POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo systemów komputerowych, PG_00047883		
Kierunek studiów	Informatyka		
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu	2028/2029
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć	Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	3	Język wykładowy	polski
Semestr studiów	6	Liczba punktów ECTS	4.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Architektury Systemów Komputerowych		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Piotr Rajchowski	
	Prowadzący zajęcia z przedmiotu	dr inż. Piotr Rajchowski	

Formy zajęć

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	30.0	0.0	0.0	15.0	0.0	45

W tym liczba godzin zajęć na odległość: 0.0

Aktywność studenta i liczba godzin pracy

Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
Liczba godzin pracy studenta	45	4.0	51.0	100

Cel przedmiotu

Celem przedmiotu jest zapoznanie studenta z ryzykiem oraz polityką bezpieczeństwa systemów komputerowych, jednocześnie poznając powszechne algorytmy kryptograficzne oraz metody dostępu do baz danych.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K6_W04] zna i rozumie w zaawansowanym stopniu zasady, metody i techniki programowania oraz zasady tworzenia oprogramowania komputerów albo programowania urządzeń lub sterowników wykorzystujących mikroprocesory albo elementy lub układy programowalne, specyficznych dla kierunku studiów, a także organizację pracy systemów wykorzystujących komputery lub te urządzenia	Student potrafi opracować i uruchomić programy implementujące poznane protokoły kryptograficzne oraz metody dostępu do baz danych. Student potrafi odnieść i osadzić sposób działania opracowywanych programów w realiach rzeczywistych rozwiązań powiązanych z zawodem.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW2] Ocena wiedzy zawartej w prezentacji

Treści przedmiotu

Treści przedmiotu - wykład
Zagrożenia, ryzyko, polityki bezpieczeństwa. Planowanie polityki bezpieczeństwa. Analiza ryzyka i wznawianie pracy po awariach. Zarządzanie bezpieczeństwem personelu. Fizyczne systemy kontroli dostępu. Techniki kryptograficzne. Podstawowe algorytmy kryptograficzne. Zasady budowy szyfrów blokowych i tryby pracy. Jednokierunkowe funkcje skrótu. Uwierzytelnianie, identyfikacja, wymiana kluczy. Podpis elektroniczny - certyfikaty kluczy publicznych. Zarządzanie kluczami. Przesyłanie danych poufnych. Wybrane modele kontroli dostępu. Zabezpieczanie systemów operacyjnych i aplikacji. Zaawansowane protokoły uwierzytelnienia z użyciem kryptografii symetrycznej oraz hybrydowe, protokoły identyfikacji i dowody o wiedzy zerowej. Ataki z użyciem aplikacji internetowych. Socjotechniczne metody penetracji. Tworzenie bezpiecznych serwisów www. Protokół SSL/TSL. Zapory ogniowe. Infrastruktury PKI. Notariat cyfrowy. Zabezpieczanie poczty elektronicznej. Zaawansowane zastosowania kryptografii – biznes internetowy. Płatności z użyciem kart płatniczych. Bezpieczeństwo systemów mobilnych. Normy i standardy bezpieczeństwa. Ocena poziomu bezpieczeństwa systemów informatycznych. Audyt bezpieczeństwa.

Wymagania wstępne i dodatkowe

znajomość podstawowych technik programowania oraz pracy z bazami danych

<table>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td colspan="2"><table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>Realizacja projektu</td><td>50.0%</td><td>40.0%</td></tr>
<tr><td>kolokwium (2)</td><td>50.0%</td><td>60.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</td><td>1. Schneier, B., Kryptografia dla praktyków, wyd.2, WNT 2000.
2. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone „Handbook of Applied Cryptography” (Kryptografia stosowana), WNT 2005.
3. J. Stokłosa, T. Bilski, T. Pankowski – Bezpieczeństwo danych w systemach informatycznych, PWN 2001
4. W. Stallings: Cryptography and Network. Security: Principles and Practice,. Prentice Hall, 1998
5. J. Pieprzyk, T. Hardjono, J. Seberry - Teoria bezpieczeństwa systemów komputerowych, 2005, Helion.
6. R. Anderson - Inżynieria zabezpieczeń, WNT, 2005.</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>1. An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12 ,http://www.nist.org
2. S. Garfinkel. G. Spafford., Bezpieczeństwo w Unixie i Internecie, Wyd. RM, W-wa 1997.</td></tr>
<tr><td>Adresy eZasobów</td><td></td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="2"></td></tr>
<tr><td>Zajęcia praktyczne w ramach przedmiotu</td><td colspan="2">Nie dotyczy</td></tr>
</table>

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.