



## Bezpieczeństwo i ochrona cyberprzestrzeni - Studia podyplomowe

Numer usługi 2025/05/17/7405/2753506

6 150,00 PLN brutto

6 150,00 PLN netto

33,06 PLN brutto/h

33,06 PLN netto/h

Uniwersytet WSB  
Merito w Poznaniu

★★★★☆ 4,4 / 5

529 ocen

📍 zdalna w czasie rzeczywistym

📚 Studia podyplomowe

🕒 186 h

📅 18.10.2025 do 14.06.2026

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

### Grupa docelowa usługi

Absolwenci uczelni wyższych, pracownicy sektora przedsiębiorstw, funkcjonariusze służb porządku publicznego, także pracownicy zatrudnieni w organach administracji rządowej i oraz samorządowej, realizujących czynności związane z administrowaniem sieciami IT lub planujących w przyszłości zajmować się zawodowo bezpieczeństwem teleinformatycznym w sektorze przedsiębiorstwa oraz sektorze publicznym.

### Minimalna liczba uczestników

9

### Maksymalna liczba uczestników

9

### Data zakończenia rekrutacji

22-09-2025

### Forma prowadzenia usługi

zdalna w czasie rzeczywistym

### Liczba godzin usługi

186

### 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 przygotowanie uczestników do pracy w komórkach IT w zakresie kreowania właściwej polityki bezpieczeństwa teleinformatycznego, tworzenia bezpiecznego środowiska gromadzenia i przesyłania danych, zgodnie z przyjętymi standardami oraz nabytymi umiejętnościami praktycznymi. Program studiów oparty jest na wymaganiach międzynarodowych kwalifikacji pełnomocnika ds. cyberprzestępczości oraz doświadczeniach z międzynarodowej i polskiej praktyki w tym zakresie.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p><b>1. WIEDZA</b>            Zrozumienie zagrożeń cybernetycznych            Podstawy kryptografii            Prawne i regulacyjne aspekty cyberbezpieczeństwa            Architektura bezpieczeństwa IT            Zarządzanie incydentami bezpieczeństwa</p>	<p>Rozróżnia zagrożenia cybernetyczne, w tym wirusy, malware, ataki DDoS, phishing, ransomware i inne formy cyberataków.</p> <p>Definiuje podstawowe zasady kryptografii oraz jej zastosowanie w zabezpieczaniu danych.</p> <p>Charakteryzuje krajowe oraz międzynarodowe regulacje i normy prawne dotyczące ochrony danych i cyberbezpieczeństwa.</p> <p>Projektuje zasady implementacji systemów zabezpieczeń w sieciach komputerowych i systemach informatycznych.</p> <p>Organizuje procedury i narzędzia służące do identyfikacji, analizowania i reagowania na incydenty bezpieczeństwa w cyberprzestrzeni.</p>	<p>Test teoretyczny</p>
<p><b>2. UMIEJĘTNOŚCI</b>            Identyfikacja zagrożeń i ocena ryzyka            Projektowanie systemów zabezpieczeń            Implementacja mechanizmów ochrony danych            Monitorowanie i analiza ruchu sieciowego            Reagowanie na incydenty bezpieczeństwa</p>	<p>Ocenia potencjalne zagrożenia w cyberprzestrzeni oraz poziom ryzyka z nimi związany.</p> <p>Projektuje systemy zabezpieczeń chroniące przed zagrożeniami cybernetycznymi.</p> <p>Implementuje mechanizmy kryptograficzne oraz inne technologie zabezpieczeń do ochrony danych.</p> <p>Monitoruje ruch sieciowy oraz analizuje logi w celu wykrywania i przeciwdziałania zagrożeniom.</p> <p>Reaguje na incydenty bezpieczeństwa, minimalizując ich skutki i zapobiegając przyszłym zagrożeniom.</p>	<p>Test teoretyczny</p>

