Możliwość dofinansowania

Zarządzanie Cyberbezpieczeństwem. Certyfikat ISO 27001

Numer usługi 2025/03/26/7100/2651271

6 100,00 PLN brutto
6 100,00 PLN netto
34,66 PLN brutto/h
34,66 PLN netto/h

Uniwersytet WSB Merito w Gdańsku

4,5 / 5

49 ocen

Gdańsk / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

Studia podyplomowe

176 h

25.10.2025 do 28.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Adresatami studiów są osoby pragnące zdobyć wiedzę i umiejętności umożliwiające podjęcie pracy w komórkach bezpieczeństwa IT oraz niezbędne do dalszego rozwoju w dziedzinie cyberbezpieczeństwa w wybranym z wielu rozpoczętych podczas nauki kierunków. Celem studiów jest zapoznanie uczestników z podstawowymi problemami zabezpieczeń sieci komputerowych, systemów komputerowych i aplikacji. Równocześnie wiedza z zakresu cyberbezpieczeństwa, którą uczestnicy posiądą na poziomie średniozaawansowanym umożliwi im dalszy rozwój na jednej z wielu możliwych ścieżek certyfikacji czyniąc z nich ekspertów od zabezpieczeń w przedsiębiorstwach dowolnej skali.
Minimalna liczba uczestników	20
Maksymalna liczba uczestników	36
Data zakończenia rekrutacji	23-10-2025
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	176
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

Celem studiów jest zapoznanie uczestników z podstawowymi problemami zabezpieczeń sieci komputerowych, systemów komputerowych i aplikacji. Równocześnie wiedza z zakresu cyberbezpieczeństwa, którą uczestnicy posiądą na poziomie średniozaawansowanym umożliwi im dalszy rozwój na jednej z wielu możliwych ścieżek certyfikacji czyniąc z nich ekspertów od zabezpieczeń w przedsiębiorstwach dowolnej skali.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA rozumie w zaawansowanym stopniu zagadnienia z zakresu cyberbezpieczeństwa oraz charakteryzuje związek z innymi dyscyplinami z zakresu nauk społecznych rozumie w zaawansowanym stopniu procesy, zjawiska, podmioty, struktury i instytucje bezpieczeństwa wewnętrznego oraz elementy na nie wpływające	osiąga w zaawansowanym stopniu właściwe dla cyberbezpieczeństwa metody i narzędzia i techniki pozyskiwania danych, pozwalające opisywać zjawiska, procesy, podmioty, struktury i instytucje bezpieczeństwa w tym dobiera w zaawansowanym stopniu procesy zmian podmiotów, instytucji i struktur cyberbezpieczeństwa oraz jego przyczyny, przebieg i skalę	Test teoretyczny Prezentacja Wywiad ustrukturyzowany
UMIEJĘTNOŚCI obserwować i interpretować zjawiska oraz procesy zachodzące w zakresie lokalnym i globalnym w kontekście cyberbezpieczeństwa w tym w sektozre energetycznym wykorzystywać wiedzę teoretyczną do pozyskiwania danych w celu praktycznego analizowania procesów i zjawisk z zakresu cyberbezpieczeństwa w tym w sektozre energetycznym KOMPETENCJE SPOŁECZNE Samodzielnie wykorzystuje wiedzę, metody, narzędzia i techniki służące tworzeniu skutecznych treści.	ocenia, wdraża rozwiązania problemów z zakresu bezpieczeństwa oraz dobiera metody oraz instrumenty pozwalające racjonalnie je rozstrzygać etycznie postępuje w ramach wyznaczonych ról organizacyjnych i społecznych oraz identyfikacji i rozstrzygania dylematów oraz różnych wariantów rozwiązań związanych z wykonywaniem zawodu komunikowania się z otoczeniem; dostosowuje się do nowych sytuacji i warunków, podejmuje nowe zadania, potrafi działać w sposób przedsiębiorczy	Prezentacja Wywiad ustrukturyzowany Prezentacja Wywiad ustrukturyzowany

