

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Podstawy projektowania bezpiecznego oprogramowania				Designing secure software					
Kod przedmiotu	WCYKACSI_.....									
Język wykładowy	polski									
Profil studiów	ogólnoakademicki									
Forma studiów	studia stacjonarne									
Poziom studiów	studia pierwszego stopnia									
Rodzaj przedmiotu										
Obowiązuje od naboru	2026/2027									
Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS	semestr	(x egzamin, + zaliczenie, # projekt)						punkty ECTS		
		razem	wykłady	ćwiczenia	laboratoria	projekt	seminarium			
	V	44x	12		8+	24+		5.0		
	razem		12		8	24		5.0		
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających									
Semestr/kierunek studiów	semestr 5 / Kryptologia i cyberbezpieczeństwo / Bezpieczeństwo systemów informatycznych									
Autor	mgr inż. Michał Zimoń									
Jednostka odpowiedzialna za przedmiot	WCY/Instytut Systemów Informatycznych/Zakład Badań Operacyjnych i Wspomagania Decyzji, Zakład Inżynierii Oprogramowania									
Skrócony opis przedmiotu	● Wykład z prezentacją ● Egzamin ● Ćwiczenia laboratoryjne ● Projekt zespołowy									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr V temat/tematyka zajęć				liczba godzin				
						wkł.	ćw.	lab.	prj.	sem.
	1	Cele i wymagania bezpieczeństwa oprogramowania: aktywa, właściwości bezpieczeństwa, założenia, przeciwnik i granice zaufania. Cykl życia systemu. Ochrona danych od fazy projektowania i domyślna, minimalizacja danych i ograniczenie przechowywania.				2				
	2	Zasady bezpiecznego projektowania: minimalne uprawnienia, pełna kontrola dostępu, bezpieczne ustawienia domyślne, izolacja, prostota oraz użyteczność mechanizmów ochronnych. Porównywanie wariantów architektury.				2				
	3	Tożsamość, uwierzytelnianie i autoryzacja. Oddzielenie danych od sterowania, walidacja i reprezentacja danych. Bezpieczeństwo stanów i procesów, współbieżność, unieważnianie uprawnień i obsługa błędów.				2				
	4	Bezpieczeństwo wytwarzania, ponownego wykorzystania, konfiguracji, wydawania, aktualizacji i wycofywania oprogramowania. Zaufanie do komponentów, zależności, pochodzenia i integralności artefaktów.				2				
	5	Przeglądy projektu i weryfikacja bezpieczeństwa. Możliwości i ograniczenia metod statycznych i dynamicznych, testów negatywnych i eksperymentów. Odtwarzalność, interpretacja wyników i ryzyko rezydualne.				2				
	6	Praktyki biznesowe korzystania z oprogramowania: odpowiedzialność za aktualizacje, nabywanie i użytkowanie komponentów, koszty cyklu życia. Kompromisy projektowe i wstępna analiza ekonomiczna. Krytyczna ocena źródeł. Dostosowanie projektu do zmiany wymagań, zagrożeń i mechanizmów technicznych; ocena bezpieczeństwa nowych rozwiązań.				2				
	7	Wyprowadzenie wymagań bezpieczeństwa i modelu zagrożeń z opisu systemu. Analiza granic zaufania; powiązanie zagrożeń, zabezpieczeń i kryteriów weryfikacji, w tym minimalizacji danych i ich retencji.						2		
	8	Analiza i naprawa błędów autorvzacji oraz przebieau operacji.						2		