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>3. KOMPETENCJE</p> <p>Praca w zespole</p> <p>Stałe doskonalenie zawodowe</p> <p>Etyka i odpowiedzialność zawodowa</p>	<p>Organizuje pracę zespołową w zakresie cyberbezpieczeństwa, współpracując z innymi specjalistami oraz użytkownikami systemów informatycznych.</p> <p>Planuje rozwój zawodowy, uwzględniając dynamiczne zmiany w obszarze cyberbezpieczeństwa.</p> <p>Nadzoruje przestrzeganie zasad etyki zawodowej, uwzględniając przepisy prawa i normy dotyczące ochrony danych oraz prywatności.</p>	<p>Test teoretyczny</p>

## 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 rozdzielanie procesów kształcenia i szkolenia od walidacji?

TAK

## Program

PROGRAM STUDIÓW PODYPLOMOWYCH:

1. Społeczeństwo informacyjne - 8 godz.
2. Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO - 32 godz.
3. Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 2700 - 16 godz.
4. Organizacja Krajowego Systemu Cyberbezpieczeństwa - 8 godz.
5. Organizacja i zadania Security Operations Center - 8 godz.
6. Prawno-karne aspekty cyberprzestępczości - 16 godz.
7. Zarządzanie i obsługa incydentów cyberbezpieczeństwa - 16 godz.
8. Postępowanie wyjaśniające i dochodzenie w przypadku wystąpienia incydentów cyberbezpieczeństwa - 8 godz.
9. Wykorzystanie Internetu jako narzędzia śledczego - 16 godz.
10. Techniki analizy elektronicznego materiału dowodowego - 32 godz.
11. Metodyka przeprowadzania analizy śledczej - 16 godz.
12. Szacowanie ryzyka w systemach informatycznych - 8 godz.
13. Egzamin - 2 godz.

## INFORMACJE DODATKOWE:

- **Czas trwania studiów (liczbę semestrów):** 2 semestry
- **Liczbę możliwych do zdobycia punktów ECTS:** 30 pkt. ECTS
- **Liczbę godzin:** 186 godzin (lekcyjnych)
- **Harmonogram uwzględnia przerwy.**
- **Informację o sposobie walidacji:** Test semestralny oraz końcowy
- **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 Bazy 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: 186 godzin dydaktycznych = 139,5 godzin zegarowych.
- **Liczba godzin zajęć praktycznych:** 82 godziny lekcyjne
- **Liczba godzin zajęć teoretycznych:** 104 godziny lekcyjne
- Harmonogram obejmuje jeden semestr. Harmonogram na drugi semestr zostanie uzupełniony przed rozpoczęciem drugiego semestru.

