



Uniwersytet WSB
Merito w Poznaniu

★★★★☆ 4,4 / 5

798 ocen

Bezpieczeństwo i ochrona cyberprzestrzeni - studia podyplomowe

Numer usługi 2026/09/30/7405/3845806

6 250,00 PLN brutto

6 250,00 PLN netto

38,34 PLN brutto/h

38,34 PLN netto/h

- 📅 Studia podyplomowe
- 📖 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe
- 🕒 163:00 h
- 📅 24.10.2026 do 04.07.2027

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. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	19-10-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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
1. WIEDZA W1. Charakteryzuje zasady zarządzania bezpieczeństwem informacji oraz regulacje prawne dotyczące cyberbezpieczeństwa.	Rozróżnia zagrożenia cybernetyczne, w tym wirusy, malware, ataki DDoS, phishing, ransomware i inne formy cyberataków. Definiuje podstawowe zasady kryptografii oraz jej zastosowanie w zabezpieczaniu danych. Charakteryzuje krajowe oraz międzynarodowe regulacje i normy prawne dotyczące ochrony danych i cyberbezpieczeństwa. Projektuje zasady implementacji systemów zabezpieczeń w sieciach komputerowych i systemach informatycznych. Rozróżnia wymagania norm ISO 27001 i ISO 22301. Identyfikuje obowiązki wynikające z RODO i przepisów dotyczących Krajowego Systemu Cyberbezpieczeństwa.	Test teoretyczny
W2. Wyjaśnia mechanizmy powstawania zagrożeń cyberbezpieczeństwa oraz zasady reagowania na incydenty	Ocenia potencjalne zagrożenia w cyberprzestrzeni oraz poziom ryzyka z nimi związany. Projektuje systemy zabezpieczeń chroniące przed zagrożeniami cybernetycznymi. Implementuje mechanizmy kryptograficzne oraz inne technologie zabezpieczeń do ochrony danych. Monitoruje ruch sieciowy oraz analizuje logi w celu wykrywania i przeciwdziałania zagrożeniom. Klasyfikuje rodzaje cyberzagrożeń i incydentów. Rozróżnia zadania SOC oraz etapy postępowania wyjaśniającego i analizy śledczej.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
UMIEJĘTNOŚCI U1. Analizuje ryzyko cyberbezpieczeństwa i dobiera działania ograniczające zagrożenia w systemach informatycznych.	Identyfikuje podatności i zagrożenia na podstawie opisu przypadku. Ocenia poziom ryzyka i dobiera adekwatne środki bezpieczeństwa. Planuje rozwój zawodowy, uwzględniając dynamiczne zmiany w obszarze cyberbezpieczeństwa. Nadzoruje przestrzeganie zasad etyki zawodowej, uwzględniając przepisy prawa i normy dotyczące ochrony danych oraz prywatności.	Test teoretyczny
U2. Analizuje incydenty cyberbezpieczeństwa i dobiera metody zabezpieczania elektronicznego materiału dowodowego.	Identyfikuje etapy postępowania po wystąpieniu incydentu. Dobiera techniki analizy śledczej i zabezpieczania dowodów cyfrowych do przedstawionego przypadku.	Test teoretyczny
KOMPETENCJE K1. Ocenia znaczenie odpowiedzialności zawodowej i przestrzegania zasad etycznych w działaniach związanych z cyberbezpieczeństwem.	Rozpoznaje sytuacje wymagające zachowania poufności informacji. Wybiera postępowanie zgodne z zasadami etyki zawodowej i ochrony danych.	Test teoretyczny
		Wywiad swobodny
K2. Ocenia znaczenie współpracy i komunikacji w procesie reagowania na incydenty cyberbezpieczeństwa.	Identyfikuje role i odpowiedzialność uczestników procesu obsługi incydentu. Wybiera właściwy sposób przekazywania informacji i eskalacji zagrożeń w opisanej sytuacji.	Test teoretyczny
		Wywiad swobodny

Kwalifikacje i kompetencje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 1. Czy dokument jest wydany przez podmiot systemu oświaty lub szkolnictwa wyższego na podstawie odrębnych przepisów?

