KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Systemy eksperckie i sztuczna inteligencja

Przedmiot

Kierunek studiów
Inżynieria Bezpieczeństwa
Studia w zakresie (specjalność)
Zintegrowane zarządzanie bezpieczeństwem organizacji
Poziom studiów
drugiego stopnia
Forma studiów
niestacjonarne

Rok/semestr
1/2
Profil studiów
ogólnoakademicki
Język oferowanego przedmiotu
polski
Wymagalność
obligatoryjny

Liczba godzin

Wykład
16
Ćwiczenia
10
Laboratoria
Projekty/seminaria
Inne (np. online)

Liczba punktów ECTS

5

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
prof. dr hab. inż. Leszek Pacholski

e-mail: leszek.pacholski@put.poznan.pl

Wydział Inżynierii Zarządzania
ul. J. Rychlewskiego 2, 60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student posiada wiedzę z zakresu podstaw zarządzania oraz technologii informatycznych prowadzonych na studiach I stopnia. 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 przyszłościową problematyką zastosowań Systemów Eksperckich oraz metod i technik Sztucznej Inteligencji w rozwiązywaniu zarówno technologicznych jak i decyzyjnych problemów tej dyscypliny wiedzy.

Przedmiotowe efekty uczenia się

Wiedza

student zna podstawowe metody, techniki, narzędzia i materiały wykorzystywane przy rozwiązywaniu prostych zadań inżynierskich w obszarze ergonomii i bezpieczeństwa pracy z zastosowaniem inteligentnych technologii cyfrowych i bezpieczeństwa biznesu w warunkach zagrożenia cyberatakami [P7S_WK_03]

student zna pojęcie człowieka i świata jego wartości oraz podstawowe kategorie etyczne a także rolę człowieka w zapewnieniu bezpieczeństwa systemom człowiek-obiekt techniczny [P7S_WK_03]

student rozróżnia kategorie pojęciowe: dane, informacja, wiedza i mądrość oraz zna zasady budowy i funkcjonowania Systemów Eksperckich, Sztucznych Sieci Neuronowych i Algorytmów Ewolucyjnych [P7S_WK_04]

Umiejętności

student potrafi dostrzegać i formułować w zadaniach inżynierskich aspekty systemowe i pozatechniczne, a także społeczno-techniczne, organizacyjne i ekonomiczne [P7S_UW_01, P7S_UW_02]

student potrafi wykorzystać metody badawcze, analityczne, symulacyjne oraz eksperymentalne do formułowania i rozwiązywania zadań inżynierskich, również z wykorzystaniem inteligentnych metod i narzędzi [P7S_UW_03, P7S_UW_04]

student potrafi dokonać krytycznej analizy sposobu funkcjonowania i ocenić - w powiązaniu z Inżynierią Bezpieczeństwa - istniejące rozwiązania techniczne, w szczególności maszyny, urządzenia, obiekty, systemy, procesy i usługi w zakresie inteligentnych technologii cyfrowych [P7S_UW_06]

Kompetencje społeczne

student ma świadomość dostrzegania zależności przyczynowo - skutkowych w realizacji postawionych celów i rangowania istotności alternatywnych bądź konkurencyjnych zadań w zakresie inteligentnych technologii cyfrowych [P7S_KK_01]

student ma świadomość uznawania znaczenia wiedzy w rozwiązywaniu problemów inżynierii cyberbezpieczeństwa i ciągłego doskonalenia się w zakresie korzystania z inteligentnych technologii cyfrowych [P7S_KK_02]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu weryfikowana jest przez przeprowadzenie egzaminu ustnego, w trakcie którego student wybiera losowo 3 pytania, za które student otrzymuje punkty. Próg zaliczeniowy: 50% punktów (ocena dostateczna).

Wiedza nabyta w ramach ćwiczeń weryfikowana jest na podstawie rozwiązywania poszczególnych zadań objętych programem zajęć. Za każde zadanie student otrzymuje punkty. Próg zaliczeniowy: 50% punktów (ocena dostateczna).

