



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Cyberbezpieczeństwo w mediach publicznych i społecznościowych [S1Cybez1>CwMPiS]

Przedmiot

Kierunek studiów

Cyberbezpieczeństwo

Rok/Semestr

4/7

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

0

Inne

0

Ćwiczenia

0

Projekty/seminaria

30

Liczba punktów ECTS

4,00

Koordynatorzy

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

Wykładowcy

Wymagania wstępne

Student posiada wiedzę z zakresu cyberbezpieczeństwa, mediów społecznościowych, środowiska medialnego i technologii informacyjnej. Podstawowe pojęcia i zasady cyberbezpieczeństwa, takie jak zagrożenia, podatności, ryzyko, ataki i mechanizmy obronne. Działanie i specyfika mediów społecznościowych oraz ich rolę w komunikacji i dystrybucji informacji. Ogólna wiedza na temat mediów publicznych i społecznościowych, ich funkcji i wpływu na społeczeństwo, wiedza z zakresu technologii informacyjnej, w tym sieci komputerowych, systemów operacyjnych i baz danych.

Cel przedmiotu

Zapoznanie studentów z zagrożeniami cyberbezpieczeństwa w mediach publicznych i społecznościowych oraz wyposażenie ich w wiedzę i umiejętności inżynierskie niezbędne do analizy, projektowania i wdrażania zabezpieczeń w tym obszarze.

Przedmiotowe efekty uczenia się

Wiedza:

K1_W12 Ma pogłębioną wiedzę w zakresie autentykacji, autoryzacji i zasad kontroli dostępu do systemów komputerowych; jest świadom konieczności stosowania polityk kontroli dostępu oraz ich

adaptacji do poziomu ryzyka; zna zasady uwierzytelniania biometrycznego

K1_W17 Ma pogłębioną wiedzę w odniesieniu do przepisów prawa, regulacji, zasad i etyki w zakresie cyberbezpieczeństwa i prywatności; jest świadom skutków operacyjnych naruszeń cyberbezpieczeństwa; ma pogłębioną wiedzę w zakresie zasad cyberbezpieczeństwa i ochrony prywatności oraz wymagań organizacyjnych (odnoszących się do poufności, integralności, dostępności, uwierzytelniania i niezaprzeczalności)

K1_W20 Zna i rozumie zagrożenia, na które narażona jest współczesna cywilizacja masowo wykorzystująca usługi cyfrowe; orientuje się w najnowszych trendach rozwojowych związanych ze studiowanym kierunkiem

K1_W21 Ma podstawową wiedzę niezbędną do zrozumienia społecznych, etycznych, ekonomicznych, ekologicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej

Umiejętności:

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

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_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

K1_K05 Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu

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: 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. Projekt: przygotowanie samodzielnego lub grupowego projektu dotyczącego zagadnień poruszanych na wykładzie.

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 do cyberbezpieczeństwa w mediach
2. Bezpieczeństwo platform mediów społecznościowych
3. Cyberbezpieczeństwo w mediach publicznych
4. Socjotechnika i inżynieria społeczna w mediach
5. Cyberprzemoc i mowa nienawiści w mediach

Tematyka zajęć

- Specyfika mediów publicznych i społecznościowych w kontekście cyberbezpieczeństwa
- Rodzaje zagrożeń: dezinformacja, propaganda, cyberprzemoc, ataki socjotechniczne, phishing, malware
- Podstawowe pojęcia i definicje: autentyczność, integralność, poufność, dostępność

- Przegląd standardów i regulacji prawnych
- Architektura i mechanizmy bezpieczeństwa popularnych platform
- Analiza podatności i zagrożeń specyficznych dla mediów społecznościowych (podstawy OSINT, OPSEC)
- Prywatność i ochrona danych osobowych w mediach społecznościowych
- Zabezpieczanie stron internetowych i portali publicznych
- Cyberbezpieczeństwo w e-administracji

Metody dydaktyczne

Wykłady online z wykorzystaniem prezentacji multimedialnych i analizy przypadków.
Projekty indywidualne lub grupowe realizowane w formie projektu.

Literatura

Podstawowa:

Wprowadzenie do bezpieczeństwa IT, tom I i II, Wielu autorów, Securitum

Sztuka podstęp. Łamałem ludzi, nie hasła, Kevin Mitnick, William L. Simon, Helion

Uzupełniająca

Uzupełniająca:

-

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	114	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	54	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	60	2,00