TAK

ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, 1871 i 1897)

Informacje

Nazwa Podmiotu prowadzącego walidację	Uniwersytet WSB Merito
Nazwa Podmiotu certyfikującego	Uniwersytet WSB Merito

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 27001 - 16 godz.
4. Organizacja Krajowego Systemu Cyberbezpieczeństwa - 8 godz.
5. Organizacja i zadania Security Operations Center - 8 godz.
6. Prawno-karne aspekty cyberprzestępczości - 8 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 - 16 godz.
13. Egzamin - 2 godz. (test końcowy na platformie)

INFORMACJE DODATKOWE:

- **Wszystkie zajęcia są prowadzone w formie rozmowy na żywo z wykładowcą.**
- **Czas trwania studiów (liczbę semestrów):** 2 semestry
- **Liczbę możliwych do zdobycia punktów ECTS:** 30 pkt. ECTS
- **Liczbę godzin:** 186 godzin (lekcyjnych)
- **Harmonogram uwzględnia przerwy.** Na wniosek uczestników lub prowadzącego przerwy o planowanej długości mogą odbyć się innych niż zaplanowano pierwotnie godzinach, może mieć to związek z tokiem zajęć lub różną intensywnością realizowanych zajęć.
- **Informację o sposobie walidacji:** Test 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 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: 186 godzin dydaktycznych = 139,5 godzin zegarowych.
- **Liczba godzin zajęć praktycznych:** 82 godziny lekcyjne
- **Liczba godzin zajęć teoretycznych:** 104 godziny lekcyjne

