Program studiów

Kierunek: Kwalifikacyjne studia podyplomowe dla nauczycieli w zawodzie technik cyberbezpieczeństwa

Spis treści

Opis studiów podyplomowych 3
Efekty uczenia się 7

Opis studiów podyplomowych

Ogólne informacje o studiach podyplomowych

Wydział:	Wydział Informatyki, Elektroniki i Telekomunikacji
Nazwa studiów podyplomowych (w j. polskim):	Kwalifikacyjne studia podyplomowe dla nauczycieli w zawodzie technik cyberbezpieczeństwa
Nazwa studiów podyplomowych (w j. angielskim):	Qualification Postgraduate Studies for Teachers in the Cybersecurity Technician Profession
Poziom:	Studia podyplomowe
Termin rozpoczęcia cyklu:	2026/2027,semestr zimowy
Czas trwania jednej edycji studiów podyplomowych (liczba semestrów):	3
Język wykładowy:	polski
Liczba punktów ECTS wymagana do ukończenia studiów podyplomowych:	42
w tym: liczba punktów ECTS przypisanych do zajęć kształtujących umiejętności praktyczne:	30
w tym: liczba punktów ECTS przypisanych do zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość:	0

Data planowanego rozpoczęcia i zakończenia pierwszej edycji studiów podyplomowych

01.10.2026 - 29.02.2028

Zakres tematyczny

Kwalifikacyjne Studia Podyplomowe dla nauczycieli w zawodzie technik cyberbezpieczeństwa powstały w odpowiedzi na zlecenie Ministra Edukacji (pismo DKZ-SSPPKZ.5113.9.2026.UB z dnia 3 czerwca 2026 r.), realizowane na podstawie art. 464 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce. Celem studiów jest przygotowanie merytoryczne i dydaktyczne co najmniej 30 nauczycieli do prowadzenia zajęć w zakresie kształcenia zawodowego w nowym zawodzie technik cyberbezpieczeństwa (symbol cyfrowy zawodu 351304), wprowadzonym rozporządzeniem Ministra Edukacji z dnia 20 marca 2026 r. (Dz.U. 2026 poz. 404), w którym kształcenie może być prowadzone od roku szkolnego 2026/2027. Program studiów obejmuje pełny zakres podstawy programowej kształcenia w zawodzie, tj. kwalifikacje INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych oraz INF.12. Programowanie bezpiecznych aplikacji webowych, a także moduł dydaktyki kształcenia zawodowego (90 godzin) i praktyki zawodowe (90 godzin), zgodnie ze standardem kształcenia przygotowującego do wykonywania zawodu nauczyciela (rozporządzenie MNiSW z dnia 25 lipca 2019 r., Dz.U. 2019 poz. 1450 z późn. zm.) w zakresie przygotowania merytorycznego i dydaktycznego do nauczania kolejnego przedmiotu (prowadzenia kolejnych zajęć). Zajęcia merytoryczne obejmują m.in.: podstawy cyberbezpieczeństwa systemów IT, programowanie w języku Python z wykorzystaniem narzędzi AI, projektowanie i administrację bazami danych, administrowanie sieciami TCP/IP, użytkowanie, konfigurację i utwardzanie systemów Windows i Linux, testowanie bezpieczeństwa systemów i sieci, implementację i weryfikację bezpieczeństwa aplikacji webowych oraz testy penetracyjne w środowisku testowym z wykorzystaniem platform typu CTF. W trakcie studiów uczestnicy opracują – pod kierunkiem kadry dydaktycznej – kompletny pakiet materiałów edukacyjnych (scenariusze lekcji, instrukcje laboratoryjne, zadania egzaminacyjne), w który zostaną wyposażeni na potrzeby późniejszej pracy dydaktycznej, zgodnie z założeniem wskazanym w piśmie Ministra Edukacji.

Do kogo adresowane są studia podyplomowe

Studia adresowane są do nauczycieli, w szczególności do: nauczycieli przedmiotów zawodowych branży teleinformatycznej (technik informatyk, technik programista, technik teleinformatyk), nauczycieli informatyki szkół ponadpodstawowych zamierzających uzyskać przygotowanie do prowadzenia zajęć w zawodzie technik cyberbezpieczeństwa, nauczycieli teoretycznych przedmiotów zawodowych i

praktycznej nauki zawodu, kadry branżowych centrów umiejętności w dziedzinach informatyka, programowanie i telekomunikacja. Warunkiem udziału jest posiadanie kwalifikacji nauczycielskich (przygotowania pedagogicznego) oraz dyplomu ukończenia studiów wyższych.