Treści programowe

Wykład: Na tle definicji takich pojęć jak: szeroko rozumiana inteligencja oraz dane, informacja, wiedza i mądrość wyprowadzane zostają (dla przykładu Inżynierii Bezpieczeństwa) definicje Systemu Eksperckiego i Sztucznej Inteligencji. W podobnym kontekście rozwijane są dalej kwestie pozyskiwania wiedzy, metod jej reprezentacji w systemach inteligentnych, tworzenia i przebudowy baz wiedzy profesjonalnej oraz strategii eksperckiego i inteligentnego rozwiązywania problemów. Ta część wykładu ma charakter metodologiczny i traktuje między innymi o heurystykach i strategiach przeszukiwania grafów a także o klasycznych i rozmytych metodach wnioskowania. Systemy Eksperckie prezentowane są w wariantach rozwiązań opartych na logice dwuwartościowej oraz jako systemy rozmyte. Wśród rozwiązań Sztucznej Inteligencji zaliczanych do opartych na naśladowaniu natury (Computational Intelligence), przedstawiane są Sztuczne Sieci Neuronowe (w wariantach: Self Organizing Maps i Learning Vector Quantization) oraz Algorytmy Ewolucyjne (w wariantach: Algorytmy Genetyczne, Strategie Ewolucyjne, Programowanie Ewolucyjne). Prezentowane są tzw. systemy hybrydowe oraz elementy teorii chaosu. Zastosowania inteligencji sztucznej dla potrzeb wspomagania systemów informacyjnych zarządzania (w tym rozwiązania takie jak: Business Intelligence System w zarządzaniu bezpieczeństwem) oraz gospodarka oparta o inteligentne technologie cyfrowe (z problematyką bezpieczeństwo biznesu, jako obiektu cyberataków) stanowią wraz zagadnieniem tak zwanego „inteligentnego dylematu szóstego cyklu koniunkturalnego” finalną część wykładu.

Ćwiczenia: Ten rodzaj zajęć realizowany jest w postaci wspólnej z prowadzącym ćwiczenia analizy studenckich, zespołowych opracowań praktycznych dla zagadnień: a), b), c) i d) oraz wspólnej z prowadzącym ćwiczenia analizy przygotowanego przez niego przykładowego zagadnienia e).
Wykaz zagadnień ćwiczeniowych obejmuje:
a) wybrane metody symbolicznej reprezentacji wiedzy z zakresu inżynierii bezpieczeństwa dla potrzeb tworzenia i przebudowy baz wiedzy profesjonalnej,
b) metody budowy i przeszukiwania grafów wiedzy z zakresu inżynierii bezpieczeństwa,
c) działania na trójkątnych i trapezoidalnych formach funkcji przynależności dla potrzeb wnioskowania w rozmytym systemie ekspertowym wybranego zagadnienia inżynierii bezpieczeństwa,
d) przygotowania programów szkoleń w zakresie inżynierii bezpieczeństwa biznesu w warunkach zagrożenia cyberatakami,
e) generowanie w MATLAB-ie Sztucznej Sieci Neuronowej z wielowarstwowym sprzężeniem zwrotnym i jedną warstwą ukrytą o 15 węzłach wejściowych i jednym węźle w warstwie wyjściowej (jako algorytm uczenia sieci - gradientowa propagacja wsteczną Levenberga-Marquardta, jako funkcja przenoszenia zarówno w warstwie wejściowej, jak i wyjściowej - styczna hiperboliczna; liczba neuronów w ukrytej warstwie ustalana metodą prób i błędów, zmieniając liczbę neuronów z zestawu: {7, 10, 13, 16, 19, 22, 25, 27, 29, 31}).

Metody dydaktyczne

Wykład informacyjny w formie prezentacji multimedialnej, z elementami wykładu konwersatoryjnego
Ćwiczenia: ćwiczenia audytoryjne, rozwiązywanie zadań oraz case study.

Literatura

Podstawowa

1. Pacholski L. (2011), Systemy ekspertowe i sztuczna inteligencja, Wydawnictwo Politechniki Poznańskiej, Poznań.
2. Zieliński J.S. (red.) (2000), Inteligentne systemy w zarządzaniu, PWN, Warszawa.
3. Mulawka J.J. (1996), Systemy ekspertowe, WNT, Warszawa.
4. Rutkowska D., Piliński M., Rutkowski L. (1997), Sieci neuronowe, algorytmy genetyczne i systemy rozmyte, PWN, Warszawa.
5. Cytowski J. (1996), Algorytmy genetyczne. Podstawy i zastosowania, Akademicka Oficyna Wydawnicza, Warszawa.

Uzupełniająca

1. Medsker L.M. (1994), Hybryd Neural Networks and Expert Systems, Kluwer Academic Publisher, Boston.
2. Żurada J.M., Barski M., Jędruch W. (1996), Sztuczne sieci neuronowe, PWN, Warszawa.
3. Budrewicz J. (1993), Fraktale i chaos, WNT, Warszawa.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	125	5,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć ćwiczeniowych, przygotowanie do egzaminu)[1]	95	3,5

[1] niepotrzebne skreślić lub dopisać inne czynności