POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo systemów informatycznych, PG_00071527		
Kierunek studiów	Fizyka Techniczna		
Data rozpoczęcia studiów	październik 2024 r.	Rok akademicki realizacji przedmiotu	2026/2027
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	5.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	egzamin
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Fizyki Technicznej i Matematyki Stosowanej -> Instytut Fizyki i Informatyki Stosowanej -> Zakład Fizyki Teoretycznej i Informatyki Kwantowej		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Paweł Syty	
	Prowadzący zajęcia z przedmiotu	dr inż. Paweł Syty	

Formy zajęć							
	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	45.0	0.0	0.0	75
	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	75	5.0	45.0	125

Cel przedmiotu	
	Celem przedmiotu jest zapoznanie studentów z podstawowymi pojęciami, zagrożeniami oraz mechanizmami ochrony systemów IT w środowiskach współczesnych organizacji. Studenci zdobędą wiedzę z zakresu ochrony danych, zabezpieczania sieci, systemów operacyjnych oraz aplikacji, a także poznają zasady zarządzania bezpieczeństwem informacji. Przedmiot kształtuje umiejętność identyfikacji podatności, analizy ryzyka oraz doboru adekwatnych mechanizmów zabezpieczeń w systemach informatycznych.

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K6_U08] posiada umiejętność przygotowywania prac i opracowań pisemnych oraz wystąpień ustnych, w językach polskim i angielskim, dotyczących zagadnień szczegółowych z zakresu fizyki oraz pokrewnych dziedzin i dyscyplin nauki	Potrafi przygotować raport z analizy bezpieczeństwa systemu informatycznego oraz przedstawić jego wyniki w formie pisemnej i ustnej, w języku polskim lub angielskim.	[SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu [SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania
	[K6_K01] rozumie potrzebę uczenia się przez całe życie oraz potrzebę podnoszenia kompetencji zawodowych i osobistych, inspiruje i organizuje proces uczenia się innych osób	Rozumie znaczenie ciągłego aktualizowania wiedzy w obszarze cyberbezpieczeństwa w związku z dynamicznie zmieniającym się charakterem zagrożeń.	[SK4] Ocena umiejętności komunikacji, w tym poprawności językowej [SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce
	[K6_W02] posiada uporządkowaną wiedzę w zakresie podstaw fizyki, obejmującą mechanikę, termodynamikę, elektryczność i magnetyzm, optykę, fizykę atomu i cząsteczki, fizykę ciała stałego, fizykę jądra atomowego i cząstek elementarnych	Zna metody analizy ryzyka, modele kontroli dostępu oraz architektury bezpieczeństwa stosowane w projektowaniu i eksploatacji systemów IT.	[SW1] Ocena wiedzy faktograficznej [SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym
	[K6_W05] posiada wiedzę w zakresie metodyki i technik programowania oraz wykorzystywania wybranych narzędzi informatycznych w fizyce i technice	Ma uporządkowaną wiedzę w zakresie zagrożeń i podatności systemów informatycznych, obejmującą bezpieczeństwo systemów operacyjnych, sieci komputerowych, aplikacji oraz środowisk chmurowych	[SW1] Ocena wiedzy faktograficznej [SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym
	[K6_U07] przedstawia w sposób popularny fakty z zakresu fizyki oraz pokrewnych dziedzin i dyscyplin nauki	Potrafi w przystępny sposób wyjaśnić podstawowe zagrożenia cyberbezpieczeństwa oraz znaczenie stosowanych mechanizmów ochronnych odbiorcom o różnym poziomie wiedzy technicznej.	[SU2] Ocena umiejętności analizy informacji [SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania

