KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Cyberbezpieczeństwo w pojazdach [S2Elmob1>CwP]

Przedmiot

Kierunek studiów
Elektromobilność

Rok/Semestr
2/3

Studia w zakresie (specjalność)
Systemy przetwarzania energii

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
15

Laboratorium
0

Inne (np. online)
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

1,00

Koordynatorzy

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie zaawansowanych systemów teleinformatycznych w pojazdach, komputerowego wspomagania projektowania układów elektronicznych oraz metod gromadzenia i analizy danych oraz wizualizacji wyników. Student ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie podstaw teleinformatyki, protokołów i usług w sieciach telekomunikacyjnych. Student 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. Student potrafi pracować indywidualnie i w zespole. Student ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera i związaną z tym odpowiedzialność za podejmowane decyzji. Powinien również rozumieć konieczność poszerzania swoich kompetencji. Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu

W ramach przedmiotu studenci zapoznają się z problematyką zarządzania bezpieczeństwem teleinformatycznym w firmie lub instytucji, a więc w oparciu o normy i standardy, sposobami przeprowadzania analizy ryzyka i odpowiednim doborem zabezpieczeń (minimalizujących prawdopodobieństwo i/lub skutki zagrożeń), metod reagowania na incydenty oraz przywracania systemu informatycznego do stanu sprzed incydentu.

Przedmiotowe efekty uczenia się

Wiedza:
Ma podstawową wiedzę w zakresie ochrony danych, bezpieczeństwa systemów informatycznych, analizy ryzyka oraz modelowania zagrożeń w systemach informatycznych pojazdów.

Umiejętności:
Potrafi, przy formułowaniu i rozwiązywaniu zadań inżynierskich, uwzględnić nieprzewidywalne warunki, zadaną specyfikację techniczną oraz kryteria pozatechniczne zapewniając oszczędności surowców i energii oraz bezpieczeństwo systemów informatycznych pojazdów elektrycznych

Kompetencje społeczne:
Rozumie, że w obszarze techniki wiedza i umiejętności szybko się dewaluują co wymaga ciągłego ich uzupełniania.
Ma świadomość znaczenia najnowszych osiągnięć naukowych i technicznych w rozwiązywaniu problemów badawczych i praktycznych oraz w razie potrzeby wspierania się opiniami ekspertów.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład - wiedza zdobyta na wykładach weryfikowana jest na kolokwium. Próg zaliczenia kolokwium to 50%. Oceniana jest poprawność odpowiedzi oraz stopień zrozumienia problemu przez studenta.

Treści programowe

-Podstawowe pojęcia: zagrożenie, podatność, ryzyko, naruszenie bezpieczeństwa, uwierzytelnianie a autoryzacja
-Podstawowe zasady ochrony (w tym zasada minimum koniecznego, zasada ciągłości zabezpieczeń, zasady poprawnego wyboru zabezpieczeń kryptograficznych, zasady stosowania haseł). Funkcjonalność systemu a poziom bezpieczeństwa.
-Podstawowe etapy procesu ochrony (prewencja, detekcja, reagowanie, testowanie)
-Modelowanie zagrożeń
-Analiza i zarządzanie ryzykiem (model ryzyka, etapy procesu, ilościowa i jakościowa metoda analizy ryzyka, metody oddziaływania na ryzyko, czynniki determinujące akceptowalne ryzyko szczątkowe)
-Dokumentacja systemu (elementy dokumentacji, wymagania prawne)
-Struktura organizacyjna firmy i hierarchia podmiotów odpowiedzialnych za bezpieczeństwo danych. Obowiązki osób i podmiotów związane z zarządzaniem bezpieczeństwem (obowiązki IOD, obowiązki operatorów usług kluczowych, obowiązki podmiotów telekomunikacyjnych)
-Ekonomiczne aspekty bezpieczeństwa w systemach informatycznych (finansowe skutki naruszeń bezpieczeństwa, koszt zabezpieczeń)
-Informatyczne narzędzia wspierające procesy zarządzania bezpieczeństwem, w tym zastosowania sztucznej inteligencji w ochronie danych.
-Certyfikacja systemów informatycznych (w tym ISO 15408). Kryteria oceny zabezpieczeń.

Metody dydaktyczne

Wykład: 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.

Literatura

Podstawowa:
1. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Białas A. WNT, Warszawa 2017.

2. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, NIST 800-37 rev.2, 2018

Uzupełniająca:
1. Normy ISO (13335, 2700x).

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	30	1,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	17	0,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	13	0,50