Możliwość dofinansowania

Cyberbezpieczeństwo - studia podyplomowe

Numer usługi 2025/07/02/9407/2852746

9 000,00 PLN brutto
9 000,00 PLN netto
54,22 PLN brutto/h
54,22 PLN netto/h

Akademia Górnośląska im. Wojciecha Korfantego w Katowicach

4,5 / 5

851 ocen

zdalna w czasie rzeczywistym
Studia podyplomowe
166 h
01.10.2025 do 30.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Adresatami studiów podyplomowych „Cyberbezpieczeństwo” są osoby posiadające wykształcenie wyższe, które pracują lub planują podjąć zatrudnienie w obszarze IT i chcą pogłębić swoją wiedzę z zakresu bezpieczeństwa informatycznego. Studia skierowane są do administratorów systemów, inżynierów bezpieczeństwa, specjalistów ds. IT, menedżerów projektów, a także osób zainteresowanych tematyką cyberbezpieczeństwa w sektorze prywatnym i publicznym.
Minimalna liczba uczestników	11
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	29-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	166
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742, z późn. zm.)
Zakres uprawnień	studia podyplomowe

Cel

Cel edukacyjny

Usługa „Cyberbezpieczeństwo – studia podyplomowe” potwierdza przygotowanie do planowania, wdrażania i nadzorowania działań z zakresu bezpieczeństwa informatycznego w organizacjach. Uczestnik zdobywa wiedzę i umiejętności niezbędne do ochrony systemów IT przed zagrożeniami cybernetycznymi, zarządzania ryzykiem oraz reagowania na incydenty bezpieczeństwa w środowisku zawodowym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe zagrożenia dla bezpieczeństwa systemów informatycznych.	Rozróżnia typy zagrożeń cybernetycznych. Opisuje skutki ataków dla ciągłości działania organizacji.	Test teoretyczny
Definiuje zasady ochrony danych osobowych i zgodności z RODO i normą ISO 27001.	Wyjaśnia wymogi prawne dotyczące ochrony danych. Wskazuje kluczowe obszary objęte normą ISO 27001.	Test teoretyczny
Charakteryzuje elementy architektury bezpieczeństwa systemów operacyjnych i sieci.	Wymienia komponenty systemów zabezpieczających. Opisuje funkcje narzędzi Microsoft, Linux i Azure w kontekście bezpieczeństwa.	Test teoretyczny
Monitoruje środowisko IT pod kątem zagrożeń i incydentów bezpieczeństwa.	Identyfikuje wskaźniki kompromitacji (IoC). Analizuje logi systemowe i sieciowe.	Test teoretyczny
Wdraża środki techniczne zapewniające bezpieczeństwo danych i systemów.	Konfiguruje ustawienia zabezpieczające system Windows/Linux. Stosuje mechanizmy kontroli dostępu w środowisku Microsoft 365/Azure.	Test teoretyczny
Planuje i przeprowadza testy penetracyjne oraz proponuje działania naprawcze.	Opracowuje scenariusze testów w oparciu o MITRE ATT&CK. Ocenia skuteczność istniejących zabezpieczeń.	Test teoretyczny
Współpracuje z zespołem w celu zarządzania incydentami i kryzysami bezpieczeństwa.	Uczestniczy w ćwiczeniach zespołowych dotyczących reagowania na incydenty. Komunikuje zagrożenia w sposób zrozumiały dla różnych interesariuszy.	Test teoretyczny
Przestrzega zasad etyki zawodowej w działaniach związanych z cyberbezpieczeństwem.	Identyfikuje sytuacje naruszające dobre praktyki.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Bezpieczeństwo cybernetyczne - wprowadzenie (8 godzin)

• Wprowadzenie do bezpieczeństwa cybernetycznego

• Bezpieczeństwo danych

• Normy prawne i branżowe (RODO, ISO 27001)

• Cyberbezpieczeństwo w organizacji

• Sytuacje kryzysowe

• Zachowanie ciągłości biznesowej organizacji

• Zarządzanie ryzykiem

2. OSINT (Biały wywiad) (8 godzin)

• Wprowadzenie do OSINTu

• Przygotowanie środowiska – zachowanie anonimowości

• Podstawowe techniki poszukiwania informacji

• Metadane i ich analiza

• Socjotechniki w służbie wywiadu

• Wyszukiwanie informacji o firmach i osobach

• Jak zadbać o swoje bezpieczeństwo

3. Microsoft Security, Compliance, and Identity Fundamentals (8 godzin)

• Podstawowe pojęcia dotyczące bezpieczeństwa, zgodności i tożsamości

• Koncepcje i możliwości rozwiązań firmy Microsoft do zarządzania tożsamością i dostępem

• Możliwości rozwiązań zabezpieczających firmy Microsoft

• Możliwości rozwiązań Microsoft zapewniających zgodność

4. Bezpieczeństwo systemu Windows 11 (16 godzin)

• Uwierzytelnianie i autoryzacja w Windows 11

• Ochrona wrażliwych danych

• Sposoby ochrony przed złośliwym oprogramowaniem

• Klient Hyper-V

• Wdrażanie rekomendowanych zasad bezpieczeństwa w kontekście bazowych ustawień systemu Windows 11

• Narzędzia SCM i SCT

• Przykładowe ustawienia bezpiecznego Windows 11

5. Bezpieczeństwo systemów w domenie Active Directory Windows Server 2022 w połączeniu z Windows 11 (32 godziny)

• Wprowadzenie do bezpieczeństwa systemów Microsoft

• Planowanie i konfigurowanie strategii autoryzacji i uwierzytelniania

• Zabezpieczanie serwerów Windows Server 2022

• Instalacja, konfigurowanie i zarządzanie urzędem certyfikacji (Certification Authority)

