ochrony i odbudowy. Mierniki poziomów ochrony infrastruktury krytycznej. Modelowanie awarii infrastruktury krytycznej. Projektowanie systemów ochrony infrastruktury krytycznej.

Metody dydaktyczne

Ćwiczenia wspomagane prezentacją multimedialną z rozwiązywaniem zadań. Zajęcia projektowe realizowane w pracowni komputerowej z wykorzystaniem programów specjalistycznych.

Literatura

Podstawowa:
1. Krajowy Plan Zarządzania Kryzysowego RP.
2. Narodowy Program Ochrony Infrastruktury Krytycznej RP.

3. Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP.
4. Strategia Bezpieczeństwa Narodowego RP.

Uzupełniająca:
1. Bagińska J.M. (2017), Ochrona baz paliw płynnych jako elementu infrastruktury krytycznej w aspekcie wybranych aktów normatywnych, Wydawnictwo SAN, Przedsiębiorczość i Zarządzania, Tom XVIII, Zeszyt 5, Część I, ss. 103-117.
2. Jakubiak E. (2018), Ochrona infrastruktury krytycznej w Polsce, Zeszyty Naukowe SGSP, Szkoła Główna Służby Pożarniczej, Nr 66, 165-175.
3. Kaak W. (2017), Faza odbudowy w wojewódzkich planach zarządzania kryzysowego. Studia Administracji i Bezpieczeństwa, nr 3, ss. 219-229.
4. Radziejewski R. (2014), Ochrona infrastruktury krytycznej. Teoria i praktyka, Wydawnictwo Naukowe PWN, Warszawa.
5. Sadowski J. (2018), Ochrona infrastruktury krytycznej : geneza problemu, Instytut Naukowo-Wydawniczy "SPATIUM". sp. z o.o., Autobusy : technika, eksploatacja, systemy transportowe, R. 19, nr 6, ss. 1237-1241.
6. Dahlke G. (2020), The anthropometric criterion in the modelling of evacuation, Informatyka Ekonomiczna, nr 1, s. 21-37.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	60	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	30	1,00