KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo w Systemach Komputerowych

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
2/3

Studia w zakresie (specjalność)
Informatyka w Procesach Biznesowych

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
niestacjonarne

Wymagalność
obligatoryjny

Liczba godzin

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

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr inż. Tomasz Łukaszewski

Odpowiedzialny za przedmiot/wykładowca:
mgr inż. Bartosz Zgrzeba

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu sieci komputerowych, systemów operacyjnych, aplikacji internetowych i bezpieczeństwa systemów informatycznych. Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

Cel przedmiotu

Przekazanie studentom rozszerzonej wiedzy o systemach komputerowych i internecie rzeczy, w zakresie bezpieczeństwa tych systemów. Rozwijanie u studentów umiejętności rozwiązywania problemów związanych z bezpieczeństwem w systemach komputerowych i w internecie przedmiotów.

Przedmiotowe efekty uczenia się

Wiedza

1. Ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie systemów operacyjnych, technologii sieciowych 2. Ma podbudowaną teoretycznie szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki, takimi jak: bezpieczeństwo systemów informatycznych i internetu

przedmiotów 3. Ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce w zakresie ochrony danych i bezpieczeństwa systemów komputerowych

Umiejętności

1. Umie korzystać z usług dostępnych w systemach komputerowych i internecie rzeczy biorąc pod uwagę aspekt bezpieczeństwa. 2. Jest przygotowany do wykorzystania w pracy zawodowej składowych systemów komputerowych i internetu rzeczy w sposób uwzględniający bezpieczeństwo tworzonych rozwiązań.

Kompetencje społeczne

Rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana na egzaminie pisemnym. Egzamin składa się z około 30 pytań (zamkniętych). Próg zaliczeniowy: 50% punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania zostaną przesłane studentom przed egzaminem. Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są podstawie prezentacji z realizacji projektu polegającego na analizie wskazanego problemu związanego z bezpieczeństwem w internecie przedmiotów.

Treści programowe

Program wykładu obejmuje następujące zagadnienia:

1. Wprowadzenie do problematyki bezpieczeństwa: zdefiniowanie pojęcia hakingu, analiza działania programów destrukcyjnych, definicja pojęć bezpieczeństwa, zagrożeń, podatności i ataków. Przedstawienie aktualnych inicjatyw na rzecz bezpieczeństwa.

2. Kwestie prawne związane z wykorzystaniem systemów komputerowych: piractwo komputerowe, naruszenie praw autorskich, naruszenie dóbr osobistych i inne.

3. Bezpieczeństwo haseł (zagrożenia związane z używaniem rodzajów haseł) i Biometria (zastosowanie w procesie uwierzytelniania).

4. Bezpieczeństwo usług elektronicznych: bankowość elektroniczna, handel elektroniczny.

5. Bezpieczeństwo kart płatniczych, technologii RFID, kryptowalut.

6. Prywatność i anonimowość w systemach komputerowych.

7. Bezpieczeństwo cyberprzestrzeni i mediów społecznościowych.

8. Zagrożenia: spam, phishing, spyware, phishing, stalking, scam.

9. Ataki: SSL strip, Clickjacking, HTTP Session hijacking

10. Bezpieczeństwo sieci WiFi: omówienie podatności mechanizmów WEP, WPA, WPA2.

Program laboratorium obejmuje pogłębienie zagadnień omawianych na wykładach. Ponadto na ostatnich laboratoriach studenci bronią projekt - omawiają wyniki analizy problemu związanego z bezpieczeństwem w systemach komputerowych i internetem przedmiotów.

Metody dydaktyczne

wykład: prezentacja multimedialna, demonstracja przykładowych zagrożeń i metod obrony

ćwiczenia laboratoryjne: ćwiczenia praktyczne, dyskusja, praca w zespole, analiza materiałów multimedialnych

Literatura

Podstawowa

1. Viega J., Mity bezpieczeństwa IT, Helion, 2010

2. Strebe M., Podstawy bezpieczeństwa sieci, Mikom, 2005

3. Sikorski M., Roman A. M., Internet rzeczy, PWN 2020

Uzupełniająca

1. Zalewski M., Cisza w sieci, Helion, 2005

2. Zalewski M., Splątana sieć, Helion, 2012

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	37	2
Praca własna studenta (studia literaturowe, realizacja projektu, przygotowanie do egzaminu)[1]	63	2

[1] niepotrzebne skreślić lub dopisać inne czynności