Treści przedmiotu	Treści przedmiotu - wykład 1. Wprowadzenie do bezpieczeństwa systemów informatycznych Podstawowe pojęcia: poufność, integralność, dostępność, podatność, zagrożenie, ryzyko. Aktualne trendy w cyberbezpieczeństwie. 2. Modele bezpieczeństwa i polityka bezpieczeństwa Modele kontroli dostępu, polityka bezpieczeństwa w organizacji. 3. Analiza ryzyka w systemach IT Identyfikacja aktywów, zagrożeń i podatności. Metody jakościowe i ilościowe oceny ryzyka. 4. Architektura bezpieczeństwa systemów informatycznych Security by Design i Security by Default, Model Zero Trust, Segmentacja i mikrosegmentacja sieci, Defense in Depth, Strefy bezpieczeństwa (DMZ), Modelowanie powierzchni ataku 5. Standardy i normy bezpieczeństwa informacji System Zarządzania Bezpieczeństwem Informacji, Rodzina norm ISO/IEC 27000 6. Bezpieczeństwo systemów operacyjnych Mechanizmy kontroli dostępu, aktualizacje, hardening systemu, izolacja procesów. 7. Bezpieczeństwo sieci komputerowych Zapory sieciowe, IDS/IPS, segmentacja sieci, VPN. 8. Bezpieczeństwo aplikacji webowych Najczęstsze podatności (np. SQL Injection, XSS), podstawy bezpiecznego programowania. 9. Uwierzytelnianie i autoryzacja Mechanizmy haseł, MFA, SSO, zarządzanie tożsamością. 10. Bezpieczeństwo danych i ochrona prywatności Szyfrowanie danych w spoczynku i w transmisji, kopie zapasowe, podstawy regulacji prawnych (np. RODO). 11. Ataki socjotechniczne i zagrożenia wewnętrzne Phishing, spear phishing, inżynieria społeczna, świadomość użytkowników. 12. Testowanie bezpieczeństwa i audyt Testy penetracyjne, skanery podatności, podstawy audytu bezpieczeństwa. 13. Zarządzanie incydentami bezpieczeństwa Reagowanie na incydenty, analiza powłamaniowa, plan ciągłości działania. 14. Bezpieczeństwo w chmurze i systemach rozproszonych Modele usług (IaaS, PaaS, SaaS), zagrożenia i dobre praktyki. 15. Trendy i wyzwania w cyberbezpieczeństwie AI w bezpieczeństwie, zagrożenia typu ransomware, bezpieczeństwo IoT. Treści przedmiotu - laboratoria 1. Środowisko testowe i analiza podatności - Konfiguracja izolowanego środowiska laboratoryjnego (np. maszyny wirtualne). - Podstawy bezpieczeństwa systemu Linux/Windows. - Skanowanie sieci i identyfikacja usług. - Wykrywanie podatności w systemach i aplikacjach. 2. Monitoring i analiza bezpieczeństwa systemów - Logowanie zdarzeń w systemach operacyjnych - Centralizacja logów - Wprowadzenie do systemów SIEM - Wykrywanie anomalii w logach - Korelacja zdarzeń 3. Bezpieczeństwo aplikacji webowych - Identyfikacja podatności aplikacji webowych. - Analiza ruchu HTTP. - Testowanie podatności typu SQL Injection, XSS. - Podstawy bezpiecznej konfiguracji serwera WWW 4. Mechanizmy uwierzytelniania i kontroli dostępu - Konfiguracja polityk haseł. - Mechanizmy kontroli dostępu w systemie operacyjnym. - Konfiguracja zapory sieciowej. - Wprowadzenie do uwierzytelniania wieloskładnikowego (MFA). 5. Reagowanie na incydenty i analiza powłamaniowa - Identyfikacja incydentu bezpieczeństwa. - Analiza logów systemowych. - Podstawy informatyki śledczej (digital forensics). - Opracowanie raportu z incydentu.
Wymagania wstępne i dodatkowe	

<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>zalicznie ustne</td><td>50.0%</td><td>30.0%</td></tr>
<tr><td>realizacja zadań laboratoryjnych</td><td>50.0%</td><td>50.0%</td></tr>
<tr><td>ocena opracowania pisemnego</td><td>50.0%</td><td>20.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</td><td>Lawrie Brown, William Stallings, Bezpieczeństwo systemów informatycznych, Helion, 2023
Michał Szychowiak, Bezpieczeństwo systemów informatycznych, Wydawnictwo Politechniki Poznańskiej, 2017</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>Franciszek Wołowski, Bezpieczeństwo systemów informacyjnych, s.c. edu-Libri, 2012</td></tr>
<tr><td>Adresy eZasobów</td><td></td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="2">Przeprowadzenie analizy ryzyka dla przykładowego systemu informatycznego z identyfikacją aktywów, zagrożeń i podatności.

Konfiguracja podstawowych mechanizmów zabezpieczeń systemu operacyjnego oraz ocena ich skuteczności.

Wykonanie skanowania sieci i interpretacja wyników w kontekście potencjalnych podatności bezpieczeństwa.</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.