Możliwość dofinansowania

Cyberbezpieczeństwo i Ochrona Danych

Numer usługi 2025/04/04/172310/2671451

7 000,00 PLN brutto
7 000,00 PLN netto
38,89 PLN brutto/h
38,89 PLN netto/h

WYŻSZA SZKOŁA ADMINISTRACJI I BIZNESU IM. EUGENIUSZA KWIATKOWSKIEGO W GDYNI (WSAiB)

Brak ocen dla tego dostawcy

Gdynia
Studia podyplomowe
mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
180:00 h
31.10.2026 do 20.06.2027

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Studia podyplomowe **Cyberbezpieczeństwo i Zarządzanie Usługą IT** łączą wiedzę z zakresu ochrony danych, zarządzania ryzykiem cyfrowym i wykorzystania sztucznej inteligencji w bezpieczeństwie IT. Adresowane są do: • **Managerów IT i pracujących w działach IT**, którzy chcą podnieść swoje kwalifikacje w zakresie ochrony danych i reagowania na cyfrowe zagrożenia. • **Przedsiębiorców i kadry zarządzającej**, którym zależy na zapewnieniu bezpieczeństwa i rozwoju technologicznego swoich firm. • **Osób odpowiedzialnych za zgodność z przepisami (compliance)** w zakresie regulacji dotyczących ochrony danych i współczesnych wyzwań technologicznych. • **Pracowników działów technologicznych**, którzy chcą zdobyć praktyczne umiejętności wykorzystywania AI w obszarze bezpieczeństwa. • **Pracowników**, którzy chcą poszerzyć swoje kompetencje w traktowaniu IT jako narzędzia będącego elementem koniecznym każdego przedsiębiorstwa / organizacji.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	23-10-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

Liczba godzin usługi	180
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 2024 r. poz. 1571, z późn. zm.)
Zakres uprawnień	studia podyplomowe

Cel

Cel edukacyjny

Studia podyplomowe przygotowują do zarządzania bezpieczeństwem cyfrowym, inwestowania w nowoczesne technologie oraz reagowania na incydenty z użyciem zaawansowanych narzędzi i metod sztucznej inteligencji. Program kładzie szczególny nacisk na aspekty business continuity, ucząc, jak skutecznie minimalizować skutki ataków i zapewniać ciągłość działania przedsiębiorstwa nawet w najtrudniejszych sytuacjach, a także budowę zespołów odpowiedzialnych za rozwój i redukcję długu technologicznego.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA • Zna rodzaje zagrożeń cybernetycznych i metody ochrony danych • Rozumie przepisy prawa dotyczące bezpieczeństwa informacji i usług cyfrowych • Zna nowoczesne technologie wspierające cyberbezpieczeństwo, w tym AI • Rozumie zasady zarządzania ryzykiem, ciągłością działania i architekturą IT • Zna zasady funkcjonowania zespołów DevSecOps oraz systemów zgodnych z ISO	• Opisuje typy ataków i metody przeciwdziałania • Analizuje przypadki naruszenia bezpieczeństwa • Wyjaśnia zasady stosowania przepisów prawnych w kontekście bezpieczeństwa • Interpretuje procesy związane z zarządzaniem usługą IT i bezpieczeństwem danych	Test teoretyczny
UMIEJĘTNOŚCI • Potrafi identyfikować zagrożenia i przeprowadzać analizę ryzyka • Tworzy i wdraża strategie bezpieczeństwa informacji • Umie obsługiwać narzędzia do monitorowania i reagowania na incydenty • Prowadzi audyty bezpieczeństwa i planuje działania naprawcze • Potrafi zarządzać zespołem ds. bezpieczeństwa oraz wdrażać DevSecOps	• Realizuje projekt zabezpieczenia systemu IT • Przeprowadza symulację incydentu i wdraża procedury reagowania • Ocenia poziom ryzyka w organizacji i opracowuje strategię zarządzania • Wdraża model zarządzania usługą IT zgodny z najlepszymi praktykami	Prezentacja

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETENCJE SPOŁECZNE • Działa odpowiedzialnie w zakresie decyzji wpływających na bezpieczeństwo • Pracuje zespołowo w strukturach IT i DevSecOps • Rozumie znaczenie ochrony danych i odpowiedzialności etycznej • Gotowy do uczenia się i dostosowywania do zmieniających się zagrożeń • Wykazuje inicjatywę w rozwijaniu polityki bezpieczeństwa w organizacji	• Uczestniczy w projektach zespołowych z zakresu bezpieczeństwa • Podejmuje decyzje w oparciu o analizę etyczną i regulacyjną • Reflektuje nad własną rolą i wpływem działań IT na bezpieczeństwo firmy • Tworzy plan podnoszenia dojrzałości bezpieczeństwa w organizacji	Obserwacja w warunkach rzeczywistych

