UNIWERSYTET MORSKI W GDYNI
Wydział Informatyki

KWALIFIKACYJNE STUDIA PODYPLOMOWE DLA NAUCZYCIELI DO NAUCZANIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

PROGRAM STUDIÓW 2026–2028

Program zatwierdzony uchwałą nr 120/XVIII
Senatu Uniwersytetu Morskiego w Gdyni z dnia 30 września 2026 r.

Gdynia, wrzesień 2026

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

Spis treści

1. Cel studiów podyplomowych 3
2. Założenia techniczno-organizacyjne 4
3. Związek z misją uczelni i jej strategią rozwoju 5
4. Zasady rekrutacji i wymagane dokumenty 6
5. Sylwetka absolwenta 6
6. Siatka przedmiotów 7
7. Efekty uczenia się 8
8. Wykaz przedmiotów realizowanych na studiach podyplomowych 10
9. Wykaz osób prowadzących zajęcia w ramach studiów podyplomowych 12
10. Plan studiów 13
11. Wewnętrzny system zapewniania jakości kształcenia 13
12. Karty przedmiotów 13

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

1. Cel studiów podyplomowych

Studia podyplomowe z cyberbezpieczeństwa dla nauczycieli są realizowane jako zadanie zlecone przez Ministra Edukacji na podstawie art. 464 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, z późn. zm.), polegające na organizacji i przeprowadzeniu kwalifikacyjnych studiów podyplomowych dla nauczycieli w zakresie przygotowania merytorycznego i dydaktycznego do nauczania kolejnego przedmiotu lub prowadzenia kolejnych zajęć w zawodzie **technik cyberbezpieczeństwa**.

Podstawą prawną realizacji Studiów podyplomowych jest umowa nr MEN/2026/DKZ/936 zawarta pomiędzy Uniwersytetem Morskim w Gdyni a Skarbem Państwa reprezentowanym przez Ministra Edukacji, finansowana ze środków Ministerstwa Edukacji Narodowej.

Dnia 1 września 2026 r. weszło w życie Rozporządzenie Ministra Edukacji z dnia 20 marca 2026 r. zmieniające rozporządzenie w sprawie ogólnych celów i zadań kształcenia w zawodach szkolnictwa branżowego oraz klasyfikacji zawodów szkolnictwa branżowego (Dz. U. z 2026 r., poz. 404), wprowadzające nowy zawód **technik cyberbezpieczeństwa**.

Podstawa programowa nauczania zawodu **technik cyberbezpieczeństwa** w szkołach ponadpodstawowych została określona Rozporządzeniem Ministra Edukacji z dnia 22 czerwca 2026 r. zmieniającego rozporządzenie w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego (Dz. U. z 2026 r., poz. 1009).

Załącznik do powyższego rozporządzenia zawiera podstawy programowe kształcenia w zawodzie szkolnictwa branżowego przyporządkowanego do branży teleinformatycznej – **technik cyberbezpieczeństwa** (kod zawodu 351304), z kwalifikacjami wyodrębnionymi w zawodzie na poziomie V Polskiej Ramy Kwalifikacji (V PRK):

- INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych
- INF.12. Programowanie bezpiecznych aplikacji webowych

Program **Studiów podyplomowych z cyberbezpieczeństwa dla nauczycieli** został przygotowany zgodnie z wymaganiami zawartymi w Obwieszczeniu Ministra Nauki z dnia 9 lutego 2024 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie standardu kształcenia przygotowującego do wykonywania zawodu nauczyciela (Dz. U. z 2024 r., poz. 453).

Ukończenie **Studiów podyplomowych z cyberbezpieczeństwa dla nauczycieli** przygotowuje do wykonywania zawodu nauczyciela w zakresie przygotowania do nauczania kolejnego przedmiotu lub prowadzenia kolejnych zajęć na kierunku **technik cyberbezpieczeństwa**.

Program studiów łączy merytoryczną wiedzę z zakresu cyberbezpieczeństwa z metodyką nauczania przedmiotów zawodowych i przygotowuje słuchaczy do nauczania kolejnego przedmiotu lub prowadzenia zajęć w zawodzie **technik cyberbezpieczeństwa**.

