

<b>KARTA OPISU MODUŁU KSZTAŁCENIA</b>		
Nazwa modułu/przedmiotu <b>Polityka bezpieczeństwa</b>		Kod <b>1010332521010337164</b>
Kierunek studiów <b>Informatyka</b>	Profil kształcenia (ogólnoakademicki, praktyczny) <b>(brak)</b>	Rok / Semestr <b>1 / 2</b>
Ścieżka obieralności/specjalność <b>Technologie informatyczne</b>	Przedmiot oferowany w języku: <b>polski</b>	Kurs (obligatoryjny/obieralny) <b>obieralny</b>
Stopień studiów: <b>II stopień</b>	Forma studiów (stacjonarna/niestacjonarna) <b>stacjonarna</b>	
Godziny Wykłady: <b>30</b> Ćwiczenia: - Laboratoria: <b>15</b> Projekty/seminaria: -		Liczba punktów <b>4</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>4 100%</b>
<b>Odpowiedzialny za przedmiot / wykładowca:</b>		
dr inż. Tomasz Bilski email: tomasz.bilski@put.poznan.pl tel. 061 66 53 554 Wydział Elektryczny ul. Piotrowo 3A 60-965 Poznań		
<b>Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:</b>		
<b>1</b>	<b>Wiedza:</b>	ma wiedzę odpowiadającą studiom pierwszego stopnia  K_W02: ma poszerzoną i pogłębioną wiedzę w zakresie wybranych zagadnień prawa  K_W10: ma pogłębioną wiedzę w zakresie bezpieczeństwa danych
<b>2</b>	<b>Umiejętności:</b>	K_U01: potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie  K_U11: potrafi ocenić przydatność narzędzi i technologii informatycznych w realizacji konkretnego zadania informatycznego
<b>3</b>	<b>Kompetencje społeczne</b>	ma kompetencje odpowiadające studiom pierwszego stopnia
<b>Cel przedmiotu:</b>		
Opanowanie praktycznych umiejętności definiowania dokumentów polityki bezpieczeństwa informacyjnego zgodnie z wymaganiami prawnymi.		
<b>Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia</b>		
<b>Wiedza:</b>		
1. ma poszerzoną i pogłębioną wiedzę w zakresie wybranych zagadnień prawa - [K_W02] 2. ma pogłębioną, podbudowaną teoretycznie wiedzę w zakresie modelowania i analizy systemów informatycznych - [K_W05] 3. ma pogłębioną wiedzę w zakresie bezpieczeństwa danych - [K_W10]		
<b>Umiejętności:</b>		
1. potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie - [K_U01] 2. potrafi modelować i analizować systemy informatyczne - [K_U05] 3. potrafi ocenić przydatność narzędzi i technologii informatycznych w realizacji konkretnego zadania informatycznego - [K_U11]		
<b>Kompetencje społeczne:</b>		

1. potrafi myśleć i działać w sposób kreatywny i przedsiębiorczy - [K\_K01]
2. rozumie potrzebę przekazywania społeczeństwu informacji dotyczących osiągnięć informatyki i innych aspektów działalności inżyniera-informatyka; podejmuje starania, aby przekazać informacje w sposób zrozumiały, przedstawiając różne punkty widzenia - [K\_K02]

### Sposoby sprawdzenia efektów kształcenia

#### Wykład

Kolokwium zaliczeniowe w formie pisemnej, w ostatnim tygodniu zajęć, 8 pytań. Na ocenę pozytywną trzeba uzyskać ponad połowę wszystkich punktów.

