UNIWERSYTET MORSKI W GDYNI
Wydział Informatyki

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	C1	Przedmiot	PODSTAWY CYBERBEZPIECZEŃSTWA SYSTEMÓW IT

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	Liczba punktów ECTS	Liczba godzin w semestrze			
		W	C	L	P
1	1	15			
Razem w czasie studiów		**15**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
brak

Cele przedmiotu
Nabycie wiedzy w zakresie podstaw cyberbezpieczeństwa systemów IT

Przedmiotowe efekty uczenia się (PEU)

Symbol	Po zakończeniu przedmiotu student:	Odniesienie do kierunkowych efektów uczenia się
PEU_01	zna terminologię związana z cyberbezpieczeństwem oraz jego zagrożeniami	K_W01, K_W08, K_W11
PEU_02	charakteryzuje mechanizmy kontroli tożsamości, uwierzytelniania wieloskładnikowego oraz kontroli dostępu	K_W01, K_W08 K_W11
PEU_03	wyjaśnia podstawy kryptografii i jej zastosowanie w bezpieczeństwie IT	K_W01, K_W08 K_W11
PEU_04	charakteryzuje organizację i funkcjonowanie KSC (Krajowego Systemu Cyberbezpieczeństwa)	K_W01, K_W08 K_W11
PEU_05	rozpoznaje właściwe normy i procedury oceny zgodności	K_W01, K_W08 K_W11

Treści programowe	Liczba godzin				Odniesienie do PEU
	W	C	L	P	
Terminologia związana z cyberbezpieczeństwem	1				PEU_01
Zagrożenia cyberbezpieczeństwa	2				PEU_01
Ataki socjotechniczne	1				PEU_01
Mechanizmy kontroli tożsamości	2				PEU_02
Uwierzytelnianie wieloskładnikowe MFA (*Multi-Factor Authentication*)	1				PEU_02
Zasady kontroli dostępu	2				PEU_02
Podstawy kryptografii i jej zastosowanie w bezpieczeństwie IT	3				PEU_03
Podstawowe operacje kryptograficzne	1				PEU_03
Organizacja i funkcjonowanie KSC (Krajowego Systemu Cyberbezpieczeństwa)	1				PEU_04
Normy i procedury oceny zgodności	1				PEU_05
Łącznie godzin	**15**				

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X								
PEU_02	X								
PEU_03	X								
PEU_04	X								
PEU_05	X								

Kryteria zaliczenia przedmiotu
Zaliczenie treści wykładu: ocena z wykładu (W) wyznaczana jest na podstawie liczby zdobytych punktów z zaliczenia pisemnego, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia.

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	15			
Czytanie literatury	10			
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych				
Przygotowanie do egzaminu, zaliczenia	5			
Opracowanie dokumentacji projektu/sprawozdania				
Uczestnictwo w zaliczeniach i egzaminach	1			
Łącznie godzin	**31**			
Sumaryczna liczba godzin dla przedmiotu	**31**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**1**			
Obciążenie studenta związane z zajęciami praktycznymi				
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	16 godzin 1 ECTS			

Literatura podstawowa
1. Singh, A. K.: Introduction to Cybersecurity, Orient Blackswan Pvt Ltd, 2023. 2. Banasiński C., Rojszczak M. (red.): Cyberbezpieczeństwo. Zarys wykładu, PWN (Wolters Kluwer), Warszawa 2024. 3. Ciemski W.: Cybersecurity w pytaniach i odpowiedziach, SELF-PUBLISHER, 2026.
Literatura uzupełniająca
1. Wosiński K.: Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu, PWN, 2024. 2. Janczewski R.: Cyberwalka. Militarny wymiar działań, PWN, Warszawa 2023. 3. Zalewski M.: Cisza w sieci: praktyczny przewodnik po pasywnym rozpoznawaniu i atakach pośrednich, Helion, Gliwice 2005.

Osoba odpowiedzialna za przedmiot	
dr inż. Łukasz Apiecionek	
Pozostałe osoby prowadzące przedmiot	
mgr inż. Mateusz Dampc	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

UNIWERSYTET MORSKI W GDYNI
Wydział Informatyki

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	C2	Przedmiot	PROGRAMOWANIE W JĘZYKU PYTHON

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	Liczba punktów ECTS	Liczba godzin w semestrze			
		W	C	L	P
1	2	10		10	
Razem w czasie studiów		**20**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Znajomość zasad programowania, w tym obiektowego.

Cele przedmiotu
Poznanie zasad projektowania, implementowania i analizowania programów w języku Python wykorzystywanych w administracji systemami i przetwarzaniu danych. Nabycie podstawowych umiejętności praktycznych w zakresie programowania z wykorzystaniem języka Python.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	potrafi wyjaśnić i scharakteryzować zagadnienia związane z programowaniem strukturalnym i obiektowym przy zachowaniu podstawowych zasad bezpieczeństwa	K_W04, K_U03
PEU_02	potrafi projektować i implementować programy w języku Python wykorzystując mechanizmy programowania obiektowego, obsługę danych oraz wybrane biblioteki do automatyzacji zadań administracyjnych	K_W04, K_U03, K_K03
PEU_03	potrafi zastosować w programie podstawowe mechanizmy bezpieczeństwa oraz wykorzystać narzędzia do analizy jakości oprogramowania	K_W04, K_U03, K_U11, K_K02
PEU_04	jest przygotowany do odpowiedzialnego wykorzystania narzędzi programistycznych oraz do doskonalenia własnych kompetencji w zakresie programowania w języku Python	K_W04, K_U03, K_U11, K_K03

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Podstawy programowania w języku Python: składnia języka, typy danych, instrukcje warunkowe i iteracyjne, funkcje, moduły, obsługa wyjątków, operacje na plikach	2		2		PEU_01, PEU_02
Programowanie obiektowe: klasy i obiekty, dziedziczenie i polimorfizm, enkapsulacja, prosta aplikacja obiektowa	3		3		PEU_02, PEU_03
Tworzenie bezpiecznego kodu: zasady, walidacja danych wejściowych, obsługa wyjątków i błędów, bezpieczna obsługa plików, ochrona danych poufnych	2		2	0	PEU_01, PEU_03, PEU_04
Automatyzacja zadań administracyjnych: przetwarzanie plików tekstowych CSV i JSON, wykonywanie poleceń systemowych i ich automatyzacja, tworzenie prostych narzędzi administracyjnych,	3		3	0	PEU_02, PEU_04

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

harmonogramowanie wykonania skryptów, analiza logów systemowych					
Łącznie godzin	**10**		**10**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X								
PEU_02	X				X				
PEU_03	X				X				
PEU_04	X				X				

Kryteria zaliczenia przedmiotu
Zaliczenie treści wykładu: ocena z wykładu (W) wyznaczana jest na podstawie liczby zdobytych punktów z zaliczenia pisemnego, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Zaliczenie praktyczne laboratorium: ocena z laboratorium (L) wyznaczana jest na podstawie sprawozdań z wykonania zadań z poszczególnych części materiału, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Ocena końcowa jest wyznaczana zgodnie ze wzorem: 40%W+60%L

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	10		10	
Czytanie literatury	10		15	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			4	
Przygotowanie do egzaminu, zaliczenia	5		2	
Opracowanie dokumentacji projektu/sprawozdania			6	
Uczestnictwo w zaliczeniach i egzaminach	1		1	
Łącznie godzin	**26**		**38**	
Sumaryczna liczba godzin dla przedmiotu	**64**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi	38 godzin 1 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	22 godziny 1 ECTS			

Literatura podstawowa
1. Fluent Python. 2nd Edition, Ramalho L., O'Reilly Media 2022. 2. Dokumentacja online języka Python - https://docs.python.org/3/ 3. Podręczniki i dokumentacje online wybranych bibliotek języka Python.
Literatura uzupełniająca
1. Python for Security and Networking. Leverage Python modules and tools in securing your network and applications - Third Edition, Ortega J. M., Packt Publishing 2023. 2. Security Automation with Python. Practical Python solutions for automating and scaling security operations, Corey C. Sr., McMahon F., Packt Publishing 2025.

Osoba odpowiedzialna za przedmiot	
dr hab. Ewa Ratajczak-Ropel	
Pozostałe osoby prowadzące przedmiot	
mgr inż. Maciej Godek	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C3**	Przedmiot	**PROJEKTOWANIE I ADMINISTRACJA BAZAMI DANYCH**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
1	2	10		10	
Razem w czasie studiów		**20**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Wiedza z zakresu podstaw informatyki i technologii informacyjnych.

