



UNIWERSYTET
IM. ADAMA MICKIEWICZA
W POZNANIU

Cyberbezpieczeństwo

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Aplikacje Internetu Rzeczy Specjalność - Jednostka organizacyjna Wydział Fizyki Poziom studiów studia drugiego stopnia poinżynierskie Forma studiów studia stacjonarne Profil studiów profil ogólnoakademicki		Cykl dydaktyczny 2023/24 Kod zajęć 04AIRS.44S.00078.23 Języki wykładowe polski Obligatoryjność Fakultatywny Blok zajęciowy Przedmioty specjalnościowe
Koordynator zajęć	Henryk Gierszał	
Prowadzący zajęcia		
Okres Semestr 3	Forma zajęć / liczba godzin / forma zaliczenia • Wykład: 15, Zaliczenie z oceną • Ćwiczenia: 15, Zaliczenie z oceną	Liczba punktów ECTS 3

Cele kształcenia dla zajęć

Kod	Cel
C1	zapoznanie z aspektami cyberbezpieczeństwa
C2	przekazanie wiedzy w zakresie dobrych praktyk stosowania rozwiązań dotyczących cyberbezpieczeństwa

Wymagania wstępne

- podstawy programowania

- konfigurowanie systemów operacyjnych

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	wyjaśnia pojęcia z dziedziny cyberbezpieczeństwa	AIR_K4_W01, AIR_K4_W02, AIR_K4_W03, AIR_K4_W09, AIR_K4_W15	Kolokwium pisemne
W2	rozumie sposób działania i klasyfikuje cyberataki oraz inne zagrożenia bezpieczeństwa umiejac je nazwać w języku polskim i angielskim	AIR_K4_W02, AIR_K4_W03, AIR_K4_W04, AIR_K4_W05, AIR_K4_W09, AIR_K4_W15	Kolokwium pisemne, Projekt
W3	rozumie sposób działania i kategoryzuje narzędzia oraz technologie zwiększające poziom bezpieczeństwa, a także łączy zagrożenia z odpowiednimi technologiami zabezpieczającymi	AIR_K4_W01, AIR_K4_W02, AIR_K4_W03, AIR_K4_W04, AIR_K4_W05, AIR_K4_W09, AIR_K4_W15	Kolokwium pisemne, Projekt
Umiejętności - Student/ka:			
U1	ocenia wpływ nowych modeli i technologii takich jak przetwarzanie w „chmurze” czy internet rzeczy na bezpieczeństwo systemów i użytkowników, a także na ich prywatność	AIR_K4_U01, AIR_K4_U05, AIR_K4_U07, AIR_K4_U19	Projekt
U2	stosuje zasady projektowania i tworzenia bezpiecznego oprogramowania	AIR_K4_U01, AIR_K4_U05, AIR_K4_U07, AIR_K4_U12, AIR_K4_U16, AIR_K4_U19	Projekt
U3	posiada umiejętności wykrycia podstawowych luk w bezpieczeństwie w samodzielnie tworzonym lub istniejącym oprogramowaniu	AIR_K4_U01, AIR_K4_U05, AIR_K4_U07, AIR_K4_U10, AIR_K4_U12, AIR_K4_U19	Projekt
U4	potrafi zabezpieczyć istniejące aplikacje	AIR_K4_U01, AIR_K4_U05, AIR_K4_U07, AIR_K4_U10, AIR_K4_U12, AIR_K4_U19	Projekt
Kompetencji społecznych - Student/ka:			
K1	jest gotów szerzyć zasady dotyczące bezpieczeństwa teleinformatycznego	AIR_K4_K01, AIR_K4_K06, AIR_K4_K07	Kolokwium pisemne

