UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Podstawy bezpieczeństwa komputerowego

Sylabus zajęć

Informacje podstawowe

Kierunek studiów
Informatyka

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
06INFS.41S.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 1	• 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.	INF_K4_W02, INF_K4_W03, INF_K4_W05, INF_K4_W06, INF_K4_W07	Test, Zadania wykonywane podczas zajęć
Umiejętności – Student/ka:			
U1	potrafi wykryć użycie i zapobiegać wystąpieniu popularnych wektorów ataków na infrastrukturę lokalną lub zdalną.	INF_K4_U03	Test, Zadania wykonywane podczas zajęć
U2	potrafi prowadzić przegląd kodu w celu wyeliminowania faktycznych i potencjalnych podatności.	INF_K4_U02, INF_K4_U07, INF_K4_U13	Test, Zadania wykonywane podczas zajęć
U3	potrafi czerpać informacje o bezpieczeństwie komputerowym z właściwych źródeł.	INF_K4_U08, INF_K4_U11, INF_K4_U12	Test
U4	potrafi właściwie przeciwdziałać potencjalnym incydentom w odniesieniu do bieżącego stanu zagrożeń.	INF_K4_U03, INF_K4_U04	Test, Zadania wykonywane podczas zajęć
Kompetencji społecznych – Student/ka:			
K1	rozumie potrzebę ustawicznego podnoszenia wiedzy i umiejętności z zakresu bezpieczeństwa komputerowego.	INF_K4_K02, INF_K4_K04	Test
K2	rozumie kulturowe i socjologiczne uwarunkowania bezpieczeństwa komputerowego.	INF_K4_K06	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

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
3.	Systemy monitoringu infrastruktury: Wyzwania. Przegląd produktów i rozwiązań. Przeprowadzenie eksperymentów związanych z użyciem wybranych rozwiązań.	U3, U4, K1	Wykład, Laboratorium
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

Efekty uczenia się dla kierunku

Kod	Treść
INF_K4_K02	Absolwent/ka jest gotów/gotowa do zasięgania opinii ekspertów przy rozwiązywaniu problemów teoretycznych i praktycznych
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_U02	Absolwent/ka potrafi adaptować istniejące oraz tworzyć nowe metody informatyczne do rozwiązywania nieszablonowych problemów praktycznych i teoretycznych
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_U08	Absolwent/ka potrafi posługiwać się językiem zgodnie z wymaganiami określonymi dla poziomu B2+ Europejskiego Systemu Opisu Kształcenia Językowego w co najmniej jednym języku obcym oraz zna język angielski w stopniu umożliwiającym czytanie ze zrozumieniem dokumentacji oprogramowania, podręczników i artykułów 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_U13	Absolwent/ka potrafi pracować zespołowo i pełnić w zespole rożne role, w tym kierownicze; rozumie konieczność systematycznej pracy nad wszelkimi projektami, które mają długofalowy charakter
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_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
INF_K4_W07	Absolwent/ka zna i rozumie zasady rozwoju zaawansowanych produktów informatycznych w celu ich wykorzystania w gospodarce w różnych modelach biznesowych