Cele przedmiotu
Nabycie wiedzy i umiejętności w zakresie projektowania i administracji bazami danych.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	rozumie i stosuje podstawową terminologię związaną z projektowaniem i administracją baz danych	K_W05, K_U04
PEU_02	tworzy i modyfikuje struktury bazy danych przy użyciu języka SQL oraz dokumentuje proces tworzenia i zmian w schemacie bazy danych	K_W05, K_U04, K_K03
PEU_03	zarządza danymi w relacyjnych bazach danych za pomocą złożonych zapytań SQL, z zachowaniem najwyższych standardów bezpieczeństwa, integralności, poufności i rozliczalności	K_W05, K_U04, K_K07, K_K08
PEU_04	administruje systemami zarządzania bazą danych wykorzystaniem mechanizmów autoryzacji i nadzoru dostępności zasobów bazodanowych	K_W05, K_U04
PEU_05	identyfikuje i przeciwdziała podatnościom typu wstrzykiwanie SQL (SQL Injection) oraz przeprowadza testy bezpieczeństwa pod kątem obecności luk typu injection	K_W05, K_U04, K_U11, K_K03
PEU_06	obsługuje nierelacyjne systemy baz danych (NoSQL): dobiera rodzaj bazy danych (SQL/NoSQL) do specyficznych wymagań projektu	K_W05, K_U04, K_U11

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Podstawowa terminologia związana z bazami danych: systemy i struktury baz danych, typy danych, modele danych, więzy integralności	2		2		PEU_01, PEU_02
Język SQL: język definicji danych (DDL), język manipulacji danymi (DML), różnice między składniami języka SQL głównych systemów baz danych	2		2		PEU_01, PEU_02, PEU_03
Zarządzanie bazami danych pod kątem cyberbezpieczeństwa: kontrola dostępu, identyfikacja zagrożeń, monitorowanie anomalii, uwierzytelnianie wieloskładnikowe, szyfrowanie danych,	5		4		PEU_03, PEU_04, PEU_05

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

przeprowadzanie testów bezpieczeństwa i wydajności bazy, tworzenie i zarządzanie kopiami zapasowymi					
Nierelacyjne bazy danych (NoSQL): cechy baz NoSQL, wady i zalety baz NoSQL, z uwzględnieniem zagrożeń bezpieczeństwa, przykłady zastosowań baz nierelacyjnych	1		2		PEU_06
Łącznie godzin	**10**		**10**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X							X	
PEU_02	X							X	
PEU_03	X							X	
PEU_04	X							X	
PEU_05	X							X	
PEU_06	X								

Kryteria zaliczenia przedmiotu
Pozytywna ocena z wykładu otrzymywana jest po uzyskaniu min. 50% punktów z testu zaliczeniowego. Pozytywna ocena z laboratorium otrzymywana jest po wykonaniu wszystkich zaplanowanych ćwiczeń laboratoryjnych. Ocena końcowa jest średnią arytmetyczną ocen z wszystkich form zajęć i może być pozytywna pod warunkiem zaliczenia testu i zajęć laboratoryjnych.

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	10		10	
Czytanie literatury	15		10	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			6	
Przygotowanie do egzaminu, zaliczenia	5			
Opracowanie dokumentacji projektu/sprawozdania			5	
Uczestnictwo w zaliczeniach i egzaminach	1		1	
Łącznie godzin	**31**		**32**	
Sumaryczna liczba godzin dla przedmiotu	**63**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi	32 godziny 1 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	22 godziny 1 ECTS			

Literatura podstawowa
1. Diaz C.: Database Security. Master the Art of Protecting Your Data with Cutting-Edge Techniques, Mercury Learning, 2024. 2. Sarma Danturthi R.: Database and Application Security: A Practitioners Guide, 1st edition, Published by Addison-Wesley Professional, 2024. 3. Cherry D.: Securing SQL Server - Protecting Your Database from Attackers, Elsevier, 2015.
Literatura uzupełniająca
1. Basta A.: Zgola M., Database Security, Cengage Learning, 2011. 2. Hassan A.A.: Database Security and Auditing: Protecting Data Integrity and Accessibility, Cengage Learning, 2005. 3. Dokumentacja techniczna i materiały producentów systemów zarządzania bazami danych (Oracle Database, Microsoft SQL Server, PostgreSQL, MySQL, MongoDB) dotyczące mechanizmów bezpieczeństwa, kontroli dostępu i audytu.

Osoba odpowiedzialna za przedmiot	
dr inż. Mirosław Łącki	
Pozostałe osoby prowadzące przedmiot	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C4**	Przedmiot	**ADMINISTROWANIE SIECIAMI**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
1	2	10		10	
Razem w czasie studiów		**20**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Brak wymagań wstępnych.

Cele przedmiotu
Zapoznanie studentów z podstawami funkcjonowania sieci teleinformatycznych oraz modeli OSI/TCP-IP, a także wykształcenie umiejętności praktycznych w zakresie adresacji IPv4/IPv6, konfiguracji i diagnostyki urządzeń sieciowych, projektowania podsieci oraz stosowania mechanizmów segmentacji, kontroli ruchu, routingu i translacji adresów w sieciach TCP/IP.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	wyjaśnia podstawowe pojęcia sieci teleinformatycznych oraz charakteryzuje ich działanie w oparciu o modele OSI/TCP-IP i protokoły transmisji danych	K_W03
PEU_02	stosuje adresację IPv4 i IPv6	K_W03, K_U02
PEU_03	konfiguruje podstawowe parametry sieciowe urządzeń końcowych i posługuje się narzędziami diagnostycznymi TCP/IP	K_W03, K_U02, K_K04
PEU_04	przeprowadza konfigurację podsieci oraz stosuje mechanizmy segmentacji i kontroli ruchu	K_W03, K_U02, K_K04
PEU_05	konfiguruje mechanizmy routingu i translacji adresów	K_W03, K_U02, K_K04

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Podstawowe pojęcia sieci teleinformatycznych oraz modele OSI/TCP-IP – rodzaje sieci, topologie, urządzenia sieciowe, media transmisyjne, warstwy modeli i protokoły transmisji danych (TCP, UDP, HTTP, DNS, DHCP, FTP)	2				PEU_01
Adresacja IPv4 i IPv6 – klasy adresów, adresy publiczne/prywatne, maska podsieci, notacja CIDR, budowa i zapis adresów IPv6, koegzystencja z IPv4	2		2		PEU_02
Konfiguracja urządzeń końcowych i diagnostyka sieci – parametry sieciowe (IP, maska, brama, DNS), konfiguracja statyczna i dynamiczna (DHCP), narzędzia diagnostyczne TCP/IP (ping, tracert,	2		3		PEU_03

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

ipconfig, netstat, nslookup)					
Podsieci, segmentacja i kontrola ruchu – subnetting, VLSM, sieci VLAN, listy ACL, podstawy QoS	2		2		PEU_04
Routing i translacja adresów – rodzaje routingu, tablice routingu, protokoły routingu, NAT/PAT	2		3		PEU_05
Łącznie godzin	**10**		**10**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X								
PEU_02	X								
PEU_03								X	
PEU_04								X	
PEU_05								X	

Kryteria zaliczenia przedmiotu
Zaliczenie treści wykładu: ocena z wykładu (W) wyznaczana jest na podstawie liczby zdobytych punktów z egzaminu pisemnego, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Zaliczenie praktyczne laboratorium: ocena z laboratorium (L) wyznaczana jest na podstawie sprawozdań z wykonania zadań z poszczególnych części materiału, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Ocena końcowa jest wyznaczana zgodnie ze wzorem: 40%W+60%L

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	10		10	
Czytanie literatury	10		10	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			5	
Przygotowanie do egzaminu, zaliczenia	10			
Opracowanie dokumentacji projektu/sprawozdania				
Uczestnictwo w zaliczeniach i egzaminach	1		1	
Udział w konsultacjach	2		2	
Łącznie godzin	**33**		**28**	
Sumaryczna liczba godzin dla przedmiotu	**61**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi	28 godzin 1 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	26 godzin 1 ECTS			

Literatura podstawowa
1. Sajdak M.: Wprowadzenie bo bezpieczeństwa IT, Tom 2, wyd. Securitum, Kraków 2024. 2. Tanenbaum A.S., Wetherall D.J.: Sieci komputerowe. Wydanie V, Helion, Gliwice 2016.
Literatura uzupełniająca
1. Fall K.R., Stevens W.R.: TCP/IP od środka. Protokoły. Wydanie II, Helion, Gliwice. 2. Parker T., Sportack M.: TCP/IP. Księga eksperta, Helion. 3. Kluczewski J.: Bezpieczeństwo sieci komputerowych. Praktyczne ujęcie, Helion.

