Możliwość dofinansowania

Akademia WSB

4,4 / 5

1 194 oceny

Zarządzanie cyberbezpieczeństwem - online

Numer usługi 2025/12/16/8729/3216669

7 500,00 PLN brutto
7 500,00 PLN netto
45,18 PLN brutto/h
45,18 PLN netto/h

zdalna w czasie rzeczywistym
Studia podyplomowe
166 h
11.04.2026 do 28.02.2027

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Studia adresowane są do osób zainteresowanych **rozwijaniem ścieżki kariery w branży Cyber Security**, np. menedżerów i specjalistów ds. cyberbezpieczeństwa w firmach i instytucjach sektora publicznego, osób odpowiedzialnych za wdrożenie systemu cyberbezpieczeństwa w organizacji, pełnomocników zarządu ds. cyberbezpieczeństwa, specjalistów i konsultantów ds. cyberbezpieczeństwa, ochrony danych osobowych i zarzadzania bezpieczeństwem informacji, adwokatów i prawników, którzy mogą procesować projekty czy sprawy sądowe w zakresie cyberbezpieczeństwa. **Usługa rozwojowa adresowana również dla Uczestników projektu Zachodniopomorskie Bony Szkoleniowe**
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	03-04-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	166
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

Usługa „Zarządzanie cyberbezpieczeństwem” przygotowuje uczestnika do skutecznego zarządzania bezpieczeństwem systemów informatycznych. W ramach usługi uczestnik m.in. zdobędzie wiedzę umożliwiającą identyfikację zasobów IT wymagających ochrony, nauczy się projektować rozwiązania zapewniające bezpieczeństwo infrastruktury informatycznej, pozna metody prewencji przed atakami komputerowymi oraz scenariusze współczesnych cyberprzestępstw wymierzonych w dane cyfrowe.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA : Projektuje i zarządza bezpieczeństwem systemów informatycznych, przeciwdziałania, wykrywania i zwalczania cyberprzestępczości. Prawidłowo określa zasoby informatyczne, które podlegać muszą ochronie, projektowania bezpieczeństwa systemów IT, prewencji przed atakami komputerowymi.	Wskazuje i klasyfikuje zasoby informatyczne wymagające ochrony. Wykazuje znajomość zasad projektowania systemów IT z uwzględnieniem bezpieczeństwa. Określa metody przeciwdziałania i reagowania na incydenty cyberbezpieczeństwa. Rozróżnia zależności między różnymi elementami systemu bezpieczeństwa a specyfiką zagrożeń.	Test teoretyczny
UMIEJĘTNOŚCI: Przeprowadza wstępną analizę powłamaniową systemu komputerowego oraz zabezpiecza dowody cyfrowe. Przeprowadza audyt bezpieczeństwa sieci komputerowych. Przeprowadza analizę zagrożeń bezpieczeństwa danych.	Poprawnie wykonuje procedurę zabezpieczenia danych (np. sporządza kopię binarną, stosuje techniki utrwalania metadanych, tworzy łańcuch dowodowy). Sporządza raport audytowy zawierający ocenę stanu bezpieczeństwa i rekomendacje działań naprawczych. Identyfikuje potencjalne źródła zagrożeń (wewnętrzne i zewnętrzne) oraz ich wpływ na dane organizacji (np. naruszenie poufności, integralności, dostępności). W analizie zagrożeń stosuje wybrane metody i techniki oceny ryzyka.	Test teoretyczny
KOMPETENCJE SPOŁECZNE: Dba o rozwój wiedzy o cyberbezpieczeństwie oraz świadomym zastosowaniu w organizacji, dąży do ciągłego doskonalenia i aktualizacji wiedzy z zakresu cyberbezpieczeństwa.	Proponuje i uzasadnia konkretne działania lub rozwiązania poprawiające bezpieczeństwo informatyczne w środowisku pracy lub projektach. Aktywnie angażuje się w dyskusje zespołowe dotyczące cyberbezpieczeństwa i promuje dobre praktyki. Planuje i realizuje własny rozwój zawodowy, uwzględniając zmieniające się wymagania i nowe trendy w cyberbezpieczeństwie. Potrafi krytycznie ocenić własne kompetencje i identyfikuje obszary do dalszego rozwoju.	Test teoretyczny

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 2. Czy wydany dokument jest potwierdzeniem nabycia kwalifikacji lub uzyskania uprawnień zawodowych nadawanych przez organy władz publicznych lub instytutów badawczych, lub samorządów zawodowych, lub samorządów gospodarczych na podstawie odrębnych przepisów?

