KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Zarządzanie bezpieczeństwem systemów informatycznych

Przedmiot

Kierunek studiów

Inżynieria Zarządzania

Rok/semestr

3/6

Studia w zakresie (specjalność)

Profil studiów

ogólnoakademicki

Poziom studiów

pierwszego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obieralny

Liczba godzin

Wykład

15

Laboratoria

Inne (np. online)

Ćwiczenia

15

Projekty/seminaria

Liczba punktów ECTS

2

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Maciej Siemieniak

email: maciej.siemieniak@put.poznan.pl

Wydział Inżynierii Zarządzania

ul. J. Rychlewskiego 2, 60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę nt. systemów informatycznych i informacyjnych. Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

Cel przedmiotu

Przekazanie studentom podstawowej wiedzy z zakresu bezpieczeństwa informacji i systemów informatycznych, niezbędnych do prawidłowego projektowania, zarządzania i usprawniania systemów bezpieczeństwa teleinformatycznego. Rozwijanie u studentów umiejętności rozwiązywania problemów bezpieczeństwa informacji i systemów informatycznych.

Przedmiotowe efekty uczenia się

Wiedza

1. ma rozszerzoną i pogłębioną wiedzę w zakresie nauk niezbędnych dla zrozumienia i opisania problematyki zarządzania bezpieczeństwem informacji i systemów informatycznych w organizacjach.

2. ma podstawową wiedzę o cyklu życia informacji i systemów społeczno-technicznych.

3. ma podstawową wiedzę dotyczącą organizacji i zarządzania bezpieczeństwem informacji i systemów informatycznych w organizacji, dotyczącą zarządzania jakością i prowadzenia działalności gospodarczej.

Umiejętności

1. potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe dotyczące bezpieczeństwa informacji, interpretować uzyskane wyniki i wyciągać wnioski o poziomie bezpieczeństwa systemów informatycznych.

2. potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich metody analityczne, symulacyjne oraz eksperymentalne.

3. potrafi, przy formułowaniu i rozwiązywaniu zadań inżynierskich, dostrzegać ich aspekty systemowe, społeczno-techniczne, organizacyjne, ekonomiczne i pozatechniczne.

Kompetencje społeczne

1. ma świadomość, że kreowanie działań zaspokajających potrzeby bezpieczeństwa informacji i systemów informatycznych w organizacji wymaga podejścia systemowego z uwzględnieniem zagadnień technicznych, ekonomicznych, marketingowych, prawnych, organizacyjnych i finansowych.

2. ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta na wykładach weryfikowana jest przez jedno kolokwium, które odbywa się na ostatnich zajęciach. Kolokwium składa się z 10 pytań testowych różnie punktowanych. Próg zaliczeniowy: 50% prawidłowych odpowiedzi. Zagadnienia zaliczeniowe obejmują wyłącznie materiał z wykładów.

Na ćwiczeniach studenci pracują w grupach nad zadanymi tematami, które prezentują w formie prezentacji multimedialnej. Za każde z 7. zadań studenci otrzymują oceny (7 ocen). Ocena końcowa jest średnią z tych 7. ocen. Treść zadań związana jest z przedmiotem, a zakres zadań obejmuje zagadnienia z wykładów.

Treści programowe

Wykłady:

1. bezpieczeństwo informacji (znaczenie i definicje informacji, cykl życia informacji, istota bezpieczeństwa informacji, pojęcia związane z bezpieczeństwem informacji, incydenty, elementy bezpieczeństwa informacji, ewolucja systemu zarządzania bezpieczeństwem informacji (ISMS), standardy ISMS, polityka ISMS w organizacji, model ISMS, ryzyko, wdrożenie ISMS w organizacji, metody szacowania ryzyka).

2. bezpieczeństwo systemów informatycznych (pojęcia, definicje, odniesienie do bezpieczeństwa informacji, atrybuty bezpieczeństwa, strategie zarządzania ryzykiem i jego redukcji, trójpoziomowy model odniesienia, model hierarchi zasobów, strategia wyboru zabezpieczeń, czynności wdożeniowe i powdrożeniowe).

Zajęcia ćwiczeniowe:

Prowadzący:

Istota narzędzi i sposób wykonania zadań dla poniższych tematów: mapa myśli, diagram Ishikawy, drzewo błędów i zdarzeń, diagram przepływu, mini wykład o maxi sprawach, wykład z przedmiotu;

Studenci:

1. mapa myśli dla pojęcia "informacja" - prezentacja multimedialna lub graficzna (plakat) z omówieniem;

2. diagram Ishikawy dla problemu "nieuprawniony dostęp do danych lub informacji w przedsiębiorstwie" (rodzaj danych/informacji dowolny: finansowe, osobowe, technologiczne, produkcyjne, badanie i rozwój, strategii sprzedaży, itp.) - prezentacja multimedialna lub graficzna (plakat) z omówieniem;

3. drzewo błędów i zdarzeń dla zdarzenia "skradziono laptop z samochodu prezesa" - prezentacja multimedialna z omówieniem;

4. diagram przepływu - na podstawie tekstu opisującego proces wprowadzania danych do systemu IT (algorytm, procesy decyzyjne, działania, wykonawcy) - prezentacja multimedialna z omówieniem;

5. mini wykład o maxi sprawach - prezentacja multimedialna w formie wykładu/odczytu (kryptologia, przestępczość komputerowa, cyberterroryzm, spam, łańcuszek internetowy, hacker, cracker, złośliwe oprogramowanie - profilaktyka i zabezpieczenia, zagrożenia w internecie - ochrona, zapobieganie, najpopularniejsze serwisy społecznościowe - negatywne zjawiska, jak bezpiecznie z nich korzystać, bezpieczne zakupy w internecie, bezpieczne logowanie, bezpieczne hasła);

6. zarządzanie bezpieczeństwem systemów informatycznych - prezentacja multimedialna w formie wykładu/odczytu (zarys problemu, najważniejsze zagadnienia, na podstawie wykładów);

Metody dydaktyczne

Wykłady: prezentacja multimedialna - tekst, rysunki, schematy, tabele, przykłady wyjaśniające, krótka rozmowa ze studentami.

Ćwiczenia: prowadzący - prezentacja multimedialna, studenci - prezentacja multimedialna, graficzna (plakat), krótki wykład, odczyt.

Literatura

Podstawowa

1. Jacek Łuczak, Marcin Tyburski, Systemowe zarządzanie bezpieczeństwem informacji. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Poznań 2010.

2. Andrzej Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Wydawnictwo naukowo-techniczne, Warszawa 2006, 2007.

Uzupełniająca

1. Andrzej Borucki, Gospodarka elektroniczna. Wydawnictwo Politechniki Poznańskiej, 2013.

2. Andrzej Borucki, E-biznes. Wydawnictwo Politechniki Poznańskiej, 2012.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	60	2,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,0
Praca własna studenta (studia literaturowe, przygotowanie do ćwiczeń, przygotowanie do kolokwiów)[1]	30	1,0

[1] niepotrzebne skreślić lub dopisać inne czynności