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 pozycji harmonogramu: 164

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 164 Wykorzystanie Internetu jako narzędzia śledczego	Zajęcia	Artur Gębicz	24-10-2026	08:00	09:30	01:30
2 z 164 -	Przerwa	-	24-10-2026	09:30	09:45	00:15
3 z 164 Wykorzystanie Internetu jako narzędzia śledczego	Zajęcia	Artur Gębicz	24-10-2026	09:45	11:15	01:30
4 z 164 -	Przerwa	-	24-10-2026	11:15	11:45	00:30
5 z 164 Wykorzystanie Internetu jako narzędzia śledczego	Zajęcia	Artur Gębicz	24-10-2026	11:45	13:15	01:30
6 z 164 -	Przerwa	-	24-10-2026	13:15	13:30	00:15
7 z 164 Wykorzystanie Internetu jako narzędzia śledczego	Zajęcia	Artur Gębicz	24-10-2026	13:30	15:00	01:30
8 z 164 Wykorzystanie Internetu jako narzędzia śledczego	Zajęcia	Artur Gębicz	25-10-2026	08:00	09:30	01:30
9 z 164 -	Przerwa	-	25-10-2026	09:30	09:45	00:15
10 z 164 Wykorzystanie Internetu jako narzędzia śledczego	Zajęcia	Artur Gębicz	25-10-2026	09:45	11:15	01:30
11 z 164 -	Przerwa	-	25-10-2026	11:15	11:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 164 Wykorzystanie Internetu jako narzędzia śledczego	Zajęcia	Artur Gębicz	25-10-2026	11:45	13:15	01:30
13 z 164 -	Przerwa	-	25-10-2026	13:15	13:30	00:15
14 z 164 Wykorzystanie Internetu jako narzędzia śledczego	Zajęcia	Artur Gębicz	25-10-2026	13:30	15:00	01:30
15 z 164 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001	Zajęcia	Natalia Jagodzińska	14-11-2026	09:00	10:30	01:30
16 z 164 -	Przerwa	-	14-11-2026	10:30	10:45	00:15
17 z 164 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001	Zajęcia	Natalia Jagodzińska	14-11-2026	10:45	12:15	01:30
18 z 164 -	Przerwa	-	14-11-2026	12:15	12:45	00:30
19 z 164 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001	Zajęcia	Natalia Jagodzińska	14-11-2026	12:45	14:15	01:30
20 z 164 -	Przerwa	-	14-11-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 164 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeńst wem Informacji ISO 27001	Zajęcia	Natalia Jagodzińska	14-11-2026	14:30	16:00	01:30
22 z 164 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeńst wem Informacji ISO 27001	Zajęcia	Natalia Jagodzińska	15-11-2026	09:00	10:30	01:30
23 z 164 -	Przerwa	-	15-11-2026	10:30	10:45	00:15
24 z 164 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeńst wem Informacji ISO 27001	Zajęcia	Natalia Jagodzińska	15-11-2026	10:45	12:15	01:30
25 z 164 -	Przerwa	-	15-11-2026	12:15	12:45	00:30
26 z 164 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeńst wem Informacji ISO 27001	Zajęcia	Natalia Jagodzińska	15-11-2026	12:45	14:15	01:30
27 z 164 -	Przerwa	-	15-11-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 164 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeńst wem Informacji ISO 27001	Zajęcia	Natalia Jagodzińska	15-11-2026	14:30	16:00	01:30
29 z 164 Społeczeństw o informacyjne	Zajęcia	dr Marek Jasztal	05-12-2026	09:30	11:00	01:30
30 z 164 -	Przerwa	-	05-12-2026	11:00	11:15	00:15
31 z 164 Społeczeństw o informacyjne	Zajęcia	dr Marek Jasztal	05-12-2026	11:15	12:45	01:30
32 z 164 -	Przerwa	-	05-12-2026	12:45	13:15	00:30
33 z 164 Społeczeństw o informacyjne	Zajęcia	dr Marek Jasztal	05-12-2026	13:15	14:45	01:30
34 z 164 -	Przerwa	-	05-12-2026	14:45	15:00	00:15
35 z 164 Społeczeństw o informacyjne	Zajęcia	dr Marek Jasztal	05-12-2026	15:00	16:30	01:30
36 z 164 Prawno-karne aspekty cyberprzestęp czości	Zajęcia	dr Marek Jasztal	06-12-2026	09:00	10:30	01:30
37 z 164 -	Przerwa	-	06-12-2026	10:30	10:45	00:15
38 z 164 Prawno-karne aspekty cyberprzestęp czości	Zajęcia	dr Marek Jasztal	06-12-2026	10:45	12:15	01:30
39 z 164 -	Przerwa	-	06-12-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
40 z 164 Prawno-karne aspekty cyberprzestęp czości	Zajęcia	dr Marek Jasztal	06-12-2026	12:45	14:15	01:30
41 z 164 -	Przerwa	-	06-12-2026	14:15	14:30	00:15
42 z 164 Prawno-karne aspekty cyberprzestęp czości	Zajęcia	dr Marek Jasztal	06-12-2026	14:30	16:00	01:30
43 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	16-01-2027	08:00	09:30	01:30
44 z 164 -	Przerwa	-	16-01-2027	09:30	09:45	00:15
45 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	16-01-2027	09:45	11:15	01:30
46 z 164 -	Przerwa	-	16-01-2027	11:15	11:45	00:30
47 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	16-01-2027	11:45	13:15	01:30
48 z 164 -	Przerwa	-	16-01-2027	13:15	13:30	00:15
49 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	16-01-2027	13:30	15:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
50 z 164 Techniki analizy elektronicznej go materiału dowodowego	Zajęcia	Artur Gębicz	17-01-2027	08:00	09:30	01:30
51 z 164 -	Przerwa	-	17-01-2027	09:30	09:45	00:15
52 z 164 Techniki analizy elektronicznej go materiału dowodowego	Zajęcia	Artur Gębicz	17-01-2027	09:45	11:15	01:30
53 z 164 -	Przerwa	-	17-01-2027	11:15	11:45	00:30
54 z 164 Techniki analizy elektronicznej go materiału dowodowego	Zajęcia	Artur Gębicz	17-01-2027	11:45	13:15	01:30