TAK

W ramach kierunku studiów

Informacje

Nazwa Podmiotu prowadzącego walidację	Akademia WSB
Nazwa Podmiotu certyfikującego	Akademia WSB

Program

Lp.	Nazwa przedmiotu	Liczba godzin zajęć teoretycznych	Liczba godzin zajęć praktycznych	Liczba punktów ECTS
1.	Technologie informacyjne	-	12	3
2.	Biały wywiad internetowy	6	14	4
3.	Prawne aspekty przestępstw komputerowych z elementami kryminalistyki	8	8	3
4.	Techniczne aspekty ataków komputerowych	8	8	3
5.	Zarządzanie i audytowanie bezpieczeństwa informacji zgodnie z normą ISO 27001	18	6	4

6.	Elementy informatyki śledczej	8	16	2
7.	Prawno-karna ochrona zasobów IT	12	-	3
8.	Projektowanie bezpieczeństwa w chmurze	8	8	4
9.	Audyt bezpieczeństwa sieci komputerowych	7	7	2
10.	Strategie i technologie IT w służbie ciągłości usług biznesowych	12	-	2
	Razem:	87	79	30

Studia trwają dwa semestry.

Proces uczenia się jest rozdzielny od procesu walidacji usługi.

Walidacja zostaje przeprowadzona za pośrednictwem testu z wiedzy na platformie internetowej.

Linki do poszczególnych zajęć zostaną zamieszczane w zakładce "Kody dostępowe do usługi" z kilkudniowym wyprzedzeniem przed każdymi realizowanymi zajęciami.

Harmonogram

Liczba przedmiotów/zajęć: 2

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 2 Technologie informacyjne	dr inż. Krystian Mączka	11-04-2026	08:00	14:35	06:35
2 z 2 Technologie informacyjne	dr inż. Krystian Mączka	12-04-2026	08:00	11:10	03:10

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 500,00 PLN
Koszt przypadający na 1 uczestnika netto	7 500,00 PLN
Koszt osobogodziny brutto	45,18 PLN
Koszt osobogodziny netto	45,18 PLN
W tym koszt walidacji brutto	0,00 PLN
W tym koszt walidacji netto	0,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 7

1 z 7

dr inż. Krystian Mączka

Biegły sądowy z zakresu informatyki śledczej przy Sądzie Okręgowym w Katowicach, wykładowca akademicki, adiunkt w Akademii WSB w Dąbrowie Górniczej, wykładowca Krajowej Szkoły Sądownictwa i Prokuratury, specjalista z zakresu przestępstw komputerowych. Od lat zajmujący się m.in. problemami bezpieczeństwa sieci i systemów teleinformatycznych, zabezpieczaniem i odzyskiem danych, analizą nośników, problemami szyfrowania, monitoringiem. Autor wielu publikacji z zakresu zastosowań metod sztucznej inteligencji. Posiada Certyfikat X-Ways Forensic, Certyfikowany Informatyk Śledczy, Microsoft Certified Professional oraz Auditora Systemów Zarządzania Bezpieczeństwem Informacji.

2 z 7

dr Jarosław Homa

Funkcje i stanowiska:
• MBA – Chief Information Security Officer (CISO).
• Pełnomocnik Rektora ds. Cyberbezpieczeństwa, Politechnika Śląska.
• Wicedyrektor Centrum Cyberbezpieczeństwa Politechniki Śląskiej.

