



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Zarządzanie ryzykiem w systemach informatycznych [N2Inf1>ZRYZ]

Przedmiot

Kierunek studiów
Informatyka

Rok/Semestr
2/4

Studia w zakresie (specjalność)
Aplikacje mobilne i wbudowane dla Internetu
Przedmiotów

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
niestacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
16

Laboratorium
0

Inne
0

Ćwiczenia
12

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

dr inż. Tomasz Bilski
tomasz.bilski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę w zakresie budowy i funkcjonowania systemów informatycznych. Powinien mieć wiedzę w zakresie architektury systemów komputerowych, zasad działania systemów operacyjnych, sieci komputerowych, podstaw ochrony danych.

Cel przedmiotu

Przekazanie studentom wiedzy z zakresu modeli, standardów, etapów procesów zarządzania ryzykiem w systemach informatycznych. Przekazanie umiejętności zarządzania ryzykiem w przykładowych systemach informatycznych.

Przedmiotowe efekty uczenia się

Wiedza:

Student/ka ma szczegółową wiedzę na temat:

- etapów procesu zarządzania ryzykiem,
- modeli analizy ryzyka,
- parametrów używanych w analizie ryzyka,

- psychologii ryzyka.

Umiejętności:

Student/ka potrafi:

- wybrać właściwy model analizy ryzyka,
- przeprowadzić analizę ryzyka w przykładowym systemie informatycznym
- wybrać właściwe metody oddziaływania na ryzyko,

Kompetencje społeczne:

Student/ka rozumie:

- przyczyny i konsekwencje popełniania błędów poznawczych,
- psychologiczne aspekty ryzyka.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana podczas 45-minutowego kolokwium obejmującego teorię, odbywającego się na ostatnim wykładzie. Kolokwium składa się z 8 pytań. Próg zaliczeniowy: ponad 50% punktów. Umiejętności nabyte w ramach zajęć ćwiczeniowych weryfikowane są na bieżąco podczas zajęć oraz podczas kolokwium końcowego obejmującego zadania praktyczne na ostatnich zajęciach. Próg zaliczeniowy: ponad 50% punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania są przesyłane studentom pocztą elektroniczną na początku semestru.

Treści programowe

Moduł obejmuje następujące zagadnienia:

1. Wprowadzenie.
2. Wymagania prawne
3. Etapy procesu zarządzania ryzykiem
4. Analiza ryzyka.
5. Oddziaływanie na ryzyko.
6. Psychologia ryzyka.

Tematyka zajęć

Wykład obejmuje następujące zagadnienia

1. Wprowadzenie
2. Wymagania prawne, standardy
3. Proces zarządzania ryzykiem
4. Analiza ryzyka. Najważniejsze etapy procesu, w tym: etap wstępny, identyfikacja zagrożeń, identyfikacja podatności, wyznaczenie prawdopodobieństw, wyznaczenie skutków i wyznaczenie ryzyka. Metody analizy ryzyka (ilościowa, jakościowa i półilościowa). Parametry i sposoby ich wyznaczania: wartość zasobu AV (asset value), współczynnik narażenia EF (exposure factor), współczynnik strat wynikających z pojedynczego naruszenia bezpieczeństwa SLE (single loss expectancy), roczny współczynnik wystąpień ARO (annual rate of occurrence), oczekiwany roczny współczynnik strat ALE (annual loss expectancy), współczynnik zwrotu z inwestycji w bezpieczeństwo ROSI (risk on security investment). Wady i zalety każdej z trzech metod analizy ryzyka.
5. Oddziaływanie na ryzyko. Metody, ograniczenia.
6. Psychologia ryzyka. Sytuacyjne i indywidualne czynniki percepcji ryzyka. Błędy poznawcze i ich wpływ na podejmowane decyzje, błędy w przekonaniach i ocenie prawdopodobieństwa (w tym: paradoks hazardzisty, tzw. „gorąca ręka”, błąd koniunkcji, efekt pewności, teoria kompensacji ryzyka, polaryzacja grupowa).

Ćwiczenia

W ramach ćwiczeń studenci przeprowadzają analizę ryzyka w wybranych, konkretnych systemach informatycznych.

Metody dydaktyczne

Wykład prowadzony w sposób interaktywny (z formułowaniem pytań do studentów) przy użyciu

prezentacji multimedialnych. Materiały udostępniane studentom w wersji elektronicznej. Ćwiczenia prowadzone w formie tablicowej. Zadania wykonywane przez studentów indywidualnie i zespołach przy użyciu sprzętu komputerowego, narzędzi programistycznych oraz Internetu.

Literatura

Podstawowa

T. Bilski, Problemy społeczne i zawodowe informatyki, Poznań: Wydawnictwo Politechniki Poznańskiej, 2018 (Sygnatura w Bibliotece PP: W 171571).

K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa, 2009 (Sygnatura w Bibliotece PP: W 119656).

J. Łuczak, M. Tyburski, Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Wyd. Uniwersytetu Ekonomicznego, Poznań, 2010 (sygnatura w Bibliotece PP: A 167841).

J. Krawiec, A. Stefaniak, System Zarządzania Bezpieczeństwem Informacji w praktyce : zasady wyboru zabezpieczeń, Polski Komitet Normalizacyjny, Warszawa, 2011 (sygnatura w Bibliotece PP: CzO 174604).

Uzupełniająca

T. Polaczek, Audyt bezpieczeństwa informacji w praktyce : praktyczny przewodnik po zagadnieniach ochrony informacji, Helion, Gliwice, 2006.

D. J. Landoll, The security risk assessment handbook : a complete guide for performing security risk assessments, Boca Raton, FL : CRC Press, cop. 2011.

T. Bilski, Quantitative Risk Analysis for Data Storage Systems, 20th International Conference, CN 2013 Proceedings, [A. Kwiecień, P. Gaj, P. Stera, Editors] Communications in Computer Science and Information Science 370, Springer Verlag, Heidelberg, 2013, s. 124-135.

T. Bilski, Some Remarks Related to Human Behaviour Impact on Data Protection Processes, Information Systems Architecture and Technology [Editors L. Borzemski, A. Grzech, J. Świątek, Z. Wilimowska] Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2014, s. 89–98.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	78	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	28	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	50	2,00