



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Podstawy bezpieczeństwa w cyberprzestrzeni [S1IBiJ1>PBwC]

Przedmiot

Kierunek studiów

Inżynieria bezpieczeństwa i jakości

Rok/Semestr

3/6

Studia w zakresie (specjalność)

–

Profil studiów

ogólnoakademicki

Poziom studiów

pierwszego 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. Sebastian Kubasiński

sebastian.kubasinski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student posiada wiedzę z zakresu podstaw zarządzania oraz technologii informatycznych prowadzonych na studiach I stopnia. Student ma świadomość związku pomiędzy ryzykiem zagrożeń w cyberprzestrzeni, a ich skutkami dla funkcjonowania organizacji. Ponadto, powinien również posiadać umiejętność wykorzystywania zdobytej już wiedzy w praktyce oraz jest gotowy do pracy w ramach struktur zespołowych.

Cel przedmiotu

Zainteresowanie studentów kierunku Inżynieria Bezpieczeństwa problematyką cyberbezpieczeństwa oraz rodzajami zagrożeń i technikami ich ograniczania, w rozwiązywaniu zarówno technologicznych jak i decyzyjnych problemów tej dyscypliny wiedzy.

Przedmiotowe efekty uczenia się

Wiedza:

1. Student zna fundamentalne dylematy współczesnej cywilizacji i trendy rozwoju oraz najlepsze praktyki w zakresie inżynierii bezpieczeństwa, dotyczące cyberbezpieczeństwa w organizacjach. [K1_W10]
2. Student zna w stopniu zaawansowanym metody, techniki, narzędzia i materiały stosowane przy przygotowaniu do prowadzenia badań naukowych oraz rozwiązywaniu prostych zadań inżynierskich z

zastosowaniem technologii informacyjnych, ochrony informacji i wspomagania komputerowego, w odniesieniu do bezpieczeństwa w cyberprzestrzeni. [K1_W11]

3. Student zna w pogłębionym stopniu pojęcia i zasady z zakresu ochrony prawa autorskiego, bezpieczeństwa informacji i ochrony własności intelektualnej w gospodarce rynkowej, w kontekście funkcjonowania organizacji w cyberprzestrzeni [K1_W12].

Umiejętności:

1. Student potrafi właściwie dobierać źródła oraz informacje z nich pochodzące dokonywanie oceny, krytycznej analizy i syntezy tych informacji. [K1_U01]
2. Student potrafi zastosować różne techniki w celu porozumiewania się w środowisku zawodowym oraz w innych środowiskach. [K1_U02]
3. Student potrafi wykorzystać metody analityczne, symulacyjne oraz eksperymentalne do formułowania i rozwiązywania zadań inżynierskich, również z wykorzystaniem metod i narzędzi informacyjno-komunikacyjnych, w kontekście zapewnienia bezpieczeństwa w cyberprzestrzeni. [K1_U04]
4. Student potrafi identyfikować zmiany wymagań, standardów, przepisów i postępu technicznego i rzeczywistości rynku pracy, w kontekście zapewnienia bezpieczeństwa w cyberprzestrzeni, i na ich podstawie określać potrzeby uzupełniania wiedzy. [K1_U12]

Kompetencje społeczne:

1. Student ma świadomość uznawania znaczenia wiedzy w rozwiązywaniu problemów z zakresu inżynierii bezpieczeństwa i jakości i ciągłego doskonalenia się. [K1_K02]
2. Student ma świadomość rozumienia pozatechnicznych aspektów i skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, w kontekście funkcjonowania organizacji w cyberprzestrzeni. [K1_K03]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Ocena formująca:

Laboratorium: bieżąca ocena wykonywanych zadań w skali 2- 5; próg zaliczenia pierwszego i drugiego podejścia - 50% + 1%;

Projekt: bieżąca ocena poszczególnych części projektu w skali 2- 5; próg zaliczenia pierwszego i drugiego podejścia - 50% + 1%;

Ocena podsumowująca:

Laboratorium: średnia ocen cząstkowych za poszczególne zadania; próg zaliczenia pierwszego i drugiego podejścia - 50% + 1%,

Projekt: średnia ocen cząstkowych za realizację poszczególnych faz projektu + ocena za poziom edycyjny projektu i postęp w trakcie zajęć; próg zaliczenia pierwszego i drugiego podejścia - 50% + 1%.

Treści programowe

Bezpieczeństwo informacji; główne zagrożenia dla firm: Phishing, ataki typu "Man-in-the-Middle", atak typu Denial of Service (DOS); cyberbezpieczeństwo w pracy zdalnej; cyberatak; zasady ochrony przed zagrożeniami zewnętrznymi.

Tematyka zajęć

Laboratorium:

1. Wprowadzenie do cyberbezpieczeństwa. 2. Wymogi i standardy cyberbezpieczeństwa. 3. Identyfikacja problemów i zagrożeń związanych z cyberbezpieczeństwem. 4. Praktyczne działania w zakresie ograniczania zagrożeń związanych z cyberbezpieczeństwem. 5. Zarządzanie incydentami i ciągłością działania organizacji w cyberprzestrzeni. 6. Programy edukacyjne i budowanie świadomości cyberbezpieczeństwa.

Projekt: Studenci projektują instrukcję bezpiecznego reprezentowania organizacji w cyberprzestrzeni, dla wybranego stanowiska pracy wskazanego przez prowadzącego.

Metody dydaktyczne

Laboratorium:

- metody eksponujące (prezentacja multimedialna, film, pokaz), dyskusja panelowa, case study, burza mózgów, ćwiczenia praktyczne.

Projekt:
- prezentacja multimedialna, case study

Literatura

Podstawowa:

1. ISO/IEC 27032 - Technologia informacyjna - Techniki bezpieczeństwa - Wytyczne dotyczące bezpieczeństwa cybernetycznego.
2. Normy ISO rodziny 27000, PKN 2014 lub późniejsze.
3. Karpiński M., Bezpieczeństwo Informacji: praca zbiorowa, Wydawnictwo PAK, 2012.
4. Brdulak J. J., Sobczak P., Wybrane problemy zarządzania bezpieczeństwem informacji, OW SGH, 2014.
5. Gałach A., Zarządzanie Bezpieczeństwem Informacji w Sektorze Publicznym, Wydawnictwo C.H. Beck, 2009.
6. Campbell T., Practical Information Security Management, A Complete Guide to Planning and Implementation, Springer 2016.

Uzupełniająca:

1. Shuttonm R. J., Bezpieczeństwo w telekomunikacji, WKŁ, Warszawa, 2004.
2. Bilski T., Pankowski T., Stokłosa J., Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN, 2001.
3. Stallings W., Cryptography and Network Security: Principles and Practice, Pearson Education, 2011.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	50	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	20	0,50