Studia podyplomowe z cyberbezpieczeństwa dla nauczycieli są bezpłatne dla słuchaczy, koszty zostaną pokryte z budżetu zadania realizowanego na zlecenie Ministra Edukacji, zgodnie z umową nr MEN/2026/DKZ/936.

2. Założenia techniczno-organizacyjne

1. **Liczba godzin zajęć** (ogółem): **Studia podyplomowe z cyberbezpieczeństwa dla nauczycieli** trwają trzy semestry i obejmują łącznie 360 godz. zajęć:
   – 270 godz. zajęć dydaktycznych,
   – 90 godz. praktyki zawodowej.
2. **Liczba punktów ECTS**: 30 pkt.

Grupy zajęć, w ramach których osiąga się szczegółowe efekty uczenia się	**Liczba godzin**	**Liczba punktów ECTS**
Podyplomowe przygotowanie merytoryczne do nauczania przedmiotu lub prowadzenia zajęć	180	20
Przygotowanie dydaktyczne do nauczania kolejnego przedmiotu lub prowadzenia kolejnych zajęć:		
– dydaktyka przedmiotu nauczania lub zajęć	90	4
– praktyki zawodowe	90	6
Łącznie	**360**	**30**

3. **Miejsce zajęć**: Uniwersytet Morski w Gdyni.
4. **Częstotliwość zajęć**: zajęcia odbywać się będą w trybie niestacjonarnym, w formie zjazdów weekendowych, średnio jeden zjazd w miesiącu (sobotnio-niedzielny) dla słuchaczy studiów. Zajęcia rozpoczną się w grudniu 2026 r. i zakończą w maju 2028 r.
5. **Warunki uczestnictwa**: kwalifikacyjne studia podyplomowe z cyberbezpieczeństwa są przeznaczone dla czynnych zawodowo nauczycieli, którzy mają ukończone studia co najmniej pierwszego stopnia oraz są nauczycielami kształcenia zawodowego, w szczególności uczącymi przedmiotów zawodowych w zawodach technik informatyk i technik programista, technik teleinformatyk, technik telekomunikacji (zawody z branży teleinformatycznej) lub nauczycielami kształcenia zawodowego w zawodach pokrewnych, a także nauczycielami szkół podstawowych i szkół ponadpodstawowych po kierunkach związanych z informatyką lub nauczycielami akademickimi związani z kształceniem na kierunkach informatycznych.

   Planowa jest rekrutacja 36 słuchaczy studiów podyplomowych. Minimalna liczba słuchaczy wynosi 300 osób (warunek uruchomienia studiów
6. **Forma zajęć**: wykłady (113 godz.), ćwiczenia (77 godz.), laboratoria (80 godz.), praktyki zawodowe (90 godz.)
7. **Forma zaliczenia**: każdy przedmiot kończy się zaliczeniem, bądź przygotowaniem zadania, projektu, raportu lub sprawozdania w zależności od typu zajęć.
8. **Podstawa wydania świadectwa**: uzyskanie wszystkich zaliczeń i złożenie wszystkich egzaminów oraz uzyskanie wymaganej liczby punktów ECTS, a następnie złożenie egzaminu kończącego studia podyplomowe, obejmującego problematykę całych studiów, z wynikiem pozytywnym.
9. **Egzamin końcowy** odbędzie przed komisją powołaną przez kierownika jednostki organizacyjnej na wniosek kierownika studiów podyplomowych, przed upływem 30 dni licząc od dnia uzyskania i zdania, niezbędnych dla ukończenia studiów zaliczeń.

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

3. Związek z misją uczelni i jej strategią rozwoju

Uruchomienie **Studiów podyplomowych z cyberbezpieczeństwa dla nauczycieli** w Uniwersytecie Morskim w Gdyni wpisuje się w priorytety ujęte w Strategii Rozwoju UMG na lata 2024–2028. Inicjatywa ta buduje pomost między tradycją kształcenia na rzecz bezpieczeństwa a wyzwaniami ery cyfrowej.

1. Transformacja cyfrowa i podnoszenie kompetencji dydaktycznych

Strategia UMG akcentuje potrzebę ciągłej transformacji cyfrowej oraz dostosowywania oferty edukacyjnej do zmieniającego się otoczenia rynkowego i technologicznego.