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

LP.	NAZWA PRZEDMIOTU	ŁĄCZNA LICZBA GODZIN ZAJĘĆ	ŁĄCZNA LICZBA PUNKTÓW ECTS	Godziny praktyczne	Godziny teoretyczne
I.	PRAWNE ASPEKTY ZASOBÓW INFORMACYJNYCH W CYBERPRZESTRZENI				
1.	Ramy systemu cyberbezpieczeństwa w Unii Europejskiej. Zadania państw członkowskich, zakres podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa	8	1,00	0	8
2.	Obowiązki podmiotów kluczowych i ważnych, podmiotów działających w sektorach krytycznych, podmiotów publicznych	6	1,00	0	6
3.	Organy właściwe do spaw cyberprzestępstwa	4	1,00	0	4
4.	Sankcje karne w cyberprzestępczości	4	1,00	0	4
5.	Prawne aspekty ochrony prywatności w sieci	4	1,00	0	4

6.	Dowody elektroniczne, a przepisy kodeksu postępowania	6	1,00	2	4
7.	Postępowanie z incydentem informatycznym - środki zarządzania ryzykiem w cyberbezpieczeństwie	8	1,00	4	4
II.	ORGANIZACYJNE ASPEKTY ZARZĄDZANIA BEZPIECZEŃSTWEM CYBERPRZESTRZENI				
1.	Funkcjonalne systemy bezpieczeństwa – bezpieczeństwo fizyczne i środowiskowe	8	1,00	8	0
2.	Zagrożenia dla bezpieczeństwa w cyberprzestrzeni	8	1,00	8	0
3.	Wymagania i metody szacowania ryzyka oraz zapewnienia ciągłości działania	10	1,00	10	0
4.	Ochrona zasobów informacyjnych w systemach IT	8	1,00	8	0
5.	Reagowanie na incydenty bezpieczeństwa IT	6	1,00	6	0
6.	Wymagania i metody audytów systemów informatycznych	8	1,00	8	0
III.	INFORMATYCZNE ASPEKTY CYBERBEZPIECZEŃSTWA				
1.	Bezpieczeństwo sieci komputerowych i telekomunikacyjnych	6	1,00	6	0
2.	Identyfikowanie podatności w systemach teleinformatycznych	8	1,00	8	0
3.	Metodyka testów penetracyjnych z elementami socjotechniki	10	1,00	10	0

4.	Rozpoznanie w cyberprzestrzeni oraz analiza cyfrowych śladów	8	1,00	8	0
5.	Przełamywanie zabezpieczeń klasycznych systemów operacyjnych i IoT	6	1,00	6	0
6.	Technologie zabezpieczania i szyfrowania zasobów i informacji	8	1,00	8	0
7.	Bezpieczeństwo systemów i aplikacji	6	1,00	6	0
8.	Podstawy kryptografii	8	1,00	8	0
9.	Wykorzystanie złośliwego oprogramowania	6	1,00	6	0
10.	Skanowanie sieci i enumeracja systemów informatycznych	6	1,00	6	0
11.	OSINT jako technika wywiadu i jego znaczenie dla bezpieczeństwa IT	6	1,00	6	0
IV.	PROJEKT				
1.	Seminarium podyplomowe	8	6,00	8	0
	FORMA ZALICZENIA				
	Test końcowy	1	-	1	0
	Egzamin końcowy	1	-	1	0
	Razem	176	30	142	34

Harmonogram

Liczba przedmiotów/zajęć: 36

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 36 Spotkanie z opiekunem merytorycznym	Klaudia Skelnik	25-10-2025	08:00	08:30	00:30	Nie
2 z 36 Ramy systemu cyberbezpieczeństwa w Unii Europejskiej. Zadania państw członkowskich, zakres podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa	Klaudia Skelnik	25-10-2025	08:45	11:00	02:15	Nie
3 z 36 Organy właściwe do spraw cyberprzestępstwa	Marcin Jurgilewicz	25-10-2025	11:30	14:45	03:15	Nie
4 z 36 Obowiązki operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych	Piotr Robakowski	26-10-2025	08:00	13:00	05:00	Nie
5 z 36 Sankcje karne w cyberprzestępczości	Marcin Jurgilewicz	26-10-2025	13:30	16:45	03:15	Nie

