KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Bezpieczeństwo w Internecie Przedmiotów	**1010512331010510008**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**ogólnoakademicki**	**2 / 3**

Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
Internet Przedmiotów	**polski**	**obligatoryjny**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)
II stopień	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **30** Ćwiczenia: **-** Laboratoria: **30** Projekty/seminaria: **-**	**3**

Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny)	(ogólnouczelniany, z innego kierunku)
kierunkowy	**z danego kierunku**

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**
nauki techniczne	**3 100%**
nauki techniczne	**3 100%**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Tomasz Łukaszewski
email: Tomasz.Lukaszewski@put.poznan.pl
tel. 61 6652920
Instytut Informatyki
ul. Piotrowo 2, 60-965 Poznań

Odpowiedzialny za przedmiot / wykładowca:

mgr inż. Bartosz Zgrzeba
email: Bartosz.Zgrzeba@put.poznan.pl
tel. 61 6652925
Instytut Informatyki
ul. Piotrowo 2, 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu sieci komputerowych, systemów operacyjnych, aplikacji internetowych i bezpieczeństwa systemów informatycznych.
2	**Umiejętności:**	Powinien posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł.
3	**Kompetencje społeczne**	Powinien również rozumieć konieczność poszerzania swoich kompetencji. Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu:

1. Przekazanie rozszerzonej wiedzy o systemach komputerowych, w zakresie bezpieczeństwa tych systemów.
2. Rozwijanie umiejętności rozwiązywania problemów związanych z bezpieczeństwem w systemach komputerowych

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie systemów operacyjnych, technologii sieciowych - [K2st_W2]
2. ma szczegółową wiedzę związaną z bezpieczeństwem w internecie przedmiotów - [K2st_W3]
3. ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce w zakresie ochrony danych i bezpieczeństwa w internecie przedmiotów - [K2st_W4]
4. ma podstawową wiedzę o cyklu życia systemów informatycznych - [K2st_W5]

Umiejętności:

1. potrafi pozyskiwać informacje z literatury oraz innych źródeł (w języku ojczystym i angielskim), integrować je, dokonywać ich interpretacji i krytycznej oceny, wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie - [K2st_U1]

2. potrafi formułować i planować i przeprowadzać eksperymenty związane z problemami inżynierskimi i prostymi problemami badawczymi w zakresie bezpieczeństwa w internecie przedmiotów - [K2st_U3]

3. potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych metody eksperymentalne w zakresie bezpieczeństwa w internecie przedmiotów - [K2st_U4]

4. potrafi - przy formułowaniu i rozwiązywaniu zadań z bezpieczeństwa w intermecie przedmiotow - integrować wiedzę z różnych obszarów informatyki oraz zastosować podejście systemowe, uwzględniające także aspekty pozatechniczne - [K2st_U5]

5. potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych w bezpieczeństwie w internecie przedmiotów - [K2st_U6]

Kompetencje społeczne:

1. rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe - [K2st_K1]

2. rozumie znaczenie wykorzystania najnowszej wiedzy z zakresu bezpieczeństwa systemów informatycznych i internetu przedmiotów - [K2st_K2]

Sposoby sprawdzenia efektów kształcenia

Ocena formująca:

a) w zakresie wykładów:

- na podstawie odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach,

b) w zakresie laboratoriów / ćwiczeń:

- na podstawie oceny bieżącego postępu realizacji zadań,

Ocena podsumowująca:

a) w zakresie wykładów weryfikowanie założonych efektów kształcenia realizowane jest przez:

- ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym o charakterze problemowym. Egzamin składa się z pytań zamkniętych. Każde z pytań wymaga dobrej znajomości materiału i umiejętności rozwiązywania problemów. Otrzymanie oceny pozytywnej wymaga uzyskania co najmniej 50% punktów.

b) w zakresie laboratoriów / ćwiczeń weryfikowanie założonych efektów kształcenia realizowane jest przez:

- ocenę i obronę przez studenta sprawozdania z realizacji prezentacji/projektu,

Uzyskiwanie punktów dodatkowych za aktywność podczas zajęć, a szczególnie za:

- omówienia dodatkowych aspektów zagadnienia,
- efektywność zastosowania zdobytej wiedzy podczas rozwiązywania zadanego problemu,
- umiejętność współpracy w ramach zespołu praktycznie realizującego zadanie szczegółowe w laboratorium,
- uwagi związane z udoskonaleniem materiałów dydaktycznych,
- wskazywanie trudności percepcyjnych studentów umożliwiające bieżące doskonalenia procesu dydaktycznego.

Treści programowe

Program wykładu obejmuje następujące zagadnienia:

1. Wprowadzenie do problematyki bezpieczeństwa: zdefiniowanie pojęcia hakingu, podanie przykładów 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. Websecurity: XSS, CSRF, SQL Injection, SSL strip, Clickjacking, HTTP Session hijacking

10. Bezpieczeństwo sieci WiFi: omówienie mechanizmów bezpieczeństwa takich jak SSID, MAC, WEP, WPA, WPA2, WPA3; omówienie podatności mechanizmów WEP, WPA, WPA2.

11. Bezpieczeństwo Internetu przedmiotów (rzeczy).

12. Kulturowe aspekty bezpieczeństwa.

Program laboratorium obejmuje pogłębienie zagadnień omawianych na wykładach. Ponadto na ostatnich laboratoriach studenci bronią (prezentują) zrealizowany przez nich projekt związany z bezpieczeństwem w systemach komputerowych.

Metody dydaktyczne:

1. wykład: prezentacja multimedialna, demonstracja przykładowych zagrożeń i metod obrony

2. ćwiczenia laboratoryjne: ćwiczenia praktyczne, dyskusja, praca w zespole, analiza materiałów multimedialnych
Literatura podstawowa: 1. Strebe M., Podstawy bezpieczeństwa sieci, Mikom, 2005. 2. Viega J., Mity bezpieczeństwa IT, Helion, 2010. 3. Strebe M., Firewalls: ściany ogniowe, Mikom, 2000. 4. Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii, Helion, 2012.
Literatura uzupełniająca: 1. Miller M., Internet rzeczy, PWN 2016. 2. Zalewski M., Cisza w sieci, Helion, 2005. 3. Zalewski M., Splątana sieć, Helion, 2012.

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. udział w wykładach	30
2. przygotowanie do zajęć laboratoryjnych	1
3. udział w zajęciach laboratoryjnych	30
4. dokończenie (w ramach pracy własnej) ćwiczeń laboratoryjnych	1
5. realizacja projektu (czas poza zajęciami laboratoryjnymi)	2
6. udział w konsultacjach związanych z realizacją ćwiczeń laboratoryjnych i projektu	2
7. zapoznanie się ze wskazaną literaturą (10 stron tekstu naukowego = 1 godz.), 50 stron	5
8. przygotowanie do egzaminu i obecność na egzaminie: 4 godz. + 2 godz.	6

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	77	3
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	62	2
Zajęcia o charakterze praktycznym	33	1