Punktacja poszczególnych odpowiedzi:

3 pkt ? odpowiedź wyczerpująca, bez błędów merytorycznych

2 pkt ? odpowiedź z jednym mniej ważnym błędem lub niepełna (ale zawierająca większość wymaganych informacji)

1 pkt ? odpowiedź z większą liczbą mniej ważnych błędów, ogólnikowa lub niepełna (niezawierająca większości wymaganych informacji)

0 pkt ? brak odpowiedzi lub poważne błędy merytoryczne w odpowiedzi

#### Oceny:

Max 3 pkt za każdą odpowiedź (łącznie 24 pkt)

Punkty ujemne za wszelkie próby nieuczciwego zaliczenia

Ocena pozytywna od 13 pkt

13-14 pkt ? dostateczny

15-17 pkt ? dostateczny plus

18-19 pkt ? dobry

20-22 pkt ? dobry plus

23-24 pkt ? bardzo dobry

Laboratorium: Zaliczenie na ocenę na podstawie dokumentacji zrealizowanego projektu polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym.

### Treści programowe

#### Wykład.

Modele, procesy i etapy zarządzania bezpieczeństwem informacyjnym. Elementy składowe polityki bezpieczeństwa (w tym instrukcja zarządzania systemem informatycznym, analiza ryzyka, plan odtwarzania po awarii). Ogólne zasady kształtowania polityki bezpieczeństwa. Bezpieczeństwo osobowe: odpowiedzialność, systemy certyfikacji specjalistów (np. CISSP). Zarządzanie ryzykiem w systemach informatycznych. Ilościowa i jakościowa analiza ryzyka. Różne metody oddziaływania na ryzyko. Planowanie awaryjne, odtwarzanie stanu po awarii (RTO, RPO), zarządzanie ciągłością działania firmy. Technologie dla odtwarzania stanu i zarządzania ciągłością działania: systemy kopii zapasowych, zapasowe systemy informatyczne (cold site, hot site), maszyny wirtualne, cloud computing, cloud storage. Rozwiązania przykładowe. Wymagania odnośnie polityki bezpieczeństwa zawarte w aktach prawnych i normatywnych (w tym w Ustawie o ochronie danych osobowych, ISO 27xxx, ISO 13335, ...).

Aktualizacja treści 2017: nowe rozporządzenie UE w sprawie ochrony danych osobowych.

Stosowane metody kształcenia:

- wykład z prezentacją multimedialną (w tym: rysunki, zdjęcia, animacje),

? wykład prowadzony w sposób interaktywny z formułowaniem pytań d grupy studentów,

? wykład uzupełniony materiałami do samodzielnego studiowania w systemie Moodle.

#### Laboratorium.

Zbieranie danych, dyskusje, prezentacje. Opracowanie założeń (w tym analiza ryzyka), dokumentów (w tym planów awaryjnych i planów odtwarzania po awarii), harmonogramu wdrażania polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym dla konkretnego systemu informatycznego (zgodnie z wymaganiami Ustawy o ochronie danych osobowych). Oszacowanie kosztów.

#### Literatura podstawowa:

1. A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2007
2. Grocholski L., Niemiec A., Wdrożenie procesu zarządzania ryzykiem w dużej firmie informatycznej, w: Inżynieria oprogramowania - metody wytwarzania i wybrane zastosowania, PWN, Warszawa, 2008.
3. Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, 2009.
4. Rozporządzenie UE w sprawie ochrony danych osobowych

<b>Literatura uzupełniająca:</b> 1. Bilski T., Wprowadzenie do ochrony danych, Wyd. WSKiZ, Poznań, 2005. 2. Normy ISO (13335, 2700x)		
<b>Bilans nakładu pracy przeciętnego studenta</b>		
<b>Czynność</b>	<b>Czas (godz.)</b>	
1. Udział w wykładach	30	
2. Udział w laboratoriach	30	
3. Przygotowanie do kolokwium zaliczeniowego	30	
4. Przygotowanie do laboratorium=opracowanie projektu	45	
5. Kolokwium zaliczeniowe	2	
6. Konsultacje	13	
<b>Obciążenie pracą studenta</b>		
<b>forma aktywności</b>	<b>godzin</b>	<b>ECTS</b>
Łączny nakład pracy	125	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	75	3
Zajęcia o charakterze praktycznym	75	3