Zarządzanie strategiczne bezpieczeństwem systemów informacyjnych - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Zarządzanie strategiczne bezpieczeństwem systemów informacyjnych
Kod przedmiotu	11.9-WZ-BezD- ZSBSI-S16
Wydział	Wydział Ekonomii i Zarządzania
Kierunek	Bezpieczeństwo narodowe / Bezpieczeństwo publiczne
Profil	praktyczny
Rodzaj studiów	drugiego stopnia z tyt. magistra
Semestr rozpoczęcia	semestr zimowy 2016/2017

Informacje o przedmiocie

Semestr	3
Liczba punktów ECTS do zdobycia	2
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• dr Sławomir Kotylak

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	15	1	9	0,6	Zaliczenie na ocenę
Ćwiczenia	15	1	9	0,6	Zaliczenie na ocenę

Cel przedmiotu

Przekazanie wiedzy z zakresu podstawowych pojęć informatycznych systemów bezpieczeństwa i zabezpieczeń. Definiowanie pojęć informatycznych z obszaru bezpieczeństwa informatycznego danych i informacji. Scharakteryzowanie metod zabezpieczeń danych i informacji. Wytłumaczenie zakresu i etapów projektowania strategii bezpieczeństwa systemów informatycznych. Kształtowanie umiejętność posługiwania się systemami zabezpieczeń przed zagrożeniami ataków z wykorzystaniem systemów informatycznych. Identyfikacja czynników wpływających na zwiększenie bezpieczeństwa systemów informacyjnych organizacji. Przedstawienie metodologii opracowania strategii bezpieczeństwa informatycznego dla systemów bezpieczeństwa publicznego. Szyfrowanie danych i bezpieczny obieg informacji. Kształtowanie umiejętności współpracy w grupie.

Wymagania wstępne

Uzyskanie zaliczenia na min ocenę dostateczną z przedmiotów: technologie informacyjne

Zakres tematyczny

Wykład:

1. Wprowadzenie
2. Proces zarządzania strategicznego (aspekt Teoretyczny).
3. Ocena jakości systemów informacyjnych (aspekt eksploatacyjny).
4. Czynnik ludzki w zapewnieniu jakości eksploatacji zasobów informatycznych - Zarządzanie personelem IT przedsiębiorstwa.
5. Czynnik ludzki w zapewnieniu jakości eksploatacji zasobów informatycznych - Organizacja współpracy z użytkownikiem.
6. Czynnik ludzki w zapewnieniu jakości eksploatacji zasobów informatycznych - Standard I T I L.
7. Wybrane metody oceny zagrożeń technicznych.
8. Regulacje miedzynarodowe dotyczace bezpieczeństwa systemów IT.

Ćwiczenia:

1. Znaczenie zarządzania bezpieczeństwem informacji dla współczesnej gospodarki.
2. Budowa i wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji.
3. Audyt systemów informacyjnych.
4. Analiza i zarządzanie ryzykiem systemów informatycznych.
5. Zarządzanie bezpieczeństwem systemów informatycznych (SI).
6. Identyfikacja zagrożeń systemowych.
7. Identyfikacja zagrożeń technicznych.
8. Aspekty i wymogi prawne dotyczące bezpieczeństwa informacji.

Metody kształcenia

Wykład: wykład konwencjonalny, dyskusja, pokaz

Ćwiczenia: Praca z wykorzystaniem komputerów, dyskusje grupowe, burza mózgów, giełda pomysłów, prace indywidualne, prace grupowe, metoda projektu, studia przypadków,

klasyczna metoda problemowa, studia literatury, praca z tekstem, praca zaliczeniowa.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Posiada pogłębioną wiedzę o znaczeniu i uwarunkowaniach bezpieczeństwa narodowego w skali lokalnej, regionalnej, narodowej i globalnej, strukturach i instytucjach bezpieczeństwa, relacjach między nimi, zna współczesne koncepcje bezpieczeństwa, rozumie rolę kultury strategicznej i edukacji w praktycznym tworzeniu strategii bezpieczeństwa narodowego.	• K_W02	• egzamin - ustny, opisowy, testowy i inne • kolokwium • odpowiedź ustna • projekt	• Wykład • Ćwiczenia
Potrafi właściwie analizować przesłanki i przebieg konkretnych działań w ramach zarządzania kryzysowego, prognozować i modelować złożone procesy zachodzące w systemie bezpieczeństwa narodowego oraz ich praktyczne skutki obejmujące zjawiska z różnych obszarów życia społecznego z wykorzystaniem zaawansowanych metod i narzędzi właściwych dla kierunku studiów bezpieczeństwo narodowe.	• K_W04	• egzamin - ustny, opisowy, testowy i inne • kolokwium • projekt	• Wykład • Ćwiczenia
Jest przygotowany do praktycznego uczestnictwa w grupach, projektach, organizacjach i instytucjach realizujących działania na rzecz bezpieczeństwa i zdolny do porozumiewania się z osobami będącymi i niebędącymi specjalistami w danej dziedzinie oraz przewidywania skutków swoich decyzji w obszarze szeroko rozumianego bezpieczeństwa.	• K_W05	• kolokwium • projekt	• Wykład • Ćwiczenia

Warunki zaliczenia

Wykład: egzamin pisemny, który będzie obejmować materiał z wykładów. Egzamin będzie w formie pytań testowych. Warunkiem otrzymania zaliczenia jest uzyskanie min. 75% prawidłowych odpowiedzi z pytań podczas egzaminu. Termin egzaminu: zgodnie z harmonogramem studiów w sesji

Oceny (punktacja):75%- 80% - dostateczny (3.0), 81%-85% - dostateczny plus (3.5), 86%-90% - dobry (4.0), 91%-95% - dobry plus (4.5), 96%-100% - bardzo bobry (5.0)

Ćwiczenia: na ocenę składać się będą oceny z: kolokwium, które będą obejmować pytania otwarte i od 2-3 pytań problemowych, projektu dotyczącego wybranego problemu dla danego typu systemów informacyjnych oraz zadań do samodzielnego rozwiązania.

Termin zaliczenia kolokwium: zgodnie z harmonogramem studiów. Termin ostatecznego oddania projektu upływa na przedostatnich zajęciach dydaktycznych w semestrze zimowym, projekt oceniany będzie w skali od 2 do 5. Warunkiem otrzymania zaliczenia kolokwium jest uzyskanie min. 51%.

Oceny (punktacja): 51%- 60% - dostateczny (3.0), 61%-70% - dostateczny plus (3.5), 71%-80% - dobry (4.0), 81%-85% - dobry plus (4.5), 86%-100% - bardzo bobry (5.0)

Literatura podstawowa

1. Terlikowski M., Madej M., (red), *Bezpieczeństwo teleinformatyczne państwa,* Polski Instytut Spraw Międzynarodowych, Warszawa 2009.
2. Niczyporuk Z., Sienkiewicz-Małyjurek K., *Systemy monitoringu wizyjnego w bezpieczeństwie publicznym,* Wydawnictwo Politechniki Śląskiej, Katowice 2008.
3. Stokłosa J., Bilski T., Pankowski T., Bezpie*czeństwo danych w systemach informatycznych*, Warszawa PWN, 2001

Literatura uzupełniająca

1. Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, Wydawnictwo Adam Marszałek,* Toruń 2008
2. Fahler W., (red), *Bezpieczeństwo publiczne w przestrzenie miejskiej,* Warszawa 2010.

Uwagi

Brak

Zmodyfikowane przez dr Paweł Szudra (ostatnia modyfikacja: 22-09-2016 08:01)