Możliwość dofinansowania

Studia podyplomowe Ochrona informacji niejawnych i administracja bezpieczeństwa informacji

Numer usługi 2025/04/24/9817/2707060

3 610,00 PLN brutto
3 610,00 PLN netto
22,56 PLN brutto/h
22,56 PLN netto/h

UNIWERSYTET ŚLĄSKI W KATOWICACH

4,7 / 5
12 ocen

mieszana (zdalna połączona z usługą zdalną w czasie rzeczywistym)
Studia podyplomowe
160 h
18.10.2025 do 30.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Kandydaci** Adresatami studiów są absolwenci wyższych uczelni posiadający tytuł licencjata, magistra lub inżyniera, zwłaszcza osoby zajmujące się problematyką ochrony informacji niejawnych, danych osobowych i bezpieczeństwa informacji.
Minimalna liczba uczestników	25
Maksymalna liczba uczestników	50
Data zakończenia rekrutacji	15-10-2025
Forma prowadzenia usługi	mieszana (zdalna 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 2024 r. poz. 1571, z późn. zm.)
Zakres uprawnień	prowadzenie studiów podyplomowych

Cel

Cel edukacyjny

Studia dają możliwość zdobycia wiedzy i praktycznych umiejętności w zakresie zabezpieczania różnych rodzajów informacji, dzięki czemu absolwenci zyskują wyjątkową pozycję na współczesnym rynku pracy. Uczestnicy po zakończeniu edukacji mogą pełnić rolę pełnomocników ds. ochrony informacji niejawnych, kierowników kancelarii tajnych i innych pracowników pionów ochrony, administratorów danych, inspektorów ochrony danych osobowych, administratorów bezpieczeństwa informacji. Podczas studiów uczestnicy