Osoba odpowiedzialna za przedmiot	
dr inż. Łukasz Apiecionek	
Pozostałe osoby prowadzące przedmiot	
mgr inż. Mateusz Dampc	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

UNIWERSYTET MORSKI W GDYNI
Wydział Informatyki

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	C5	Przedmiot	UŻYTKOWANIE, KONFIGURACJA I UTWARDZANIE SYSTEMU WINDOWS I LINUX

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	Liczba punktów ECTS	Liczba godzin w semestrze			
		W	C	L	P
1	2	10		10	
Razem w czasie studiów		**20**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
brak

Cele przedmiotu
Wykształcenie u studentów wiedzy i umiejętności w zakresie bezpiecznej administracji systemami operacyjnymi Linux i Windows.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	charakteryzuje i analizuje architekturę oraz mechanizmy bezpieczeństwa systemów operacyjnych pod kątem wektorów ataków	K_W01, K_W02
PEU_02	wdraża systemy operacyjne w standardzie utwardzonej instalacji oraz utwardza konfigurację systemów Windows i Linux	K_W02, K_U01
PEU_03	automatyzuje zadania administracyjne za pomocą skryptów oraz narzędzi sztucznej inteligencji	K_W04, K_U03, K_U10
PEU_04	administruje usługami, harmonogramem zadań oraz systemami logowania i audytu zdarzeń	K_W02, K_U01, K_K04
PEU_05	zarządza zaporą sieciową i bezpieczeństwem sieciowym hosta oraz zabezpiecza niskopoziomową konfigurację systemu	K_W02, K_U01, K_K04
PEU_06	wykorzystuje wirtualizację i konteneryzację oraz wdraża bezpieczne środowiska wirtualne i kontenerowe w środowisku chmurowym	K_W10, K_U08, K_K04

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Architektura i mechanizmy bezpieczeństwa systemów operacyjnych – budowa systemu, wektory ataków, mechanizmy ochronne (Windows i Linux)	2				PEU_01
Utwardzona instalacja i konfiguracja systemów operacyjnych – standardy hardeningu, utwardzanie Windows i Linux	1		3		PEU_02
Tożsamość, kontrola dostępu i ochrona danych – model zerowego zaufania, uwierzytelnianie i autoryzacja, zarządzanie systemami plików	2		2		PEU_02
Wykrywanie zagrożeń i ochrona przed złośliwym oprogramowaniem – analiza procesów i usług, wykrywanie anomalii, mechanizmy	1		1		PEU_02

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

antywirusowe/EDR					
Automatyzacja i administracja systemem – skrypty administracyjne, narzędzia AI, zarządzanie usługami i harmonogramem zadań.	1		1		PEU_03, PEU_04
Logowanie, audyt i bezpieczeństwo sieciowe hosta – systemy logów i audytu zdarzeń, konfiguracja zapory sieciowej, niskopoziomowa konfiguracja systemu	2		2		PEU_04, PEU_05
Wirtualizacja, konteneryzacja i środowiska chmurowe – bezpieczne wdrażanie maszyn wirtualnych i kontenerów w Linux i chmurze	1		1		PEU_06
Łącznie godzin	**10**		**10**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X								
PEU_02								X	
PEU_03								X	
PEU_04	X								
PEU_05								X	
PEU_06	X								

Kryteria zaliczenia przedmiotu
Zaliczenie treści wykładu: ocena z wykładu (W) wyznaczana jest na podstawie liczby zdobytych punktów z egzaminu pisemnego, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Zaliczenie praktyczne laboratorium: ocena z laboratorium (L) wyznaczana jest na podstawie sprawozdań z wykonania zadań z poszczególnych części materiału, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Ocena końcowa jest wyznaczana zgodnie ze wzorem: 40%W+60%L

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	10		10	
Czytanie literatury	12		9	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			6	
Przygotowanie do egzaminu, zaliczenia	8			
Opracowanie dokumentacji projektu/sprawozdania				
Uczestnictwo w zaliczeniach i egzaminach	1		1	
Udział w konsultacjach	2		2	
Łącznie godzin	**33**		**28**	
Sumaryczna liczba godzin dla przedmiotu	**61**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi	28 godzin 1 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	26 godzin 1 ECTS			

Literatura podstawowa
1. Szafrański, K.: *Twierdza Linux: bezpieczeństwo dla dociekliwych*, wyd. Securitum, Kraków 2026. 2. Sajdak M.: Wprowadzenie bo bezpieczeństwa IT, Tom 2, wyd. Securitum, Kraków 2024.
Literatura uzupełniająca
1. Tevault D.A.: Bezpieczeństwo systemu Linux. Hardening i najnowsze techniki zabezpieczania przed cyberatakami. Wydanie III, Helion, Gliwice 2023. 2. Kalsi T.: Bezpieczeństwo systemu Linux w praktyce. Receptury. Wydanie II, Helion. 3. Nemeth E., Snyder G., Hein T.R., Whaley B.: Unix i Linux. Przewodnik administratora systemów. Wydanie IV, Helion.

Osoba odpowiedzialna za przedmiot	
dr inż. Łukasz Apiecionek	
Pozostałe osoby prowadzące przedmiot	
mgr inż. Mateusz Dampc	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

UNIWERSYTET MORSKI W GDYNI
Wydział Informatyki

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C6**	Przedmiot	**PODSTAWY DYDAKTYKI ZAWODOWEJ**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
1	1	3	10		
Razem w czasie studiów		**13**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Gotowość do pracy metodami aktywizującymi, problemowymi i projektowymi Podstawowa znajomość organizacji pracy szkoły i specyfiki pracy nauczyciela

Cele przedmiotu
Przygotowanie słuchaczy do planowania, projektowania, realizowania i oceniania zajęć z zakresu cyberbezpieczeństwa

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	rozumie specyfikę dydaktyki cyberbezpieczeństwa jako obszaru łączącego wiedzę, umiejętności praktyczne, kompetencje społeczne i odpowiedzialne zachowania	K_W09, K_U09
PEU_02	określa cele kształcenia w zakresie przedmiotu i przekłada je na oczekiwane efekty uczenia się	K_W09, K_K05
PEU_03	zna zasady konstruowania programu nauczania i scenariusza zajęć	K_W09, K_U09, K_K03
PEU_04	dobiera metody, formy i środki dydaktyczne odpowiednie do celów zajęć i poziomu uczniów	K_W09, K_U09, K_K01, K_K08
PEU_05	planuje proces dydaktyczny i własny rozwój z kontekście idei uczenia się przez całe życie (LLL), z uwzględnieniem założeń reformy edukacji zawodowej, w tym doradztwa zawodowego (edukacji karierowej)	K_W09, K_U09, K_K01, K_K08

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Specyfika uczenia cyberbezpieczeństwa z uwzględnieniem efektów kształcenia i kompetencji zawodowych	0,5	2			PEU_01, PEU_02
Projektowanie scenariuszy zajęć z cyberbezpieczeństwa	0,5	2			PEU_02, PEU_03
Metodyka nauczania przedmiotów zawodowych	1	4			PEU_01, PEU_03, PEU_04
Planowanie procesu dydaktycznego w perspektywie idei uczenia się przez całe życie. PRK a ERK (kwalifikacje sektorowe, wolnorynkowe, inne). Metodyka projektowania zadań interdyscyplinarnych dla technika cyberbezpieczeństwa w kontekście rozwoju kompetencji przekrojowych	1	2			PEU_05
Łącznie godzin	**3**	**10**			

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01							X		
PEU_02							X		
PEU_03							X		
PEU_04							X		
PEU_05							X		

Kryteria zaliczenia przedmiotu
Zaprojektowanie scenariusza zajęć interdyscyplinarnych w obszarze cyberbezpeieczeństwa oraz przygotowanie i zaprezentowanie planu rozwoju zawodowego w kontekście całożyciowego uczenia się (nauczyciel, uczeń).

