Możliwość dofinansowania

Cyberbezpieczeństwo energetyczne

Numer usługi 2025/04/15/7100/2691055

7 500,00 PLN brutto
7 500,00 PLN netto
42,13 PLN brutto/h
42,13 PLN netto/h

Uniwersytet WSB Merito w Gdańsku

Gdańsk / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Studia podyplomowe
178 h
18.10.2025 do 28.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	**Adresatami studiów są osoby pragnące** zdobyć wiedzę i umiejętności umożliwiające podjęcie pracy w komórkach bezpieczeństwa w organizacjach z sektora publicznego i prywatnego świadczących usługi energetyczne. Celem studiów jest zapoznanie uczestników z podstawowymi problemami zabezpieczeń sieci komputerowych, systemów komputerowych i aplikacji. Ukończenie studiów podyplomowych na kierunku Cyberbezpieczeństwo energetyczne gwarantuje zdobycie kwalifikacji oraz umiejętności, które sprawdzą się przy zarządzaniu zespołem cyberbezpieczeństwa infrastruktury energetycznej. Podczas wykładów i ćwiczeń zapoznasz się z nowoczesnymi metodami działań, poznasz organy ścigania cyberprzestępstw, dowiesz się więcej o ochronie infrastruktury energetycznej.
Minimalna liczba uczestników	20
Maksymalna liczba uczestników	40
Data zakończenia rekrutacji	13-10-2025
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	178

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

Głównym celem studiów jest przekazanie praktycznej wiedzy z zakresu zarządzania cyberbezpieczeństwem w organizacjach z sektora publicznego i prywatnego świadczących usługi energetyczne i przygotowanie kadry dla nowych wyzwań prognozowanych w tym zakresie.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA - Opisuje podstawy prawne funkcjonowania systemu cyberbezpieczeństwa w sektorze energetycznym. - Omawia zasady ochrony infrastruktury krytycznej oraz wymogi audytów bezpieczeństwa. - Wyjaśnia zagrożenia i mechanizmy ryzyka w cyberprzestrzeni. - Objaśnia podstawy informatyczne cyberbezpieczeństwa.	- Tłumaczypolskie i unijne regulacje dotyczące cyberbezpieczeństwa infrastruktury energetycznej. - Objaśnia procedury bezpieczeństwa fizycznego i informatycznego stosowane w sektorze energetycznym. - Omawia źródła zagrożeń cybernetycznych dla systemów energetycznych oraz zasady szacowania ryzyka i zapewnienia ciągłości działania. - Opisuje działanie sieci komputerowych, systemów operacyjnych, IoT i aplikacji z perspektywy bezpieczeństwa.	Wywiad ustrukturyzowany Prezentacja
UMIEJĘTNOŚCI - Rozpoznaje i analizuje incydenty w sektorze energetycznym. - Stosuje metody testów bezpieczeństwa i analizuje podatności - Zabezpiecza systemy IT w sektorze energetycznym. - Projektuje rozwiązania zwiększające odporność organizacji na zagrożenia cybernetyczne.	- Identyfikuje, analizuje i dokumentuje incydenty bezpieczeństwa informatycznego. - Wykorzystuje metody OSINT i analizuje cyfrowe ślady. - Wdraża standardy ISO oraz zasady ochrony informacji zgodnie z dobrymi praktykami. - Wdraża procedury zapewniające ciągłość działania.	Wywiad ustrukturyzowany Prezentacja
KOMPETENCJE SPOŁECZNE - Działa odpowiedzialnie w zakresie bezpieczeństwa informacji. - Współpracuje w zespole ds. bezpieczeństwa. - Świadomie ocenia zagrożenia i proponuje rozwiązania.	- Przestrzega norm etycznych oraz przepisów prawa dotyczących ochrony danych i infrastruktury krytycznej. - Efektywnie komunikuje się z członkami zespołów IT, analitykami bezpieczeństwa i przedstawicielami administracji publicznej. - Podejmuje inicjatywę w podnoszeniu świadomości i kultury bezpieczeństwa w organizacji.	Wywiad ustrukturyzowany Prezentacja

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

Podstawy prawne bezpieczeństwa w cyberprzestrzeni w sektorze energetycznym (52 godz.)

- Prawne ramy polskiej i europejskiej regulacji cyberbezpieczeństwa sektora energii. (6 godz.)
- Organy właściwe do spaw cyberprzestępstwa. (6 godz.)
- Postępowanie z incydentem informatycznym (8 godz.)
- Obowiązki podmiotów w sektorze energetycznym. (8 godz.)
- Wymagania i metody audytów systemów informatycznych. (8 godz.)
- Ochrona infrastuktury kytycznej w Polsce - bzpieczeństwo fizyczne. (8 godz.)