- wsparcie dla środowiska oświatowego: nauczyciele są kluczowymi pośrednikami w przekazywaniu wiedzy nowym pokoleniom – kształcenie kadry pedagogicznej z zakresu higieny cyfrowej, ochrony danych oraz zagrożeń sieciowych realnie podnosi poziom bezpieczeństwa w szkołach.
- strategiczne partnerstwo z edukacją: inicjatywa ta wpisuje się bezpośrednio w cele uczelni dotyczące promocji i współpracy z otoczeniem szkolnym oraz budowania relacji z nauczycielami i doradcami zawodowymi.

2. Bezpieczeństwo jako filar tożsamości uczelni

Misja Uniwersytetu Morskiego w Gdyni od ponad wieku koncentruje się wokół zagadnień bezpieczeństwa – historycznie w wymiarze morskim, transportowym i technologicznym.

- ewolucja pojęcia bezpieczeństwa: współczesne bezpieczeństwo infrastruktur krytycznych, systemów nawigacyjnych czy logistycznych jest nierozerwalnie związane z cyberbezpieczeństwem.
- rozszerzenie misji: dzielenie się wiedzą z zakresu cyberbezpieczeństwa z otoczeniem społeczno-gospodarczym stanowi naturalne rozszerzenie akademickiej odpowiedzialności uczelni za bezpieczeństwo powszechne.

3. Odpowiedź na wyzwania otoczenia społeczno-gospodarczego

Strategia rozwoju UMG zakłada aktywne reagowanie na zapotrzebowanie rynku pracy oraz elastyczne kształtowanie oferty studiów podyplomowych i kursów podnoszących kwalifikacje.

- dynamiczny rozwój technologii AI, cyberzagrożeń oraz nowych regulacji (takich jak dyrektywa NIS2 czy krajowe standardy cyberbezpieczeństwa) wymaga bieżącego dokształcania kadr.
- przygotowanie dedykowanego programu dla nauczycieli pozwala uczelni efektywnie realizować funkcję opiniotwórczą i ekspercką w regionie.

Oferta **Studiów podyplomowych z cyberbezpieczeństwa dla nauczycieli** to synergia tradycji akademickiej UMG i nowoczesnego podejścia do edukacji cyfrowej. Pozwala uczelni umacniać pozycję nowoczesnego ośrodka naukowo-dydaktycznego, który reaguje na kluczowe wyzwania cywilizacyjne i buduje trwałe relacje ze środowiskiem oświatowym.

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

4. Zasady rekrutacji i wymagane dokumenty

Rekrutacja na **Studia podyplomowe z cyberbezpieczeństwa dla nauczycieli** odbędzie się w listopadzie 2026 r. Do rekrutacji mogą przystąpić:

- nauczyciele kształcenia zawodowego, w szczególności uczący przedmiotów zawodowych w zawodach technik informatyk i technik programista, technik teleinformatyk, technik telekomunikacji (zawody z branży teleinformatycznej) lub
- nauczyciele kształcenia zawodowego w zawodach pokrewnych,

a w miarę dostępności miejsc również:

- nauczyciele szkół podstawowych i szkół ponadpodstawowych po kierunkach związanych z informatyką,
- nauczyciele akademiccy związani z kształceniem na kierunkach informatycznych.

Zgłoszenia przyjmowane będą wyłącznie poprzez System Rekrutacji Internetowej UMG dostępny pod stroną https://irk.umg.edu.pl. Dokumenty wymagane w procesie rekrutacji po zarejestrowaniu w systemie elektronicznej rekrutacji IRK:

- podanie o przyjęcie na studia (formularz zgłoszeniowy wygenerowany w systemie IRK),
- odpis dyplomu ukończenia studiów co najmniej pierwszego stopnia,
- zaświadczenie wydane przez dyrektora szkoły /placówki edukacyjnej,
- oświadczenie RODO (dostępne w systemie IRK lub w załączniku na stronie).

Jeżeli liczba zgłoszeń przekroczy limit dostępnych miejsc, kandydaci będą kwalifikowani:

- w pierwszej kolejności osoby uczące przedmiotów zawodowych w zawodach technik informatyk i technik programista, technik teleinformatyk, technik telekomunikacji (zawody z branży teleinformatycznej).
- w przypadku gdy liczba kandydatów uczących ww. przedmioty przekroczy liczbę dostępnych miejsc o przyjęciu na studia podyplomowe decydować będzie kolejność zgłoszeń,
- ostateczną decyzję o przyjęciu na studia podejmuje Komisja Rekrutacyjna, składającą się z co najmniej trzech osób, w tym kierownika studiów podyplomowych.

