KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Bezpieczeństwo w systemach komputerowych	**1010515331010513917**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**ogólnoakademicki**	**2 / 3**
Ścieżka obieralności/specjalność: **Informatyka w procesach biznesowych**	Przedmiot oferowany w języku: **polski**	Kurs (obligatoryjny/obieralny) **obligatoryjny**
Stopień studiów: **II stopień**	**Forma studiów** (stacjonarna/niestacjonarna) **niestacjonarna**	
Godziny: Wykłady: **16** Ćwiczenia: **-** Laboratoria: **16** Projekty/seminaria: **-**		Liczba punktów: **4**
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny): **kierunkowy**	(ogólnouczelniany, z innego kierunku) **z danego kierunku**	
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki: **nauki techniczne**	**Podział ECTS (liczba i %)**: **4 100%**	

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

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Efekty kształcenia ze studiów I stopnia zdefiniowane w Uchwale Senatu PP, a szczególnie efekty K_W1-2, K_W4, K_W6-15, weryfikowane w procesie rekrutacji na studia 2 stopnia ? efekty te prezentowane są w serwisie internetowym wydziału www.fc.put.poznan.pl Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu sieci komputerowych, systemów operacyjnych, aplikacji internetowych i bezpieczeństwa systemów informatycznych.
2	**Umiejętności:**	Efekty kształcenia ze studiów I stopnia zdefiniowane w Uchwale Senatu PP, a szczególnie efekty K_U1-2, K_U4, K_U7-8, K_U14-20, K_U22-23, K_U26, weryfikowane w procesie rekrutacji na studia 2 stopnia ? efekty te prezentowane są w serwisie internetowym wydziału www.fc.put.poznan.pl Powinien posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł.
3	**Kompetencje społeczne**	Efekty kształcenia ze studiów I stopnia zdefiniowane w Uchwale Senatu PP, a szczególnie efekty K_K1-9, weryfikowane w procesie rekrutacji na studia 2 stopnia ? efekty te prezentowane są w serwisie internetowym wydziału www.fc.put.poznan.pl 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 studentom rozszerzonej wiedzy o systemach komputerowych, w zakresie bezpieczeństwa tych systemów.
2. Rozwijanie u studentów 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, architektury systemów komputerowych, systemów operacyjnych, technologii sieciowych - [K_W4]

2. ma podbudowaną teoretycznie szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki, takimi jak bezpieczeństwo systemów informatycznych - [K_W5]

3. ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce w zakresie ochrony danych, zabezpieczania sieci komputerowych - [K_W6]

4. ma podstawową wiedzę o cyklu życia systemów informatycznych - [K_W7]

5. zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich z wybranego obszaru informatyki - [K_W8]

6. rozumie zagrożenia związane z przestępczością elektroniczną i zna podstawowe oraz zaawansowane mechanizmy ochrony - [K_W9]

Umiejętności:

1. potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł (w języku ojczystym i angielskim), integrować je, dokonywać ich interpretacji i krytycznej oceny, wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie - [K_U1]

2. potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia - [K_U5]

3. potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych metody eksperymentalne - [K_U9]

4. potrafi - przy formułowaniu i rozwiązywaniu zadań inżynierskich - integrować wiedzę z różnych obszarów informatyki (a w razie potrzeby także wiedzę z innych dyscyplin naukowych) oraz zastosować podejście systemowe, uwzględniające także aspekty pozatechniczne - [K_U10]

5. potrafi formułować i testować hipotezy związane z problemami inżynierskimi i prostymi problemami badawczymi - [K_U12]

6. potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych - [K_U13]

7. potrafi zaproponować ulepszenia (usprawnienia) istniejących rozwiązań technicznych - [K_U21]

Kompetencje społeczne:

1. rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe, - [K_K1]

2. zna przykłady i rozumie przyczyny wadliwie działających systemów informatycznych, które doprowadziły do poważnych strat finansowych, społecznych lub też do poważnej utraty zdrowia, a nawet życia - [K_K4]

3. potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania - [K_K6]

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 (student może korzystać z materiałów dydaktycznych). Egzamin składa się z 20 pytań problemowych. Każde z pytań wymaga dobrej znajomości materiału i umiejętności rozwiązywania problemów. Otrzymanie oceny pozytywnej wymaga uzyskania co najmniej 60% punktów.
- omówienie wyników egzaminu,

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

- ocenę sprawozdania z realizacji 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. Bezpieczeństwo lokalnych sieci bezprzewodowych: wprowadzenie do sieci bezprzewodowych, omówienie mechanizmów bezpieczeństwa takich jak SSID, MAC, WEP, WPA, WPA2. Omówienie podatności mechanizmów WEP, WPA, WPA2.
3. Bezpieczeństwo sieci bezprzewodowych Bluetooth i GSM.
4. Bezpieczeństwo haseł (tęczowe tablice, polityka bezpieczeństwa) i Biometria
5. Kwestie prawne związane z wykorzystaniem systemów komputerowych: piractwo komputerowe, naruszenie praw autorskich, naruszenie dóbr osobistych, pomawianie.
6. Prywatność i anonimowość: metody zachowania prywatności i anonimowości w systemach komputerowych (Remailery, proxy, TOR, I2P, IPredator)
7. Cyberprzestrzeń: cyberszpiegostwo, cyberwywiad, cyberatak, cyberkontrola, cyberpolicja (opis z podaniem przykładów).
8. Zagrożenia: spam, phishing, spyware, phishing, stalking (opis z podaniem przykładów)
9. Bezpieczeństwo usług elektronicznych: bankowość elektroniczna, handel elektroniczny.
10. Bezpieczeństwo kart (płatnicze, smartcard): skimming, charge back, karty paypass, technologia RFID.
11. Wirtualizacja i przetwarzanie w chmurze a bezpieczeństwo przetwarzanych danych.
12. Kulturowe aspekty bezpieczeństwa systemów komputerowych.
13. Websecurity: XSS, CSRF,SQL Injection, SSL strip,
14. Websecurity: kradzież domen, Clickjacking, HTTP Session hijacking,
15. Test wielokrotnego wyboru będący weryfikacją zdobytej wiedzy, przygotowujący do egzaminu z przedmiotu.

Zajęcia laboratoryjne prowadzone są w formie 15 2-godzinnych ćwiczeń, odbywających się w laboratorium, Ćwiczenia realizowane są przez 2-osobowe zespoły studentów. Program laboratorium obejmuje zagadnienia omawiane na wykładach. Ponadto na ostatnich 2-3 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 pokazów multimedialny

Literatura podstawowa:

1. Hack Proofing Your Network. Edycja polska, praca zbiorowa, Helion, Gliwice, 2002

Literatura uzupełniająca:

1. Mity bezpieczeństwa IT, Viega J., Helion, Gliwice, 2012
2. Cisza w sieci, Zalewski M., Helion, Gliwice, 2005
3. Splątana sieć, Zalewski M., Helion, Gliwice, 2012

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. udział w zajęciach laboratoryjnych / ćwiczeniach	16
2. przygotowanie do ćwiczeń laboratoryjnych:	16
3. udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych / projektu	2
4. realizacja projektu (czas poza zajęciami laboratoryjnymi)	20
5. udział w wykładach	16
6. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi	10
7. przygotowanie do egzaminu i obecność na egzaminie: 18 godz. + 2 godz	20

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	100	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	36	1
Zajęcia o charakterze praktycznym	52	2