UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Bezpieczeństwo informatyczne

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka	**Cykl dydaktyczny** 2024/25
Specjalność -	**Kod zajęć** 06INFN.42S.01019.24
Jednostka organizacyjna Wydział Matematyki i Informatyki	**Języki wykładowe** polski
Poziom studiów studia drugiego stopnia poinżynierskie	**Obligatoryjność** Fakultatywny
Forma studiów studia niestacjonarne	**Blok zajęciowy** Przedmioty specjalnościowe
Profil studiów profil ogólnoakademicki	

Koordynator zajęć	Michał Ren
Prowadzący zajęcia	Michał Ren

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr 2	• Wykład: 15, Egzamin; w tym zajęcia zdalne: ◦ Wykład synchroniczny: 15 • Laboratorium: 15, Zaliczenie z oceną	6

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie z teorią i praktyką bezpieczeństwa informatycznego, w tym z narzędziami i metodami używanych do zapewnienia go we współczesnych rozwiązaniach.
C2	Zapoznanie z uregulowaniami prawnymi mającymi wpływ na bezpieczeństwo informatyczne.
C3	Zapewnienie wystarczającej wiedzy teoretycznej i praktycznej pozwalającej na całościowe ujęcie bezpieczeństwa informatycznego, niezbędnego zarówno w projektowaniu jak i zarządzaniu złożonymi projektami informatycznymi.

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 teoretyczne i praktyczne aspekty kryptologii oraz narzędzia i metody zapewniające bezpieczeństwo komputerowe projektowanych i zarządzanych systemów informatycznych.	INF_K4_W01, INF_K4_W02, INF_K4_W03, INF_K4_W04, INF_K4_W05, INF_K4_W06	Egzamin pisemny, Test, Zadania wykonywane podczas zajęć
Umiejętności – Student/ka:			
U1	potrafi korzystać z narzędzi zapewniających bezpieczeństwo informatyczne oraz demonstrujących jego potencjalne słabe punkty.	INF_K4_U01, INF_K4_U03, INF_K4_U04, INF_K4_U06, INF_K4_U07, INF_K4_U11, INF_K4_U12	Egzamin pisemny, Test, Zadania wykonywane podczas zajęć
Kompetencji społecznych – Student/ka:			
K1	jest świadomy problemów prawnych i zagadnień etycznych związanych z atakami na systemy informatyczne.	INF_K4_K03, INF_K4_K04, INF_K4_K06	Egzamin pisemny, Test, Zadania wykonywane podczas zajęć

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Terminologia kryptologii, definicje bezpieczeństwa. Ewolucja metod łamania zabezpieczeń od czasów historycznyych do współczesnych.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
2.	Szyfry symetryczne. Ataki na szyfry. Kryteria oceny siły szyfru. Sposoby budowania szyfrów. Schemat Feistela.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
3.	Funkcje jednokierunkowe, ataki na nie i zastosowania. Redukcja trudności ataków i kompromisy między złożonością pamięciową a czasową. Rainbow tables - metody konstrukcji i użycia.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
4.	Losowość. Generatory pseudolosowe. Niebezpieczeństwa systemów o małej entropii. Sprzętowe generowanie danych losowych. Zastosowania.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
5.	Uwierzytelnianie, hasła, kryteria doboru, strategie łamania haseł przez hardware (FPGA/ASIC). Key stretching. Challenge-response, hasła jednorazowe, schemat Lamporta. Biometria, karty chipowe.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
6.	Zarządzanie kluczami, uzgadnianie kluczy, protokół Diffie-Hellmana, infrastruktura klucza publicznego, certyfikaty, unieważnianie kluczy, wykluczanie użytkowników, podział sekretów.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
7.	Typowe schematy ataków programistycznych, buffer overflow, SQL injection, cross-site scripting, reply attack, atak z rozmnożeniem, reflection attack.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
8.	Prawidłowe traktowanie danych od użytkownika - podział na tainted/clean. Urządzenia czarne i czerwone. Sprzętowa ochrona przed atakami łamiącymi barierę dane/kod. Wirtualizacja.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
9.	Social engineering i ataki łamiące abstrakcję modelu bezpieczeństwa. Wirusy, wormy, denial of service, spam, phishing. Podsłuch klawiatury, monitora. Sposoby ochrony.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
10.	Inwigilacja. Dobre praktyki tworzenia systemów inwigilacji. Inwigilacja wizualna. DORI. Sprzętowe ograniczenia współczesnych urządzeń.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
11.	Przechowywanie i bezpieczne niszczenie danych. Standardy dla różnych nośników. Szyfrowanie systemu plików - tryby szyfrowania XEX, XTS. Urządzenia tamper proof i tamper resistant.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny
12.	Informacje uzyskane pośrednio (side-channel attacks). Analiza poboru mocy (power analysis). Ulot elektromagnetyczny (tempest), ulot optyczny (optical tempest). Urządzenia czarne i czerwone.	W1, U1, K1	Wykład, Laboratorium, Wykład synchroniczny