55 z 164 -	Przerwa	-	17-01-2027	13:15	13:30	00:15
56 z 164 Techniki analizy elektronicznej go materiału dowodowego	Zajęcia	Artur Gębicz	17-01-2027	13:30	15:00	01:30
57 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	30-01-2027	09:00	10:30	01:30
58 z 164 -	Przerwa	-	30-01-2027	10:30	10:45	00:15
59 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	30-01-2027	10:45	12:15	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
60 z 164 -	Przerwa	-	30-01-2027	12:15	12:45	00:30
61 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	30-01-2027	12:45	14:15	01:30
62 z 164 -	Przerwa	-	30-01-2027	14:15	14:30	00:15
63 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	30-01-2027	14:30	16:00	01:30
64 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	31-01-2027	09:00	10:30	01:30
65 z 164 -	Przerwa	-	31-01-2027	10:30	10:45	00:15
66 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	31-01-2027	10:45	12:15	01:30
67 z 164 -	Przerwa	-	31-01-2027	12:15	12:45	00:30
68 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	31-01-2027	12:45	14:15	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
69 z 164 -	Przerwa	-	31-01-2027	14:15	14:30	00:15
70 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	31-01-2027	14:30	16:00	01:30
71 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	27-02-2027	09:00	10:30	01:30
72 z 164 -	Przerwa	-	27-02-2027	10:30	10:45	00:15
73 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	27-02-2027	10:45	12:15	01:30
74 z 164 -	Przerwa	-	27-02-2027	12:15	12:45	00:30
75 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	27-02-2027	12:45	14:15	01:30
76 z 164 -	Przerwa	-	27-02-2027	14:15	14:30	00:15
77 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	27-02-2027	14:30	16:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
78 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	28-02-2027	09:00	10:30	01:30
79 z 164 -	Przerwa	-	28-02-2027	10:30	10:45	00:15
80 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	28-02-2027	10:45	12:15	01:30
81 z 164 -	Przerwa	-	28-02-2027	12:15	12:45	00:30
82 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	28-02-2027	12:45	14:15	01:30
83 z 164 -	Przerwa	-	28-02-2027	14:15	14:30	00:15
84 z 164 Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO	Zajęcia	Natalia Jagodzińska	28-02-2027	14:30	16:00	01:30
85 z 164 Techniki analizy elektronicznego materiału dowodowego	Zajęcia	Artur Gębicz	13-03-2027	08:00	09:30	01:30
86 z 164 -	Przerwa	-	13-03-2027	09:30	09:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
87 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	13-03-2027	09:45	11:15	01:30
88 z 164 -	Przerwa	-	13-03-2027	11:15	11:45	00:30
89 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	13-03-2027	11:45	13:15	01:30
90 z 164 -	Przerwa	-	13-03-2027	13:15	13:30	00:15
91 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	13-03-2027	13:30	15:00	01:30
92 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	14-03-2027	08:00	09:30	01:30
93 z 164 -	Przerwa	-	14-03-2027	09:30	09:45	00:15
94 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	14-03-2027	09:45	11:15	01:30
95 z 164 -	Przerwa	-	14-03-2027	11:15	11:45	00:30
96 z 164 Techniki analizy elektroniczne go materiału dowodowego	Zajęcia	Artur Gębicz	14-03-2027	11:45	13:15	01:30
97 z 164 -	Przerwa	-	14-03-2027	13:15	13:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
98 z 164 Techniki analizy elektronicznego materiału dowodowego	Zajęcia	Artur Gębicz	14-03-2027	13:30	15:00	01:30
99 z 164 Metodyka przeprowadzania analizy śledczej	Zajęcia	Marcin Paprocki	10-04-2027	09:00	10:30	01:30
100 z 164 -	Przerwa	-	10-04-2027	10:30	10:45	00:15
101 z 164 Metodyka przeprowadzania analizy śledczej	Zajęcia	Marcin Paprocki	10-04-2027	10:45	12:15	01:30
102 z 164 -	Przerwa	-	10-04-2027	12:15	12:45	00:30
103 z 164 Metodyka przeprowadzania analizy śledczej	Zajęcia	Marcin Paprocki	10-04-2027	12:45	14:15	01:30
104 z 164 -	Przerwa	-	10-04-2027	14:15	14:30	00:15
105 z 164 Metodyka przeprowadzania analizy śledczej	Zajęcia	Marcin Paprocki	10-04-2027	14:30	16:00	01:30
106 z 164 Metodyka przeprowadzania analizy śledczej	Zajęcia	Marcin Paprocki	11-04-2027	09:00	10:30	01:30
107 z 164 -	Przerwa	-	11-04-2027	10:30	10:45	00:15
108 z 164 Metodyka przeprowadzania analizy śledczej	Zajęcia	Marcin Paprocki	11-04-2027	10:45	12:15	01:30
109 z 164 -	Przerwa	-	11-04-2027	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
110 z 164 Metodyka przeprowadzania analizy śledczej	Zajęcia	Marcin Paprocki	11-04-2027	12:45	14:15	01:30
111 z 164 -	Przerwa	-	11-04-2027	14:15	14:30	00:15
112 z 164 Metodyka przeprowadzania analizy śledczej	Zajęcia	Marcin Paprocki	11-04-2027	14:30	16:00	01:30
113 z 164 Organizacja Krajowego Systemu Cyberbezpieczeństwa	Zajęcia	Magdalena Kotyś	15-05-2027	09:00	10:30	01:30
114 z 164 -	Przerwa	-	15-05-2027	10:30	10:45	00:15
115 z 164 Organizacja Krajowego Systemu Cyberbezpieczeństwa	Zajęcia	Magdalena Kotyś	15-05-2027	10:45	12:15	01:30