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

BLOK 1: Fundamenty cyberbezpieczeństwa

- Wprowadzenie do cyberbezpieczeństwa
- Bezpieczeństwo informacji i systemów informatycznych
- Podstawy prawne ochrony informacji (RODO, KRI, NIS2, ustawa o KSC)

BLOK 2: Zarządzanie bezpieczeństwem

- Zarządzanie ryzykiem w cyberbezpieczeństwie
- Zarządzanie incydentami i reagowanie na naruszenia
- Tworzenie i wdrażanie polityk bezpieczeństwa informacji
- Planowanie ciągłości działania i zarządzanie kryzysowe

BLOK 3: Infrastruktura i architektura bezpieczeństwa

- Architektura systemów bezpieczeństwa IT
- Audyt bezpieczeństwa IT
- Bezpieczeństwo sieci komputerowych
- Systemy wykrywania włamań i monitorowanie zagrożeń

BLOK 4: Bezpieczeństwo aplikacji i DevSecOps

- Bezpieczeństwo aplikacji webowych – OWASP Top 10
- Zabezpieczanie środowisk chmurowych
- DevSecOps – integracja bezpieczeństwa z cyklem życia oprogramowania
- Testy penetracyjne i analiza podatności

BLOK 5: Technologie wspierające bezpieczeństwo

- Nowoczesne technologie w cyberbezpieczeństwie (AI, blockchain, automatyzacja)
- Systemy SIEM i narzędzia do monitoringu
- Kryptografia i bezpieczna komunikacja

BLOK 6: Kompetencje miękkie i etyka

- Psychologia bezpieczeństwa – czynnik ludzki i socjotechnika
- Kultura bezpieczeństwa w organizacji
- Etyka zawodowa w cyberbezpieczeństwie
- Komunikacja kryzysowa i współpraca z interesariuszami

Harmonogram

Liczba pozycji harmonogramu: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 000,00 PLN
Koszt przypadający na 1 uczestnika netto	7 000,00 PLN
Koszt osobogodziny brutto	38,89 PLN
Koszt osobogodziny netto	38,89 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Jakub Ubych

OPIEKUN KIERUNKU

Od ponad 15 lat uczestniczy w realizowaniu projektów informatycznych dla przedsiębiorstw m.in. przy wytwarzaniu oprogramowania, a także wdrażaniu rozwiązań teleinformatycznych. Uczestniczył w powstaniu centrum usług wspólnych integrujących działania sektora IT w samorządzie.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy studiów podyplomowych otrzymują materiały dydaktyczne w trakcie trwania studiów podyplomowych, podczas zajęć. Po zakończeniu zajęć materiały są zamieszczane na platformie e-learningowej Moodle.

Materiały dydaktyczne przygotowują wykładowcy danego przedmiotu w różnych formatach, dostosowując je do potrzeb uczestników i specyfiki prowadzonego przedmiotu i tematu.

Warunki uczestnictwa

Studia adresowane są do absolwentów wszystkich kierunków studiów, posiadających co najmniej dyplom na poziomie licencjackim, inżynierskim lub magisterskim.

O przyjęciu na studia decyduje kolejność zgłoszeń.

Ważna informacja: W przypadku niewystarczającej liczby zgłoszeń, Uczelnia (Dostawca Usług) zastrzega sobie prawo do odwołania edycji studiów.

Warunki techniczne

Zjazdy stacjonarne odbywają się w siedzibie Uczelni. Sale wyposażone są w :

- rzutniki multimedialne,
- nowoczesne ekrany projekcyjne,
- komputery,
- dostęp do Wi-Fi.

Zajęcia online odbywają się na platformie Teams, do których niezbędne są :

- komputer (z wbudowanym lub podłączonymi głośnikami i mikrofonem),
- dostęp do Internetu,
- słuchawki (opcjonalnie),
- kamera umieszczona w laptopie/ komputerze (opcjonalnie).

Adres

ul. Kielecka 7

81-303 Gdynia

woj. pomorskie

Wyższa Szkoła Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni dysponuje dwoma nowoczesnymi kampusami zlokalizowanymi przy ul. Kieleckiej 7 i Łużyckiej 2B. Oba znajdują się w doskonałej lokalizacji blisko centrum miasta, na pograniczu Trójmiejskiego Parku Krajobrazowego, obok kolejki miejskiej i węzła komunikacyjnego, co zapewnia wygodny dojazd. Uczelnia dysponuje własnymi bezpłatnymi parkingami dla studentów i wykładowców, a bliskość Centrum Riviera jest dodatkowym udogodnieniem. Przestronne kampusy dostosowane są dla osób z niepełnosprawnościami. Budynki znajdują się w niedalekiej odległości od plaży i morza, w nowoczesnej, biznesowej części Gdyni.

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe
- Nowoczesny kampus dostosowany jest dla osób z niepełnosprawnościami

Kontakt

Aleksandra Molesta

E-mail podyplomowe@wsaib.pl

Telefon (+48) 586 607 428