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
posiada uporządkowaną, podbudowaną teoretycznie wiedzę obejmującą kluczowe zagadnienia z zakresu bezpieczeństwa informacji, P6S_WG; P6S_WK	- charakteryzuje podstawowe zagadnienia dotyczące zasad ochrony informacji niejawnych - definiuje pojęcia i zasady z zakresu ochrony danych osobowych - definiuje podstawowe pojęcia związane z bezpieczeństwem państwa - charakteryzuje zagadnienia dotyczące zasad organizacji i funkcjonowania w podmiocie prawa handlowego systemu bezpieczeństwa przemysłowego - omawia podstawowe zagadnienia dotyczące bezpieczeństwa w cyberprzestrzeni (ochrona przed wnikaniem w obszary militarne ekonomiczne i gospodarcze) oraz zagrożeń związanych z cyberterroryzmem i jego formami	Test teoretyczny
rozróżnia i definiuje metody, narzędzia i techniki pozwalające opisywać struktury i instytucje uczestniczące w procesie tworzenia systemu bezpieczeństwa informacji, P6S_WG; P6S_WK	- wyjaśnia istotę i dynamikę współczesnych systemów ochrony informacji i przetwarzania danych - wymienia procedury charakterystyczne dla działań podejmowanych w obszarze ochrony danych osobowych - identyfikuje i wyjaśnia, w świetle współczesnych ujęć teoretycznych, skutki wprowadzenia zmian w systemie ochrony danych osobowych - interpretuje procesy zachodzące w zakresie bezpieczeństwa informacji	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
zdobywa wiedzę o normach prawnych, organizacyjnych, etycznych organizujących struktury i instytucje w zakresie bezpieczeństwa narodowego, infrastruktury informacyjnej, ochrony informacji niejawnych i innych tajemnic prawnie chronionych, ochrony danych osobowych, P6S_WG; P6S_WK	- przedstawia obowiązujące rozwiązania w zakresie ochrony informacji niejawnych i danych osobowych na tle systemu informacji prawnie chronionych - charakteryzuje zasady dostępu do informacji publicznej - definiuje pojęcia z zakresu słownictwa administracyjnego - wymienia zasady ustanawiania i funkcjonowania w podmiocie prawa handlowego systemu ochrony tajemnic przedsiębiorstwa - omawia mechanizmy ochrony przed penetracją wywiadów: cywilnego, militarnego, ekonomicznego i gospodarczego w zakresie utraty informacji	Test teoretyczny
charakteryzuje podstawowe metody, techniki, narzędzia i środki ochrony informacji w kancelariach, systemach i sieciach teleinformatycznych oraz cyberprzestrzeni, a także w sytuacjach kryzysowych, P6S_WG; P6S_WK	- charakteryzuje podstawowe wymagania bezpieczeństwa teleinformatycznego - definiuje zasady przetwarzania informacji niejawnych w systemach teleinformatycznych - rozróżnia mechanizmy ochrony, kontroli dostępu i uwierzytelniania, w tym biometryczne, podsłuch transmisji danych, metody ochrony elektromagnetycznej - identyfikuje zastosowane środki ochrony w zależności od najwyższej klauzuli informacji niejawnych przetwarzanych w systemie TI	Test teoretyczny
zdobywa wiedzę o trendach rozwojowych i najistotniejszych osiągnięciach techniki i technologii w zakresie bezpieczeństwa informacji, P6S_WG; P6S_WK	- określa wymagania na zachowanie poufności, integralności i dostępności informacji niejawnych przetwarzanych w systemie TI - rozwiązuje zadane problemy dotyczące ochrony oraz utrzymaniem właściwego poziomu bezpieczeństwa infrastruktury IT - prezentuje istniejące metody zabezpieczeń danych - planuje informatyzację systemów informacyjnych w jednostkach administracji publicznej	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
zdobywa podstawową wiedzę dotyczącą zarządzania, systemów zarządzania jakością i bezpieczeństwem informacji oraz szacowania i zarządzania ryzykiem, P6S_WG; P6S_WK	- charakteryzuje, terminologię, strukturę i zasady zarządzania systemem jakości - charakteryzuje terminologię, strukturę i zasady zarządzania systemem bezpieczeństwa informacji - porównuje i określa praktyczne możliwości integracji systemów zarządzania - analizuje kryteria oceny ryzyka oraz metodykę zarządzania ryzykiem - definiuje i analizuje ryzyko związane z bezpieczeństwem informacji niejawnych	Test teoretyczny
rozróżnia zasady, metody i techniki archiwizacji dokumentów, P6S_WG; P6S_WK	- wymienia przepisy prawa regulujące postępowanie z dokumentacją współczesną w jednostkach organizacyjnych - rozróżnia podstawowe zasady klasyfikacji i kwalifikacji archiwalnej dokumentacji - ustala zakres zastosowania narzędzi informatycznych w tworzeniu, gromadzeniu i przechowywaniu dokumentacji w formie dokumentów elektronicznych z uwzględnieniem uwarunkowań prawnych i technicznych	Test teoretyczny
ocenia i analizuje przyczyny i przebieg procesów zagrożenia bezpieczeństwa informacji, P7S_UW	- identyfikuje zagrożenia dla bezpieczeństwa informacji niejawnych i dobiera środki dla zachowania tego bezpieczeństwa - wyjaśnia zagrożenia dla określonych zasobów systemu TI - analizuje sposoby wykorzystania i użyteczność systemów informatycznych w zarządzaniu bezpieczeństwem - charakteryzuje wyzwania, zagrożenia, szanse, interesy państwa oraz społeczne w dziedzinie bezpieczeństwa, polityki i strategii bezpieczeństwa oraz służb specjalnych	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
sprawnie posługuje się systemami normatywnymi, normami i regułami (prawnymi, zawodowymi, etycznymi) w celu rozwiązywania konkretnych problemów, P7S_UW; P6S_UK; P6S_UO	- uzasadnia informacje zawarte w Biuletynie Informacji Publicznej - sporządza instrukcję bezpieczeństwa przemysłowego, kwestionariusz bezpieczeństwa przemysłowego, plan ochrony informacji niejawnych - wykorzystuje znajomość zasad sprawozdawania przez wykonawcę umowy lub zlecenia zamawiającemu chronionych z mocy prawa powszechnego - wiąże zdobytą wiedzę teoretyczną i praktyczną: podaje podstawy prawne, orzecznictwo i literaturę dotyczącą badanych zagadnień	Test teoretyczny
posiada umiejętność przygotowania różnych prac pisemnych, analiz, raportów, właściwych dla studiowanego kierunku studiów podyplomowych, P7S_UW; P6S_UU	- posługuje się terminami z zakresu teorii bezpieczeństwa w pracach pisemnych - sporządza dokumentację opracowanego projektu z zakresu studiów - formułuje założenia do dokumentacji bezpieczeństwa teleinformatycznego - sporządza instrukcję bezpieczeństwa przemysłowego, kwestionariusz bezpieczeństwa przemysłowego, plan ochrony informacji niejawnych	Prezentacja
nadzoruje, współdziała i pracowuje w grupie, przyjmując w niej różne role, określić priorytety służące realizacji zadania, P6S_UO	- współpracuje w rozwiązywaniu problemów z zakresu infrastruktury i bezpieczeństwa informacji - demonstruje odpowiedzialność za własne realizowane zadania w ramach zespołu - współpracuje w rozwiązywaniu kazusów - współdziała w zespole wdrażającym systemy zarządzania bezpieczeństwem	Debata swobodna
kontroluje, inspiruje i organizuje proces własnego uczenia się przez całe życie oraz uczenia się innych osób; P8S_UU	- wiąże zdobytą wiedzę teoretyczną i praktyczną: podaje podstawy prawne, orzecznictwo i literaturę dotyczącą badanych zagadnień - ocenia dokumenty z zakresu polityki bezpieczeństwa państwa - śledzi na bieżąco zmiany w zakresie działań podejmowanych przez instytucje publiczne - uzasadnia potrzeby minimalizowania ryzyka podatności na ataki cyberterrorystyczne pod kątem potencjalnych strat finansowych, gospodarczych i wizerunkowych	Debata swobodna