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	3	10		
Czytanie literatury	10	2		
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych		2		
Przygotowanie do egzaminu, zaliczenia				
Opracowanie dokumentacji projektu/sprawozdania		5		
Uczestnictwo w zaliczeniach i egzaminach				
Uczestnictwo w konsultacjach	1	1		
Łącznie godzin	**14**	**20**		
Sumaryczna liczba godzin dla przedmiotu	**34**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**1**			
Obciążenie studenta związane z zajęciami praktycznymi				
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	15 godziny 1 ECTS			

Literatura podstawowa
1. Okoń W.: Wprowadzenie do dydaktyki ogólnej, Żak, Warszawa, 1998. 2. Niemierko B.: Kształcenie szkolne. Podręcznik skutecznej dydaktyki, WAiP, Warszawa, 2007. 3. Kolb A., Kolb D.: Uczenie na podstawie doświadczania, wyd. Dialogi i Zmysły, Opole,2022. 4. Sektorowa Rama Kwalifikacji dla Cyberbezpieczeństwa (SRK CYBER); E. Cieszkowska, A. Cieślak, M. Drzymulska-Derda i in., Instytut Badań Edukacyjnych (IBE), Warszawa 2024; MEN, Warszawa 2026. 5. Zintegrowany System Kwalifikacji (ZSK) – Przewodnik po rejestrze i pojęciach (ZRK); Instytut Badań Edukacyjnych (IBE) / Portal kwalifikacje.gov.pl. 6. Zintegrowana Strategia Umiejętności 2030 (część szczegółowa); MEN / MC, Warszawa.
Literatura uzupełniająca
1. Arends R.I.: Uczymy się nauczać, WSiP, Warszawa 1995. 2. Siemak-Tylikowska A, Sobolewska A.: Dydaktyka przedmiotów zawodowych, PW, 2009. 3. Grocholiński P. i inni, Design thinking dla edukatorów, UŁ, Łódź 2021. 4. Zadania interdyscyplinarne. Konstruowanie i stosowanie; Autorzy: M. Skura, M. Lisicki, Centrum Edukacji Obywatelskiej (CEO), Warszawa 2022. 5. Dydaktyka rozwoju kompetencji proinnowacyjnych; Autor: J. Witkowski (red.), Centrum Edukacji Obywatelskiej (CEO), Warszawa 2022. 6. Kształcenie dla przyszłości a kompetencje przekrojowe; Autorzy: H. Dębowski, W. Stęchły, Fundacja Rektorów Polskich, Warszawa 2019.

Osoba odpowiedzialna za przedmiot	
mgr Urszula Kornas-Krzyżykowska	
Pozostałe osoby prowadzące przedmiot	
mgr Grażyna Kurowska	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C7**	Przedmiot	**TESTOWANIE BEZPIECZEŃSTWA SIECI TCP/IP**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
2	2	10		5	
Razem w czasie studiów		**15**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Wiedza z zakresu budowy i działania sieci komputerowych oraz podstaw administrowania systemami operacyjnymi Windows i Linux.

Cele przedmiotu
Wykształcenie u studentów umiejętności rozpoznawania i weryfikowania zagrożeń bezpieczeństwa w sieciach TCP/IP wraz z przygotowaniem odpowiedniej dokumentacji analitycznej z zakresu cyberbezpieczeństwa.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	rozpoznaje zagrożenia bezpieczeństwa występujące w sieciach TCP/IP	K_W01, K_W03
PEU_02	weryfikuje konfigurację sieci pod kątem bezpieczeństwa	K_W03, K_U01, K_U02, K_U06
PEU_03	monitoruje i dokumentuje operacyjne działanie infrastruktury sieciowej	K_W03, K_U02, K_U07
PEU_04	rozpoznaje i analizuje próby naruszenia bezpieczeństwa sieci TCP/IP	K_W01, K_U06, K_K06
PEU_05	analizuje incydenty sieciowe oraz opracowuje dokumentację analityczną	K_U06, K_U07, K_K01

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Zagrożenia bezpieczeństwa w sieciach TCP/IP – rodzaje ataków (sniffing, spoofing, DoS/DDoS, man-in-the-middle), podatności protokołów i usług sieciowych	2				PEU_01
Weryfikacja konfiguracji sieci pod kątem bezpieczeństwa – audyt ustawień urządzeń sieciowych, reguły firewall i listy kontroli dostępu (ACL), zasady hardeningu konfiguracji	1		1		PEU_02
Monitorowanie infrastruktury sieciowej – narzędzia i metody monitoringu ruchu sieciowego, logowanie zdarzeń sieciowych	2		1		PEU_03
Dokumentowanie operacyjnego działania infrastruktury sieciowej – zasady prowadzenia dokumentacji technicznej i raportowania stanu sieci	1				PEU_03

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Rozpoznawanie prób naruszenia bezpieczeństwa – identyfikacja anomalii i symptomów ataków w ruchu sieciowym	1		1		PEU_04
Analiza prób naruszenia bezpieczeństwa sieci TCP/IP – badanie logów i śladów incydentów, wstępna klasyfikacja zdarzeń	1		1		PEU_04
Analiza incydentów sieciowych – proces reagowania na incydenty, ustalanie przyczyn i skutków naruszeń	1		1		PEU_05
Dokumentacja analityczna incydentów – opracowywanie raportów z analizy incydentów wraz z wnioskami i rekomendacjami	1				PEU_05
Łącznie godzin	**10**		**5**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X								
PEU_02	X							X	
PEU_03	X							X	
PEU_04								X	
PEU_05								X	

Kryteria zaliczenia przedmiotu
Zaliczenie treści wykładu: ocena z wykładu (W) wyznaczana jest na podstawie liczby zdobytych punktów z egzaminu pisemnego, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Zaliczenie praktyczne laboratorium: ocena z laboratorium (L) wyznaczana jest na podstawie sprawozdań z wykonania zadań z poszczególnych części materiału, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Ocena końcowa jest wyznaczana zgodnie ze wzorem: 40%W+60%L

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	10		5	
Czytanie literatury	8		5	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			6	
Przygotowanie do egzaminu, zaliczenia	10			
Opracowanie dokumentacji projektu/sprawozdania			4	
Uczestnictwo w zaliczeniach i egzaminach	1			
Udział w konsultacjach	2		2	
Łącznie godzin	**31**		**22**	
Sumaryczna liczba godzin dla przedmiotu	**53**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi	22 godzin 1 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	20 godzin 1 ECTS			

Literatura podstawowa
1. Tanenbaum A.S., Wetherall D.J., *Sieci komputerowe*, wyd. Helion, Gliwice 2012. 2. Sajdak M.: Wprowadzenie bo bezpieczeństwa IT, Tom 2, wyd. Securitum, Kraków 2024.
Literatura uzupełniająca
1. Velu V.K.: Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite. Wydanie IV, Helion, Gliwice 2022. 2. Singh G.D.: Kali Linux. Zaawansowane testy penetracyjne za pomocą narzędzi Nmap, Metasploit, Aircrack-ng i Empire. Wydanie II, Helion. 3. Messier R.: Kali Linux. Testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie. Wydanie II, Helion.

Osoba odpowiedzialna za przedmiot	
dr inż. Łukasz Apiecionek	
Pozostałe osoby prowadzące przedmiot	
mgr inż. Mateusz Dampc	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C8**	Przedmiot	**IMPLEMENTAJA APLIKACJI WEBOWYCH**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
1	2	15		15	
Razem w czasie studiów		**30**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Znajomość podstawowych zagadnień związanych z technologiami internetowymi i umiejętność programowania obiektowego oraz znajomość systemów baz danych i języka SQL.

Cele przedmiotu
Zapoznanie z zagadnieniami związanymi z programowaniem aplikacji webowych na przykładzie technologii Java. Wykształcenie praktycznych umiejętności programowania aplikacji webowych w języku Java z wykorzystaniem HTML, XML, CSS, frameworka Spring i wybraną bazą danych.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	potrafi wyjaśnić i scharakteryzować podstawowe pojęcia związane z aplikacjami WWW zasadami ich budowy, projektowaniem i programowaniem oraz wykorzystywanymi technologiami	K_W06, K_U05
PEU_02	potrafi wykorzystać praktycznie poznane technologie internetowe, np. Jakarta EE do programowania wybranej aplikacji WWW	K_W06, K_U05, K_K03
PEU_03	potrafi zaprojektować i napisać prostą aplikację WWW korzystając z poznanych technologii np. Jakarta EE	K_W06, K_U05, K_U11, K_K03
PEU_04	jest przygotowany do doskonalenia własnych kompetencji programistycznych oraz odpowiedzialnego wykorzystania narzędzi programistycznych w zakresie technologii Java	K_W06, K_U05, K_U11, K_K07

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Wprowadzenie: programowanie aplikacji webowych, budowa i architektura aplikacji webowych (klient-serwer, MVC, REST API, JWT). Środowiska programowania i programy współpracujące, np. Eclipse, VS Code	2		2		PEU_01, PEU_02
Technologie Java dla aplikacji Web, np.: Java/Jakarta Servlet, JSP, JSTL, EL, Java API for JSON, Thymeleaf. Framework Spring Boot	3		3		PEU_02, PEU_03
Współpraca z serwerem i kontenerem srwletów, łączenie kodu Java z innymi językami. Współpraca z bazami danych: JDBC, ORM, JPA, Spring Data JPA	3		3	0	PEU_01, PEU_03, PEU_04
Przegląd wybranych frameworków np. JSF, Hibernate, Spring dla	5		5	0	PEU_02, PEU_04

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

standardu Jakarta. Wzorce oprogramowania, np. MVC, REST i ich zastosowania					
Zarządzanie projektami Java: Maven, Gradle	2		2		PEU_02, PEU_03
Łącznie godzin	**15**		**15**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X								
PEU_02	X				X				
PEU_03	X				X	X			
PEU_04	X				X				

