



UNIWERSYTET
IM. ADAMA MICKIEWICZA
W POZNANIU

Bezpieczeństwo systemów komputerowych

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka Specjalność - Jednostka organizacyjna Wydział Matematyki i Informatyki Poziom studiów studia drugiego stopnia poinżynierskie Forma studiów studia niestacjonarne Profil studiów profil ogólnoakademicki		Cykl dydaktyczny 2023/24 Kod zajęć 06INFN.44S.01039.23 Języki wykładowe polski Obligatoryjność Fakultatywny Blok zajęciowy Przedmioty specjalnościowe
Koordynator zajęć	Michał Ren	
Prowadzący zajęcia	Michał Ren	
Okres Semestr 3	Forma zajęć / liczba godzin / forma zaliczenia • Wykład: 8, Zaliczenie z oceną • Laboratorium: 7, Zaliczenie z oceną	Liczba punktów ECTS 3

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie z najczęściej spotykanymi błędami prowadzącymi do powstania luk w bezpieczeństwie i technikami ich unikania.
C2	Zapewnienie wystarczającej wiedzy teoretycznej i praktycznej niezbędnej do krytycznej oceny bezpieczeństwa zapewnianego przez systemy autorstwa osób trzecich, jak i samodzielnej implementacji własnych rozwiązań.

Wymagania wstępne

Brak.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy - Student/ka:			
W1	zna podstawowe metody rozwiązywania problemów bezpieczeństwa stosowane w złożonych systemach informatycznych.	INF_K4_W03	Kolokwium pisemne, Zadania wykonywane podczas zajęć
W2	przestrzega podstawowych zasad bezpieczeństwa przy używaniu i implementacji systemów informatycznych.	INF_K4_W05	Kolokwium pisemne, Zadania wykonywane podczas zajęć
W3	jest świadomy prawnych wymogów stawianych przed bezpiecznymi systemami informatycznymi.	INF_K4_W06	Kolokwium pisemne, Zadania wykonywane podczas zajęć
W4	posiada wiedzę o narzędziach stosowanych do zapewniania bezpieczeństwa systemów komputerowych.	INF_K4_W03	Kolokwium pisemne, Zadania wykonywane podczas zajęć
Umiejętności - Student/ka:			
U1	potrafi wykorzystywać odpowiednio dobrane metody rozwiązywania problemów bezpieczeństwa stosowane w złożonych systemach informatycznych.	INF_K4_U03, INF_K4_U04	Kolokwium pisemne, Zadania wykonywane podczas zajęć
U2	potrafi ocenić daną implementację pod kątem potencjalnych zagrożeń i zaproponować metody ich ograniczeń.	INF_K4_U03, INF_K4_U07	Kolokwium pisemne, Zadania wykonywane podczas zajęć
U3	potrafi dobierać odpowiednie narzędzia stosowane do zapewniania bezpieczeństwa systemów komputerowych.	INF_K4_U03, INF_K4_U04, INF_K4_U12	Kolokwium pisemne, Zadania wykonywane podczas zajęć

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Podstawowe pojęcia kryptologii i inżynierii bezpieczeństwa, poufność danych, terminologia, proste szyfry.	W1, W3, U1	Wykład, Laboratorium
2.	Integralność danych, tworzenie używalnych kopii zapasowych. Strategie działań odtworzeniowych.	W2, W3	Wykład, Laboratorium
3.	Tryby szyfrowania szyfrów symetrycznych, konsekwencje doboru trybów szyfrowania. Szyfrowanie dysków w locie na przykładzie programu Veracrypt. Plausible deniability.	W1, W4, U1, U2, U3	Wykład, Laboratorium
4.	Klasyfikacja malware, techniki tworzenia wirusów. Zaawansowane mechanizmy używane w złośliwym oprogramowaniu na przykładzie Stuxnet. Ochrona antywirusowa.	W2, W4, U3	Wykład, Laboratorium