116 z 164 -	Przerwa	-	15-05-2027	12:15	12:45	00:30
117 z 164 Organizacja Krajowego Systemu Cyberbezpieczeństwa	Zajęcia	Magdalena Kotyś	15-05-2027	12:45	14:15	01:30
118 z 164 -	Przerwa	-	15-05-2027	14:15	14:30	00:15
119 z 164 Organizacja Krajowego Systemu Cyberbezpieczeństwa	Zajęcia	Magdalena Kotyś	15-05-2027	14:30	16:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
120 z 164 Szacowanie ryzyka w systemach informatyczny ch	Zajęcia	Magdalena Kotyś	16-05-2027	09:00	10:30	01:30
121 z 164 -	Przerwa	-	16-05-2027	10:30	10:45	00:15
122 z 164 Szacowanie ryzyka w systemach informatyczny ch	Zajęcia	Magdalena Kotyś	16-05-2027	10:45	12:15	01:30
123 z 164 -	Przerwa	-	16-05-2027	12:15	12:45	00:30
124 z 164 Szacowanie ryzyka w systemach informatyczny ch	Zajęcia	Magdalena Kotyś	16-05-2027	12:45	14:15	01:30
125 z 164 -	Przerwa	-	16-05-2027	14:15	14:30	00:15
126 z 164 Szacowanie ryzyka w systemach informatyczny ch	Zajęcia	Magdalena Kotyś	16-05-2027	14:30	16:00	01:30
127 z 164 Szacowanie ryzyka w systemach informatyczny ch	Zajęcia	Magdalena Kotyś	05-06-2027	09:00	10:30	01:30
128 z 164 -	Przerwa	-	05-06-2027	10:30	10:45	00:15
129 z 164 Szacowanie ryzyka w systemach informatyczny ch	Zajęcia	Magdalena Kotyś	05-06-2027	10:45	12:15	01:30
130 z 164 -	Przerwa	-	05-06-2027	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
131 z 164 Szacowanie ryzyka w systemach informatycznych	Zajęcia	Magdalena Kotyś	05-06-2027	12:45	14:15	01:30
132 z 164 -	Przerwa	-	05-06-2027	14:15	14:30	00:15
133 z 164 Szacowanie ryzyka w systemach informatycznych	Zajęcia	Magdalena Kotyś	05-06-2027	14:30	16:00	01:30
134 z 164 Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Zajęcia	Arkadiusz Kozak	06-06-2027	09:00	10:30	01:30
135 z 164 -	Przerwa	-	06-06-2027	10:30	10:45	00:15
136 z 164 Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Zajęcia	Arkadiusz Kozak	06-06-2027	10:45	12:15	01:30
137 z 164 -	Przerwa	-	06-06-2027	12:15	12:45	00:30
138 z 164 Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Zajęcia	Arkadiusz Kozak	06-06-2027	12:45	14:15	01:30
139 z 164 -	Przerwa	-	06-06-2027	14:15	14:30	00:15
140 z 164 Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Zajęcia	Arkadiusz Kozak	06-06-2027	14:30	16:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
141 z 164 Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Zajęcia	Arkadiusz Kozak	19-06-2027	09:00	10:30	01:30
142 z 164 -	Przerwa	-	19-06-2027	10:30	10:45	00:15
143 z 164 Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Zajęcia	Arkadiusz Kozak	19-06-2027	10:45	12:15	01:30
144 z 164 -	Przerwa	-	19-06-2027	12:15	12:45	00:30
145 z 164 Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Zajęcia	Arkadiusz Kozak	19-06-2027	12:45	14:15	01:30
146 z 164 -	Przerwa	-	19-06-2027	14:15	14:30	00:15
147 z 164 Zarządzanie i obsługa incydentów cyberbezpieczeństwa	Zajęcia	Arkadiusz Kozak	19-06-2027	14:30	16:00	01:30
148 z 164 Organizacja i zadania Security Operations Center	Zajęcia	Zbigniew Łatowski	20-06-2027	09:00	10:30	01:30
149 z 164 -	Przerwa	-	20-06-2027	10:30	10:45	00:15
150 z 164 Organizacja i zadania Security Operations Center	Zajęcia	Zbigniew Łatowski	20-06-2027	10:45	12:15	01:30
151 z 164 -	Przerwa	-	20-06-2027	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
152 z 164 Organizacja i zadania Security Operations Center	Zajęcia	Zbigniew Łatowski	20-06-2027	12:45	14:15	01:30
153 z 164 -	Przerwa	-	20-06-2027	14:15	14:30	00:15
154 z 164 Organizacja i zadania Security Operations Center	Zajęcia	Zbigniew Łatowski	20-06-2027	14:30	16:00	01:30
155 z 164 -	Przerwa	-	20-06-2027	16:00	16:15	00:15
156 z 164 Postępowanie wyjaśniające i dochodzenie w przypadku wystąpienia incydentów cyberbezpieczeństwa	Zajęcia	Zbigniew Łatowski	03-07-2027	09:00	10:30	01:30
157 z 164 -	Przerwa	-	03-07-2027	10:30	10:45	00:15
158 z 164 Postępowanie wyjaśniające i dochodzenie w przypadku wystąpienia incydentów cyberbezpieczeństwa	Zajęcia	Zbigniew Łatowski	03-07-2027	10:45	12:15	01:30
159 z 164 -	Przerwa	-	03-07-2027	12:15	12:45	00:30
160 z 164 Postępowanie wyjaśniające i dochodzenie w przypadku wystąpienia incydentów cyberbezpieczeństwa	Zajęcia	Zbigniew Łatowski	03-07-2027	12:45	14:15	01:30
161 z 164 -	Przerwa	-	03-07-2027	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
162 z 164 Postępowanie wyjaśniające i dochodzenie w przypadku wystąpienia incydentów cyberbezpieczeństwa	Zajęcia	Zbigniew Łatowski	03-07-2027	14:30	16:00	01:30
163 z 164 -	Przerwa	-	03-07-2027	16:00	16:15	00:15
164 z 164 -	Walidacja	-	04-07-2027	09:00	10:30	01:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	163:00
w tym suma godzin zajęć	138:00
w tym suma godzin walidacji	01:30
w tym suma przerw	23:30
Suma godzin dydaktycznych bez przerw	186:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 250,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	6 250,00 PLN
Koszt osobogodziny brutto	38,34 PLN
Koszt osobogodziny netto	38,34 PLN