Techniczne i organizacyjne aspekty zarządzania bezpieczeństwem w cyberprzestrzeni w sektorze energetycznym

(56 godz.)

- Budowania w organizacjach odporności w cyberprzestzreni dla sektora energetycznego. (8 godz.)
- Zagrożenia dla bezpieczeństwa w cyberprzestrzeni w sektorze energetycznym. (8 godz.)
- Wymagania i metody szacowania ryzyka oraz zapewnienia ciągłości działania (14 godz.)
- Ochrona zasobów informacyjnych w systemach IT w sektorze energetycznym (norma ISO 27001;27002;27032). (10 godz.)
- Reagowanie na incydenty bezpieczeństwa IT w sektorze energetycznym. (8 godz.)
- OSINT jako technika wywiadu i jego znaczenie. (8 godz.)

INFORMATYCZNE ASPEKTY CYBERBEZPIECZEŃSTWA w sektorze energetycznym (62 godz.)

- Bezpieczeństwo sieci komputerowych i telekomunikacyjnych. (6 godz.)
- Identyfikowanie podatności w systemach teleinformatycznych. (6 godz.)
- Metodyka testów penetracyjnych z elementami socjotechniki. (6 godz.)
- Rozpoznanie w cyberprzestrzeni oraz analiza cyfrowych śladów. (6 godz.)
- Przełamywanie zabezpieczeń klasycznych systemów operacyjnych i IoT. (6 godz.)
- Technologie zabezpieczania i szyfrowania zasobów i informacji. (6 godz.)
- Bezpieczeństwo systemów i aplikacji. (6 godz.)
- Podstawy kryptografii. (8 godz.)
- Wykorzystanie złośliwego oprogramowania. (6 godz.)
- Skanowanie sieci i enumeracja systemów informatycznych. (6 godz.)

Projekt (8 godz.)

- seminarium projektowe (8 godz.)

Harmonogram

Liczba przedmiotów/zajęć: 1

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 1 Wprowadzenie do studiów	18-10-2025	08:00	16:00	08:00	Tak

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 500,00 PLN
Koszt przypadający na 1 uczestnika netto	7 500,00 PLN
Koszt osobogodziny brutto	42,13 PLN
Koszt osobogodziny netto	42,13 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

kmdr por. rez. dr inż. Ernest Lichocki

kmdr por. rez. dr inż. Ernest Lichocki, doktor nauk wojskowych w specjalności zarządzanie bezpieczeństwem. Doktorant Akademii Obrony Narodowej. Posiada podyplomowe wykształcenie wyższe w zakresie bezpieczeństwa informacyjnego. Doświadczenie zawodowe i naukowe zdobył głównie pełniąc przez wiele lat szereg stanowisk służbowych związanych z bezpieczeństwem teleinformacyjnym i teleinformatycznym. Posiada uprawnienia związane z bezpieczeństwem teleinformatycznym, w tym z ochroną informacji niejawnych. Ukończył w kraju i zagranicą ponad 20 kursów specjalistycznych związanych z bezpieczeństwem systemów łączności, systemów wspomagania informacji i systemów teleinformatycznych. Autor kilkunastu projektów wdrożonych do resortu MON i MSWiA. Autor i współautor ponad 40 publikacji związanych z bezpieczeństwem teleinformatycznym i bezpieczeństwem Infrastruktury Krytycznej Państwa. Promotor ponad 60 prac magisterskich i licencjackich.

Zainteresowania naukowe: cyberterroryzm oraz bezpieczeństwo morskie państwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały w wersji elektronicznej udostępniane na platformie moodle/teams.

Warunki uczestnictwa

Zasady rekrutacji:

https://www.merito.pl/gdansk/studia-i-szkolenia/studia-podyplomowe/zasady-rekrutacji

Szczegóły kierunku dostępne pod linkiem:

https://www.merito.pl/gdansk/studia-i-szkolenia/studia-podyplomowe/kierunki/cyberbezpieczenstwo-energetyczne

Informacje dodatkowe

Wymagany jest dodatkowy zapis poprzez formularz rekrutacyjny dostępny pod linkiem:

https://www.merito.pl/rekrutacja/krok1

Warunki techniczne

Wymagania techniczne: komputer z dostępem do internetu, monitor, klawiatura.

Adres

al. Aleja Grunwaldzka 238A
80-266 Gdańsk
woj. pomorskie

Kampus Uniwersytetu WSB Merito (dawniej Wyższa Szkoła Bankowa w Gdańsku).
Na terenie uczelni znajdują się kantyna, bufet, automaty z przekąskami.
Oferujemy bezpłatny parking. Swobodny dojazd na Uczelnię komunikacją miejską (tramwaj, autobus, SKM, PKM).

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

Kontakt

Agata Orlich

E-mail rekrutacjasp@gdansk.merito.pl
Telefon (+48) 585 227 513