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
6 z 36 Ramy systemu cyberbezpieczeństwa w Unii Europejskiej. Zadania państw członkowskich, zakres podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa	Klaudia Skelnik	22-11-2025	08:00	11:15	03:15	Nie
7 z 36 Dowody elektroniczne, a przepisy kodeksu postępowania	Klaudia Maciejewska	22-11-2025	11:45	16:45	05:00	Nie
8 z 36 Prawne aspekty ochrony prywatności w sieci	Klaudia Maciejewska	23-11-2025	08:00	11:15	03:15	Nie
9 z 36 Ramy systemu cyberbezpieczeństwa w Unii Europejskiej. Zadania państw członkowskich, zakres podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa	Klaudia Skelnik	23-11-2025	11:45	12:30	00:45	Nie
10 z 36 Postępowanie z incydentem informatycznym - środki zarządzania ryzykiem w cyberbezpieczeństwie	Klaudia Skelnik	23-11-2025	12:45	16:00	03:15	Nie

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
11 z 36 Wymagania i metody szacowania ryzyka oraz zapewnienia ciągłości działania	Klaudia Skelnik	12-12-2025	17:00	21:00	04:00	Tak
12 z 36 Zagrożenia dla bezpieczeństwa w cyberprzestrzeni	Klaudia Skelnik	13-12-2025	07:45	14:30	06:45	Tak
13 z 36 Ochrona zasobów informacyjnych w systemach IT	Dariusz Kłos	14-12-2025	07:45	14:30	06:45	Tak
14 z 36 Postępowanie z incydentem informatycznym - środki zarządzania ryzykiem w cyberbezpieczeństwie	Klaudia Skelnik	10-01-2026	08:00	11:15	03:15	Nie
15 z 36 seminarium	Klaudia Skelnik	10-01-2026	11:30	13:00	01:30	Nie
16 z 36 Bezpieczeństwo sieci komputerowych i telekomunikacyjnych	Przemysław Świeboda	11-01-2026	08:00	13:00	05:00	Nie
17 z 36 OSINT jako technika wywiadu i jego znaczenie dla bezpieczeństwa IT - online	Ernest Lichocki	14-02-2026	08:00	13:15	05:15	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
18 z 36 seminarium online	Klaudia Skelnik	14-02-2026	13:30	15:00	01:30	Tak
19 z 36 Funkcjonalne systemy bezpieczeństwa – bezpieczeństwo fizyczne i środowiskowe -stacjonarne	Grzegorz Wydrowski	15-02-2026	07:45	14:30	06:45	Tak
20 z 36 Wymagania i metody szacowania ryzyka oraz zapewnienia ciągłości działania	Klaudia Skelnik	07-03-2026	08:00	13:00	05:00	Tak
21 z 36 seminarium	Klaudia Skelnik	07-03-2026	13:30	15:00	01:30	Tak
22 z 36 Wymagania i metody audytów systemów informatycznych	Klaudia Skelnik	08-03-2026	08:00	15:00	07:00	Tak
23 z 36 Reagowanie na incydenty bezpieczeństwa IT - sala C210	Grzegorz Piotrowski	28-03-2026	07:45	12:45	05:00	Tak
24 z 36 Metodyka testów penetracyjnych z elementami socjotechniki - SALA C 204	Grzegorz Piotrowski	29-03-2026	07:45	16:15	08:30	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
25 z 36 Przełamywanie zabezpieczeń klasycznych systemów operacyjnych i IoT	Paweł Bernacik	18-04-2026	07:45	12:45	05:00	Tak
26 z 36 Technologie zabezpieczania i szyfrowania zasobów i informacji	Przemysław Świeboda	18-04-2026	13:00	16:15	03:15	Tak
27 z 36 Technologie zabezpieczania i szyfrowania zasobów i informacji	Przemysław Świeboda	19-04-2026	07:45	11:00	03:15	Tak
28 z 36 Bezpieczeństwo systemów i aplikacji	Paweł Bernacik	19-04-2026	11:15	16:15	05:00	Tak
29 z 36 Rozpoznanie w cyberprzestrzeni oraz analiza cyfrowych śladów	Dariusz Kłos	09-05-2026	07:45	14:30	06:45	Tak
30 z 36 Identyfikowanie podatności w systemach teleinformatycznych	Klaudia Skelnik	10-05-2026	07:45	14:30	06:45	Tak
31 z 36 seminarium	Klaudia Skelnik	29-05-2026	17:00	18:30	01:30	Tak
32 z 36 Test z wynikiem generowanym automatycznie	Klaudia Skelnik	29-05-2026	18:45	19:30	00:45	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
33 z 36 Wykorzystanie złośliwego oprogramowania	Dariusz Kłos	30-05-2026	07:45	12:45	05:00	Tak
34 z 36 Podstawy kryptografii	Ernest Lichocki	30-05-2026	13:00	16:15	03:15	Tak
35 z 36 Skanowanie sieci i enumeracja systemów informatycznych	Dariusz Kłos	31-05-2026	07:45	12:45	05:00	Tak
36 z 36 Podstawy kryptografii	Ernest Lichocki	31-05-2026	13:00	16:15	03:15	Tak

