



Uniwersytet WSB
Merito w Poznaniu



Zarządzanie cyberbezpieczeństwem

Numer usługi 2025/05/31/7405/2784789

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

📖 Studia podyplomowe

🕒 160 h

📅 18.10.2025 do 28.06.2026

7 450,00 PLN brutto

7 450,00 PLN netto

46,56 PLN brutto/h

46,56 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Studia przeznaczone są dla osób, które chcą podjąć pracę lub pracują i zarządzają zespołem w obszarach cyberbezpieczeństwa.
Minimalna liczba uczestników	18
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	12-10-2025
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	160
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

Studia podyplomowe na kierunku „Zarządzanie cyberbezpieczeństwem” pozwalają zdobyć niezbędną wiedzę o tym, jak powinien działać zespół odpowiedzialny za cyberbezpieczeństwo, jak nim zarządzać i czego oczekiwać.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: 1. Ma pogłębioną wiedzę dotyczącą infrastruktury teleinformatycznej i zabezpieczeń systemów informatycznych. 2. Zna zasady zarządzania ryzykiem w kontekście cyberzagrożeń w łańcuchu dostaw i rozwoju oprogramowania. 3. Rozumie obowiązujące regulacje prawne i normy dotyczące ochrony danych osobowych oraz cyberbezpieczeństwa.	1. Charakteryzuje elementy infrastruktury teleinformatycznej i wskazuje środki ich ochrony. 2. Uzasadnia dobór metod analizy ryzyka w zależności od rodzaju zagrożenia. 3. Rozróżnia akty prawne i normy istotne dla funkcjonowania systemu bezpieczeństwa informacji.	Prezentacja
		Wywiad swobodny
Umiejętności: 1. Analizuje incydenty bezpieczeństwa i planuje działania w ramach procedur reagowania. 2. Projektuje politykę bezpieczeństwa informacji z uwzględnieniem norm i standardów europejskich. 3. Organizuje pracę zespołu reagowania na incydenty i koordynuje działania w sytuacjach kryzysowych.	1. Planuje procedury reagowania na konkretne scenariusze incydentów. 2. Projektuje dokument polityki bezpieczeństwa zgodny z wymaganiami norm ISO i RODO. 3. Organizuje harmonogram pracy zespołu CSIRT/IRT w symulowanym scenariuszu awarii.	Prezentacja
		Wywiad swobodny
Kompetencje społeczne: 1. Wykazuje odpowiedzialność za podejmowanie decyzji w obszarze cyberbezpieczeństwa z uwzględnieniem skutków społecznych i etycznych. 2. Potrafi efektywnie współpracować w interdyscyplinarnym zespole ds. bezpieczeństwa informacji. 3. Jest świadomy roli przeciwdziałania dezinformacji oraz wpływu manipulacji informacyjnej na społeczeństwo.	1. Uzasadnia wybór rozwiązań technicznych i organizacyjnych pod kątem ich wpływu na użytkowników. 2. Charakteryzuje zasady komunikacji i podziału ról w zespole realizującym projekt bezpieczeństwa. 3. Definiuje przykłady manipulacji informacyjnej i ocenia ich wpływ na decyzje społeczne.	Prezentacja
		Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak. Świadectwo studiów podyplomowych zawiera program kierunku wraz ze zrealizowanymi godzinami i punktami ECTS. Absolwent uzyskuje zaświadczenie potwierdzające zdobyte efekty kształcenia.

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

Tak. Świadectwo ukończenia studiów podyplomowych jest wydawane na podstawie uzyskania pozytywnej oceny z każdego semestru zgodnie z Regulaminem Studiów Podyplomowych. Studia kończą się zaliczeniem na ocenę określonym w karcie kierunku.

