KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Wirtualna i rozszerzona rzeczywistość [S1Cybez1>WiRR]

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
obligatoryjny

Liczba godzin

Wykład
24

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
24

Liczba punktów ECTS

5,00

Koordynatorzy

dr hab. inż. Dawid Mieloch prof. PP
dawid.mieloch@put.poznan.pl

Wykładowcy

Wymagania wstępne

Ma podstawową wiedzę z zakresu akwizycji, przetwarzania, kompresji, transmisji oraz prezentacji obrazu i dźwięku. Ma wiedzę z zakresu programowania w językach C++ i Python.

Cel przedmiotu

Poznanie mediów wszechogarniających, systemów wirtualnej rzeczywistości oraz rzeczywistości rozszerzonej. Zapoznanie z rozwiązaniami technicznymi dotyczącymi wspomnianych systemów. Przygotowanie własnych realizacji wybranych elementów omawianych systemów oraz ich integracja z istniejącymi systemami.

Przedmiotowe efekty uczenia się

Wiedza:
K1_W04 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_W08 Ma szczegółową wiedzę na temat budowy elektronicznych układów cyfrowych, w tym cyfrowych układów programowalnych; ma pogłębioną wiedzę na temat budowy komputerów oraz ich

komponentów; zna i rozumie zjawiska i mechanizmy w nich wykorzystywane
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_U06 Przy formułowaniu zadań inżynierskich potrafi dokonać wstępnej oceny ekonomicznej zaprojektowania, implementacji, konfiguracji i utrzymania oprogramowania i systemów spełniających wymogi cyberbezpieczeństwa i zachowania prywatności
K1_U11 Na podstawie dokumentacji technicznej, obowiązujących standardów, przy użyciu właściwych metod, narzędzi i elementów, potrafi zbudować, skonfigurować i uruchomić typowy system lub sieć komputerową spełniające wymogi cyberbezpieczeństwa
K1_U15 Potrafi planować oraz organizować pracę indywidualną i w zespole (w tym opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminu), stosuje zasady bezpieczeństwa i higieny pracy, a także umie pracować w zespołach o charakterze interdyscyplinarnym

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

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:
Wykład: Zaliczenie w formie pisemnej lub ustnej, pytania o charakterze otwartym, z oczekiwaną odpowiedzią opisową. Zagadnienia wymagane do opanowania udostępniane są podczas wykładów.
Laboratorium: sprawozdania z jednolitych tematycznie bloków ćwiczeń laboratoryjnych.
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

1. Wprowadzenie
2. Aspekty techniczne
3. Zastosowania
4. Cyberbezpeczeństwo w VR i AR
5. Warsztaty i demonstracje (laboratoria)
6. Przyszłość VR i AR

Tematyka zajęć

• Definicje, historia: Przedstawienie krótkiej historii rozwoju tych technologii, od pierwszych koncepcji do obecnego stanu.
• Rodzaje, sprzęt i oprogramowanie: Prezentacja popularnych urządzeń VR (gogle, kontrolery) i AR (smartfony, tablety, okulary AR) oraz oprogramowania wykorzystywanego do tworzenia aplikacji VR/AR.
• Śledzenie ruchu (tracking): Omówienie różnych metod śledzenia ruchu (np. sensory, kamery).
• Renderowanie grafiki 3D: Wyjaśnienie jak generowana jest grafika 3D i jakie są techniki optymalizacji.
• Interakcja człowiek-komputer: Przedstawienie sposobów interakcji użytkownika z wirtualnym środowiskiem (np. kontrolery, gesty, głos).
• Kompresja treści VR: Obraz (MPEG immersive video), dźwięk (MPEG-I Immersive audio)
• Gry i rozrywka: Omówienie zastosowania w grach komputerowych, symulatorach, parkach rozrywki.

• Edukacja i szkolenia: Przedstawienie przykładów wykorzystania w edukacji (np. wirtualne wycieczki, interaktywne modele) i szkoleniach (np. symulacje medyczne, szkolenia BHP).
• Medycyna: Zastosowanie w diagnostyce, leczeniu, rehabilitacji i szkoleniu personelu medycznego.
• Przemysł: Wykorzystanie w projektowaniu, produkcji, konserwacji i kontroli jakości.
• Architektura i design: Wizualizacja projektów architektonicznych i wnętrz.
• Śledzenie i gromadzenie danych: ruchy, mimika twarzy, lokalizacja, dane biometryczne. Identyfikacja i profilowanie. Ataki socjotechniczne, phishing.
• Metaverse: Omówienie specyficznych zagrożeń związanych z cyberbezpieczeństwem w Metaverse, który jest połączeniem VR, AR i internetu. Manipulacja środowiskiem VR/AR: Atakujący mogą manipulować środowiskiem VR/AR, aby wprowadzić użytkownika w błąd, wywołać dezorientację lub strach. Manipulacja danymi sensorycznymi: Atakujący mogą manipulować danymi sensorycznymi w VR, aby wywołać u użytkownika fałszywe wrażenia lub reakcje. Zabezpieczenia sprzętowe i programowe: Omówienie zabezpieczeń wbudowanych w urządzenia , takich jak szyfrowanie danych, autoryzacja i kontrola dostępu.
• Odpowiedzialność za działania w VR: Omówienie kwestii odpowiedzialności za działania użytkowników w wirtualnym środowisku. Regula prawne dotyczące Przedstawienie istniejących i planowanych regulacji prawnych dotyczących.
• Praktyczne doświadczenie: umożliwienie studentom przetestowania różnych urządzeń oraz aplikacji.
• Tworzenie prostych aplikacji VR/AR: Wprowadzenie do narzędzi i technik tworzenia prostych aplikacji VR/AR.

Metody dydaktyczne

Wykład: egzamin pisemny lub ustny, pytania o charakterze otwartym, z oczekiwaną odpowiedzią opisową. Próg zaliczeniowy: 50% możliwych do zdobycia punktów. Zagadnienia wymagane do opanowania udostępniane są podczas wykładów.
Laboratorium: sprawozdania z jednolitych tematycznie bloków ćwiczeń laboratoryjnych.

Literatura

Podstawowa:
- Gauthier Lafruit, Mehrdad Teratani, "Virtual Reality and Light Field Immersive Video Technologies for Real-World Applications," Institution of Engineering and Technology, 2021.

Uzupełniająca:
- Reinhard Klette, "Concise Computer Vision," Springer, 2014.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	132	5,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	72	3,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	60	2,00