Ocena kandydatów prowadzona jest wyłącznie na podstawie dokumentów złożonych w procesie rekrutacji, zgodnie z obowiązującymi kryteriami. Proces kwalifikacji prowadzony jest z zachowaniem zasad równego traktowania kandydatów.

Studia podyplomowe są finansowane ze środków Ministerstwa Edukacji Narodowej, uczestnicy nie ponoszą opłat.

5. Sylwetka absolwenta

Absolwent **Studiów podyplomowych z cyberbezpieczeństwa dla nauczycieli** zdobędzie wymagane kwalifikacje przygotowania merytorycznego do nauczania przedmiotu lub prowadzenia zajęć na kierunku technik cyberbezpieczeństwa z zakresu:

- podstaw cyberbezpieczeństwa systemów IT,
- programowania w języku Python,
- projektowania i administracji bazami danych,
- administrowania sieciami,
- użytkowanie, konfiguracji i utwardzania systemu Windows i Linux,

- testowania bezpieczeństwa sieci TCP/IP,
- implementacji aplikacji webowych,
- weryfikowanie bezpieczeństwa implementacji aplikacji webowych,
- przeprowadzanie testów penetracyjnych aplikacji webowych w środowisku testowym

oraz przygotowania dydaktycznego do nauczania przedmiotów zawodowych z cyberbezpieczństwa kolejnego przedmiotu lub prowadzenia kolejnych zajęć w obszarze:

- podstaw dydaktyki zawodowej,
- komunikacji dydaktycznej w cyberbezpieczeństwie,
- warsztatu pracy nauczyciela cyberbezpieczeństwa,
- projektowania zajęć dydaktycznych z cyberbezpieczeństwa.

Absolwent **Studiów podyplomowych z cyberbezpieczeństwa dla nauczycieli** uzyska wymagane kwalifikacje do nauczania kolejnego przedmiotu lub prowadzenia zajęć w zawodzie **technik cyberbezpieczeństwa** na poziomie szkoły ponadpodstawowej.

6. Siatka przedmiotów

Lp.	Przedmiot	Liczba ECTS	Liczba godzin	W	C	L	P
	Semestr I						
1	Podstawy cyberbezpieczeństwa systemów IT	1	15	15			
2	Programowanie w języku Python	2	20	10		10	
3	Projektowanie i administracja bazami danych	2	20	10		10	
4	Administrowanie sieciami	2	20	10		10	
5	Użytkowanie, konfiguracja i utwardzanie systemu Windows i Linux	2	20	10		10	
6	Podstawy dydaktyki zawodowej	1	13	3	10		
	Łącznie	**10**	**108**	**58**	**10**	**40**	**0**
	Semestr II						
7	Testowanie bezpieczeństwa sieci TCP/IP	2	15	10		5	
8	Implementacja aplikacji webowych	3	30	15		15	
9	Weryfikowanie bezpieczeństwa implementacji aplikacji webowych	2	20	10		10	
10	Przeprowadzanie testów penetracyjnych aplikacji webowych w środowisku testowym	2	20	10		10	
11	Komunikacja dydaktyczna w cyberbezpieczeństwie	1	17	10	7		
	Łącznie	**10**	**102**	**55**	**7**	**40**	**0**
	Semestr III						
12	Warsztat pracy nauczyciela cyberbezpieczeństwa	2	30		30		
13	Projektowanie zajęć dydaktycznych z cyberbezpieczeństwa	2	30		30		
14	Praktyki zawodowe	6	90				90
	Łącznie	**10**	**150**	**0**	**60**	**0**	**90**
	SUMA	**30**	**360**	**113**	**77**	**80**	**90**