• Konfiguracja, dostarczanie i zarządzanie certyfikatami

• Bezpieczna transmisja danych

• Zabezpieczanie zdalnego dostępu

• Wdrażanie WSUS

• Bezpieczeństwo stacji roboczej Windows 11

• Sposoby ochrony przed złośliwym oprogramowaniem

6. Microsoft Azure Security Technologies (32 godziny)

• Tożsamość i dostęp

• Wdrożenie ochrony platformy

• Bezpieczeństwo danych i aplikacji

• Operacje bezpieczeństwa

7. Warsztaty z CompTIA Security+ (28 godzin)

• Podstawowe koncepcje bezpieczeństwa

• Porównanie różnych typów zagrożeń

• Omówienie podstawowych pojęć kryptografii

• Wdrażanie zarządzania tożsamością i kontrolą dostępu

• Zabezpieczanie architektury sieci korporacyjnej

• Zabezpieczanie architektury sieci w usługach chmurowych

• Omówienie koncepcji odporności

• Zarządzanie podatnościami

• Bezpieczeństwo sieciowe

• Ocena bezpieczeństwa punktów końcowych

• Wdrażanie zabezpieczeń aplikacji

• Zarządzanie incydentami i monitorowanie środowiska

• Po czym rozpoznać atak – wskaźniki kompromitacji

• Zarządzania bezpieczeństwem w organizacji poprzez polityki, standardy i procedury

• Podstawowe pojęcia związane zarządzania ryzykiem

• Ochrona danych i dbałość o ich zgodność w organizacji

8. Testy penetracyjne (16 godzin)

• Wprowadzenie

• Testy bezpieczeństwa

• Praktyczne ataki w testach penetracyjnych (na bazie taktyk i technik Mitre Attack)

• Ogólne inne typy ataków hackerskich – prezentacja

• Dobre praktyki, formy obrony przed atakami

9. Bezpieczeństwo systemów Linux (16 godzin)

• Monitorowanie systemu Linux pod kątem bezpieczeństwa

• Zabezpieczanie systemu

• Zabezpieczanie logów systemowych

• Bezpieczeństwo fizyczne serwera

• System okiem hakera

• Elementy kryptografii

• Kali Linux – system Linux okiem hakera

Egzamin (2 godziny)

Program studiów jest realizowany według godzin dydaktycznych (1h dydaktyczna = 45 minut (zegarowych). Przerwy nie są wliczane w czas trwania usługi rozwojowej.

Czas trwania: 2 semestry.

Dni zajęć: soboty, niedziele średnio w jeden weekend w miesiącu w godz. 09:00-17:00.

Łączna ilość godzin: 166 godzin kontaktowych.

Zajęcia na studiach realizowane są w formie ćwiczeń, rozmów na żywo, analizy kazusów, testów, współdzielenia ekranu.

Zajęcia prowadzone są przez ekspertów z wieloletnim doświadczeniem w branży IT i cyberbezpieczeństwa.

Aktywizująca Uczestników forma prowadzenia zajęć pozwoli na wyćwiczenie umiejętności rozwiazywania problemów zarówno przedstawianych przez wykładowcęjak i podnoszonych na bieżąco przez słuchaczy.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	9 000,00 PLN
Koszt przypadający na 1 uczestnika netto	9 000,00 PLN
Koszt osobogodziny brutto	54,22 PLN
Koszt osobogodziny netto	54,22 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne przekazywane są uczestnikom drogą elektroniczną – za pośrednictwem poczty e-mail. Uczestnicy otrzymają materiały bezpośrednio związane z realizowaną usługą rozwojową, takie jak: pliki dokumentów przygotowanych w różnych formatach.

Warunki uczestnictwa

Na studia przyjmowane są osoby z wyższym wykształceniem.

Zapis w Bazie Usług Rozwojowych (BUR) nie jest równoznaczny z przyjęciem na studia w Uczelni. Warunkiem przyjęcia na studia jest rejestracja w systemie internetowej rekrutacji, złożenie kompletu wymaganych dokumentów oraz dopełnienie wszystkich formalności

Informacje dodatkowe

Organizator zapewnia rozdzielność walidacji od procesu kształcenia.

Dokumentem potwierdzającym ukończenie studiów podyplomowych jest Świadectwo ukończenia studiów podyplomowych.

Usługi realizowane przez Akademię są zwolnione z VAT na podstawie Art. 43 ust. 1 pkt. 26 ustawy o Vat i §3 ust. 1 pkt 13 rozporządzenia Ministra Finansów z dnia20.12.2013 r. w sprawie wykonania niektórych przepisów ustawy o podatku od towarów i usług.

Na terenie Uczelni dostępne są udogodnienia dla osób ze szczególnymi potrzebami, w tym: winda, dostosowane wejście, toaleta, parking z miejscami dla osób z niepełnosprawnościami oraz możliwość skorzystania ze wsparcia Centrum Osób ze Szczególnymi Potrzebami.

Warunki techniczne

Zajęcia realizowane zdalnie - poprzez platformy Ms Teams, Zoom.

Minimalne wymagania sprzętowe: Urządzenie z dostępem do Internetu (telefon, tablet, komputer). Sprawny mikrofon i kamera internetowa.

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: download 8 mb/s, upload 8 mb/s,ping 15 ms

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: Zalecamy wykorzystanie przeglądarki internetowej najnowszej wersji.

Kontakt

SVITLANA BLINOVA

E-mail svitlana.blinova@akademiagornoslaska.pl
Telefon (+48) 32 3570 583