Kryteria zaliczenia przedmiotu
Zaliczenie treści wykładu: ocena z wykładu (W) wyznaczana jest na podstawie liczby zdobytych punktów z zaliczenia pisemnego, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Zaliczenie praktyczne laboratorium: ocena z laboratorium (L) wyznaczana jest na podstawie sprawozdań z wykonania zadań z poszczególnych części materiału, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Ocena końcowa jest wyznaczana zgodnie ze wzorem: 40%W+60%L

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	15		15	
Czytanie literatury	10		15	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			8	
Przygotowanie do egzaminu, zaliczenia	12			
Opracowanie dokumentacji projektu/sprawozdania			8	
Uczestnictwo w zaliczeniach i egzaminach	1			
Łącznie godzin	**38**		**46**	
Sumaryczna liczba godzin dla przedmiotu	**84**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**3**			
Obciążenie studenta związane z zajęciami praktycznymi	46 godzin 2 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	31 godzin 1 ECTS			

Literatura podstawowa
1. Spilca L.: Spring Start Here. Learn what you need and learn it well. Manning 2021. 2. Building an Application with Spring Boot, https://spring.io/projects/spring-boot. 3. Specyfikacja Jakarta EE. 4. Podręczniki i dokumentacje on-line wybranych technologii, systemów i narzędzi.
Literatura uzupełniająca
1. Hackler M., Spring Boot: Up and Running. O'Reilly Media 2021 2. Walls C.: Spring in action, Manning 2021 3. Dokumentacja Thymeleaf: https://www.thymeleaf.org/documentation.html 4. Introduction to Using Thymeleaf in Spring, https://www.baeldung.com/thymeleaf-in-spring-mvc

Osoba odpowiedzialna za przedmiot	
dr hab. Ewa Ratajczak-Ropel	
Pozostałe osoby prowadzące przedmiot	
mgr inż. Juliusz Łosiński	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C9**	Przedmiot	**WERYFIKOWANIE BEZPIECZEŃSTWA IMPLEMENTACJI APLIKACJI WEBOWYCH**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
2	2	10		10	
Razem w czasie studiów		**20**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Projektowanie i administracja bazami danych oraz implementacja aplikacji webowych.

Cele przedmiotu
Nabycie wiedzy i umiejętności w zakresie weryfikowania bezpieczeństwa implementacji aplikacji webowych.

Przedmiotowe efekty uczenia się (PEU)

Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	identyfikuje błędy w kodzie źródłowym związane z poprawnością działania i bezpieczeństwem	K_W01, K_W02, K_W04, K_W05, K_W06, K_U04, K_U05
PEU_02	identyfikuje typowe podatności aplikacji webowych na podstawie analizy kodu źródłowego	K_W01, K_W02, K_W04, K_W05, K_W06, K_U04, K_U05
PEU_03	wykorzystuje narzędzia do analizy i poprawy bezpieczeństwa aplikacji webowych	K_W01, K_W02, K_W04, K_W05, K_W06, K_U04, K_U05, K_K04
PEU_04	zabezpiecza aplikacje webowe przed atakiem	K_W01, K_W02, K_W04, K_W05, K_W06, K_W07, K_U04, K_U05, K_U06, K_K04

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Wybrane błędy w kodzie źródłowym związane z poprawnością działania i bezpieczeństwem	2		2		PEU_01
Typowe podatności aplikacji webowych na podstawie analizy kodu źródłowego	4		4		PEU_02
Wybrane narzędzia do analizy i poprawy bezpieczeństwa aplikacji webowych	2		2		PEU_03

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Metody zabezpieczania aplikacji webowych przed atakiem	2		2		PEU_04
Łącznie godzin	**10**		**10**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X				X				
PEU_02	X				X				
PEU_03	X				X				
PEU_04	X				X				

Kryteria zaliczenia przedmiotu
Zaliczenie treści wykładu: ocena z wykładu (W) wyznaczana jest na podstawie liczby zdobytych punktów z zaliczenia pisemnego, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Zaliczenie praktyczne laboratorium: ocena z laboratorium (L) wyznaczana jest na podstawie sprawozdań z wykonania zadań z poszczególnych części materiału, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Ocena końcowa jest wyznaczana zgodnie ze wzorem: 40%W+60%L

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	10		10	
Czytanie literatury	12		7	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			8	
Przygotowanie do egzaminu, zaliczenia	5			
Opracowanie dokumentacji projektu/sprawozdania			7	
Uczestnictwo w zaliczeniach i egzaminach	1			
Łącznie godzin	**28**		**32**	
Sumaryczna liczba godzin dla przedmiotu	**60**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi	32 godziny 1 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	21 godzin 1 ECTS			

Literatura podstawowa
1. Velu V.K.: Kali Linux i zaawansowane testy penetracyjne. Wydanie IV, Helion, Gliwice 2022. 2. OWASP Top 10 – Dokumentacja online (dostępne bezpłatnie), https://owasp.org/www-project-top-ten/
Literatura uzupełniająca
1. Aumasson J.P.: Nowoczesna kryptografia. Praktyczne wprowadzenie, Helion. 2. Kluczewski J.: Bezpieczeństwo sieci komputerowych. Praktyczne ujęcie, Helion. 3. Ball C.J.: Cybersecurity w pytaniach i odpowiedziach, Helion.

Osoba odpowiedzialna za przedmiot	
dr inż. Łukasz Apiecionek	
Pozostałe osoby prowadzące przedmiot	
mgr inż. Mateusz Dampc	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C10**	Przedmiot	**PRZEPROWADZANIE TESTÓW PENETRACYJNYCH APLIKACJI WEBOWYCH W ŚRODOWISKU TESTOWYM**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
2	2	10		10	
Razem w czasie studiów		**20**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Projektowanie i administracja bazami danych oraz implementacja aplikacji webowych

Cele przedmiotu
Nabycie wiedzy i umiejętności w zakresie przeprowadzania testów penetracyjnych aplikacji webowych w środowisku testowym

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	planuje i przygotowuje testy penetracyjne aplikacji webowych	K_W01, K_W02, K_W03, K_W04, K_W05, K_W06, K_W07
PEU_02	analizuje podatności aplikacji webowych	K_W01, K_W07, K_U02, K_U04, K_U05, K_U06, K_U07, K_K06
PEU_03	wykorzystuje narzędzia do automatyzacji testowania bezpieczeństwa aplikacji webowych	K_W01, K_W07, K_U02, K_U04, K_U05, K_U06, K_U07, K_K06
PEU_04	przeprowadza ataki na mechanizmy uwierzytelniania i sesji aplikacji webowych działających w środowisku kontrolowanym	K_W01, K_W07, K_U02, K_U04, K_U05, K_U06, K_U07, K_K06
PEU_05	analizuje wyniki testów penetracyjnych i sporządza podstawową dokumentację testową	K_W01, K_W07, K_W08, K_U02, K_U04, K_U05, K_U06, K_U07

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Planowanie i przygotowywanie testów penetracyjnych aplikacji webowych	1				PEU_01

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Przeprowadzanie rekonesans i analiza powierzchni ataku aplikacji webowej	1				PEU_02
Identyfikacja podstawowych podatności aplikacji webowych metodą „czarnej skrzynki” (black box)	1		2		PEU_02
Narzędzia do automatyzacji testowania bezpieczeństwa aplikacji webowych	2		2		PEU_02, PEU_03
Ataki na mechanizmy uwierzytelniania i sesji aplikacji webowych działających w środowisku kontrolowanym	2		4		PEU_04
Atak typu Man-in-the-Middle (MiTM)	2		2		PEU_04
Analiza wyników testów penetracyjnych i dokumentacja testowa	1				PEU_05
Łącznie godzin	**10**		**10**		

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01	X								
PEU_02	X				X				
PEU_03	X				X				
PEU_04	X				X				
PEU_05	X								

Kryteria zaliczenia przedmiotu
Zaliczenie treści wykładu: ocena z wykładu (W) wyznaczana jest na podstawie liczby zdobytych punktów z zaliczenia pisemnego, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Zaliczenie praktyczne laboratorium: ocena z laboratorium (L) wyznaczana jest na podstawie sprawozdań z wykonania zadań z poszczególnych części materiału, próg zaliczenia – uzyskanie co najmniej 55% punktów możliwych do zdobycia. Ocena końcowa jest wyznaczana zgodnie ze wzorem: 40%W+60%L

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	10		10	
Czytanie literatury	10		7	
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych			5	
Przygotowanie do egzaminu, zaliczenia	7			
Opracowanie dokumentacji projektu/sprawozdania			6	
Uczestnictwo w zaliczeniach i egzaminach	2			
Łącznie godzin	**29**		**28**	
Sumaryczna liczba godzin dla przedmiotu	**57**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi	28 godzin 1 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	22 godziny 1 ECTS			

Literatura podstawowa
1. Velu V.K.: Kali Linux i zaawansowane testy penetracyjne. Wydanie IV, Helion, Gliwice 2022. 2. Messier R.: Kali Linux. Testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie. Wydanie II, Helion.
Literatura uzupełniająca
1. Singh G.D.: Kali Linux. Zaawansowane testy penetracyjne za pomocą narzędzi Nmap, Metasploit, Aircrack-ng i Empire. Wydanie II, Helion. 2. Parasram S.V.N.: Informatyka śledcza i Kali Linux: przeprowadź analizy nośników pamięci, ruchu sieciowego i zawartości RAM-u, Helion. 3. Muniz J., Lakhani A.: Kali Linux. Testy penetracyjne, Helion. 4. Ansari J.A.: Kali Linux. Testy penetracyjne. Wydanie II, Helion, 2017.