	lp.	Semestr V temat/tematyka zajęć	liczba godzin				
			wkł.	ćw.	lab.	prj.	sem.
		Przypadki dostępu do niewłaściwego obiektu, przekroczenia uprawnień i wykorzystania nieaktualnego stanu.					
	9	Zaprojektowanie i wykonanie eksperymentu bezpieczeństwa. Przypadek poprawny i negatywny, obserwacje, poprawka, test regresji oraz ocena ograniczeń wyniku.			2		
	10	Weryfikacja dowodów integralności i pochodzenia wydania oraz informacji o zależnościach. Decyzja o aktualizacji, konfiguracji i odtworzeniu bezpiecznego stanu.			2		
	11	Ustalenie zakresu projektu zespołowego, podziału odpowiedzialności, wymagań i założeń bezpieczeństwa. Wstępny model zagrożeń, wymagania ochrony danych i kryteria akceptacji.				4	
	12	Porównanie wariantów architektury i dobór zabezpieczeń. Przegląd projektu, dokumentacja decyzji oraz aktualizacja projektu na podstawie informacji zwrotnej.				4	
	13	Implementacja wybranych mechanizmów bezpieczeństwa i integracja rozwiązania. Przygotowanie pozytywnych i negatywnych przypadków testowych.				4	
	14	Odtwarzalna weryfikacja, przegląd i eksperyment. Interpretacja wyników, naprawa ujawnionej słabości i testy regresji.				4	
	15	Przygotowanie wydania, zasad wdrożenia, utrzymania i aktualizacji. Ocena zależności i konfiguracji; wstępna analiza ekonomiczna dwóch wariantów rozwiązania.				4	
	16	Dostosowanie rozwiązania do zmiany założeń lub wymagań, ponowna weryfikacja, końcowa dokumentacja i indywidualna obrona wkładu w projekt.				4	
	Razem		12		8	24	
Literatura	podstawowa: - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), art. 5, 25 i 32: zasady przetwarzania, ochrona danych w fazie projektowania i domyślna oraz bezpieczeństwo przetwarzania; tekst oficjalny EUR-Lex. Dla danej edycji zajęć stosuje się aktualnie obowiązujące przepisy. - Saltzer J.H., Schroeder M.D., The Protection of Information in Computer Systems, Proceedings of the IEEE, 63(9), 1975, s. 1278-1308; część I: Basic Principles of Information Protection. - IEEE Computer Society, Center for Secure Design, Avoiding the Top 10 Software Security Design Flaws, 2014; wybrane części dotyczące zaufania, autoryzacji, interpretacji danych, zależności i zmian. - Anderson R., Security Engineering: A Guide to Building Dependable Distributed Systems, wyd. 3, Wiley, 2020; wybrane fragmenty dotyczące polityk bezpieczeństwa, ekonomii, użyteczności oraz zapewniania bezpieczeństwa. - NIST, Secure Software Development Framework (SSDF), seria SP 800-218; wybrane praktyki dotyczące wymagań, projektowania, weryfikacji i reagowania na podatności. Wydanie odniesienia w zgromadzonych materiałach: wersja 1.1, 2022. - OWASP Foundation, Threat Modeling Cheat Sheet oraz Authorization Cheat Sheet; wybrane części określone w materiałach do danej edycji zajęć. uzupełniająca: - NIST, Engineering Trustworthy Secure Systems, SP 800-160 Vol. 1 Rev. 1, 2022; wybrane fragmenty dotyczące wymagań, architektury i argumentacji bezpieczeństwa. - OWASP Foundation, Application Security Verification Standard (ASVS) oraz Software Assurance Maturity Model (SAMM); wybrane wymagania i praktyki adekwatne do analizowanego systemu. - OpenSSF, Supply-chain Levels for Software Artifacts (SLSA), specyfikacja i materiały dotyczące integralności oraz pochodzenia artefaktów; wybrane części.						
Efekty uczenia się	Symbol	Efekty kształcenia		odniesienie do efektów kształcenia dla kierunku			
	W1	Rozróżnia klasy systemów informatycznych i wyjaśnia wpływ architektury oraz metod projektowania i wytwarzania oprogramowania na rozmieszczenie i działanie mechanizmów bezpieczeństwa.		K_W06			
	W2	Zna i rozumie właściwości bezpieczeństwa, modele zaufania i zagrożeń oraz typowe błędy projektowe, wyjaśnia projektowe konsekwencje ochrony danych osobowych oraz zastosowania i ograniczenia metod analizy i weryfikacji bezpieczeństwa na przykładach implementacyjnych.		K_W14			
	U1	Formułuje weryfikowalne wymagania bezpieczeństwa i ochrony danych osobowych, opracowuje model zagrożeń, krytycznie ocenia istniejące rozwiązanie i porównuje warianty projektu, uzasadniając dobór metod, mechanizmów i dokumentacji.		K_U05			
	U2	Uczestniczy w zespołowym projektowaniu, implementacji i testowaniu oprogramowania, opracowuje zasady wdrożenia, utrzymania i doskonalenia rozwiązania oraz wstępnie analizuje ekonomiczne skutki rozważanych decyzji.		K_U07			
	U3	Formułuje i analizuje problem bezpieczeństwa, planuje i przeprowadza odtwarzalny eksperyment, interpretuje wyniki,		K_U12			