W tym koszt walidacji brutto	95,00 PLN
W tym koszt walidacji netto	95,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	163:00

Prowadzący

Liczba prowadzących: 7



1 z 7

Arkadiusz Kozak

Naczelnik Wydziału dw. z cyberprzestępczością KWP w Szczecinie „Cyberprzestępczość – zagrożenia Web Of Profit”. Posiada doświadczenie i kwalifikacje zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.



2 z 7

Natalia Jagodzińska

Z wykształcenia Inżynier Budowy Maszyn, z pasji Doktor nauk o zarządzaniu. Od 2006 roku Konsultant w obszarze systemów zarządzania prowadzący wdrożenia, szkolenia, audyty wewnętrzne w ramach systemów zarządzania: ISO 9001, ISO 14001, ISO 45001, ISO 50001, ISO 37001, ISO 27001, ISO 20000, ISO 22000, ISO 26000, AQAP, WSK, ZKP, HACCP, GMP, GHP, RODO. Od ponad 15 lat weryfikuje funkcjonowanie powyższych systemów zarządzania jako Audytor Wiodący z ramienia jednostek certyfikujących. Od 2010r. dzieli się wiedzą prowadząc szkolenia dla biznesu oraz wykłady na uczelniach wyższych. Posiada doświadczenie i kwalifikacje zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.