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Cyberbezpieczeństwo – podstawowe pojęcia z zakresu bezpieczeństwa informacji, kontroli dostępu i kryptografii	W1, W2, W3, K1	Wykład
2.	Włamania do systemów informatycznych, ataki sieciowe, ataki na użytkowników końcowych, socjotechnika	W1, W2, W3, K1	Wykład
3.	Prywatność użytkowników w cyberprzestrzeni	W1, W2, K1	Wykład
4.	Zabezpieczenia biometryczne	W1, W2, W3, K1	Wykład
5.	Bezpieczeństwo w procesie tworzenia i rozwoju oprogramowania	W1, W2, W3	Wykład
6.	Przetwarzanie w „chmurze” – wyzwania bezpieczeństwa	W1, W2, W3, K1	Wykład
7.	Internet rzeczy – wyzwania bezpieczeństwa	W1, W2, W3, K1	Wykład
8.	Projektowanie i budowa bezpiecznych systemów kontroli dostępu	W1, W2, W3, K1	Wykład
9.	Popularne błędy wdrożeniowe wpływające na bezpieczeństwo, dobre praktyki	W1, W2, W3, K1	Wykład
10.	Kryptografia stosowana	W1, W2, W3, U3, K1	Wykład, Ćwiczenia
11.	Stosowanie środowisk zwiększających bezpieczeństwo aplikacji sieciowych web	W1, W2, W3, U3, U4	Wykład, Ćwiczenia
12.	Podnoszenie bezpieczeństwa (utwardzanie) usług sieciowych	U1, U2, U3, U4	Ćwiczenia
13.	Wykrywanie błędów w istniejących aplikacjach sieciowych web	U1, U2, U3	Ćwiczenia
14.	Analiza bezpieczeństwa kodu źródłowego	U1, U2, U3	Ćwiczenia
15.	Ocena podatności i testy penetracyjne	U1, U2, U3, U4	Ćwiczenia

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień
Ćwiczenia	Metoda analizy przypadków, Metoda ćwiczeniowa, Metoda laboratoryjna

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem zaliczenia jest napisanie kolokwium na ocenę pozytywną. bardzo dobry (bdb; 5,0): <90%;100%> punktów dobry plus (+db; 4,5): <80%;90%> punktów dobry (db; 4,0): <70%;80%> punktów dostateczny plus (+dst; 3,5) <60%;70%> punktów dostateczny (dst; 3,0): <50%;60%> punktów niedostateczny (ndst; 2,0): mniej niż 50% punktów

Forma zajęć	Warunki zaliczenia zajęć
Ćwiczenia	Warunkiem zaliczenia jest zrealizowanie projektu na ocenę pozytywną. bardzo dobry (bdb; 5,0): <90%;100%> punktów dobry plus (+db; 4,5): <80%;90%> punktów dobry (db; 4,0): <70%;80%> punktów dostateczny plus (+dst; 3,5) <60%;70%> punktów dostateczny (dst; 3,0): <50%;60%> punktów niedostateczny (ndst; 2,0): mniej niż 50% punktów lub nieprzedstawienie projektów

Literatura

Obowiązkowa

1. Rojszczak Marcin, Banasiński Cezary, Cyberbezpieczeństwo, Wolters Kluwer, 2020
2. John R. Vacca, Computer and Information Security Handbook, 3rd Edition, Morgan Kaufmann, 2017
3. Conklin, A., White, G., Cothren, C., Davis, R., Williams, D., Principles of Computer Security, CompTIA Security+ and Beyond, Fifth Edition, McGraw-Hill, 2018

Dodatkowa

1. The Open Web Application Security Project, OWASP, www.owasp.org

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	15
Ćwiczenia	15
Czytanie wskazanej literatury	10
Przygotowanie projektu	30
Przygotowanie do egzaminu	20
Łączny nakład pracy studenta	Liczba godzin 90
Liczba punktów ECTS	ECTS 3