Osoba odpowiedzialna za przedmiot	
dr inż. Łukasz Apiecionek	
Pozostałe osoby prowadzące przedmiot	
mgr inż. Mateusz Dampc	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C11**	Przedmiot	**KOMUNIKACJA DYDAKTYCZNA W CYBERBEZPIECZEŃSTWIE**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
II	1	10	7		
Razem w czasie studiów		**17**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Podstawy dydaktyki zawodowej

Cele przedmiotu
Przygotowanie nauczyciela do przystępnego przekazywania trudnych treści technicznych z cyberbezpieczeństwa uczniom o zróżnicowanym poziomie wiedzy oraz rozwijanie kompetencji komunikacyjnych w sytuacjach trudnych.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	charakteryzuje specyfikę i bariery komunikacji dydaktycznej w nauczaniu cyberbezpieczeństwa uczniów o zróżnicowanym poziomie wiedzy technicznej	K_W09, K_K03
PEU_02	dostosowuje terminologię, język i formę przekazu treści z cyberbezpieczeństwa do poziomu rozwoju poznawczego, potrzeb edukacyjnych i stylów uczenia się uczniów	K_W09, K_U09, K_K10
PEU_03	stosuje techniki wyjaśniania pojęć abstrakcyjnych oraz komunikacji wizualnej w nauczaniu cyberbezpieczeństwa i odpowiedzialnie wykorzystuje narzędzia sztucznej inteligencji do wspomagania komunikacji dydaktycznej	K_U09, K_U10, K_K07
PEU_04	prowadzi komunikację w sytuacjach trudnych (błędy uczniowskie, incydenty, cyberprzemoc, dezinformacja) oraz współpracuje komunikacyjnie z rodzicami, nauczycielami i otoczeniem szkoły w sprawach cyberbezpieczeństwa	K_K01, K_K02, K_K10

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Komunikacja dydaktyczna jako element warsztatu nauczyciela cyberbezpieczeństwa: model komunikacji, autorytet nauczyciela, interakcje, bariery w przekazywaniu treści technicznych	3				PEU_01
Język nauczania cyberbezpieczeństwa: terminologia branżowa, dostosowanie przekazu do rozwoju poznawczego ucznia i zasad projektowania uniwersalnego w uczeniu się (UDL)	3				PEU_02
Wyjaśnianie pojęć abstrakcyjnych: analogie i metafory w cyberbezpieczeństwie, modele i symulacje, komunikacja wizualna, storytelling i scenariusze zagrożeń jako narzędzie dydaktyczne	1	3			PEU_03
Narzędzia sztucznej inteligencji we wspomaganiu komunikacji dydaktycznej w cyberbezpieczeństwie: krytyczna ocena treści, ochrona danych i prawa autorskie	1	1			PEU_03

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Komunikacja w sytuacjach trudnych: komunikacja podczas incydentu bezpieczeństwa i w przypadku cyberprzemocy, rozmowa o ryzyku bez wzbudzania lęku, przeciwdziałanie dezinformacji	1	1			PEU_04
Komunikacja z otoczeniem szkoły: rozmowa z rodzicami o bezpieczeństwie cyfrowym dziecka, komunikowanie zasad higieny cyfrowej, etyka komunikacji i ochrona danych osobowych	1	2			PEU_04
Łącznie godzin	**10**	**7**			

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01				X					
PEU_02				X			X		
PEU_03						X	X		
PEU_04						X	X		

Kryteria zaliczenia przedmiotu
Ocena z jest wyznaczana na podstawie: kolokwium pisemnego (40%), prezentacji mikronauczania (30%) oraz projektu (30%). Próg zaliczenia – uzyskanie co najmniej 55% punktów łącznie oraz oddanie wszystkich elementów.

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe	10	7		
Czytanie literatury	3	2		
Przygotowanie do zajęć		2		
Przygotowanie do kolokwium zaliczeniowego	2	1		
Przygotowanie prezentacji mikronauczania i projektu zaliczeniowego	5	3		
Uczestnictwo w zaliczeniach	1			
Łącznie godzin	**21**	**15**		
Sumaryczna liczba godzin dla przedmiotu	**36**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**1**			
Obciążenie studenta związane z zajęciami praktycznymi	15 godzin 1 ECTS			
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	18 godzin 1 ECTS			

Literatura podstawowa

1. Sterna D.: Uczę (się) w szkole, Centrum Edukacji Obywatelskiej, Warszawa 2014.
2. Petty G.: Nowoczesne nauczanie. Praktyczne wskazówki i techniki dla nauczycieli, wykładowców i szkoleniowców, GWP, Sopot 2018.
3. Żylińska M.: Neurodydaktyka. Nauczanie i uczenie się przyjazne mózgowi, UMK, Toruń 2013.
4. Podstawa programowa kształcenia w zawodzie technik cyberbezpieczeństwa (351304) , Dz. U. 2026 poz. 404.
5. Materiały edukacyjne CERT Polska / NASK dotyczące bezpieczeństwa w sieci – https://cert.pl

Literatura uzupełniająca

1. Rosenberg M. B.: Porozumienie bez przemocy. O języku życia, wyd. III rozszerzone, Czarna Owca, Warszawa 2016.
2. Roam D.: Narysuj swoje myśli. Jak skutecznie prezentować i sprzedawać pomysły na kartce papieru, Helion, Gliwice 2010.
3. Brophy J.: Motywowanie uczniów do nauki, PWN, Warszawa 2007.
4. ENISA, Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education, European Union Agency for Cybersecurity, listopad 2021.
5. Harasim L.: Learning Theory and Online Technologies, 2nd Edition, Routledge, New York 2017.

Osoba odpowiedzialna za przedmiot	
mgr inż. Cezary Graul	
Pozostałe osoby prowadzące przedmiot	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

UNIWERSYTET MORSKI W GDYNI
Wydział Informatyki

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C12**	Przedmiot	**WARSZTAT PRACY NAUCZYCIELA CYBERBEZPIECZEŃSTWA**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
III	2	30			
Razem w czasie studiów		**30**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Podstawy dydaktyki zawodowej oraz komunikacja dydaktyczna w cyberbezpieczeństwie.

Cele przedmiotu
Nabycie wiedzy i umiejętności w zakresie projektowania i przygotowania warsztatu pracy nauczyciela cyberbezpieczeństwa.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	projektuje architekturę pracowni oraz dobiera infrastrukturę sprzętową pracowni i oprogramowanie oraz środowiska wirtualne i konteneryzowane z uwzględnieniem licencji i możliwości odtwarzania środowisk	K_W09, K_W10, K_U08, K_U09, K_K03
PEU_02	uwzględnia w projekcie pracowni zasady BHP, bezpiecznego korzystania z narzędzi ofensywnych, regulacje prawne i ochronę danych osobowych oraz odpowiedzialnie wykorzystuje narzędzia sztucznej inteligencji	K_W08, K_K07
PEU_03	organizuje pracę zespołu nauczycielskiego metodą projektu oraz przygotowuje dokumentację projektową pracowni	K_K06, K_U09
PEU_04	charakteryzuje mechanizmy powstawania oporu wobec nowych technologii i IoT oraz profiluje zespół nauczycielski i klasę pod kątem motywacji i ról zespołowych, w tym w pracy z uczniami neuroróżnorodnymi i introwertycznymi	K_W09, K_W11, K_U09, K_K05, K_K06
PEU_05	organizuje pracę zespołową i rozwiązuje konflikty w sytuacjach związanych z cyberbezpieczeństwem oraz projektuje mikro-szkolenie dla kadry pedagogicznej dopasowane do profilu motywacyjnego odbiorców	K_U09, K_K01, K_K05, K_K06, K_K10

