KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Zarządzanie bezpieczeństwem systemów informatycznych	**1010331571010334974**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**(brak)**	**4 / 7**

Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
Bezpieczeństwo systemów informatycznych	**polski**	**obligatoryjny**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)
I stopień	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **30** Ćwiczenia: **-** Laboratoria: **-** Projekty/seminaria: **15**	**5**

Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny)	(ogólnouczelniany, z innego kierunku)
(brak)	**(brak)**

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**
nauki techniczne	**5 100%**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Anna Grocholewska-Czuryło
email: anna.grocholewska-czurylo@put.poznan.pl
tel. 061 66 53 531
Wydział Elektryczny
ul. Piotrowo 3A, 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	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	**Umiejętności:**	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	**Kompetencje społeczne**	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.

Treści programowe

Zastosowane metody kształcenia: wykłady - wykład prowadzony w sposób interaktywny z formułowaniem pytań do grupy studentów lub do wskazywanych konkretnych studentów, uwzględnia się aktywność studentów w czasie zajęć przy wystawianiu oceny końcowej, w trakcie wykładu inicjowanie dyskusji; projekt - szczegółowe recenzowanie dokumentacji projektowej przez prowadzącego projekt i dyskusje nad komentarzami, praca w zespołach dwu osobowych.

Treści wykładów: klasyfikacja zagrożeń zarówno sieciowych, kryptograficznych jak i eksploatacyjnych systemów komputerowych. Analiza i zarządzanie ryzykiem. Definiowanie oraz dyskusja nad sposobami osiągania 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. Aktualizacja 2017: Bezpieczny system w praktyce, testy penetracyjne.

Projekt (aktualizacja 2017):

Opracowanie projektu oraz dokumentacji systemu zarządzania bezpieczeństwa w wybranym środowisku uwzględniając inwentaryzację zasobów IT, typ przetwarzanych danych (analiza systemu pod kątem wymagań GIODO).

Literatura podstawowa:

1. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Białas A., WNT, Warszawa 2006
2. Teoria bezpieczeństwa systemów komputerowych, Pieprzyk J., Hardjono T., Seberry J., Helion, 2003

Literatura uzupełniająca:

1. Normy ISO (13335, 2700x)
2. Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne, Weidman G., Helion 2014.

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Udział w wykładach	30
2. Udział w projekcie	15
3. Przygotowanie do egzaminu	30
4. Przygotowanie do projektu = opracowanie projektu	30
5. Egzamin	2
6. Konsultacje	13

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	120	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	3
Zajęcia o charakterze praktycznym	45	2