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
wykazuje gotowość krytycznej oceny i samodzielnego uzupełniania wiedzy i umiejętności, P7S_KK	- rozwiązuje problemy państwa w zakresie jego bezpieczeństwa w aspekcie interesów społecznych – zbiorowych i jednostkowych - rozróżnia stopień odpowiedzialności za ujawnienie informacji niejawnych osobom nieuprawnionym - wykazuje się obiektywizmem, profesjonalizmem, otwartością, krytycyzmem, kreatywnością w trakcie oceny prawidłowości funkcjonowania systemów zarządzania - rozumie potrzebę ustawicznego kształcenia celem doskonalenia umiejętności zawodowych	Debata swobodna
wykazuje gotowość użycia wiedzy i umiejętności niezbędnej do podjęcia działań jako inspektor ochrony danych osobowych, pełnomocnik ochrony informacji niejawnych, P7S_KO	- asystuje pełnomocnikowi ochrony przy realizacji jego zadań, jako kandydat na zastępcę pełnomocnika - posiada kompleksowe spojrzenie na całość procesu przetwarzania danych - proponuje rozwiązania systemowe związane z potencjalnymi atakami w cyberprzestrzeni - zarządza dokumentacją w jednostce organizacyjnej stosując procedury rejestracji, obiegu, kompletowania, przechowywania i brakowania - projektuje strukturę organizacyjną pionu ochrony dla jednostki organizacyjnej - obsługuje sprzęt komputerowy i oprogramowanie dedykowane bezpieczeństwu powszechnemu	Debata swobodna
uzasadnia świadomość ważności i zrozumienia dylematów związane z wykonywaniem zawodu, P7S_KR	- kontroluje świadomość odpowiedzialności zawodowej wymagającej przestrzegania tajemnicy przedsiębiorstwa i tajemnic prawnie chronionych - doradza kierownikowi przedsiębiorstwa w zakresie zorganizowania systemu ochrony informacji niejawnych, w tym w zakresie zarządzania ryzykiem bezpieczeństwa informacji niejawnych - prezentuje istniejące zaawansowane rozwiązania związane z bezpieczeństwem informacji w cyberprzestrzeni	Debata swobodna

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
planuje i organizuje proces własnego uczenia się przez całe życie oraz uczenia się innych osób, P8S_UU	- wiąże zdobytą wiedzę teoretyczną i praktyczną: podaje podstawy prawne, orzecznictwo i literaturę dotyczącą badanych zagadnień - ocenia dokumenty z zakresu polityki bezpieczeństwa państwa - śledzi na bieżąco zmiany w zakresie działań podejmowanych przez instytucje publiczne - uzasadnia potrzeby minimalizowania ryzyka podatności na ataki cyberterrorystyczne pod kątem potencjalnych strat finansowych, gospodarczych i wizerunkowych	Debata swobodna

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

Czas trwania:

Semestry: 2

Liczba godzin: 160 (w tym 80h zajęć teoretycznych i 80h praktycznych)

1 godzina dydaktyczna = 1 godzina akademicka (45 minut)

W czas realizacji usługi nie zostały wliczone przerwy między zajęciami.