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 100,00 PLN
Koszt przypadający na 1 uczestnika netto	6 100,00 PLN
Koszt osobogodziny brutto	34,66 PLN
Koszt osobogodziny netto	34,66 PLN

Prowadzący

Liczba prowadzących: 10

1 z 10

Dariusz Kłos

Project Manager, Architect IT, współzałożyciel firmy teleinformatycznej.

Przygodę z informatyką zaczął ponad dwadzieścia lat temu. Konsultant z zakresu rozwiązań, architektury i bezpieczeństwa rozwiązań IT. Posiada kompetencje oparte na projektowaniu, wdrażaniu nowych technologii, nadzorowaniu zespołów oraz ponad dziesięcioletnie doświadczenie konsultingowe w zakresie wdrażania nowych technologii w środowisku biznesowym. Popularyzuje nowe technologie i promuje nowe rozwiązania w branży teleinformatycznej.

Na co dzień zajmuje się projektowaniem i integracją mechanizmów zwiększających bezpieczeństwo oraz dynamikę hybrydowej infrastruktury informatycznej, a także różnorodnych produktów i połączonych z nimi usług w celu budowania rozwiązań Cloud Computing. Posiada wiele certyfikacji technologicznych takich jak Cirtix, Microsoft, VMWare, prowadzenia projektów PRINCE2 oraz ITIL.

Aktywnie dzieli się swoją wiedzą w ramach społeczności profesjonalistów IT oraz na prowadzonych szkoleniach, wykładach, konferencjach i warsztatach w sektorze publicznym i prywatnym w kraju i za granicą.
Kwalifikacje nabyte nie wcześniej niż 5 lat przed tą samą datą.

2 z 10

Klaudia Skelnik

Prodziekan Wydziału Prawa i Administracji

opiekun merytoryczny kierunku Analityk Bezpieczeństwa Informacji (studia podyplomowe)

Doktor nauk społecznych w dyscyplinie nauki o bezpieczeństwie, absolwentka studiów MBA zarządzanie bezpieczeństwem, mgr politologii w specjalizacji ustrojowo-samorządowej, posiadająca podyplomowe wykształcenie wyższe w zakresie prawa Unii Europejskiej, Edukacji dla bezpieczeństwa, Bezpieczeństwa i Higiena Pracy oraz szereg kursów i szkoleń z zakresu ratownictwa i bezpieczeństwa, bezpieczeństwa informacji, zarządzania oraz specjalistycznych administracyjnych i systemowych wydawanych w służbach policyjnych. Doświadczenie zawodowe zdobyła głównie pełniąc wieloletnią służbę cywilną w Policji przede wszystkim w pionie ochrony informacji niejawnych głównie zajmując stanowiska związane z bezpieczeństwem informacji, pełniąc najpierw funkcje nieetatowego Kierownika Kancelarii Tajnej, Koordynatora Zespołu Prezydialnego, Zastępcy Pełnomocnika Ochrony Informacji Niejawnych, Administratora Bezpieczeństwa Informacji, Administratora Systemu KSI, ESOD i SIDAS, Administratora Bezpieczeństwa Teleinformatycznego systemów niejawnych. Aktywnie uczestniczyła w projektach wdrożenia systemu KSI w Policji oraz obiegu elektronicznego dokumentów jawnych ESOD/SIDAS w województwie pomorskim.
Kwalifikacje nabyte nie wcześniej niż 5 lat przed tą samą datą.