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Pokaz i obserwacja, Demonstracje dźwiękowe i/lub video
Laboratorium	Praca z tekstem, Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda ćwiczeniowa, Metoda laboratoryjna

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem przystąpienia do egzaminu jest uzyskanie zaliczenia z laboratoriów. Na końcową ocenę składa się wynik uzyskany na egzaminie. 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.

Forma zajęć	Warunki zaliczenia zajęć
Laboratorium	Końcowa ocena składa się z testu i zadań wykonywanych podczas zajęć. 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.

Literatura

Obowiązkowa

1. Bruce Schneier "Kryptografia dla praktyków"
2. Mirosław Kutyłowski, Willy-B. Strothmann "Kryptografia: teoria i praktyka zabezpieczania systemów komputerowych"
3. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone "Handbook of Applied Cryptography"
4. Douglas R. Stinson "Kryptografia w teorii i praktyce"

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	15
Laboratorium	15
Przygotowanie do zajęć	60
Czytanie wskazanej literatury	30
Przygotowanie do egzaminu	30
Łączny nakład pracy studenta	**Liczba godzin** 150
Liczba punktów ECTS	**ECTS** 6

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K4_K03	Absolwent/ka jest gotów/gotowa do zrozumienia i docenienia znaczenia uczciwości intelektualnej w działaniach własnych i innych osób; postępuje etycznie
INF_K4_K04	Absolwent/ka jest gotów/gotowa do rozpoznania najważniejszych osiągnięć w swojej dziedzinie i stojących przed nią wyzwań; potrafi je przedstawić laikom w sposób popularny
INF_K4_K06	Absolwent/ka jest gotów/gotowa do pogłębiania świadomości roli informatyki w kształtowaniu życia społecznego
INF_K4_U01	Absolwent/ka potrafi zastosować zaawansowaną wiedzę matematyczną do formułowania, analizowania i rozwiązywania złożonych i nietypowych zadań związanych z informatyką
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_U06	Absolwent/ka potrafi rozwiązywać złożone problemy z wybranych obszarów informatyki oraz proponować nowe algorytmy, narzędzia i metody wykorzystując odpowiednio dobrane źródła, które poddaje krytycznej analizie, syntezie i twórczej interpretacji
INF_K4_U07	Absolwent/ka potrafi wyrażać krytyczne opinie na temat architektury oraz użyteczności wykorzystywanych systemów informatycznych
INF_K4_U11	Absolwent/ka potrafi pozyskiwać informacje z literatury, baz wiedzy, Internetu oraz innych wiarygodnych źródeł, integrować je, dokonywać ich interpretacji oraz wyciągać wnioski i formułować opinie
INF_K4_U12	Absolwent/ka potrafi samodzielnie pogłębiać i aktualizować wiedzę i umiejętności z zakresu informatyki oraz określać kierunki dalszego rozwoju zawodowego
INF_K4_W01	Absolwent/ka zna i rozumie w pogłębionym stopniu pojęcia z działów matematyki niezbędne do rozwiązywania zaawansowanych problemów w informatyce
INF_K4_W02	Absolwent/ka zna i rozumie współczesny stan badań i tendencje rozwojowe w wiodących obszarach informatyki
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_W04	Absolwent/ka zna i rozumie zasady rozwiązywania problemów z wykorzystaniem zaawansowanych algorytmów i metod informatycznych
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