## 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: 24

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>1 z 24</b> Postępowanie wyjaśniające i dochodzenie w przypadku wystąpienia incydentów cyberbezpieczeństwa	Zbigniew Łatowski	18-10-2025	09:00	16:00	07:00
<b>2 z 24</b> Organizacja i zadania Security Operations Center	Zbigniew Łatowski	19-10-2025	09:00	16:00	07:00
<b>3 z 24</b> Wykorzystanie Internetu jako narzędzia śledczego	Artur Gębicz	08-11-2025	08:00	15:00	07:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>4 z 24</b> Społeczeństwo informacyjne	dr Marek Jaształ	09-11-2025	09:00	16:00	07:00
<b>5 z 24</b> Metodyka przeprowadzania analizy śledczej	Marcin Paprocki	22-11-2025	09:00	16:00	07:00
<b>6 z 24</b> Metodyka przeprowadzania analizy śledczej	Marcin Paprocki	23-11-2025	09:00	16:00	07:00
<b>7 z 24</b> Wykorzystanie Internetu jako narzędzia śledczego	Artur Gębicz	06-12-2025	08:00	15:00	07:00
<b>8 z 24</b> Organizacja Krajowego Systemu Cyberbezpieczeństwa	Magdalena Kotyś	07-12-2025	09:00	16:00	07:00
<b>9 z 24</b> Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji ISO 2700	Jarosław Wojcieszek	20-12-2025	09:00	16:00	07:00
<b>10 z 24</b> Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji ISO 2700	Jarosław Wojcieszek	21-12-2025	09:00	16:00	07:00
<b>11 z 24</b> Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Jarosław Wojcieszek	21-02-2026	09:00	16:00	07:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>12 z 24</b> Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Jarosław Wojcieszek	22-02-2026	09:00	16:00	07:00
<b>13 z 24</b> Techniki analizy elektronicznego materiału dowodowego	Artur Gębicz	28-02-2026	09:00	15:00	06:00
<b>14 z 24</b> Techniki analizy elektronicznego materiału dowodowego	Artur Gębicz	01-03-2026	08:00	15:00	07:00
<b>15 z 24</b> Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Jarosław Wojcieszek	21-03-2026	09:00	16:00	07:00
<b>16 z 24</b> "Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO Egzamin DEKRA: Pełnomocnik ds. Cyberbezpieczeństwa"	Jarosław Wojcieszek	22-03-2026	09:00	16:00	07:00
<b>17 z 24</b> Techniki analizy elektronicznego materiału dowodowego	Artur Gębicz	18-04-2026	08:00	15:00	07:00
<b>18 z 24</b> Techniki analizy elektronicznego materiału dowodowego	Artur Gębicz	19-04-2026	08:00	15:00	07:00
<b>19 z 24</b> Prawno-karne aspekty cyberprzestępczości	dr Marek Jaształ	09-05-2026	09:00	15:30	06:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>20 z 24</b> Prawno-karne aspekty cyberprzestępczości	dr Marek Jasztal	10-05-2026	09:00	15:30	06:30
<b>21 z 24</b> Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Arkadiusz Kozak	23-05-2026	09:00	15:30	06:30
<b>22 z 24</b> Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Arkadiusz Kozak	24-05-2026	09:00	15:30	06:30
<b>23 z 24</b> Społeczeństwo informacyjne	dr Marek Jasztal	13-06-2026	09:00	15:30	06:30
<b>24 z 24</b> Test	-	14-06-2026	15:00	16:00	01:00

## Cennik

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 150,00 PLN
Koszt przypadający na 1 uczestnika netto	6 150,00 PLN
Koszt osobogodziny brutto	33,06 PLN
Koszt osobogodziny netto	33,06 PLN

## Prowadzący

Liczba prowadzących: 7

**1 z 7**

**dr Marek Jasztal**



Doktor nauk ekonomicznych, wykładowca akademicki, praktyk. Doświadczenie zawodowe/kwalifikacje zdobył nie wcześniej niż w okresie ostatnich 5 lat. Obszar jego działalności naukowej obejmuje tematy z zakresu analizy ryzyka, zarządzania finansowego oraz praktyki związanej z przygotowaniem, realizacją i rozliczeniem procesów inwestycyjnych, wyceny przedsiębiorstw, badania sprawozdań budżetowych i finansowych, zwalczanie przestępczości podatkowej, identyfikacji przestępstw przeciwko budżetowi państwa i budżetowi UE oraz finansowania terroryzmu. Zdołał doświadczenie w kluczowych obszarach zarządzania operacyjnego jednostką, tj. logistyce, teleinformatyce, w zamówieniach publicznych, wykorzystaniu środków europejskich, komunikacji, bezpieczeństwie. Pracował na stanowisku Kierownika Sekcji Księgowości i Rozliczeń. W 2004 został audytorem wewnętrznym, a następnie Zastępcą Komendanta Wojewódzkiego Policji. Nadzoruje obszar logistyki, finansów, łączności i informatyki, transportu, zamówień publicznych, funduszy UE oraz BHP.



2 z 7

### Artur Gębicz

Ponad 5 lat doświadczenia w zawodzie przed opublikowaniem karty usługi w BUR. Zastępca Dyrektora Departamentu ds. Audytu IT w IPS-SGB, gdzie nadzoruje przeprowadzanie audytów IT w blisko 200 bankach spółdzielczych. Wcześniej Zastępca Dyrektora Audytu w banku komercyjnym. Menadżer z ponad 20 letnim doświadczeniem w przeprowadzaniu audytów informatycznych w sektorze finansowym oraz telekomunikacyjnym. Z wykształcenia matematyk, a z zamiłowania informatyk, który lubi poszukiwać w danych anomalii i ukrytych prawd. Wykładowca na studiach podyplomowych zagadnień związanych m.in. z audytem informatycznym oraz prelegent na konferencjach i seminariach poświęconych audytowi oraz bezpieczeństwu informatycznemu. Doradca aspektów bezpieczeństwa w projektach (startups) związanych z wykorzystaniem kryptowalut oraz technologii blockchain.

