

<b>KARTA OPISU MODUŁU KSZTAŁCENIA</b>		
Nazwa modułu/przedmiotu <b>Zarządzanie bezpieczeństwem systemów informatycznych</b>		Kod <b>1010331471010334974</b>
Kierunek studiów <b>Informatyka</b>	Profil kształcenia (ogólnoakademicki, praktyczny) <b>(brak)</b>	Rok / Semestr <b>4 / 7</b>
Ścieżka obieralności/specjalność <b>Bezpieczeństwo systemów informatycznych</b>	Przedmiot oferowany w języku: <b>polski</b>	Kurs (obligatoryjny/obieralny) <b>obligatoryjny</b>
Stopień studiów: <b>I stopień</b>	Forma studiów (stacjonarna/niestacjonarna) <b>stacjonarna</b>	
Godziny Wykłady: <b>2</b> Ćwiczenia: -    Laboratoria: -    Projekty/seminaria: <b>1</b>		Liczba punktów <b>5</b>
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) <b>(brak)</b>		(ogólnouczelniany, z innego kierunku) <b>(brak)</b>
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki <b>nauki techniczne</b>		Podział ECTS (liczba i %) <b>75 100%</b>

**Odpowiedzialny za przedmiot / wykładowca:**

dr inż. Anna Grocholewska-Czuryło  
email: anna.grocholewska-czurylo@put.poznan.pl  
tel. 61-665 35 31  
Wydział Elektryczny  
ul. Piotrowo 3A 60-965 Poznań

**Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:**

1	<b>Wiedza:</b>	K_W01: ma podstawową wiedzę w zakresie matematyki, obejmującą algebrę, analizę, logikę, probabilistykę oraz elementy matematyki dyskretnej i stosowanej K_W15: ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie podstaw teleinformatyki oraz protokołów i usług w sieciach telekomunikacyjnych
2	<b>Umiejętności:</b>	K_U01: potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie K_U02: potrafi pracować indywidualnie i w zespole; umie oszacować czas potrzebny na realizację zleconego zadania; potrafi opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminów
3	<b>Kompetencje społeczne</b>	K_K02: ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera-informatyka i związaną z tym odpowiedzialność za podejmowane decyzje

**Cel przedmiotu:**

W ramach przedmiotu studenci zapoznają się z projektowaniem systemów zarządzania bezpieczeństwem teleinformatycznym w nowoczesnej firmie, a więc w oparciu o normy i standardy, przeprowadzaniem analizy ryzyka i zaproponowaniem odpowiedniego doboru zabezpieczeń i metod reagowania na incydenty.

**Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia**

**Wiedza:**

1. ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie ochrony danych i bezpieczeństwa systemów informatycznych - [K\_W13: ]
2. ma podstawową wiedzę w zakresie administrowania systemami informatycznymi - [K\_W14: ]

**Umiejętności:**

1. potrafi zastosować odpowiednie metody ochrony danych i zapewnić bezpieczeństwo systemu informatycznego - [K\_U17: ]
2. potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania - [K\_U03: ]

**Kompetencje społeczne:**

1. ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera-informatyka i związaną z tym odpowiedzialność za podejmowane decyzje - [K\_K02: ]

**Sposoby sprawdzenia efektów kształcenia**

Przedmiot zaliczany jest na podstawie egzaminu pisemnego, ustnego lub pisemnego i ustnego, oraz projektu.		
<b>Treści programowe</b>		
Klasyfikacja zagrożeń zarówno sieciowych, kryptograficznych jak i eksploatacyjnych systemów komputerowych. Analiza i zarządzanie ryzykiem. Definiowanie oraz dyskusja nad sposobami osiągnięcia i utrzymywania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności. W oparciu o normy i zalecenia projektowanie i eksploatacja takich systemów. Na podstawie znajomości z wcześniejszych przedmiotów mechanizmów ochrony, projektowanie zintegrowanych systemów zarządzania bezpieczeństwem. W ramach przedmiotu, studenci wykonują projekty składowych systemu zarządzania bezpieczeństwem.		
<b>Literatura podstawowa:</b>		
1. 1. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Białas A., WNT, Warszawa 2006		
2. 2. Teoria bezpieczeństwa systemów komputerowych, Pieprzyk J., Hardjono T., Seberry J., Helion, 2003		
<b>Literatura uzupełniająca:</b>		
1. 11. Firewalli i bezpieczeństwo w sieci (Firewalls and Internet Security), Chestwick W. R. , Bellovin S.M. , Rubin A.D., Helion, Gliwice, 2003		
<b>Bilans nakładu pracy przeciętnego studenta</b>		
<b>Czynność</b>	<b>Czas (godz.)</b>	
1. Uczestnictwo w wykładach	30	
2. Udział w zajęciach projektowych	15	
3. Wykonanie projektu	40	
4. Udział w konsultacjach	15	
5. Przygotowanie do egzaminu.	15	
<b>Obciążenie pracą studenta</b>		
<b>forma aktywności</b>	<b>godzin</b>	<b>ECTS</b>
Łączny nakład pracy	115	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	35	1
Zajęcia o charakterze praktycznym	40	2