Organizacja zajęć:

Studia obejmują dwanaście zjazdów sobotnio-niedzielnych od 9.00 do około 16.30. Zajęcia odbywają się w formule zdalnej na MS Teams oraz w e-learningu na platformie MOODLE.

Forma świadczenia usługi: w pełni zdalna = zdalnie w czasie rzeczywistym (łącznie z wykładowcą): 108 h, w czasie nierzeczywistym (e-learning): 52 h

Wykaz treści realizowanych podczas studiów:

- Ochrona informacji niejawnych - 30 h, 6 punktów ECTS
- Infrastruktura informacyjna - 14 h, 2 punkty ECTS
- Wybrane problemy bezpieczeństwa narodowego - 8 h, 1 punkt ECTS
- Bezpieczeństwo systemówi sieci teleinformatycznych - 16 h, 3 punkty ECTS
- Bezpieczeństwo przemysłowe i tajemnica przedsiębiorstwa - 8 h, 1 punkt ECTS
- Ochrona danych osobowych - 30 h, 6 punktów ECTS
- Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem - 20 h, 4 punkty ECTS
- Cyberterroryzm i zagrożenia bezpieczeństwa informacji w cyberprzestrzeni - 10 h, 1 punkt ECTS
- Infrastruktura krytyczna i zarządzanie kryzysowe - 6 h, 1 punkt ECTS
- Archiwizacja dokumentów - 6h, 1 punkt ECTS
- Seminarium dyplomowe - 12 h, 4 punkty ECTS

Walidacja zostanie przeprowadzona pod koniec II semestru studiów podyplomowych.

Dokument ukończenia studiów:

1. świadectwo ukończenia studiów podyplomowych wydane przez Uniwersytet Śląski w Katowicach
2. zaświadczenie o uzyskanych kompetencjach wraz z opisem efektów uczenia się oraz przeprowadzonej walidacji