3 z 10

Marcin Jurgilewicz

Specjalista

4 z 10

Piotr Robakowski

Wykładowca Wydziału Prawa i Administracji, Asystent Zakład Nauk o Bezpieczeństwie, Instytut Politologii, Wydział Nauk Społecznych Uniwersytetu Gdańskiego.

Ekspert w zakresie bezpieczeństwa. Główny Specjalista ds. Bezpieczeństwa i obronności w Uniwersyteckim Centrum Klinicznym. Inspektor Ochrony Danych w Gdyńskim Centrum Zdrowia. Wykładowca na podyplomowych studiach z zakresu Cyberbezpieczeństwa i Ochrony Danych Osobowych. Prezes Zarządu Pomorskiego Biura Inspektorów Ochrony Danych.

Na co dzień porusza się w szerokim spektrum zagadnień związanych z bezpieczeństwem, ochroną infrastruktury krytycznej czy zarządzaniem kryzysowym jest uczestnikiem wielu szkoleń i konferencji poświęconych bezpieczeństwu, bezpieczeństwu informacji i ochronie danych. Pełnomocnik d/s Systemu Zarządzania Bezpieczeństwem Informacji, Pełnomocnik i Audytor Wewnętrzny SZBI ISO 27001, ISO 27032, Pełnomocnik Ochrony Informacji Niejawnych, Inspektor Bezpieczeństwa Systemów Teleinformatycznych.Jako Prezes Pomorskiego Biura Inspektorów Ochrony Danych aktywnie uczestniczy w tworzeniu koncepcji bezpieczeństwa oraz realizuje i nadzoruje projekty w tym zakresie.

Podejmuje współpracę z przedsiębiorstwami operującymi w strategicznych gałęziach gospodarki. Poprzez swoją pracę zawodową i naukową kreuje innowacyjne projekty i wyznacza nowe trendy w dziedzinie bezpieczeństwa. Kwalifikacje nabyte nie wcześniej niż 5 lat przed tą samą datą.

5 z 10

Klaudia Maciejewska

prawniczka, doktorantka Szkoły Doktorskiej Uniwersytetu Szczecińskiego z programu Ministra Edukacji i Nauki „Doktorat wdrożeniowy”, inspektor ochrony danych, stały mediator sądowy, kierowniczka Centrum badawczo – rozwojowego Currenda Lab w Currenda Sp. z o.o.; nominowana przez Perspektywy Women in Tech do Top 100 kobiet zajmujących się sztuczną inteligencją; autorka publikacji z zakresu prawa nowych technologii, ochrony danych osobowych, etycznej sztucznej inteligencji, sądowego postępowania egzekucyjnego. Kwalifikacje nabyte nie wcześniej niż 5 lat przed tą samą datą.

6 z 10

Przemysław Świeboda

Ekspert ds. cyberbezpieczeństwa w strukturach Krajowego Systemu Cyberbezpieczeństwa, etyczny haker, pentester i audytor (w tym wiodący audytor norm ISO/IEC 27001 oraz ISO/IEC 27032 Senior Lead Cybersecurity Manager).
Prowadzi zajęcia z zakresu cyberbezpieczeństwa i bezpieczeństwa wewnętrznego na studiach podyplomowych oraz studiach I i II stopnia na kierunkach: Bezpieczeństwo Wewnętrzne, Administracja, Informatyka, Finanse i Rachunkowość oraz Zarządzanie.
Członek Grupy Roboczej ds. Sztucznej Inteligencji (GRAI) w ramach KPRM (obszary: Cyberbezpieczeństwo AI oraz AI a regulacje prawne) oraz Komitetu Technicznego ds. Sztucznej Inteligencji (KT338) Polskiego Komitetu Normalizacyjnego (PKN) – jako reprezentant ISACA.
Badacz bezpieczeństwa z udokumentowanymi podatnościami krytycznymi i wysokimi w komercyjnych systemach bezpieczeństwa oraz serwisach webowych instytucji rządowych i bankowych.
Pełni funkcję Inspektora Bezpieczeństwa Teleinformatycznego (IBTI) Informacji Niejawnych.
Były ASI, ABI oraz IOD jednostek samorządu terytorialnego (JST)
Kwalifikacje nabyte nie wcześniej niż 5 lat przed tą samą datą.