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
		wyciąga wnioski oraz weryfikuje skuteczność poprawki i ograniczenia uzyskanych dowodów.		
	U4	Samodzielnie planuje i realizuje zadanie uczenia się, pozyskuje informacje z literatury, baz danych i źródeł pierwotnych, ocenia ich wiarygodność i zakres zastosowania oraz syntetyzuje ustalenia i aktualizuje decyzję projektową.	K_U17	
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	- Egzamin, każde wymagane laboratorium i projekt są oceniane w skali 0-100 punktów. Zaliczenie przedmiotu wymaga uzyskania co najmniej 51 punktów z egzaminu, co najmniej 51 punktów z każdego laboratorium i co najmniej 51 punktów z projektu. Warunkiem przystąpienia do egzaminu jest zaliczenie laboratoriów i projektu. - Projekt obejmuje ocenę wspólną: wymagania, w tym ochrony danych, model zagrożeń i porównanie wariantów - 20 pkt; implementacja - 25 pkt; eksperyment i weryfikacja - 20 pkt; wydanie, utrzymanie i analiza ekonomiczna - 15 pkt. Ocena indywidualna obejmuje notatkę źródłową - 10 pkt i obronę - 10 pkt. Z każdej części indywidualnej należy uzyskać co najmniej 5 pkt. Każdy student wykazuje własny wkład techniczny. Niezależnie od liczby punktów projekt musi spełniać opublikowane przed rozpoczęciem pracy zasadnicze wymagania bezpieczeństwa, potwierdzone pozytywnymi i negatywnymi przypadkami akceptacyjnymi. Wymagania obejmują w szczególności kontrolę uprawnień do operacji i obiektów, poprawność stanów i danych, minimalizację danych i retencję oraz bezpieczną obsługę błędów. Sam wynik narzędzia automatycznego nie zastępuje uzasadnienia i dowodów. Niespełnienie warunku wymaga poprawy w wyznaczonym terminie. - Laboratorium: poprawność wymagań i założeń - 20 pkt; analiza i rozwiązanie - 25 pkt; dowody weryfikacji - 30 pkt; interpretacja i ograniczenia - 15 pkt; odtwarzalność i źródła - 10 pkt. Wynik laboratoriów L jest średnią wyników czterech wymaganych laboratoriów.			
Bilans ECTS (nakład pracy studenta)	SEMESTR 5			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	12	0.4	
	Udział w laboratoriach	8	0.3	
	Udział w ćwiczeniach			
	Udział w seminariach			
	Samodzielne studiowanie tematyki wykładów	28	1	
	Samodzielne przygotowanie do laboratoriów	20	0.8	
	Samodzielne przygotowanie do ćwiczeń			
	Samodzielna realizacja projektu			
	Realizacja projektu	24	0.8	
	Udział w konsultacjach	2	0.1	
	Przygotowanie do egzaminu	18	0.5	
	Przygotowanie do zaliczenia	36	1	
	Udział w egzaminie / kolokwium	2	0.1	
	Sumaryczne obciążenie pracą studenta	152	5	
Zajęcia z udziałem nauczycieli	48	1.7		
Zajęcia powiązane z działalnością naukową	92	3.3		
Zajęcia o charakterze praktycznym	52	1.9		
Zajęcia realizowane z wykorzystaniem metod i technik kształcenia na odległość	SEMESTR 5			
	Rygor	Liczba godzin	Liczba ECTS	
	Wykłady			
	Laboratoria			
	Ćwiczenia			
	Projekty			
	Seminaria			
	Razem			

autor

kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot

mgr inż. Michał Zimoń
tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. inż. Nowicki Tadeusz
tytuł, stopień naukowy, imię, NAZWISKO, podpis