

<b>KARTA OPISU MODUŁU KSZTAŁCENIA</b>		
Nazwa modułu/przedmiotu <b>Zarządzanie bezpieczeństwem systemów informatycznych</b>		Kod <b>1010334591010334974</b>
Kierunek studiów <b>Informatyka</b>	Profil kształcenia (ogólnoakademicki, praktyczny) <b>(brak)</b>	Rok / Semestr <b>5 / 9</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>niestacjonarna</b>	
Godziny Wykłady: <b>16</b> Ćwiczenia: - Laboratoria: - Projekty/seminaria: <b>8</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>5 100%</b>
<b>Odpowiedzialny za przedmiot / wykładowca:</b>		
<p>dr inż. Anna Grocholewska-Czuryło            email: <a href="mailto:anna.grocholewska-czurylo@put.poznan.pl">anna.grocholewska-czurylo@put.poznan.pl</a>            tel. 061 66 53 531            Wydział Elektryczny            ul. Piotrowo 3A, 60-965 Poznań</p>		
<b>Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:</b>		
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
<b>Cel przedmiotu:</b>		
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.		
<b>Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia</b>		
<b>Wiedza:</b>		
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]		
<b>Umiejętności:</b>		
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]		
<b>Kompetencje społeczne:</b>		
1. ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera-informatyka i związaną z tym odpowiedzialność za podejmowane decyzje - [K_K02]		
<b>Sposoby sprawdzenia efektów kształcenia</b>		
Przedmiot zaliczany jest na podstawie egzaminu pisemnego, ustnego lub pisemnego i ustnego, oraz projektu.		

<b>Treści programowe</b>		
<p>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.</p>		
<p><b>Literatura podstawowa:</b></p> <ol style="list-style-type: none"> <li>1. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Białas A., WNT, Warszawa 2006</li> <li>2. Teoria bezpieczeństwa systemów komputerowych, Pieprzyk J., Hardjono T., Seberry J., Helion, 2003</li> </ol>		
<p><b>Literatura uzupełniająca:</b></p> <ol style="list-style-type: none"> <li>1. Firewall i bezpieczeństwo w sieci (Firewalls and Internet Security), Chestwick W. R. , Bellovin S.M. , Rubin A.D., Helion, Gliwice, 2003 (Addison-Wesley, 2003)</li> <li>2. Normy ISO (13335, 2700x)</li> </ol>		
<b>Bilans nakładu pracy przeciętnego studenta</b>		
<b>Czynność</b>	<b>Czas (godz.)</b>	
1. Udział w wykładach	16	
2. Udział w projekcie	8	
3. Przygotowanie do egzaminu	16	
4. Przygotowanie do projektu = opracowanie projektu	16	
5. Egzamin	2	
6. Konsultacje	2	
<b>Obciążenie pracą studenta</b>		
<b>forma aktywności</b>	<b>godzin</b>	<b>ECTS</b>
Łączny nakład pracy	60	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	44	3
Zajęcia o charakterze praktycznym	28	2