Kierownik studiów podyplomowych:dr inż. Paweł Kuraś
tel.:+12 617 48 07
mail:pkuras@agh.edu.pl

Organizator studiów podyplomowych: Wydział Informatyki, Elektroniki i Telekomunikacji, Instytut Telekomunikacji i Cyberbezpieczeństwa
tel.:+12 617 48 07
mail:pkuras@agh.edu.pl

Osoba do kontaktu:dr inż. Paweł Kuraś
tel.:+12 617 48 07
mail:pkuras@agh.edu.pl

Dodatkowe informacje

Praktyka zawodowa stanowi wyodrębnioną pozycję planu studiów (90 godzin, semestr 3, z możliwością realizacji etapami od semestru 2). Praktyki realizowane są w branżowych centrach umiejętności (BCU) – rekomendowane: Branżowe Centrum Umiejętności w dziedzinie telekomunikacji oraz Informatyczne Branżowe Centrum Umiejętności w Mszanie Dolnej – a także w szkołach prowadzących kształcenie zawodowe w branży teleinformatycznej, w podmiotach branży cyberbezpieczeństwa (SOC, CSIRT) oraz w laboratoriach Instytutu Telekomunikacji i Cyberbezpieczeństwa AGH.

Warunki rekrutacji na studia podyplomowe

- dyplom ukończenia studiów wyższych (pierwszego lub drugiego stopnia albo jednolitych magisterskich);
- kwalifikacje nauczycielskie – przygotowanie pedagogiczne w rozumieniu przepisów w sprawie szczegółowych kwalifikacji wymaganych od nauczycieli; zatrudnienie w szkole prowadzącej kształcenie zawodowe lub w branżowym centrum umiejętności (preferowane), potwierdzone zaświadczeniem lub skierowaniem dyrektora szkoły;
- podstawowa znajomość zagadnień informatycznych (systemy operacyjne, sieci komputerowe) weryfikowana ankietą kompetencji;
- kwalifikacja kandydatów według kolejności zgłoszeń, z pierwszeństwem dla nauczycieli skierowanych przez szkoły planujące uruchomienie kształcenia w zawodzie technik cyberbezpieczeństwa;
- limit przyjęć: minimalnie 30, maksymalnie 36 uczestników (zgodnie ze zleceniem Ministra Edukacji – co najmniej 30 nauczycieli);
- wymagane dokumenty: formularz zgłoszeniowy, kwestionariusz osobowy, poświadczona kopia dyplomu ukończenia studiów wyższych, dokument potwierdzający przygotowanie pedagogiczne, zaświadczenie o zatrudnieniu lub skierowanie dyrektora szkoły.

Sekretariat studiów podyplomowych Instytutu Telekomunikacji AGH, ul. Czarnowiejska 74, 30-054 Kraków, budynek B9, II piętro, pokój 2.04.

Program studiów podyplomowych

Ogólne cele kształcenia w ramach studiów podyplomowych

Ogólne cele kształcenia:

1. przygotowanie merytoryczne nauczycieli do prowadzenia zajęć obejmujących treści kwalifikacji INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych oraz INF.12. Programowanie bezpiecznych aplikacji webowych, zgodnie z podstawą programową kształcenia w zawodzie technik cyberbezpieczeństwa (351304),
2. przygotowanie dydaktyczne do nauczania kolejnych zajęć w zakresie kształcenia zawodowego, zgodnie ze standardem kształcenia przygotowującego do wykonywania zawodu nauczyciela (90 godzin dydaktyki kształcenia zawodowego oraz 90 godzin praktyk zawodowych),
3. wykształcenie praktycznych umiejętności posługiwania się narzędziami i technologiami wskazanymi w podstawie programowej, w tym organizacji i prowadzenia szkolnej pracowni bezpieczeństwa systemów i sieci komputerowych oraz pracowni

programowania i testowania aplikacji webowych,
4. wyposażenie uczestników w kompletny pakiet materiałów edukacyjnych (scenariusze zajęć, instrukcje laboratoryjne, zadania typu CTF, narzędzia oceniania) opracowany w trakcie studiów i służący późniejszej pracy dydaktycznej,
5. przygotowanie uczestników do organizowania kształcenia zgodnego z warunkami realizacji określonymi w podstawie programowej oraz do przygotowania uczniów do egzaminów zawodowych w kwalifikacjach INF.11 i INF.12,
6. ukształtowanie postaw etycznych i odpowiedzialności za legalne wykorzystanie technik cyberbezpieczeństwa w procesie dydaktycznym.

