KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
AI w cyberbezpieczeństwie multimediów [S1Cybez1>AIwC]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/5

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
24

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
16

Liczba punktów ECTS

5,00

Koordynatorzy

dr inż. Mateusz Lorkiewicz
mateusz.lorkiewicz@put.poznan.pl

dr hab. inż. Olgierd Stankiewicz prof. PP
olgierd.stankiewicz@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z podstaw programowania, teorii systemów, teorii sygnałow, cyfrowego przetwarzania sygnałów, uczeniamaszynowego, sztucznej inteligencja oraz podstaw telekomunikacji .Posiada uporządkowaną, podbudowaną matematycznie wiedzę w zakresie akwizycji, percepcji przez człowieka, oceny jakości, przetwarzania, cyfrowych reprezentacji i kompresji wizji oraz fonii. Potrafi pozyskiwać informacje z literatury i baz danych oraz innych źródeł w języku polskim lub angielskim; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, wyciągać wnioski i uzasadniać opinie. Zna ograniczenia własnej wiedzy i umiejętności, rozumie konieczność dalszego dokształcania się. Potrafi realizować projekty zespołowe.

Cel przedmiotu

Przedmiot ten ma na celu przedstawienie w jakoi sposób sztuczna inteligencja i uczenie maszynowe mogą być wykorzystywane przy stwarzaniu zagrożeń w cyberbezpieczeńwie, ale również wykrywania tych zagrożeń, analizy bezpieczeństwa i ochrony multimediów.

Przedmiotowe efekty uczenia się

Wiedza:
K1_W05 - Ma zaawansowaną wiedzę w zakresie złożonych struktur danych; zna podstawy teorii, zna zasady administrowania danymi i związanymi z nimi standardami; zna zasady cyberbezpieczeństwa i prywatności wykorzystywane do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przesyłaniem informacji lub danych
K1_W06 - Ma zaawansowaną wiedzę w zakresie zasada tworzenia programów komputerowych, struktur języków programowania, ich poziomów oraz używanych algorytmów; ma zaawansowaną wiedzę z zakresu inżynierii oprogramowania;
K1_W09 - Ma pogłębioną wiedzę o cyklu życia, projektowaniu i korzystaniu z odpornych na ataki programowych systemów informatycznych; zna i rozumie zasadę ich działania; zna narzędzia wykorzystywanych do identyfikacji luk w oprogramowaniu komunikacyjnym; zna wpływ konfiguracji oprogramowania na bezpieczeństwo;
K1_W15 - Ma wiedzę dotyczącą zasad, wymagań i procedur dotyczących bezpieczeństwa łańcucha dostaw technologii informatycznych oraz zarządzania ryzykiem w łańcuchu dostaw; jest świadom konieczności stosowania przepisów, polityk, procedur lub zarządzania istotnych dla cyberbezpieczeństwa infrastruktury krytycznej; ma wiedzę w zakresie procesów zarządzania ryzykiem (np. metod oceny i ograniczania ryzyka); zna metody identyfikacji zagrożeń oraz oceny ryzyka/zagrożenia; zna metody ograniczania ryzyka.
K1_W16 - Ma podstawową wiedzę na temat systemów maszynowego uczenia się i sztucznych sieci neuronowych; ma usystematyzowaną wiedzę w zakresie zasad oraz metod rozwiązywania problemów decyzyjnych i optymalizacyjnych z zastosowaniem algorytmów heurystycznych i nieheurystycznych przeszukiwania przestrzeni stanów w tym metod z ograniczeniami zasobowymi; zna metody sztucznej inteligencji wykorzystywane w kierunku studiów.
K1_W20- Zna i rozumie zagrożenia, na które narażona jest współczesna cywilizacji masowo wykorzystująca usługi cyfrowe; orientuje się w najnowszych trendach rozwojowych związanych ze studiowanym kierunkiem

Umiejętności:
K1_U01 - Potrafi korzystać ze źródeł literaturowych, integrować pozyskane informacje, oceniać je oraz dokonywać ich interpretacji i wyciągać wnioski, w celu rozwiązania złożonych i nietypowych problemów w obszarze cyberbezpieczeństwa
K1_U02 - Potrafi posłużyć się właściwie dobranymi metodami i narzędziami, w tym zaawansowanymi technikami informacyjno-komunikacyjnymi, a także opracować proste aplikacje lub skonfigurować proste system, w celu przeprowadzenia symulacji, analizy i projektowania systemów lub aplikacji właściwych dla kierunku studiów
K1_U07 - Potrafi, przy formułowaniu i rozwiązywaniu zadań dotyczących cyberbezpieczeństwa, dostrzegać ich aspekty systemowe i pozatechniczne, w tym etyczne, ekonomiczne i prawne
K1_U12 - Potrafi przygotować i przedstawić prezentację na temat zadania związanego z kierunkiem studiów, komunikuje się z użyciem specjalistycznej terminologii, przedstawia i uzasadnia różne opinie i stanowiska

Kompetencje społeczne:
K1_K01 - Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują
K1_K02 - Rozumie znaczenie wiedzy w rozwiązywaniu problemów z zakresu cyberbezpieczeństwa; jest świadomy konieczności wykorzystania wiedzy ekspertów podczas rozwiązywania zadań inżynierskich w zakresie wykraczającym poza własne kompetencje
K1_K03 - Rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii na temat pozytywnych i negatywnych aspektów cyberbezpieczeństwa, a także jest gotowy do działania na rzecz interesu publicznego

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
1. Projekty/Seminaria
Wykonanie projektu i prezentacja wyników na spotkaniu projektowym/seminaryjnym. Ocena zależna od stopnia skomplikowania, zaawansowania projektu/rozpatrywanego problemu oraz oceny prezentacji.