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Dialog motywujący i profil motywacyjny Reiss Motivation Profile (RMP) w dydaktyce zawodowej: analiza motywatorów jako klucz do identyfikacji potencjału i przełamywania oporu kadry pedagogicznej oraz uczniów wobec nowych technologii i IoT		4			PEU_04
Model ról zespołowych M. Belbina w planowaniu warsztatu pracy nauczyciela i zarządzaniu zespołem uczniów: identyfikacja 9 ról zespołowych, mapowanie potencjału kadry do zadań wdrożeniowych i audytowych (polityka haseł, ewidencja IoT), praca z uczniami		4			PEU_04

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

neuroróżnorodnymi i introwertycznymi w klasach IT					
Warsztat symulacyjny z organizacji pracy zespołowej i rozwiązywania konfliktów w sytuacjach związanych z cyberbezpieczeństwem; integracja narzędzi w planowaniu i realizacji lekcji z cyberbezpieczeństwa		2			PEU_05
Analiza efektów kształcenia i kryteriów weryfikacji INF.11 i INF.12 wymagających zajęć praktycznych, inwentaryzacja ćwiczeń i mapowanie ich na stanowiska, zasoby i oprogramowanie, określanie potrzeb i ograniczeń szkoły		3			PEU_01
Architektura pracowni (laboratorium) cyberbezpieczeństwa. Projektowanie topologii sieci dydaktycznej, segmentacja i izolacja środowisk ćwiczeniowych (sandbox), sieć zarządzania, stanowiska uczniowskie i stanowisko nauczyciela		4			PEU_01
Dobór infrastruktury sprzętowej pracowni: stacje robocze, host i serwer wirtualizacji, urządzenia sieciowe oraz sprzęt specjalistyczny, ustalenie parametrów wydajnościowych i opracowania specyfikacji technicznej oraz kosztorysu wyposażenia		4			PEU_01
Dobór oprogramowania i środowisk wirtualnych: hypervisor i maszyny wirtualne, konteneryzację, narzędzia open-source do ćwiczeń, obrazy i szablony laboratoryjne oraz usługi chmurowe, planowanie zarządzania środowiskami i ich odtwarzania, analiza licencjonowania i kosztów		4			PEU_01
Bezpieczeństwo, zgodność i organizacja pracy pracowni. Zasady BHP i bezpiecznego korzystania z narzędzi ofensywnych, regulamin pracowni, ochrona danych osobowych i aspekty prawne oraz wykorzystanie narzędzia sztucznej inteligencji do projektowania i dokumentowania pracowni		2			PEU_02
Dokumentacja i obrona projektu pracowni: koncepcja, specyfikacja sprzętu i oprogramowania, kosztorys oraz plan wdrożenia i utrzymania		3			PEU_03
Łącznie godzin		**30**			

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01						X	X		
PEU_02						X			
PEU_03						X	X		
PEU_04							X		
PEU_05						X	X		

Kryteria zaliczenia przedmiotu
Przedmiot kończy się zaliczeniem z oceną. Na ocenę składają się: (1) zespołowy projekt szkolnej pracowni (laboratorium) cyberbezpieczeństwa – 55%; (2) portfolio komponentu społeczno-organizacyjnego: raport z diagnozy potrzeb oraz profili motywacyjnych (RMP) i ról zespołowych (Belbin) kadry lub klasy – 20%; (3) konspekt i prezentacja 15-minutowego mikro-szkolenia dla nauczycieli z zakresu cyberbezpieczeństwa – 15%; (4) zadania cząstkowe (analiza wymagań INF.11 i INF.12, projekt pojedynczego środowiska ćwiczeniowego) – 10%. Próg zaliczenia – uzyskanie co najmniej 55% punktów łącznie oraz oddanie wszystkich elementów. Ocena końcowa jest równa ocenie z zajęć (C).

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe		30		
Czytanie literatury		8		
Przygotowanie do zajęć oraz diagnoz (ankiety RMP / role zespołowe Belbina)		7		
Przygotowanie mikro-szkolenia i prezentacji		5		
Opracowanie zespołowego projektu pracowni (architektura, specyfikacja, kosztorys, plan wdrożenia)		10		
Uczestnictwo w zaliczeniach		1		

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Łącznie godzin		**61**		
Sumaryczna liczba godzin dla przedmiotu	**61**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi				
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	31 godzin 1 ECTS			

Literatura podstawowa

1. Portnoy M.: Virtualization Essentials, 2nd Edition, Sybex, Indianapolis 2016.
2. CIS Critical Security Controls, wersja 8, Center for Internet Security, East Greenbush 2021.
3. Belbin R. M.: Zespoły w pracy. Jak osiągnąć sukces, Wolters Kluwer, Warszawa 2021.
4. Miller W. R., Rollnick S.: Dialog motywujący. Jak pomóc ludziom w zmianie i rozwoju, UJ, Kraków 2025.
5. Reiss S.: Co Cię motywuje. 16 podstawowych pragnień, które determinują nasze działania, RMP Polska – Instytut Durkalskiego, Warszawa 2019.
6. Petty G.: Nowoczesne nauczanie. Praktyczne wskazówki i techniki dla nauczycieli, wykładowców i szkoleniowców, GWP, Sopot 2018.

Literatura uzupełniająca

1. Robinson T. V.: Building Virtual Machine Labs: A Hands-On Guide, wydanie własne autora, 2017.
2. Serafin M.: Wirtualizacja w praktyce, Helion, Gliwice 2012.
3. Malewski M.: Modele i wizje edukacji dorosłych, Wydawnictwo Naukowe Dolnośląskiej Szkoły Wyższej, Wrocław 2010.
4. Janas K., Religa J.: Odkryj siłę wewnętrznych potrzeb, RMP Polska – Instytut Durkalskiego, Warszawa 2023.
5. NIST Special Publication 800-181 Revision 1, Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and Technology, Gaithersburg 2020.
6. ENISA, Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education, European Union Agency for Cybersecurity, listopad 2021.
7. Materiały instytucjonalne dla nauczycieli: NASK-PIB „ABC Cyberbezpieczeństwa", CERT Polska – baza wiedzy i zgłaszania incydentów (https://cert.pl), projekt „Cyberlekcje" (Ministerstwo Cyfryzacji / NASK), pakiety Ośrodka Rozwoju Edukacji dotyczące bezpieczeństwa cyfrowego i IoT w edukacji, materiały OWASP dla środowisk szkoleniowych (Juice Shop, WebGoat).

Osoba odpowiedzialna za przedmiot	
mgr inż. Cezary Graul	
Pozostałe osoby prowadzące przedmiot	
mgr Grażyna Kurowska	
mgr Beata Jacak-Drabik	
mgr Katarzyna Janas	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C13**	Przedmiot	**PROJEKTOWANIE ZAJĘĆ DYDAKTYCZNYCH Z CYBERBEZPIECZEŃSTWA**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
III	2		30		
Razem w czasie studiów		**30**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Podstawy dydaktyki zawodowej oraz komunikacja dydaktyczna w cyberbezpieczeństwie

Cele przedmiotu
Przygotowanie nauczyciela do samodzielnego projektowania zajęć, scenariuszy lekcji i jednostek dydaktycznych z cyberbezpieczeństwa w oparciu o podstawę programową kwalifikacji INF.11 i INF.12.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	projektuje scenariusze zajęć i jednostki dydaktyczne z cyberbezpieczeństwa z doborem metod aktywizujących do celów i treści kształcenia	K_W09, K_U09, K_K03
PEU_02	dobiera i stosuje strategie motywowania uczniów w nauczaniu cyberbezpieczeństwa oraz przeciwdziała spadkowi zaangażowania w naukę treści technicznych	K_U09, K_K03, K_K08
PEU_03	projektuje elementy grywalizacji zajęć z cyberbezpieczeństwa oraz ocenia ich wpływ na motywację i uczenie się, uwzględniając ryzyka nadmiernej rywalizacji	K_U09, K_K09
PEU_04	konstruuje narzędzia diagnozy i oceniania, stosuje ocenianie kształtujące i informację zwrotną	K_K08, K_W09, K_U09
PEU_05	projektuje zajęcia integrujące treści techniczne z kompetencjami społecznymi oraz wykorzystuje narzędzia sztucznej inteligencji do projektowania zajęć i materiałów	K_U10, K_K03, K_K07, K_K09