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

7. Efekty uczenia się

Symbol	WIEDZA	
	Treść efektu uczenia się:	**Odniesienie do PRK**
	Absolwent studiów podyplomowych zna i rozumie:	
K_W01	w pogłębionym stopniu zagadnienia cyberbezpieczeństwa systemów IT, architektury bezpieczeństwa oraz współczesnych zagrożeń.	P7S_WG
K_W02	zaawansowane metody konfiguracji i zabezpieczania systemów operacyjnych Windows i Linux oraz mechanizmy zarządzania tożsamością i kontrolą dostępu.	P7S_WG
K_W03	zasady projektowania, administracji i monitorowania sieci komputerowych TCP/IP oraz metody zapewniania ich bezpieczeństwa.	P7S_WG
K_W04	zaawansowane zagadnienia programowania w języku Python oraz jego zastosowania w automatyzacji procesów administracyjnych i cyberbezpieczeństwie.	P7S_WG
K_W05	metody projektowania, administracji, implementacji i zabezpieczania relacyjnych i nierelacyjnych baz danych oraz ochrony informacji.	P7S_WG
K_W06	technologie i architektury aplikacji webowych, metody ich programowania oraz bezpiecznego cyklu życia oprogramowania.	P7S_WG
K_W07	metody analizy bezpieczeństwa aplikacji i infrastruktury teleinformatycznej oraz organizacji testów bezpieczeństwa i testów penetracyjnych w środowisku kontrolowanym.	P7S_WG
K_W08	aktualne regulacje prawne, normy, standardy oraz dobre praktyki dotyczące cyberbezpieczeństwa, ochrony informacji i ochrony danych osobowych.	P7S_WK
K_W09	metodykę nauczania kwalifikacji INF.11 i INF.12, organizacji laboratoriów cyberbezpieczeństwa oraz przygotowania uczniów do egzaminów zawodowych.	P7S_WK
K_W10	możliwości wykorzystania technologii chmurowych, konteneryzacji, wirtualizacji oraz narzędzi sztucznej inteligencji w cyberbezpieczeństwie i edukacji zawodowej.	P7S_WG
K_W11	kierunki rozwoju technologii cyberbezpieczeństwa oraz ich wpływ na kształcenie zawodowe i doskonalenie kompetencji nauczyciela.	P8S_WG

Symbol	UMIEJĘTNOŚCI	
	Treść efektu uczenia się:	**Odniesienie do PRK**
	Absolwent studiów podyplomowych potrafi:	
K_U01	prowadzić zajęcia dydaktyczne w zakresie projektowania, konfigurowania i zabezpieczania systemów operacyjnych Windows i Linux zgodnie z aktualnymi standardami bezpieczeństwa.	P7S_UW
K_U02	prowadzić zajęcia dydaktyczne w zakresie projektowania, konfigurowania i diagnozowania sieci komputerowych oraz analizowania ich bezpieczeństwa z wykorzystaniem specjalistycznych narzędzi.	P7S_UW
K_U03	prowadzić zajęcia dydaktyczne w zakresie projektowania i implementowania programów w języku Python wspomagających automatyzację administracji oraz analizę bezpieczeństwa systemów informatycznych.	P7S_UW
K_U04	prowadzić zajęcia dydaktyczne w zakresie projektowania i administrowania i zabezpieczania systemów baz danych zgodnie z wymaganiami bezpieczeństwa informacji.	P7S_UW
K_U05	prowadzić zajęcia dydaktyczne w zakresie projektowania, implementowania i wdrażania aplikacji webowych z wykorzystaniem współczesnych technologii programistycznych.	P7S_UW

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

K_U06	prowadzić zajęcia dydaktyczne w zakresie wykorzystania specjalistycznych narzędzi do analizy bezpieczeństwa aplikacji, systemów i sieci oraz interpretowania wyników ich działania.	P7S_UW
K_U07	prowadzić zajęcia dydaktyczne w zakresie planowania i przeprowadzania testów bezpieczeństwa oraz podstawowych testów penetracyjnych w środowisku laboratoryjnym z dokumentowaniem ich przebiegu i wyników.	P7S_UW
K_U08	projektować środowiska laboratoryjne z wykorzystaniem wirtualizacji, konteneryzacji i wybranych usług chmurowych do realizacji zajęć dydaktycznych.	P7S_UW
K_U09	projektować programy nauczania, scenariusze zajęć, materiały dydaktyczne oraz zadania praktyczne zgodne z wymaganiami kwalifikacji INF.11 i INF.12.	P7S_UW
K_U10	Krytycznie dobierać i wykorzystywać narzędzia sztucznej inteligencji do wspomagania programowania, administracji systemami oraz procesu dydaktycznego.	P7S_UU
K_U11	samodzielnie aktualizować wiedzę i rozwijać kompetencje zawodowe poprzez analizę nowych technologii oraz literatury specjalistycznej.	P8S_UU