7 z 10

Grzegorz Wydrowski

specjalista

8 z 10

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. Kwalifikacje nabyte nie wcześniej niż 5 lat przed tą samą datą.

9 z 10

Grzegorz Piotrowski

Specjalista od przeprowadzania zmian od twardych technologii, po zmiany w organizacjach. Od zawsze promuje praktyczne podejście do bezpieczeństwa IT. Ćwierć wieku doświadczeń zawodowych, zawsze związanych z cyberprzestrzenią i jej zagrożeniami. Większość zawodowego życia w formie kontraktów dla międzynarodowych firm (m.in. Alliaz, BASF, ING, Microsoft, O2, Telefonica) jak i rodzimych organizacji (m.in. GKPGE, MC/COI, PP SA), gdzie zawsze dbał o podniesienie standardów bezpieczeństwa. Prelegent i ekspert na wydarzeniach związanych z technologiami i bezpieczeństwem cyberprzestrzeni od studenckich przez branżowe, po zamknięte wydarzenia dla resortów siłowych RP i zagranicznych. Jeden z pierwszych w Polsce certyfikowanych hakerów, wieloletni certyfikowany trener technologii informatycznych, jak i metodyk hakerskich, czy testów penetracyjnych. Kwalifikacje nabyte nie wcześniej niż 5 lat przed tą samą datą.

10 z 10

Paweł Bernacik

Ekspert w obszarze cyberbezpieczeństwa z ponad 20 letnim doświadczeniem w sektorze administracji publicznej, telekomunikacji, służb mundurowych i organizacji unijnych.
Posiadacz certyfikatów CISSP i CISA, absolwent studiów MBA Zarządzenie Cyberbezpieczestwem na WAT, Bezpieczeństwa wewnętrznego na AON oraz Inżynierii Oprogramowania na WWSI.
Wieloletni architekt bezpieczeństwa, lider zespołu, uczestniczył w budowie zaawansowanych rozwiązań z obszaru bezpieczeństwa, kluczowych systemów dostarczających usługi cyfrowe dla obywateli.
Od 2022 roku dyrektor departamentu cyberbezpieczeństwa w Centralnym Ośrodku Informatyki, gdzie odpowiada za bezpieczeństwo kluczowych systemów w państwie. Po godzinach wykładowca cyberbezpieczeństwa, pasjonat rozwiązań bezpieczeństwa dla inteligentnych domów. Kwalifikacje nabyte nie wcześniej niż 5 lat przed tą samą datą.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Dodatkowo wymagany jest zapis przez formularz rekrutacyjny uczelni

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

W zależności od projektu, w którym uczestnik bierze udział wymagana jest obecność na zajęciach min 80% oraz potwierdzenie listy logowań do usługi.

zwolnienie z VAT na podstawie art.43 Ustawy o Podatku od towarów i usług 1. pkt 26.

Przedstawiona powyżej cena obejmuje obecnie obowiązującą promocje w czesnym oraz obejmuje system płatności 10 rat.

Istnieje możliwość dodania ceny na życzenie - w systemie płatności 1, 2 i 12 rat.

W tym celu prosimy o kontakt z biurem rekrutacji wskazanym powyżej rekrutacjasp@gdansk.merito.pl

Warunki uczestnictwa

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

Informacje dodatkowe

https://www.merito.pl/gdansk/studia-i-szkolenia/studia-podyplomowe/kierunki/zarzadzanie-cyberbezpieczenstwem-certyfikat-iso-27001

Uniwersytet WSB Merito w Gdańsku zastrzega sobie prawo do zmiany terminów zjazdów.

Warunki techniczne

Wymagania: posiadanie sprzętu elektronicznego z dostępem do internetu, monitor, klawiatura.

Uczelnia zapewnia dostęp do platformy TEAMs.

Adres

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

Siedziba uczelni dostosowana do osób ze specjalnymi potrzebami

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

Kontakt

Agata Orlich

E-mail rekrutacjasp@gdansk.merito.pl
Telefon (+48) 58 5227 513