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Architektura procesów dydaktycznych i metody projektowej w ujęciu narracyjnym; mapowanie etapów gry na realne procesy zachodzące w szkole w obszarze cyberbezpieczeństwa		5			PEU_05
Architektura procesów dydaktycznych i metody projektowej w ujęciu; praktyczna nauka prowadzenia profesjonalnego debriefingu (wyciągania wniosków i ewaluacji)		3			PEU_05
Struktura scenariusza zajęć i jednostki dydaktycznej: wyprowadzanie celów operacyjnych z efektów kształcenia i kryteriów weryfikacji INF.11 i INF.12		3			PEU_01
Design Thinking jako metodyka projektowania zajęć i pracy uczniów: etapy procesu, zastosowanie do problemów z cyberbezpieczeństwa, moderowanie pracy zespołów		4			PEU_01, PEU_05

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Motywacja ucznia w nauczaniu cyberbezpieczeństwa: teoria autodeterminacji, przyczyny spadku zaangażowania w naukę treści technicznych, budowanie poczucia sprawstwa		4			PEU_02
Grywalizacja zajęć z cyberbezpieczeństwa: grywalizacja zespołowa i rywalizacja, ryzyka grywalizacji; projektowanie grywalizowanej jednostki dydaktycznej z cyberbezpieczeństwa		9			PEU_03
Projektowanie zajęć z treści INF.11 i INF.12 z wykorzystaniem narzędzi sztucznej inteligencji oraz integracja z kompetencjami społecznymi, pracą zespołową i doradztwem zawodowym		2			PEU_05
Łącznie godzin		**30**			

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01						X	X		
PEU_02						X	X		
PEU_03						X	X		
PEU_04						X			
PEU_05						X	X		

Kryteria zaliczenia przedmiotu
Podstawą oceny jest projekt – kompletny scenariusz jednostki dydaktycznej z cyberbezpieczeństwa wraz z obudową – 60%, jego prezentacja i obrona w formie mikronauczania – 25%, oraz zadania cząstkowe – 15%. Próg zaliczenia – uzyskanie co najmniej 55% punktów łącznie oraz oddanie wszystkich elementów.

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe		30		
Czytanie literatury		10		
Przygotowanie do zajęć		6		
Przygotowanie prezentacji i obrony projektu		7		
Opracowanie projektu zaliczeniowego (scenariusz jednostki z obudową dydaktyczną)		12		
Uczestnictwo w zaliczeniach		1		
Łącznie godzin		**68**		
Sumaryczna liczba godzin dla przedmiotu	**68**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**2**			
Obciążenie studenta związane z zajęciami praktycznymi				
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	31 godzin 1 ECTS			

Literatura podstawowa

1. Podstawa programowa kształcenia w zawodzie technik cyberbezpieczeństwa (351304), Dz. U. 2026 poz. 404.
2. Petty G.: Nowoczesne nauczanie. Praktyczne wskazówki i techniki dla nauczycieli, wykładowców i szkoleniowców, GWP, Sopot 2018.
3. Kapp K. M.: The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education, Pfeiffer, San Francisco 2012.
4. Hasso Plattner Institute of Design at Stanford (d.school), Design Thinking Bootleg – https://dschool.stanford.edu/tools/design-thinking-bootleg
5. Sterna D.: Ocenianie kształtujące w praktyce, Centrum Edukacji Obywatelskiej, Warszawa 2008.
6. Pink D. H.: Drive. Kompletnie nowe spojrzenie na motywację, Studio Emka, Warszawa 2011.
7. Karska K.: Podróż Bohatera - gra rozwojowa ze scenariuszem, dziennikiem gry i zestawem inspiracji, dodatkowych ćwiczeń, Katarzyna Karska, Sulejówek 2018.

Literatura uzupełniająca

1. Okoń W.: Wprowadzenie do dydaktyki ogólnej, wyd. 5, Wydawnictwo Akademickie Żak, Warszawa 2003.
2. Deterding S., Dixon D., Khaled R., Nacke L.: From Game Design Elements to Gamefulness: Defining „Gamification", w: Proceedings of the 15th International Academic MindTrek Conference, ACM, 2011, s. 9–15.
3. Graul C., Wachowicz J., Bielski R., Kufel K., Żółtowski M.: Enterprise Gamification – Learning as a Side Effect of Competition, INTED2017 Proceedings, IATED, Valencia 2017, s. 9637–9642.

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

4. Bergmann J., Sams A.: Flip Your Classroom: Reach Every Student in Every Class Every Day, ISTE/ASCD, Washington 2012.
5. ENISA, Cybersecurity Education Maturity Assessment, European Union Agency for Cybersecurity, 2024.
6. Shaheen K.: Praca z cieniem. Dziennik motywacyjny, dzięki któremu poznasz, przekroczysz i zintegrujesz swoje cienie; Wydawnictwo Marginesy 2024.
7. Przyborowska, B.: Pedagogika innowacyjności. Między teorią a praktyką. UMK, Toruń 2013.
8. Tanaś, M., Galanciak S. (red.) – Cyberprzestrzeń – Człowiek – Edukacja. Mistrz i uczeń w cyberprzestrzeni. Kraków: Impuls 2018.
9. Sysło M.M. :Kierunki rozwoju edukacji wspieranej technologią. Nowe technologie w edukacji. Wrocław, Toruń, Warszawa 2014

Osoba odpowiedzialna za przedmiot	
mgr inż. Cezary Graul	
Pozostałe osoby prowadzące przedmiot	
Grażyna Kurowska	
dr Katarzyna Karska	

Ministerstwo Edukacji Narodowej Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Nr	**C14**	Przedmiot	**PRAKTYKI ZAWODOWE**

Poziom kształcenia	**studia podyplomowe**
Forma studiów	**niestacjonarne**

Semestr	**Liczba punktów ECTS**	**Liczba godzin w semestrze**			
		W	**C**	**L**	**P**
3	6				90
Razem w czasie studiów		**90**			

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji
Znajomość podstawy programowej kształcenia w zawodzie technik cyberbezpieczeństwa w oparciu o podstawę programową kwalifikacji INF.11 i INF.12.

Cele przedmiotu
Realizacja praktyki zawodowej przygotowującej do nauczania na kierunku technik cyberbezpieczeństwa w szkołach średnich.

Przedmiotowe efekty uczenia się (PEU)		
Symbol	**Po zakończeniu przedmiotu student:**	**Odniesienie do kierunkowych efektów uczenia się**
PEU_01	zna wymagania prawne, organizacyjne, opiekuńczo-wychowawcze niezbędne w pracy nauczyciela na kierunku technik cyberbezpieczeństwa	K_W08, K_W09, K_W110, K_W11
PEU_02	potrafi zastosować zdobytą wiedzę do planowania i organizacji lekcji na kierunku technik cyberbezpieczeństwa	K_U08, K_U09, K_U10, K_U11
PEU_03	jest przygotowany do prowadzenie lekcji na kierunku technik cyberbezpieczeństwa we współpracy ze środowiskiem szkolnym z uwzględnieniem wymagań współczesnego procesu dydaktycznego	K_K01, K_K02, K_K04, K_K05, K_K06, K_K08, K_K09, K_K10

Treści programowe	**Liczba godzin**				**Odniesienie do PEU**
	W	**C**	**L**	**P**	
Zastosowanie w praktyce wiedzy i umiejętności zdobytych w procesie kształcenia studium podyplomowego				90	PEU_01, PEU_02, PEU_03
Łącznie godzin		**90**		**90**	

Metody weryfikacji efektów uczenia się dla przedmiotu									
Symbol PEU	**Test**	**Egzamin ustny**	**Egzamin pisemny**	**Kolokwium**	**Sprawozdanie**	**Projekt**	**Prezentacja**	**Zaliczenie praktyczne**	**Inne**
PEU_01					X				
PEU_02					X				
PEU_03					X				

Kryteria zaliczenia przedmiotu

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.

Ocena zaliczeniowa wyznaczana przez opiekuna praktyki uwzględniająca poziom kompetencji opiekuńczo-wychowawczych, dydaktycznych i organizacyjnych studenta (min. 51%).

Nakład pracy studenta				
Forma aktywności	**Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności**			
	W	**C**	**L**	**P**
Godziny kontaktowe				90
Czytanie literatury				20
Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych				30
Przygotowanie do egzaminu, zaliczenia				
Opracowanie dokumentacji projektu/sprawozdania				10
Uczestnictwo w zaliczeniach i egzaminach				
Łącznie godzin				
Sumaryczna liczba godzin dla przedmiotu	**150**			
Sumaryczna liczba punktów ECTS dla przedmiotu	**6**			
Obciążenie studenta związane z zajęciami praktycznymi				
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	90			

Literatura podstawowa
brak
Literatura uzupełniająca
brak

Osoba odpowiedzialna za przedmiot	
dr inż. Marcin Forkiewicz	
Pozostałe osoby prowadzące przedmiot	
dr Natalia Pawłowska	

Ministerstwo Edukacji Narodowej
Zadanie finansowane ze środków Ministerstwa Edukacji Narodowej, umowa nr MEN/2026/DKZ/936.