Symbol	**KOMPETENCJE SPOŁECZNE**	
	Treść efektu uczenia się:	**Odniesienie do PRK**
Absolwent studiów podyplomowych jest gotów do:		
K_K01	odpowiedzialnego wykonywania zadań zawodowych z poszanowaniem zasad etyki, bezpieczeństwa informacji i prawa.	P7S_KR
K_K02	upowszechniania kultury cyberbezpieczeństwa oraz promowania bezpiecznych zachowań w środowisku szkolnym i zawodowym.	P7S_KO
K_K03	krytycznej oceny stosowanych technologii oraz doboru rozwiązań adekwatnych do potrzeb procesu dydaktycznego, rozwijania u uczniów ciekawości, aktywności i samodzielności poznawczej oraz logicznego myślenia i krytycznej oceny technologii.	P7S_KK
K_K04	samodzielnego planowania własnego rozwoju zawodowego oraz systematycznego aktualizowania kompetencji w obszarze cyberbezpieczeństwa.	P7S_KR
K_K05	współpracy z nauczycielami, specjalistami oraz przedstawicielami środowiska gospodarczego w celu doskonalenia jakości kształcenia zawodowego.	P7S_KO
K_K06	organizowania pracy własnej i zespołu podczas realizacji projektów technicznych oraz dydaktycznych.	P7S_KO
K_K07	odpowiedzialnego wykorzystywania narzędzi sztucznej inteligencji z uwzględnieniem aspektów etycznych, prawnych i bezpieczeństwa.	P7S_KR
K_K08	krytycznej oceny posiadanej wiedzy, doskonalenia warsztatu nauczyciela i własnego rozwoju zawodowego poprzez wdrażanie nowych metod nauczania..	P8S_KK
K_K09	inicjowania i wdrażania innowacyjnych rozwiązań dydaktycznych wykorzystujących technologie cyfrowe i cyberbezpieczeństwo.	P8S_KK
K_K10	budowania środowiska uczenia się sprzyjającego odpowiedzialnemu korzystaniu z technologii informacyjno-komunikacyjnych oraz rozwijaniu kompetencji cyfrowych uczniów.	P7S_KO

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

8. Wykaz przedmiotów realizowanych na studiach podyplomowych

Lp.	Symbol przedmiotu	Nazwa przedmiotu	Symbol przedmiotowego efektu uczenia się	Odniesienie do kierunkowych efektów kształcenia	Liczba punktów ECTS
1	C1	Podstawy cyberbezpieczeństwa systemów IT	PEU_01	K_W01, K_W08, K_W11	1
			PEU_02	K_W01, K_W08 K_W11	
			PEU_03	K_W01, K_W08 K_W11	
			PEU_04	K_W01, K_W08 K_W11	
			PEU_05	K_W01, K_W08 K_W11	
2	C2	Programowanie w języku Python	PEU_01	K_W04, K_U03	2
			PEU_02	K_W04, K_U03, K_K03	
			PEU_03	K_W04, K_U03, K_U11, K_K02	
			PEU_04	K_W04, K_U03, K_U11, K_K03	
3	C3	Projektowanie i administracja bazami danych	PEU_01	K_W05, K_U04	2
			PEU_02	K_W05, K_U04, K_K03	
			PEU_03	K_W05, K_U04, K_K07, K_K08	
			PEU_04	K_W05, K_U04	
			PEU_05	K_W05, K_U04, K_U11, K_K03	
			PEU_06	K_W05, K_U04, K_U11	
4	C4	Administrowanie sieciami	PEU_01	K_W03	2
			PEU_02	K_W03, K_U02	
			PEU_03	K_W03, K_U02, K_K04	
			PEU_04	K_W03, K_U02, K_K04	
			PEU_05	K_W03, K_U02, K_K04	
5	C5	Użytkowanie, konfiguracja i utwardzanie systemu Windows i Linux	PEU_01	K_W01, K_W02	2
			PEU_02	K_W02, K_U01	
			PEU_03	K_W04, K_U03, K_U10	
			PEU_04	K_W02, K_U01, K_K04	
			PEU_05	K_W02, K_U01, K_K04	
			PEU_06	K_W10, K_U08, K_K04	
6	C6	Podstawy dydaktyki zawodowej	PEU_01	K_W09, K_U09	1
			PEU_02	K_W09, K_K05	
			PEU_03	K_W09, K_U09, K_K03	
			PEU_04	K_W09, K_U09, K_K01, K_K08	
			PEU_05	K_W09, K_U09, K_K01, K_K08	
7	C7	Testowanie bezpieczeństwa sieci TCP/IP	PEU_01	K_W01, K_W03	2
			PEU_02	K_W03, K_U01, K_U02, K_U06	
			PEU_03	K_W03, K_U02, K_U07	
			PEU_04	K_W01, K_U06, K_K06	
			PEU_05	K_U06, K_U07, K_K01	
8	C8	Implementacja aplikacji webowych	PEU_01	K_W06, K_U05	3
			PEU_02	K_W06, K_U05, K_K03	
			PEU_03	K_W06, K_U05, K_U11, K_K03	
			PEU_04	K_W06, K_U05, K_U11, K_K07	