Sekretariat

Justyna Przybylska

e-mail:justyna.przybylska@us.edu.pl

e-mail: psoin@us.edu.pl

Harmonogram

Liczba przedmiotów/zajęć: 60

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 60 Ochrona informacji niejawnych (zasady OIN)	płk. dr Stanisław Małecki	18-10-2025	10:30	17:00	06:30
2 z 60 Infrastruktura informacyjna	dr Katarzyna Trynda, prof. UŚ	19-10-2025	09:00	13:00	04:00
3 z 60 Ochrona informacji niejawnych (zasady OIN)	płk. dr Stanisław Małecki	08-11-2025	09:00	12:00	03:00
4 z 60 Infrastruktura informacyjna	dr Katarzyna Trynda, prof. UŚ	09-11-2025	09:00	11:15	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 60 Bezpieczeństwo systemów i sieci teleinformatycznych	Kmdr por. rez. mgr Marek Anzel	09-11-2025	11:30	13:45	02:15
6 z 60 Infrastruktura informacyjna	prof. dr hab. Grażyna Szpor	15-11-2025	11:00	14:10	03:10
7 z 60 Wybrane problemy bezpieczeństwa narodowego	dr hab. Sławomir Zalewski	16-11-2025	09:00	13:50	04:50
8 z 60 Bezpieczeństwo systemów i sieci teleinformatycznych	Kmdr por. rez. mgr Marek Anzel	29-11-2025	09:00	15:30	06:30
9 z 60 Ochrona informacji niejawnych (kancelaria tajna)	mgr Elżbieta Bińczyk	30-11-2025	09:00	14:40	05:40
10 z 60 Infrastruktura informacyjna	prof. dr hab. Grażyna Szpor	13-12-2025	09:00	12:00	03:00
11 z 60 Wybrane problemy bezpieczeństwa narodowego	dr hab. Sławomir Zalewski	13-12-2025	12:30	15:30	03:00
12 z 60 Ochrona informacji niejawnych (kancelaria tajna)	mgr Elżbieta Bińczyk	13-12-2025	15:40	17:10	01:30
13 z 60 Bezpieczeństwo systemów i sieci teleinformatycznych	prof. dr hab. inż. Robert Koprowski	14-12-2025	09:00	11:15	02:15
14 z 60 Bezpieczeństwo przemysłowe i tajemnica przedsiębiorstwa	płk mgr Kazimierz Ślusarczyk	14-12-2025	11:30	14:30	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
15 z 60 Ochrona informacji niejawnych (środki ochrony informacji)	dr inż. Andrzej Wójcik	14-12-2025	14:40	17:10	02:30
16 z 60 Bezpieczeństwo systemów i sieci teleinformatycznych	prof. dr hab. inż. Robert Koprowski	17-01-2026	09:00	12:10	03:10
17 z 60 Bezpieczeństwo przemysłowe i tajemnica przedsiębiorstwa	płk mgr Kazimierz Ślusarczyk	17-01-2026	12:20	17:10	04:50
18 z 60 EGZAMIN: Ochrona informacji niejawnych (e-learning)	płk. dr Stanisław Małecki	18-01-2026	09:00	09:45	00:45
19 z 60 Ochrona informacji niejawnych (środki ochrony informacji)	dr inż. Andrzej Wójcik	18-01-2026	10:00	14:50	04:50
20 z 60 Ochrona danych osobowych	prof. dr hab. Grażyna Szpor	28-02-2026	09:00	10:30	01:30
21 z 60 Ochrona danych osobowych	płk mgr Kazimierz Ślusarczyk	28-02-2026	10:40	12:10	01:30
22 z 60 Ochrona danych osobowych	płk mgr Kazimierz Ślusarczyk	28-02-2026	12:20	13:50	01:30
23 z 60 Ochrona danych osobowych	płk mgr Kazimierz Ślusarczyk	28-02-2026	13:55	14:40	00:45
24 z 60 Seminarium dyplomowe	dr Małgorzata Gajos-Gržetić, prof. UŚ	01-03-2026	09:00	10:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
25 z 60 Ochrona danych osobowych	prof. dr hab. Grażyna Szpor	01-03-2026	10:40	12:10	01:30
26 z 60 Ochrona danych osobowych	prof. dr hab. Grażyna Szpor	01-03-2026	12:20	13:50	01:30
27 z 60 Ochrona danych osobowych	prof. dr hab. Grażyna Szpor	01-03-2026	14:00	15:30	01:30
28 z 60 Ochrona danych osobowych	mgr Monika Krasińska	14-03-2026	09:00	10:30	01:30
29 z 60 Ochrona danych osobowych	mgr Monika Krasińska	14-03-2026	10:40	12:10	01:30
30 z 60 Ochrona danych osobowych	mgr Monika Krasińska	14-03-2026	12:20	13:50	01:30
31 z 60 Ochrona danych osobowych	mgr Monika Krasińska	14-03-2026	14:00	15:30	01:30
32 z 60 Infrastruktura krytyczna i zarządzanie kryzysowe	dr hab. inż. Bogdan Kosowski	15-03-2026	09:00	10:30	01:30