Sylwetka absolwenta studiów podyplomowych

Absolwent studiów posiada przygotowanie merytoryczne i dydaktyczne do prowadzenia zajęć w zakresie kształcenia zawodowego w zawodzie technik cyberbezpieczeństwa (351304), obejmujące pełny zakres kwalifikacji INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych oraz INF.12. Programowanie bezpiecznych aplikacji webowych. Zna i stosuje narzędzia oraz technologie wskazane w podstawie programowej (systemy Windows i Linux, sieci TCP/IP, bazy danych, Python, Java/C#, narzędzia bezpieczeństwa: Wireshark, nmap, OpenVAS, systemy IDS/IPS i SIEM, intercepting proxy, platformy CTF, usługi chmurowe). Potrafi planować i prowadzić zajęcia teoretyczne i praktyczne, organizować pracownię cyberbezpieczeństwa, oceniać osiągnięcia uczniów i przygotowywać ich do egzaminów zawodowych. Dysponuje opracowanym w trakcie studiów pakietem materiałów edukacyjnych do bezpośredniego wykorzystania w pracy dydaktycznej. Absolwent uzyskuje kwalifikacje do prowadzenia kolejnych zajęć (przedmiotów) w zakresie kształcenia zawodowego w zawodzie technik cyberbezpieczeństwa, zgodnie ze standardem kształcenia nauczycieli.

Zasady odbywania studiów podyplomowych, w tym zasady udziału w zajęciach, zasady zaliczania zajęć i zasady składania egzaminów, zasady zaliczania i wpisu na kolejny semestr

Zajęcia prowadzone w formie zjazdów sobotnio-niedzielnych (stacjonarnie w laboratoriach AGH). Obecność na zajęciach dydaktycznych jest obowiązkowa; sposób i tryb usprawiedliwiania nieobecności oraz zasady wyrównywania zaległości powstałych w związku z nieobecnością określają sylabusy poszczególnych przedmiotów. Warunkiem zaliczenia semestru jest uzyskanie pozytywnych ocen ze wszystkich przedmiotów przewidzianych planem studiów oraz zaliczenie praktyki zawodowej.

Wymiar, zasady , forma i miejsce odbywania praktyk, w tym w szczególności warunki ich realizacji, system kontroli praktyk i ich zaliczania (jeżeli są wymagane)

DOTYCZY: praktyka zawodowa w wymiarze 90 godzin – wyodrębniona pozycja planu studiów. Praktyka zawodowa stanowi wyodrębnioną pozycję planu studiów (90 godzin, semestr 3, z możliwością realizacji etapami od semestru 2). Praktyki realizowane są w branżowych centrach umiejętności (BCU) – rekomendowane: Branżowe Centrum Umiejętności w dziedzinie telekomunikacji oraz Informatyczne Branżowe Centrum Umiejętności w Mszanie Dolnej – a także w szkołach prowadzących kształcenie zawodowe w branży teleinformatycznej, w podmiotach branży cyberbezpieczeństwa (SOC, CSIRT) oraz w laboratoriach Instytutu Telekomunikacji i Cyberbezpieczeństwa AGH. Warunkiem zaliczenia jest zrealizowanie programu praktyki potwierdzone dziennikiem praktyk i opinią opiekuna.

Warunki ukończenia studiów podyplomowych i uzyskania świadectwa ukończenia studiów podyplomowych, w tym warunki i wymagania związane z przygotowaniem prac końcowych oraz realizacją procesu dyplomowania, a także związane z organizacją i przebiegiem egzaminu końcowego (jego zakres, tryb i sposób jego przeprowadzenia, zasady ustalania oceny z egzaminu końcowego, wytyczne dotyczące jego przebiegu), jeżeli są wymagane, zasady ustalania ostatecznego wyniku ich ukończenia

Warunkiem ukończenia studiów i uzyskania świadectwa jest uzyskanie pozytywnych ocen ze wszystkich przedmiotów, zaliczenie 90 godzin praktyk zawodowych oraz przygotowanie, zaprezentowanie i obrona dyplomowego pakietu materiałów edukacyjnych w ramach seminarium dyplomowego.

Informacja o możliwości odbycia kształcenia przygotowującego do wykonywania zawodu lub uzyskania uprawnień zawodowych w ramach nowo tworzonych studiów podyplomowych (o ile dotyczy)

Nie dotyczy.

Informacja o możliwości odbycia kształcenia zgodnie ze standardem kształcenia przygotowującego do wykonywania zawodu nauczyciela (o ile dotyczy)

Studia prowadzone zgodnie ze standardem kształcenia przygotowującego do wykonywania zawodu nauczyciela (rozporządzenie MNiSW z 25.07.2019 r., Dz.U. 2019 poz. 1450 z późn. zm.) w zakresie przygotowania merytorycznego i dydaktycznego do nauczania kolejnego przedmiotu (prowadzenia kolejnych zajęć).

