

<b>KARTA OPISU MODUŁU KSZTAŁCENIA</b>		
Nazwa modułu/przedmiotu <b>Bezpieczeństwo w Internecie Przedmiotów</b>		Kod <b>1010515331010510008</b>
Kierunek studiów <b>Informatyka</b>	Profil kształcenia (ogólnoakademicki, praktyczny) <b>ogólnoakademicki</b>	Rok / Semestr <b>2 / 3</b>
Ścieżka obieralności/specjalność <b>Aplikacje mobilne i wbudowane dla</b>	Przedmiot oferowany w języku: <b>polski</b>	Kurs (obligatoryjny/obieralny) <b>obligatoryjny</b>
Stopień studiów: <b>II stopień</b>	Forma studiów (stacjonarna/niestacjonarna) <b>niestacjonarna</b>	
Godziny Wykłady: <b>16</b> Ćwiczenia: - Laboratoria: <b>16</b> Projekty/seminaria: -		Liczba punktów <b>5</b>
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) <b>kierunkowy</b>		(ogólnouczelniany, z innego kierunku) <b>z danego kierunku</b>
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki <b>nauki techniczne</b>		Podział ECTS (liczba i %) <b>5 100%</b>
<b>Odpowiedzialny za przedmiot / wykładowca:</b>		
<p>dr inż. Tomasz Łukaszewski            email: Tomasz.Lukaszewski@put.poznan.pl            tel. 61 6652920            Instytut Informatyki            ul. Piotrowo 2, 60-965 Poznań</p>		
<b>Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:</b>		
1	<b>Wiedza:</b>	Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu sieci komputerowych, systemów operacyjnych, aplikacji internetowych i bezpieczeństwa systemów informatycznych.
2	<b>Umiejętności:</b>	Powinien posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł.
3	<b>Kompetencje społeczne</b>	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.
<b>Cel przedmiotu:</b>		
<ol style="list-style-type: none"> <li>Przekazanie studentom rozszerzonej wiedzy o systemach komputerowych, w zakresie bezpieczeństwa tych systemów.</li> <li>Rozwijanie u studentów umiejętności rozwiązywania problemów związanych z bezpieczeństwem w systemach komputerowych</li> </ol>		
<b>Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia</b>		
<b>Wiedza:</b>		
<ol style="list-style-type: none"> <li>ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie systemów operacyjnych, technologii sieciowych - [K_W4]</li> <li>ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce w zakresie ochrony danych i bezpieczeństwa systemów komputerowych - [K_W6]</li> <li>ma podbudowaną teoretycznie szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki, takimi jak: bezpieczeństwo systemów komputerowych - [K_W5]</li> <li>ma podstawową wiedzę o cyklu życia systemów informatycznych programowych - [K_W7]</li> <li>zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich z wybranego obszaru informatyki - [K_W8]</li> <li>rozumie zagrożenia związane z przestępczością elektroniczną i zna podstawowe oraz zaawansowane mechanizmy ochrony - [K_W9]</li> </ol>		
<b>Umiejętności:</b>		

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]
<b>Kompetencje społeczne:</b>
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]

<b>Sposoby sprawdzenia efektów kształcenia</b>
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 około 20 pytań. 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 i obronę przez studenta 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.
<b>Treści programowe</b>

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. Bezpieczeństwo haseł (tęczowe tablice, polityka 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. Kwestie prawne związane z wykorzystaniem systemów komputerowych: piractwo komputerowe, naruszenie praw autorskich, naruszenie dóbr osobistych.
4. Problematyka odzyskiwania danych z nośników elektronicznych
5. Prywatność i anonimowość: metody zachowania prywatności i anonimowości w systemach komputerowych (Remailery, proxy, TOR, I2P). Cyberprzestrzeń: cyberszpiegostwo, cyberatak. Zagrożenia: spam, phishing, spyware, phishing, stalking
6. Bezpieczeństwo usług elektronicznych: bankowość elektroniczna, handel elektroniczny.
7. Bezpieczeństwo kart (płatnicze, smartcard). Bezpieczeństwo technologii RFID.
8. Websecurity: XSS, CSRF, SQL Injection, SSL strip, kradzież domen, Clickjacking, HTTP Session hijacking,

Zajęcia laboratoryjne prowadzone są w formie 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-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, analiza przykładowych zagrożeń, dyskusja, praca w zespole

#### Literatura podstawowa:

1. Splątana sieć, Zalewski M., Helion, Gliwice, 2012
2. Bezpieczeństwo systemu e-commerce, czyli jak bez ryzyka prowadzić biznes w internecie, Kępa L., Tomasiak P., Dobrzyński S., Helion 2012.

#### Literatura uzupełniająca:

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

#### Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. udział w wykładach	16
2. udział w zajęciach laboratoryjnych	16
3. przygotowanie do zajęć laboratoryjnych	20
4. dokończenie (w ramach pracy własnej) ćwiczeń laboratoryjnych	14
5. realizacja projektu (czas poza zajęciami laboratoryjnymi)	26
6. udział w konsultacjach związanych z realizacją ćwiczeń laboratoryjnych i projektu (również drogą elektroniczną)	4
7. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), 100 stron	10
8. przygotowanie do egzaminu i obecność na egzaminie: 18 godz. + 2 godz.	20

#### Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	126	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	38	1
Zajęcia o charakterze praktycznym	42	2