33 z 60 Infrastruktura krytyczna i zarządzanie kryzysowe	dr hab. inż. Bogdan Kosowski	15-03-2026	10:40	12:10	01:30
34 z 60 Ochrona danych osobowych (e-learning)	prof. dr hab. Grażyna Szpor	28-03-2026	09:00	11:15	02:15
35 z 60 Ochrona danych osobowych (e-learning)	płk mgr Kazimierz Ślusarczyk	28-03-2026	11:30	13:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
36 z 60 Ochrona danych osobowych (e-learning)	mgr Monika Krasińska	29-03-2026	09:00	11:15	02:15
37 z 60 Infrastruktura krytyczna i zarządzanie kryzysowe (e-learning)	dr hab. inż. Bogdan Kosowski	29-03-2026	11:30	13:00	01:30
38 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem (e-learning)	Kmdr por. rez. mgr Marek Anzel	29-03-2026	13:15	14:45	01:30
39 z 60 Archiwizacja dokumentów	mgr Roland Banduch	11-04-2026	09:00	10:30	01:30
40 z 60 Archiwizacja dokumentów	mgr Roland Banduch	11-04-2026	10:40	12:10	01:30
41 z 60 Cyberterroryzm i zagrożenia bezpieczeństwa informacji w cyberprzestrzeni	płk. dr Piotr Potejko	12-04-2026	09:00	10:30	01:30
42 z 60 Cyberterroryzm i zagrożenia bezpieczeństwa informacji w cyberprzestrzeni	płk. dr Piotr Potejko	12-04-2026	10:40	12:10	01:30
43 z 60 Cyberterroryzm i zagrożenia bezpieczeństwa informacji w cyberprzestrzeni	płk. dr Piotr Potejko	12-04-2026	12:20	13:50	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
44 z 60 Cyberterroryzm i zagrożenia bezpieczeństwa informacji w cyberprzestrzeni	płk. dr Piotr Potejko	12-04-2026	14:00	15:30	01:30
45 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem	Kmdr por. rez. mgr Marek Anzel	25-04-2026	09:00	10:30	01:30
46 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem	Kmdr por. rez. mgr Marek Anzel	25-04-2026	10:40	12:10	01:30
47 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem	Kmdr por. rez. mgr Marek Anzel	25-04-2026	12:20	13:50	01:30
48 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem	Kmdr por. rez. mgr Marek Anzel	25-04-2026	14:00	15:30	01:30
49 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem	dr inż. Joanna Jasińska	26-04-2026	09:00	10:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
50 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem	dr inż. Joanna Jasińska	26-04-2026	10:40	12:10	01:30
51 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem	dr inż. Joanna Jasińska	26-04-2026	12:20	13:50	01:30
52 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem	dr inż. Joanna Jasińska	26-04-2026	13:55	14:40	00:45
53 z 60 Archiwizacja dokumentów (e-learning)	mgr Roland Banduch	09-05-2026	09:00	10:30	01:30
54 z 60 Cyberterroryzm i zagrożenia bezpieczeństwa informacji w cyberprzestrzeni (e-learning)	płk. dr Piotr Potejko	09-05-2026	10:45	12:15	01:30
55 z 60 Systemy zarządzania jakością i bezpieczeństwem informacji oraz szacowanie i zarządzanie ryzykiem (e-learning)	dr inż. Joanna Jasińska	09-05-2026	12:30	14:45	02:15
56 z 60 Seminarium dyplomowe (e-learning)	dr Małgorzata Gajos-Gržetić, prof. UŚ	09-05-2026	15:00	15:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
57 z 60 Egzamin z modułu Ochrona danych osobowych (e-learning)	prof. dr hab. Grażyna Szpor	10-05-2026	09:00	09:45	00:45
58 z 60 Seminarium dyplomowe (e-learning)	dr Małgorzata Gajos-Gržetić, prof. UŚ	10-05-2026	10:00	12:15	02:15
59 z 60 Seminarium dyplomowe (e-learning)	dr Małgorzata Gajos-Gržetić, prof. UŚ	10-05-2026	12:30	14:45	02:15
60 z 60 Seminarium dyplomowe (e-learning)	dr Małgorzata Gajos-Gržetić, prof. UŚ	10-05-2026	15:00	17:15	02:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 610,00 PLN
Koszt przypadający na 1 uczestnika netto	3 610,00 PLN
Koszt osobogodziny brutto	22,56 PLN
Koszt osobogodziny netto	22,56 PLN