3 z 7

Zbigniew Łatowski

Posiada doświadczenie i kwalifikacje zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji 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 Grupą 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

dr Marek Jasztal

Doktor nauk ekonomicznych, wykładowca akademicki, praktyk. Posiada doświadczenie i kwalifikacje zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR. 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. Zdobył 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.



5 z 7

Magdalena Kotyś

Posiada doświadczenie i kwalifikacje zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR. Absolwentka UAM na Wydziale Matematyki i Informatyki. Ukończyła studia podyplomowe na UE w Poznaniu (Rachunkowość i Finanse) oraz na UWSB Merito w Poznaniu (Controlling). Certyfikowana audytorka wewnętrzna z ponad 20-letnim doświadczeniem. Posiada certyfikaty CIA, Audytor Wiodący ISO 27001 oraz Audytor Wiodący ISO 22301. Wykładowczyni studiów podyplomowych UE w Poznaniu, UWSB Merito oraz PIKW z zakresu m.in. audytu IT, bezpieczeństwa systemów informatycznych, cyberbezpieczeństwa i zarządzania ciągłością działania. Odpowiada za prowadzenie projektów z wykorzystaniem narzędzi IT w procesie audytowym, wsparcie metodologiczne w audycie oraz zarządzanie i rozwój systemów informatycznych w audycie.



6 z 7

Marcin Paprocki

Absolwent Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach na kierunku bezpieczeństwo wewnętrzne, specjalność detektywistyka i kryminalistyka. Ukończył studia podyplomowe na Uniwersytecie Jagiellońskim w Krakowie: w Katedrze Prawa Rzymskiego – Prawo umów w obrocie konsumenckim i profesjonalnym oraz w Katedrze Prawa Karnego – Prawo karne skarbowe i gospodarcze. Jest również absolwentem studiów podyplomowych na Uniwersytecie Ekonomicznym we Wrocławiu o specjalności Biegły do spraw zapobiegania i wykrywania przestępstw gospodarczych i korupcji. Czynny funkcjonariusz Policji, posiadający praktykę i doświadczenie w zakresie analizy kryminalnej, ze szczególnym uwzględnieniem wykrywania przestępczości gospodarczej oraz korupcji. Certyfikowany Kontroler Wewnętrzny oraz Biegły ds. Zapobiegania i Wykrywania Przestępstw Gospodarczych i Korupcji. Ekspert Polskiego Instytutu Kontroli Wewnętrznej w obszarze audytów inwestycyjnych i finansowych oraz zarządzania procesami w organizacjach. Od 2021 roku wykładowca–praktyk prowadzący wykłady i ćwiczenia z zakresu wykrywania oraz zapobiegania oszustwom i nadużyciom w organizacjach, oparte na doświadczeniu zawodowym oraz analizie rzeczywistych przypadków. Posiada doświadczenie i kwalifikacje zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.

7 z 7

Artur Gębicz



Posiada doświadczenie i kwalifikacje zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji 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).

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.

Podczas zajęć przewidziane są ćwiczenia oraz warsztaty, w trakcie których grupa będzie pracować w podzespołach, prowadzone będą dyskusje merytoryczne oraz formy ćwiczeń case study. Podczas zajęć wykorzystywane będą również interesujące przykłady, które w praktyczny sposób pomogą w ustrukturyzowaniu informacji oraz utrwaleniu wiedzy.

Informacje dodatkowe

- Cena usługi **nie obejmuje** opłaty wpisowej.
- 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** - Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój
- Wojewódzki Urząd Pracy w Szczecinie – **Zachodniopomorskie Bony Szkoleniowe**.

Usługa **nie obejmuje** udziału uczestników projektów:

- **Małopolski Pociąg do Kariery** (Wojewódzki Urząd Pracy w Krakowie),
- **Zawodowa reaktywacja** (projekt realizowany w Łodzi).

Wymagana frekwencja na zajęciach to 80%.

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

Telefon (+48) 914 225 858