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

9	C9	Weryfikowanie bezpieczeństwa implementacji aplikacji webowych	PEU_01	K_W01, K_W02, K_W04, K_W05, K_W06, K_U04, K_U05	2
			PEU_02	K_W01, K_W02, K_W04, K_W05, K_W06, K_U04, K_U05	
			PEU_03	K_W01, K_W02, K_W04, K_W05, K_W06, K_U04, K_U05, K_K04	
			PEU_04	K_W01, K_W02, K_W04, K_W05, K_W06, K_W07, K_U04, K_U05, K_U06, K_K04	
10	C10	Przeprowadzanie testów penetracyjnych aplikacji webowych w środowisku testowym	PEU_01	K_W01, K_W02, K_W03, K_W04, K_W05, K_W06, K_W07	2
			PEU_02	K_W01, K_W07, K_U02, K_U04, K_U05, K_U06, K_U07, K_K06	
			PEU_03	K_W01, K_W07, K_U02, K_U04, K_U05, K_U06, K_U07, K_K06	
			PEU_04	K_W01, K_W07, K_U02, K_U04, K_U05, K_U06, K_U07, K_K06	
			PEU_05	K_W01, K_W07, K_W08, K_U02, K_U04, K_U05, K_U06, K_U07	
11	C11	Komunikacja dydaktyczna w cyberbezpieczeństwie	PEU_01	K_W09, K_K03	1
			PEU_02	K_W09, K_U09, K_K10	
			PEU_03	K_U09, K_U10, K_K07	
			PEU_04	K_K01, K_K02, K_K10	
12	C12	Warsztat pracy nauczyciela cyberbezpieczeństwa	PEU_01	K_W09, K_W10, K_U08, K_U09, K_K03	2
			PEU_02	K_W08, K_K07	
			PEU_03	K_K06, K_U09	
			PEU_04	K_W09, K_W11, K_U09, K_K05, K_K06	
			PEU_05	K_U09, K_K01, K_K05, K_K06, K_K10	
13	C13	Projektowanie zajęć dydaktycznych z cyberbezpieczeństwa	PEU_01	K_W09, K_U09, K_K03	2
			PEU_02	K_U09, K_K03, K_K08	
			PEU_03	K_U09, K_K09	
			PEU_04	K_K08, K_W09, K_U09	
			PEU_05	K_U10, K_K03, K_K07, K_K09	
14	C14	Praktyki zawodowe	PEU_01	K_W08, K_W09, K_W110, K_W11	6
			PEU_02	K_U08, K_U09, K_U10, K_U11	
			PEU_03	K_K01, K_K02, K_K04, K_K05, K_K06, K_K08, K_K09, K_K10	
				RAZEM	**30**