Prowadzący

Liczba prowadzących: 15

1 z 15

dr Małgorzata Gajos-Gržetić, prof. UŚ

Kierownik studiów podyplomowych, W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

2 z 15

dr Katarzyna Trynda, prof. UŚ

Prorektor ds. studenckich i kształcenia Pełni funkcje Prorektora zajmującego się kształceniem w Uniwersytecie Śląskim w Katowicach od 2020 do 2025 roku. Doświadczony i wielokrotnie nagradzany dydaktyk. Wieloletnia wykładowczyni uniwersytecka, na studiach podyplomowych OINiABI prowadzi zajęcia od 20 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie walidacji programów kształcenia.

3 z 15

prof. dr hab. inż. Robert Koprowski

Profesor w dziedzinie nauk inżynieryjno-technicznych, zajmuje się elektroniką i informatyką. Recenzent projektów unijnych w kraju i na świecie. Wieloletni wykładowca uniwersytecki, na studiach podyplomowych OINiABI prowadzi zajęcia od 20 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

4 z 15

dr hab. inż. Bogdan Kosowski

Doktor habilitowany inżynier, profesor nadzwyczajny, oficer pożarnictwa. Specjalizuje się w szeroko pojętej problematyce teorii systemów związanych z organizacją zarządzania bezpieczeństwem w podmiotach gospodarczych, w instytucjach oraz organach administracji publicznej. Wieloletni wykładowca uniwersytecki, na studiach podyplomowych OINiABI prowadzi zajęcia od 20 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

5 z 15

prof. dr hab. Grażyna Szpor

Profesor nauk społecznych, prawnik, specjalistka w zakresie prawa administracyjnego. Autorka i redaktor naukowy ponad 200 publikacji z zakresu prawa publicznego. Wieloletnia wykładowczyni uniwersytecka, na studiach podyplomowych OINiABI prowadzi zajęcia od 20 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

6 z 15

dr hab. Sławomir Zalewski

Profesor Uniwersytetu WSB Merito w Gdańsku. Zajmuje się zagadnieniami bezpieczeństwa politycznego ze szczególnym uwzględnieniem praktyki działania państwa w zakresie ochrony informacji niejawnych oraz kontroli służb specjalnych. Wieloletni wykładowca uniwersytecki, na studiach podyplomowych OINiABI prowadzi zajęcia od 20 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

7 z 15

dr inż. Joanna Jasińska

Zajmuje się problematyką systemów zarządzania jakością, zarządzaniem ryzykiem w różnych aspektach, normalizacją i kodyfikacją. Dyrektor Centrum Certyfikacji Jakości Wojskowej Akademii Technicznej. Wieloletnia wykładowczyni uniwersytecka, na studiach podyplomowych OINiABI prowadzi zajęcia od 15 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

8 z 15

płk. dr Stanisław Małecki

Radca prawny, wybitny znawca problematyki prawnej ochrony informacji niejawnych, były dyrektor Departamentu Prawa Administracyjnego Rządowego Centrum Legislacji. Prowadzi zajęcia dydaktyczne na studiach podyplomowych OINiABI od 20 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

9 z 15

płk. dr Piotr Potejko

Doktor nauk humanistycznych, prawnik, zajmuje się problematyką bezpieczeństwa wewnętrznego i międzynarodowego, służbami specjalnymi we współczesnym państwie, cyberbezpieczeństwem. Wieloletni wykładowca uniwersytecki, na studiach podyplomowych OINiABI prowadzi zajęcia od 3 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

10 z 15

dr inż. Andrzej Wójcik

doktor nauk wojskowych w specjalności bezpieczeństwo państwa , wiodący auditor systemów zarządzania bezpieczeństwem informacji, przewodniczący Komitetu Technicznego Polskiego Komitetu Normalizacyjnego ds. Bezpieczeństwa Powszechnego i Ochrony Ludności, Wiceprezes Ogólnopolskiego Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM". Prowadzi zajęcia dydaktyczne na studiach podyplomowych OINiABI od 20 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

11 z 15

Kmdr por. rez. mgr Marek Anzel

Audytor wiodący Systemów Zarządzania Bezpieczeństwem Informacji (SZBI), ekspert z zakresu ochrony informacji niejawnych i systemów teleinformatycznych, autor poradników z zakresu SZBI, w tym związanych z funkcjonowaniem systemu ochrony informacji niejawnych. Prowadzi zajęcia dydaktyczne na studiach podyplomowych OINiABI od 15 lat. W ostatnich pięciu latach prowadząca zdobyła doświadczenie w zakresie prowadzenia zajęć dydaktycznych.

12 z 15

mgr Elżbieta Bińczyk

Absolwentka Politechniki Częstochowskiej i Uniwersytetu Śląskiego, od wielu lat doświadczony trener i dydaktyk, przygotowujący na kursach i szkoleniach organizowanych przez Krajowe Stowarzyszenie Ochrony Informacji kadrę zarządzającą informacją w instytucji. Wykładowca na specjalistycznych studiach podyplomowych o kierunkach związanych z bezpieczeństwem informacji prawnie chronionych.