2. Laboratoria
Kolokwium pod koniec semestru i/lub testy sprawdzające stopień opanowania bieżącego materiału. Kolokwium/testy składają się z kilku/kilkunastu pytań sprawdzających, zależnie od charakteru przyjętych pytań. Dokładny charakter pytań zostanie przedstawiony studentom przed terminem odbycia się kolokwium/testu.
3. Wykład
Egzamin pisemny i/lub ustny. Egzamin składa się z kilku - kilkunastu pytań (w zależności od przyjętego charakteru pytań) i dotyczy treści przedstawionych podczas wykładów. Dokładny charakter pytań egzaminacyjnych zostanie studentom przedstawiony podczas jednego z ostanich wykładów.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Podstawowa wiedza dotycząca definiowania ataków na dane multimedialne oraz przy ich pomocy. Przykłady scenariuszy ataków i wycieku danych. Wykorzystanie sztucznej inteligencji do ingerencji w treść i jej wykrywania. Analiza strumienia danych mulimedialnych w celu wykrycia ataku.

Tematyka zajęć

Zdefiniowanie ataku przy pomocy/na dane multimedialne: Zmiana treści, usunięcie treści, generowanie fałszywych treści, zniszczenie treści, kradzież treści.
Przykładowe scenariusze ataków/wycieków danych: `fakenews` na podstawie wygenerowanych treści, wykorzystanie danych multimedialnych do generowania treści wykorrzystywanych w oszustwach, podszywania się pod podmioty poprzez kopiowanie interfejsów graficznych, generowanie fałszywych zgłoszeń poprzez prowokowanie treści.
Ingerencja w treść. Zastosowanie AI w analizie i wykrywaniu zagrożeń multimedialnych : analiza strumieni multimedialnych i ich nadzór, detekcja zakłóceń treści, wykrywanie wycieków danych wrażliwych, wykrywanie wycieków własności intelektualnej.
Automatyczne rozróżnianie degeneracji strumienia od ataku: rozróżnienie problemów technicznych od prób celowego wpływu na treści lub działanie systemu multimedialnego.
Wybrane techniki ataków: Phishing, kradzież danych multimedialnych używanych przez narzędzia AI, generowanie treści przez boty w celach dezinformacyjnych, ataki na CCTV.

Metody dydaktyczne

1. Projekty/Seminaria - zajęcia bazują na dyskusji na wybrane tematy związane z tematem cyberbezpieczeństwa multimediów. Główną ich częścią jest analiza zadanego problemu i dyskusji nad jego rozwiązaniami. W ramach indywidualnego lub grupowego projektu studenci rozważają zadany problem. Następnie w ramach spotkań referują jego analizę oraz zaproponowane rozwiązania. Studenci w czasie prezentacji odpowiadają na pytania związane z prezentowanym tematem (prowadzący lub inni studenci).
2.Ćwiczenia laboratoryjne dotyczą wybranych zagadnień omawianych na wykładach. Studenci mają możliwość oglądania i słuchania wyników symulowanych zagrożeń (fonia i wizja). W pewnym zakresie mogą samodzielnie kształtować analizowane metody - zarówno metody ataków jak i detekcji/przedciwdziałaniu zagrożeniom.
3. Wykład - Zajęcia z wyraźnymi elementami wykładu tradycyjnego, wykładu problemowego (dyskusja ze studentami określonego problemu) oraz wykładu konwersatoryjnego (mobilizowanie studentów do dyskusji na określony temat), zależnie od treści prezentowanego materiału. Wybrane treści wykładu są prezentowane na rzutniku multimedialnym bądź tablicy. Omówieniu zagadnień towarzyszy informacja o ich praktycznym zastosowaniu.

Literatura

Podstawowa:
Bhaskar Mondal, Shyam Singh Rajput, Multimedia Security Tools, Techniques, and Applications, CRC Press, ISBN: 9781774915028

Loveleen Gaur, DeepFakes Creation, Detection, and Impact, CRC Press, ISBN 9781032139234
Subhrajyoti Deb, Aditya Kumar Sahu, Securing the Digital World A Comprehensive Guide to Multimedia Security, CRC Press , ISBN 9781032663623

Uzupełniająca:

Ian Goodfellow, Yoshua Bengio, Aaron Courville , Deep Learning, MIT Press Ltd, ISBN: 9780262035613
Marek Domański, Obraz cyfrowy. Reprezentacja, kompresja, podstawy przetwarzania. Standardy JPEG iMPEG, Wydawnictwa Komunikacji i Łączności, 2010, ISBN: 978-83-206-1795-5.
David Foster, Deep learning i modelowanie generatywne. Jak nauczyć komputer malowania, pisania, komponowania i grania, Helion, ISBN: 978-83-283-7283-2
D. Karwowski, Zrozumieć kompresję obrazu, 2019, ISBN: 978-83-953420-0-4.
T. Zieliński T. P. Korohoda, R. Rumian (red.), Cyfrowe przetwarzanie sygnałów w telekomunikacji, PWN, Warszawa 2014.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	139	5,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	64	2,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	75	2,50