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
5.	SPAM i UCE. Sposoby przeciwdziałania na poziomie serwerów i klientów.	W2, W4, U3	Wykład, Laboratorium
6.	Bezpieczne przechowywanie haseł. Zabezpieczanie systemów hasłami na przykładzie http simple authentication.	W1, W4, U1, U2, U3	Wykład, Laboratorium
7.	Atak typu buffer overflow na integralność pamięci na przykładzie stack smashing.	W1, U1, U2	Wykład, Laboratorium
8.	Atak SQL injection na prosty program. Sposoby obrony przed atakami po stronie klienta bazy danych i silników bazodanowych.	W1, W2, U1, U2	Wykład, Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Metoda analizy przypadków
Laboratorium	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda laboratoryjna

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem przystąpienia do kolokwium pisemnego jest uzyskanie zaliczenia z laboratoriów. Na końcową ocenę składa się wynik uzyskany na kolokwium pisemnym. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 80% punktów, 2. dobry plus (db plus; 4,5) – od 70% punktów, 3. dobry (db; 4,0) – od 60% punktów, 4. dostateczny plus (dst plus; 3,5) – od 50% punktów, 5. dostateczny (dst; 3,0) – od 40% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 40% punktów.
Laboratorium	Skala ocen zgodna z Regulaminem studiów UAM. Na końcową ocenę składa się wynik uzyskany z zadań wykonywanych podczas zajęć: 1. bardzo dobry (bdb; 5,0) – od 80% punktów, 2. dobry plus (db plus; 4,5) – od 70% punktów, 3. dobry (db; 4,0) – od 60% punktów, 4. dostateczny plus (dst plus; 3,5) – od 50% punktów, 5. dostateczny (dst; 3,0) – od 40% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 40% punktów.

Literatura

Obowiązkowa

1. Ross Anderson "Security Engineering – A Guide To Building Dependable Distributed Systems"
2. Mirosław Kutyłowski, Willy-B. Strothmann "Kryptografia: teoria i praktyka zabezpieczania systemów komputerowych"
3. Bruce Schneier "Kryptografia dla praktyków"

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
------------------------	---

Wykład	8
Laboratorium	7
Przygotowanie do zajęć	35
Czytanie wskazanej literatury	15
Przygotowanie do zaliczenia	10
Łączny nakład pracy studenta	Liczba godzin 75
Liczba punktów ECTS	ECTS 3

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K4_U03	Absolwent/ka potrafi stosować zaawansowane metody budowy oprogramowania, rozstrzyga o ich przydatności, w tym podejmuje decyzje dotyczące wyboru technik prowadzących do otrzymania oprogramowania wysokiej jakości
INF_K4_U04	Absolwent/ka potrafi projektować i implementować systemy informatyczne o różnej złożoności i różnych architekturach
INF_K4_U07	Absolwent/ka potrafi wyrażać krytyczne opinie na temat architektury oraz użyteczności wykorzystywanych systemów informatycznych
INF_K4_U12	Absolwent/ka potrafi samodzielnie pogłębiać i aktualizować wiedzę i umiejętności z zakresu informatyki oraz określać kierunki dalszego rozwoju zawodowego
INF_K4_W03	Absolwent/ka zna i rozumie w pogłębionym stopniu współczesne metody, narzędzia i technologie informatyczne właściwe dla wybranych obszarów zastosowań niezbędne przy budowie złożonych systemów informatycznych oraz przy prowadzeniu prac badawczo-rozwojowych
INF_K4_W05	Absolwent/ka zna i rozumie budowę oraz cykl życia przykładowych systemów informatycznych wykorzystywanych w praktyce oraz zna ograniczenia złożonych systemów informatycznych
INF_K4_W06	Absolwent/ka zna i rozumie zagadnienia prawne i społeczne aspekty informatyki, w tym odpowiedzialności zawodowej i etycznej, kodeksów etycznych, własności intelektualnej, prywatności i swobód obywatelskich, ryzyka i odpowiedzialności związanej z systemami informatycznymi