Współpracuje, jako ekspert KSOIN w dziedzinie zarządzania informacjami, w tym informacjami prawnie chronionymi, z podmiotami zarówno w sferze gospodarczej jak i z instytucjami publicznymi.Posiada bogate własne doświadczenie zawodowe od 18 lat zajmując się jako Pełnomocnik Zarządu bezpieczeństwem i właściwą dystrybucją informacji.Laureatka wielu nagród i wyróżnień w tej dziedzinie. Jako członek Zarządu Krajowego Stowarzyszenia Ochrony Informacji, zajmującego się teoretycznym i praktycznym przygotowaniem specjalistów z dziedziny zarządzania informacjami, aktywizuje kobiety w tym obszarze udowadniając, że świat tajemnic i bezpieczeństwa to nie tylko „zaklęte męskie rewiry".

13 z 15

płk mgr Kazimierz Ślusarczyk

b. Dyrektor Delegatury ABW w Katowicach

14 z 15

mgr Monika Krasińska

Specjalista z zakresie ochrony danych osobowych, dostępu do informacji publicznej, informacji prawnie chronionych. Wykładowca akademicki. Prowadzi zajęcia dydaktyczne na studiach podyplomowych OINiABI od 12 lat.

15 z 15

mgr Roland Banduch

Zajmuje się archiwistyką. Wieloletni Kierownik Oddziału Dokumentacji Kartograficznej i Technicznej Archiwum Państwowego w Katowicach. Prowadzi zajęcia dydaktyczne na studiach podyplomowych OINiABI od 12 lat.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy studiów podyplomowych otrzymają materiały dydaktyczne w postaci: prezentacji z zajęć, plików PDF, linków

Warunki uczestnictwa

Adresatami studiów są absolwenci wyższych uczelni posiadający tytuł licencjata, magistra lub inżyniera, zwłaszcza osoby zajmujące się problematyką ochrony informacji niejawnych, danych osobowych i bezpieczeństwa informacji.

Informacje dodatkowe

Organizator zapewnia rozdzielność walidacji od procesu kształcenia.

Opłata za usługę jest zwolniona z VAT - na podstawie art. 43 ust. 1 pkt 26 ustawy o podatku od towaru i usług.

Warunki techniczne

Zajęcia będą prowadzone przez aplikację usługi MS Teams oraz na platformie MOODLE.

W przypadku zajęć w formule zdalnej uczestnik studiów otrzymuje dostęp wraz z kontem w aplikacji Microsoft Teams. Konieczne jest posiadanie przez uczestnika dostępu do urządzenia, na którym będzie mógł uczestniczyć w zajęciach (np. komputer, laptop czy tablet).

Kody dostępowe do usługi

Przedmioty realizowane są w formie e-learningu. W przypadku chęci uzyskania dostępu do kursu należy skontaktować się z Centrum Studiów Podyplomowych: studiapodyplomowe@us.edu.pl

Zajęcia w dniach 13-14 grudnia 2025 roku będą przeprowadzone za pomocą kursu e-learningowego na platformie Moodle:

1) Infrastruktura informacyjna, prof. dr hab. Grażyna Szpor

https://el.us.edu.pl/wnst/course/view.php?id=3729

2) Wybrane problemy bezpieczeństwa narodowego. prof. dr hab. Sławomir Zalewski

https://el.us.edu.pl/wnst/course/view.php?id=3727

3) Ochrona informacji niejawnych (kancelaria tajna), mgr Elżbieta Bińczyk

https://el.us.edu.pl/wnst/course/view.php?id=3731

4) Bezpieczeństwo systemów i sieci teleinformatycznych, prof. dr hab. Robert Koprowski

https://el.us.edu.pl/wnst/course/view.php?id=3730

5) Bezpieczeństwo przemysłowe i tajemnica przedsiębiorstwa, płk mgr Kazimierz Ślusarczyk

https://el.us.edu.pl/wnst/course/view.php?id=3732

6) Ochrona informacji niejawnych (środki ochrony informacji), dr inż. Andrzej Wójcik

https://el.us.edu.pl/wnst/course/view.php?id=3736

Kontakt

Paweł Ziegler

E-mail studiapodyplomowe@us.edu.pl
Telefon (+48) 513 383 312