



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo w Internecie Przedmiotów [N2Inf1-AMiWdIP>BEZIP]

Przedmiot

Kierunek studiów
Informatyka

Rok/Semestr
2/3

Studia w zakresie (specjalność)
Aplikacje mobilne i wbudowane dla Internetu
Przedmiotów

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
niestacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
18

Laboratorium
24

Inne (np. online)
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

5,00

Koordynatorzy

dr inż. Tomasz Łukaszewski
tomasz.lukaszewski@put.poznan.pl

Wykładowcy

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 teście zaliczeniowym. Próg zaliczeniowy: 50% punktów. Opcjonalnie możliwość podwyższenia oceny na drodze egzaminu ustnego. Lista zagadnień zostanie podana studentom z odpowiednim wyprzedzeniem czasowym..

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 m.in. następujące zagadnienia:

- Wprowadzenie do problematyki cyberbezpieczeństwa
- Bezpieczeństwo haseł, keylogery, Biometria, Kryptografia a komputery kwantowe
- Bezpieczeństwo usług elektronicznych: bankowość elektroniczna, handel elektroniczny
- Bezpieczeństwo kart płatniczych, technologii RFID
- Prywatność i anonimowość w systemach komputerowych
- Bezpieczeństwo mediów społecznościowych
- Zagrożenia: spam, phishing, spyware, phishing, stalking, scam, zagrożenia CBRN
- Ataki: SSL strip, HTTP Session hijacking, Metasploit
- Nowe koncepcje: antykruchość, segmentacja, Zero Trust
- Capture The Flag
- Metadane

Program laboratorium obejmuje pogłębienie zagadnień omawianych na wykładach. Ponadto na ostatnich laboratoriach studenci prezentują pracę wykonaną w ramach projektu - 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	125	5,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	44	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiiw/egzaminu, wykonanie projektu)	81	3,00