UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Podstawy bezpieczeństwa komputerowego

Sylabus zajęć

Informacje podstawowe

Kierunek studiów
Informatyka - przedmioty do wyboru

Specjalność
-

Jednostka organizacyjna
Wydział Matematyki i Informatyki

Poziom studiów
studia drugiego stopnia poinżynierskie

Forma studiów
studia stacjonarne

Profil studiów
profil ogólnoakademicki

Cykl dydaktyczny
2023/24

Kod zajęć
06INFPWS.4200000S.00996.23

Języki wykładowe
polski

Obligatoryjność
Fakultatywny

Blok zajęciowy
Przedmioty specjalnościowe

Koordynator zajęć	Tomasz Kowalski
Prowadzący zajęcia	Tomasz Kowalski

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr letni	• Wykład: 30, Egzamin • Laboratorium: 30, Zaliczenie z oceną	6

Cele kształcenia dla zajęć

Kod	Cel
C1	Przekonanie do potrzeby dążenia do systematycznego i zrównoważonego podnoszenia poziomu bezpieczeństwa komputerowego.
C2	Zapoznanie z możliwie szerokim zakresem potencjalnych problemów bezpieczeństwa w całości systemu informatycznego.
C3	Przedstawienie wybranych sposób identyfikacji problemów bezpieczeństwa oraz mechanizmów zapobiegania ich wystąpieniu.

Wymagania wstępne

Wiedza i umiejętności w zakresie programowania, znajomości systemów operacyjnych i sieci komputerowych na poziomie inżyniera informatyki.

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 popularne wektory ataku na infrastrukturę lokalną lub zdalną.		Test, Zadania wykonywane podczas zajęć
Umiejętności – Student/ka:			
U1	potrafi wykryć użycie i zapobiegać wystąpieniu popularnych wektorów ataków na infrastrukturę lokalną lub zdalną.		Test, Zadania wykonywane podczas zajęć
U2	potrafi prowadzić przegląd kodu w celu wyeliminowania faktycznych i potencjalnych podatności.		Test, Zadania wykonywane podczas zajęć
U3	potrafi czerpać informacje o bezpieczeństwie komputerowym z właściwych źródeł.		Test
U4	potrafi właściwie przeciwdziałać potencjalnym incydentom w odniesieniu do bieżącego stanu zagrożeń.		Test, Zadania wykonywane podczas zajęć
Kompetencji społecznych – Student/ka:			
K1	rozumie potrzebę ustawicznego podnoszenia wiedzy i umiejętności z zakresu bezpieczeństwa komputerowego.		Test
K2	rozumie kulturowe i socjologiczne uwarunkowania bezpieczeństwa komputerowego.		Test

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Identyfikacja i zapobieganie podatnościom. Najbardziej rozpoznawalne grupy problemów. Symptomy podatności i standardowe rozwiązania. Przeprowadzenie eksperymentów związanych z identyfikacją problemów bezpieczeństwa.	W1, U1, U2, K2	Wykład, Laboratorium
2.	Przegląd narzędzi do wykrywania podatności. Omówienie popularnych rozwiązań dla danego zastosowania. Przeprowadzenie eksperymentów polegający na wykorzystaniu podatności.	W1, U1, U2, U3, K1	Wykład, Laboratorium
3.	Systemy monitoringu infrastruktury: Wyzwania. Przegląd produktów i rozwiązań. Przeprowadzenie eksperymentów związanych z użyciem wybranych rozwiązań.	U3, U4, K1	Wykład, Laboratorium

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Systemy wykrywania wtargnięć i ich raportowania. Przegląd rozwiązań. Przeprowadzenie eksperymentów związanych z użyciem wybranych rozwiązań.	U3, U4, K1	Wykład, Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Wykład konwersatoryjny, Uczenie problemowe (Problem-based learning)
Laboratorium	Uczenie problemowe (Problem-based learning), Metoda ćwiczeniowa, Metoda laboratoryjna

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem przystąpienia do testu jest uzyskanie zaliczenia z laboratoriów. Na końcową ocenę składa się wynik uzyskany z testu. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.
Laboratorium	Na końcową ocenę składają się punkty uzyskane z zadań wykonywanych podczas zajęć. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

1. Ken Douglas, "Cyber Security for Beginners: Understanding Cybersecurity and Ways to Protect Yourself", 2019.
2. Scott Augenbaum, "The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime", Forefront Books, 2019
3. Yuri Diogenes, "Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals", Packt, 2019
4. Marcus Carey, "Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity", Wiley, 2019.
5. Marcus Carey, "Tribe of Hackers Blue Team: Tribal Knowledge from the Best in Defensive Cybersecurity", Wiley, 2020.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	30

Laboratorium	30
Przygotowanie do zajęć	15
Czytanie wskazanej literatury	45
Przygotowanie projektu	15
Inne	15
Łączny nakład pracy studenta	**Liczba godzin** 150
Liczba punktów ECTS	**ECTS** 6

* godzina (lekcyjna) oznacza 45 minut