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

Tak. Świadectwo ukończenia studiów podyplomowych jest potwierdzeniem uzyskania pozytywnego wyniku z testu semestralnego i egzaminu końcowego

Program

1. Podstawowe zasady cyberbezpieczeństwa (16 godz.)
2. Infrastruktura teleinformatyczna i zabezpieczenia cyberbezpieczeństwa (16 godz.)
3. Analiza ryzyka i modelowanie zagrożeń (16 godz.)
4. Obowiązujące akty prawne związane z cyberbezpieczeństwem (8 godz.)
5. Ochrona danych osobowych (8 godz.)
6. Cyber Threat Intelligence (8 godz.)
7. Normy i standardy w cyberbezpieczeństwie (16 godz.)
8. Podstawy zarządzania - zarządzanie zespołem i motywacja pracowników (8 godz.)
9. Zarządzanie projektem (8 godz.)
10. Budowa komórki reagowania na incydenty bezpieczeństwa komputerowego i zarządzanie incydentami (8 godz.)
11. Budowa komórki reagowania na incydenty bezpieczeństwa komputerowego i zarządzanie incydentami / Ciągłość działania i Disaster Recovery (8 godz.)
12. Zarządzanie Ryzykiem cyberbezpieczeństwa w Łańcuchu Dostaw i Rozwoju Oprogramowania (12 godz.)
13. Sztuczna inteligencja, cyberbezpieczeństwo w normach europejskich (16 godz.)
14. Dezinformacja, szum informacyjny, deep fake - manipulacja informacjami (8 godz.)
15. Projekt końcowy (2 godz.)
16. Obrona projektu (2 godz.)

INFORMACJE DODATKOWE:

- **Czas trwania studiów (liczbę semestrów):** 2 semestry
- **Liczbę możliwych do zdobycia punktów ECTS:** 30 pkt. ECTS
- **Liczbę godzin:** 160 godzin (lekcyjnych)
- **Harmonogram uwzględnia przerwy.**
- **Informację o sposobie walidacji:** projekt i jego obrona
- **Rodzaj dokumentu potwierdzającego ukończenie studiów:** Świadectwo ukończenia studiów podyplomowych
- Szczegółowy harmonogram zajęć **może ulec modyfikacjom** w zakresie realizowanych przedmiotów oraz osób realizujących zajęcia. Zmianie nie ulegają: terminy zjazdów oraz łączna liczba godzin dydaktycznych w ramach studiów podyplomowych.
- **Harmonogram zjazdów zostanie opublikowany** na stronie internetowej uczelni i w Bazie Usług Rozwojowych (BUR) **co najmniej 2 tygodnie przed rozpoczęciem zajęć.**
- Godziny zajęć w harmonogramie podawane są jako godziny zegarowe. **Liczba godzin w programie podawana jest w godzinach dydaktycznych.** Przelicznik: 160 godzin dydaktycznych = 120 godzin zegarowych.

ORGANIZACJA ZJAZDÓW:

Zjazdy odbywają się średnio jeden lub dwa razy w miesiącu:

- **sobota** w godzinach **8:00–18:00**,
- **niedziela** w godzinach **8:00–18:00**,
- **w wyjątkowych sytuacjach** zajęcia mogą odbyć się również w **piątek** w godzinach **16:00-21:00**.

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 450,00 PLN
Koszt przypadający na 1 uczestnika netto	7 450,00 PLN
Koszt osobogodziny brutto	46,56 PLN
Koszt osobogodziny netto	46,56 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Marcin Fronczak

Prezes polskiego oddziału Cloud Security Alliance. Pierwszy Polak, który zdobył certyfikat CCSK z obszaru bezpieczeństwa chmury. Przez 12 lat pracował jako Chief Information Security w sektorze finansowym i ubezpieczeniowym oraz wykonywał audyty bezpieczeństwa obszaru IT/OT dla operatora infrastruktury krytycznej. Ma wieloletnie doświadczenie jako konsultant w obszarze ryzyka i bezpieczeństwa technologicznego. Brał udział w wielu audytach i projektach w Europie, gdzie zdobył bogate doświadczenie i gruntowną wiedzę z zakresu ryzyk oraz audytowania systemów teleinformatycznych, co potwierdzają międzynarodowe certyfikaty m.in. CISA, CIA, CRISC, Comptia Security +, ISO 27001 LA.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Podczas każdego zjazdu uczestnicy programu otrzymują zestaw materiałów dydaktycznych udostępnionych na platformie Microsoft Teams. Treści te są przygotowywane przez wykładowców i dostosowywane do tematyki prowadzonych zajęć.