Posiada międzynarodowe certyfikaty w zakresie wykrywania oszustw i nadużyć (CFE), prowadzenia spraw związanych z informatyką śledczą (CDFE), uprawnienia audytora cyberbezpieczeństwa (ISO 27001 oraz ISO 22301), biegłego sądowego (m.in. w dziedzinie analiz kryminalistycznych, bankowości oraz bezpieczeństwa teleinformatycznego) oraz posiadacz licencji detektywa (w sprawach nadużyć gospodarczych i teleinformatycznych).



3 z 7

### Zbigniew Łatowski

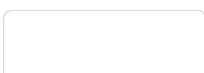
Ponad 5 lat doświadczenia w zawodzie przed opublikowaniem karty usługi w BUR. Doświadczony manager w branży Telco/IT/CyberSecurity. Pracę zawodową zaczynał u operatorów telekomunikacyjnych takich jak TDC Internet, Netia S.A i Ericsson Sp. z o.o. W kolejnych latach związany z Grupa Kapitałowa Poczty Polskiej gdzie zarządzał obszarem Strategii IT realizując między innymi projekt transformacji IT (optymalizacja struktury organizacyjnej, procesów oraz zasobów ludzkich) W kolejnych latach wiceprezes spółki Envelo – Poczta Polska Usługi Cyfrowe odpowiadał za obszar strategii, IT i cyberbezpieczeństwa. Aktualnie SOC Manager w centralnej instytucji publicznej oraz wykładowca na studiach podyplomowych, audytor wiodący PN-EN ISO 27001 oraz audytor wewnętrzny PIKW.



4 z 7

### Marcin Paprocki

Ponad 5 lat doświadczenia w zawodzie przed opublikowaniem karty usługi w BUR.

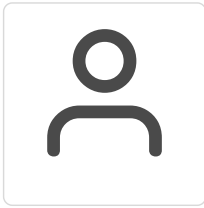


5 z 7



### Magdalena Kotyś

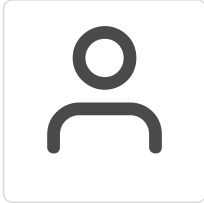
Ponad 5 lat doświadczenia w zawodzie przed opublikowaniem karty usługi w BUR.



6 z 7

### Jarosław Wojcieszek

Ponad 5 lat doświadczenia w zawodzie przed opublikowaniem karty usługi w BUR.



7 z 7

### Arkadiusz Kozak

Ponad 5 lat doświadczenia w zawodzie przed opublikowaniem karty usługi w BUR.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Podczas każdego zjazdu uczestnicy programu otrzymują zestaw materiałów dydaktycznych (prezentacje, pliki, skrypty) 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

Zapisów na studia podyplomowe można dokonać zgodnie z obowiązującym regulaminem za pośrednictwem strony internetowej Uniwersytetu WSB Merito, wybierając jedną z dostępnych filii:

- Chorzów
- Poznań
- Szczecin
- Warszawa

Rejestracja odbywa się poprzez formularz online dostępny pod adresem: <https://www.merito.pl/rekrutacja/krok1>, a także poprzez osobiste dostarczenie kompletu wymaganych dokumentów do Biura Rekrutacji wybranej filii uczelni.

#### 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.
- **Toruńska Agencja Rozwoju Regionalnego S.A.** w partnerstwie z **Kujawsko-Pomorskim Funduszem Pożyczkowym Sp. z o.o.** w ramach projektu „**REGIONALNY FUNDUSZ SZKOLENIOWY II**”

## 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).

## Kontakt



### Biuro Rekrutacji

**E-mail** [rekrutacja@szczecin.merito.pl](mailto:rekrutacja@szczecin.merito.pl)

**Telefon** (+48) 914 225 858