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

9. Wykaz osób prowadzących zajęcia w ramach studiów podyplomowych

Lp.	Imię i nazwisko osoby prowadzącej zajęcia	Nazwa przedmiotu
1	Łukasz Apiecionek	Podstawy cyberbezpieczeństwa systemów IT
2	Mateusz Dampc	Podstawy cyberbezpieczeństwa systemów IT
3	Ewa Ratajczak-Ropel	Programowanie w języku Python
4	Maciej Godek	Programowanie w języku Python
5	Mirosław Łącki	Projektowanie i administracja bazami danych
6	Łukasz Apiecionek	Administrowanie sieciami
7	Mateusz Dampc	Administrowanie sieciami
8	Łukasz Apiecionek	Użytkowanie, konfiguracja i utwardzanie systemu Windows i Linux
9	Mateusz Dampc	Użytkowanie, konfiguracja i utwardzanie systemu Windows i Linux
10	Urszula Kornas-Krzyżykowska	Podstawy dydaktyki zawodowej
11	Grażyna Kurowska	Podstawy dydaktyki zawodowej
12	Łukasz Apiecionek	Testowanie bezpieczeństwa sieci TCP/IP
13	Mateusz Dampc	Testowanie bezpieczeństwa sieci TCP/IP
14	Ewa Ratajczak-Ropel	Implementacja aplikacji webowych
15	Juliusz Łosiński	Implementacja aplikacji webowych
16	Łukasz Apiecionek	Weryfikowanie bezpieczeństwa implementacji aplikacji webowych
17	Mateusz Dampc	Weryfikowanie bezpieczeństwa implementacji aplikacji webowych
18	Łukasz Apiecionek	Przeprowadzanie testów penetracyjnych aplikacji webowych w środowisku testowym
19	Mateusz Dampc	Przeprowadzanie testów penetracyjnych aplikacji webowych w środowisku testowym
20	Cezary Graul	Komunikacja dydaktyczna w cyberbezpieczeństwie
21	Cezary Graul	Warsztat pracy nauczyciela cyberbezpieczeństwa
22	Grażyna Kurowska	Warsztat pracy nauczyciela cyberbezpieczeństwa
23	Beata Jacak-Drabik	Warsztat pracy nauczyciela cyberbezpieczeństwa
24	Katarzyna Janas	Warsztat pracy nauczyciela cyberbezpieczeństwa
25	Cezary Graul	Projektowanie zajęć dydaktycznych z cyberbezpieczeństwa
26	Grażyna Kurowska	Projektowanie zajęć dydaktycznych z cyberbezpieczeństwa
27	Katarzyna Karska	Projektowanie zajęć dydaktycznych z cyberbezpieczeństwa
28	Marcin Forkiewicz	Praktyki zawodowe
29	Natalia Pawłowska	Praktyki zawodowe

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

10. Plan studiów

Zajęcia na **Studiach podyplomowych z cyberbezpieczeństwa dla nauczycieli** trwają trzy semestry. Zajęcia będą realizowane w soboty i niedziele, średnio jeden zjazd w miesiącu. Plany studiów zostaną podane na początku semestru, na dwa tygodnie przed rozpoczęciem zajęć.

11. Wewnętrzny system zapewniania jakości kształcenia

Za jakość kształcenia na **Studiach podyplomowych z cyberbezpieczeństwa dla nauczycieli** odpowiada Kierownik Studiów Podyplomowych. Na zakończenie każdego semestru słuchacze zostaną proszeni o wypełnienie kwestionariuszy ankietowych dotyczących jakości kształcenia. Na podstawie uzyskanych wyników podjęte zostaną działania mające na celu podniesienie jakości kształcenia na studiach podyplomowych.

12. Karty przedmiotów

C1 – Podstawy cyberbezpieczeństwa systemów IT
C2 – Programowanie w języku Python
C3 – Projektowanie i administracja bazami danych
C4 – Administrowanie sieciami
C5 – Użytkowanie, konfiguracja i utwardzanie systemu Windows i Linux
C6 – Podstawy dydaktyki zawodowej
C7 – Testowanie bezpieczeństwa sieci TCP/IP
C8 – Implementacja aplikacji webowych
C9 – Weryfikowanie bezpieczeństwa implementacji aplikacji webowych
C10 – Przeprowadzanie testów penetracyjnych aplikacji webowych w środowisku testowym
C11 – Komunikacja dydaktyczna w cyberbezpieczeństwie
C12 – Warsztat pracy nauczyciela cyberbezpieczeństwa
C13 – Projektowanie zajęć dydaktycznych z cyberbezpieczeństwa
C14 – Praktyki zawodowe

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