Informacja o możliwości uzyskania przygotowania do wykonywania zawodu nauczyciela wraz ze wskazaniem przedmiotu lub rodzaju zajęć, które absolwent będzie mógł prowadzić po ukończeniu studiów podyplomowych (o ile dotyczy)

Absolwent uzyskuje przygotowanie do prowadzenia zajęć w zakresie kształcenia zawodowego w zawodzie technik cyberbezpieczeństwa (351304): kwalifikacje INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych oraz INF.12. Programowanie bezpiecznych aplikacji webowych.

Efekty uczenia się

Kierunek: Kwalifikacyjne studia podyplomowe dla nauczycieli w zawodzie technik cyberbezpieczeństwa

Wiedza

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
TCBSP_W01	wiedza - absolwenci uzyskują specjalistyczne przygotowanie w dziedzinie prawa ochrony danych osobowych w regulacjach krajowych i międzynarodowych	P7S_WG, P7Z_WZ, P8Z_WT, P8Z_WO
TCBSP_W02	zna i rozumie podstawę programową kształcenia w zawodzie technik cyberbezpieczeństwa (351304), strukturę kwalifikacji INF.11 i INF.12, cele i treści jednostek efektów kształcenia oraz wymagania egzaminów zawodowych	P7S_WG, P7Z_WT
TCBSP_W03	zna i rozumie zasady działania i bezpieczeństwa systemów operacyjnych Windows i Linux, sieci TCP/IP, baz danych oraz aplikacji webowych w zakresie wymaganym do nauczania kwalifikacji INF.11 i INF.12	P7S_WG, P7Z_WZ
TCBSP_W04	zna i rozumie metody, techniki i narzędzia cyberbezpieczeństwa (m.in. SIEM, IDS/IPS, skanery podatności, narzędzia kryptograficzne, intercepting proxy, platformy CTF) oraz zasady ich bezpiecznego wykorzystania w pracowni szkolnej	P7S_WG, P7Z_WT
TCBSP_W05	zna i rozumie metodykę kształcenia zawodowego w branży teleinformatycznej, w tym zasady planowania dydaktycznego, oceniania oraz organizacji i przeprowadzania egzaminów zawodowych	P7S_WK, P7Z_WO
TCBSP_W06	zna i rozumie zasady bezpieczeństwa i higieny pracy w pracowni komputerowej oraz prawne i etyczne uwarunkowania prowadzenia testów bezpieczeństwa	P7S_WK, P7Z_WT

Umiejętności

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
TCBSP_U01	potrafi programować w języku Python oraz w języku Java lub C#, w tym z wykorzystaniem narzędzi sztucznej inteligencji do generowania i weryfikacji kodu	P7S_UW, P7Z_UN
TCBSP_U02	potrafi konfigurować, administrować i utwardzać systemy Windows i Linux oraz sieci TCP/IP, a także projektować i administrować relacyjnymi bazami danych	P7S_UW, P7Z_UN
TCBSP_U03	potrafi przeprowadzać testy bezpieczeństwa systemów operacyjnych, sieci i aplikacji webowych, w tym testy penetracyjne w środowisku testowym, oraz interpretować i dokumentować ich wyniki	P7S_UW, P7Z_UI
TCBSP_U04	potrafi zaplanować i przeprowadzić zajęcia teoretyczne i praktyczne w zawodzie technik cyberbezpieczeństwa, opracować scenariusze lekcji, ćwiczenia laboratoryjne oraz zadania typu CTF dostosowane do możliwości uczniów	P7S_UO, P7Z_UO
TCBSP_U05	potrafi opracować materiały edukacyjne i narzędzia sprawdzania osiągnięć oraz przygotować uczniów do egzaminów zawodowych w kwalifikacjach INF.11 i INF.12	P7S_UU, P7Z_UU
TCBSP_U06	potrafi posługiwać się zawodowym językiem angielskim w obszarze cyberbezpieczeństwa, w tym korzystać z anglojęzycznej dokumentacji technicznej w pracy dydaktycznej	P7S_UK, P7Z_UI

Kompetencje społeczne

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
TCBSP_K01	jest gotów do krytycznej oceny posiadanej wiedzy wobec dynamicznych zmian technologii i zagrożeń oraz do ustawicznego doskonalenia zawodowego	P7S_KK
TCBSP_K02	jest gotów do odpowiedzialnego kształtowania postaw etycznych uczniów w zakresie legalnego i odpowiedzialnego wykorzystania technik cyberbezpieczeństwa	P7S_KO, P7Z_KO
TCBSP_K03	jest gotów do współpracy z pracodawcami, branżowymi centrami umiejętności i społecznością szkolną oraz do organizowania pracy małych zespołów uczniowskich	P7S_KR, P7Z_KW