Platforma Microsoft Teams stanowi główne narzędzie komunikacji Uczelni WSB Merito. Jej celem jest uproszczenie formalności oraz usprawnienie przepływu informacji między studentami a uczelnią. Dzięki niej uczestnicy studiów mają całodobowy dostęp – z dowolnego miejsca na świecie – do:

- harmonogramu zajęć,
- materiałów dydaktycznych,
- informacji o zmianach w planie zajęć, ogłoszeń i bieżących aktualności.

Warunki uczestnictwa

Rekrutacja na studia podyplomowe na Uniwersytecie WSB Merito w Poznaniu odbywa się poprzez wypełnienie formularza online dostępnego na stronie: <https://www.merito.pl/rekrutacja/krok1>, a następnie dostarczenie kompletu dokumentów do Biura Rekrutacji w Warszawie.

Kryteria kwalifikacyjne do udziału w programie:

- ukończone studia wyższe I lub II stopnia,
- spełnienie warunków określonych w procedurze rekrutacyjnej.

Informacje dodatkowe

- Cena usługi **nie obejmuje opłaty wpisowej oraz opłaty końcowej**.
- **Usługa kształcenia świadczona przez Uniwersytet WSB Merito jest zwolniona z podatku VAT zgodnie z art. 43 ust. 1 pkt 26 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. 2023 poz. 1570)**. Zwolnienie obejmuje usługi edukacyjne realizowane przez uczelnie wyższe na podstawie przepisów ustawy Prawo o szkolnictwie wyższym i nauce.

REALIZACJA PROJEKTÓW:

Uniwersytet WSB Merito w Poznaniu realizuje projekty szkoleniowe w ramach współpracy z instytucjami rynku pracy tj.:

- Wojewódzki Urząd Pracy w Toruniu – **Kierunek Rozwój**,
- Wojewódzki Urząd Pracy w Krakowie – **Małopolski Pociąg do Kariery**,
- Wojewódzki Urząd Pracy w Szczecinie – **Zachodniopomorskie Bony Szkoleniowe**,
- Projekt „**Zawodowa reaktywacja**” – realizowany w Łodzi.

Warunki techniczne

Uczestnik programu zdobywa nową wiedzę oraz praktyczne umiejętności dzięki zajęciom prowadzonym na platformie **Microsoft Teams**. Komunikuje się z wykładowcami i pozostałymi uczestnikami studiów w czasie rzeczywistym (w trybie synchronicznym), co umożliwia aktywne uczestnictwo i bieżącą interakcję.

Wymagania techniczne:

Aby uczestniczyć w zajęciach online, potrzebne są:

- minimalne wymagania sprzętowe: 2 GB RAM, procesor i5, niezbędne oprogramowanie: system operacyjny: windows min. 7, iOS, linux.
- komputer wyposażony w głośniki i mikrofon (wbudowane lub zewnętrzne),
- stabilne połączenie z Internetem, minimalne wymagania dot. parametrów łącza sieciowego: 30 Mbit/s
- słuchawki (zalecane, choć opcjonalne),
- kamera internetowa (opcjonalna, lecz przydatna podczas aktywnych form zajęć).

Adres

ul. Grzybowska 56
Warszawa
woj. mazowieckie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt



Dział Studiów Podyplomowych i Szkoleń

E-mail dsp@warszawa.merito.pl

Telefon (+48) 222 562 319