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
AIR_K4_K01	Absolwent/ka jest gotów/gotowa do krytycznej oceny własnej wiedzy i umiejętności; precyzyjnego formułowania pytań; dalszego kształcenia się oraz systematycznego zapoznawania się z czasopismami naukowymi i popularno-naukowymi z zakresu pytań dotyczących nauk fizycznych, informatyki i telekomunikacji oraz nauk o zarządzaniu i jakości
AIR_K4_K06	Absolwent/ka jest gotów/gotowa do formułowania opinii na temat podstawowych wyzwań, przed którymi stoi Internet Przyszłości oraz współczesna telekomunikacja i informatyka
AIR_K4_K07	Absolwent/ka jest gotów/gotowa do profesjonalnego podejścia przy rozwiązywaniu problemów technicznych i podejmowania odpowiedzialności za proponowane przez siebie rozwiązania opierając się na rzetelnej wiedzy dotyczącej podstaw fizycznych oraz osiągnięciach informatyki i telekomunikacji
AIR_K4_U01	Absolwent/ka potrafi efektywnie korzystać z dostępnych źródeł danych, zarówno w formie klasycznej (teksty i książki), jak i nowoczesnej (Internet, fora dyskusyjne, bazy danych itp.)
AIR_K4_U05	Absolwent/ka potrafi samodzielnie wyszukiwać niezbędne w procesie projektowania informacje oraz doszkalać się w miarę potrzeb, ze szczególnym uwzględnieniem możliwości oferowanych w tym zakresie przez Internet i systemy nauczania na odległość
AIR_K4_U07	Absolwent/ka potrafi posługiwać się narzędziami i metodami oferowanymi przez nowe technologie informacyjno-telekomunikacyjne; opierając się na wiedzy o zjawiskach i procesach fizycznych krytycznie i realistycznie oceniać możliwości, które oferują nowe technologie stosowane w informatyce i telekomunikacji
AIR_K4_U10	Absolwent/ka potrafi zaproponować ulepszenia aktualnie dostępnych rozwiązań z zakresu nowoczesnych technologii; projektować kompleksowe rozwiązania złożonych problemów z tego zakresu; uwzględnić okresowe aktualizacje, wynikające z postępu technologicznego
AIR_K4_U12	Absolwent/ka potrafi rozwiązać typowe zadania i problemy techniczne związane z oceną, analizą i budową popularnych sieci telekomunikacyjnych i komputerowych, zarówno przewodowych, jak i bezprzewodowych, korzystając z zależności opisujących własności fali elektromagnetycznej, technik kierowania ruchu czy ustawień konfigurujących urządzenia sieciowe
AIR_K4_U16	Absolwent/ka potrafi zaproponować wielowarstwową architekturę systemu dostępnego w sieci Internet, zarówno po stronie klienta, jak i serwera
AIR_K4_U19	Absolwent/ka potrafi opierając się na posiadanej wiedzy formułować hipotezy i testować poprawność projektowanego rozwiązania komputerowego
AIR_K4_W01	Absolwent/ka zna i rozumie w pogłębionym stopniu wybrane zagadnienia z zakresu fizyki, informatyki i telekomunikacji oraz nauk o zarządzaniu jakością, przydatne w zakresie modelowania i rozwiązywania problemów interdyscyplinarnych na styku tych dziedzin
AIR_K4_W02	Absolwent/ka zna i rozumie w pogłębionym stopniu kluczowe osiągnięcia nowoczesnej fizyki, stanowiące uporządkowaną podstawę teoretyczną rozwiązań informatyki technicznej i telekomunikacji, a także kluczowe osiągnięcia w naukach o zarządzaniu i jakości
AIR_K4_W03	Absolwent/ka zna i rozumie w pogłębionym stopniu trendy rozwojowe w zakresie fizyki, informatyki i telekomunikacji, a także nauk o zarządzaniu i jakości, ze szczególnym uwzględnieniem wzajemnego przenikania się tych dziedzin
AIR_K4_W04	Absolwent/ka zna i rozumie podstawowe technologie stosowane do rozwiązywania problemów praktycznych z pogranicza fizyki (zastosowania półprzewodników, fotonika, fizyka materiałów magnetycznych) oraz informatyki i telekomunikacji (systemy bezprzewodowe, sieci komputerowe i telekomunikacyjne)
AIR_K4_W05	Absolwent/ka zna i rozumie społeczne, ekonomiczne, prawne, psychologiczne i socjologiczne uwarunkowania i konsekwencje swoich działań, szczególnie w zakresie projektowania, wdrażania i wykorzystywania nowych systemów i technologii
AIR_K4_W09	Absolwent/ka zna i rozumie podstawowe zasady bezpieczeństwa i higieny pracy w odniesieniu do urządzeń elektrycznych, a także podstawowe zagrożenia wynikające ze stosowania nowoczesnych technologii informacyjno-telekomunikacyjnych

Kod	Treść
AIR_K4_W15	Absolwent/ka zna i rozumie w pogłębionym stopniu nowoczesne techniki informatyczne, w szczególności techniki i języki programowania imperatywnego i deklaratywnego, technologie Internetu (przygotowywanie i udostępnianie zawartości stron WWW i usług sieciowych), metodykę projektowania oprogramowania i zarządzania procesem projektowym