• Menedżer ds. Zarządzania Cyberbezpieczeństwem.
• Architekt IT i Cyberbezpieczeństwa.
Doświadczenie zawodowe (ostatnie 5 lat):
• Kierowanie i realizacja projektów w obszarze bezpieczeństwa IT i OT.
• Projektowanie i wdrażanie systemów Cyberbezpieczeństwa, w tym budowa i rozwój Security Operation Center (SOC) w oparciu o wytyczne NIS2, uKSC oraz standardy NIST.
• Pełnienie funkcji eksperta i audytora wiodącego w obszarze systemów zarządzania bezpieczeństwem informacji (ISO 27001) oraz ciągłości działania (ISO 22301).
Działalność dydaktyczna:
• Wykładowca na Politechnice Śląskiej, Akademii WSB oraz PJATK.
• Prowadzi zajęcia na studiach MBA, studiach podyplomowych (CYBER SCIENCE), a także na studiach I i II stopnia w obszarze cyberbezpieczeństwa, zarządzania IT i architektury systemów.
Kwalifikacje i certyfikaty (uzyskane i odnawiane w ostatnich 5 latach):
• Audytor wiodący ISO 27001 oraz ISO 22301.
• Certyfikaty z obszaru zarządzania i IT: PRINCE2, ITIL, AgilePM, Cisco CCNA.
• Członkostwo w organizacjach branżowych: Polskie Towarzystwo Informatyczne (PTI), ISSA Polska.
Specjalizacja:
• Ekspert w systemach IT i OT.
• Zarządzanie cyberbezpieczeństwem organizacji.
• Budowa i rozwój procesów zgodnych z wymaganiami prawa i standardów międzynarodowych (NIS2, uKSC, NIST).

3 z 7

mgr Tomasz Zemela

Prowadzący posiada aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat: od 2020 r. pracuje w strukturach zwalczania cyberprzestępczości (KWP Katowice, CBZC), a od 2024 r. prowadzi zajęcia akademickie z informatyki śledczej i cyberbezpieczeństwa. Posiada kwalifikacje nabyte w ostatnich 5 latach, m.in.. studia podyplomowe „Digital Forensics and Cybercrime Investigation" (2023), szkolenia Fortinet (2023) oraz regularny udział w konferencjach branżowych (Sekurak Mega Hacking Party). Dysponuje zaawansowaną znajomością narzędzi kryminalistycznych (Link, Autopsy, Sleuthkit), systemów Linux, OSINT oraz podstawami programowania w Pythonie. Prowadzi szkolenia wewnętrzne z zakresu kryptowalut, ransomware i współpracy międzynarodowej. Spełnia warunki dotyczące aktualnego doświadczenia i kwalifikacji zgodnie z wymaganiami BUR.

4 z 7

dr Marcin Szymczak

Doktor nauk prawnych, specjalista w dziedzinie kryminalistyki i informatyki śledczej. Sędzia Wydziału Karnego Sądu Rejonowego Katowice-Wschód. Współzałożyciel Instytutu Informatyki Śledczej, gdzie aktywnie uczestniczy w projektach i analizach z zakresu ochrony danych cyfrowych oraz cyberbezpieczeństwa.
Od wielu lat prowadzi działalność dydaktyczną, obecnie jako wykładowca Akademii WSB w Dąbrowie Górniczej, gdzie realizuje zajęcia na kierunkach związanych z bezpieczeństwem, prawem i informatyką śledczą. W ostatnich latach koncentruje się na zagadnieniach ochrony danych cyfrowych, przestępczości komputerowej i praktycznym zastosowaniu informatyki śledczej w postępowaniu karnym.
Spełnienie wymogów potencjału kadrowego:
• Doświadczenie zawodowe (ostatnie 5 lat): praca orzecznicza w wydziale karnym sądu, udział w sprawach dotyczących cyberprzestępczości i ochrony danych cyfrowych, aktywna działalność ekspercka w Instytucie Informatyki Śledczej.
• Kwalifikacje: doktor nauk prawnych w specjalności kryminalistyka – informatyka śledcza, stale rozwijane poprzez działalność dydaktyczną i praktykę zawodową w obszarze prawa karnego i cyberbezpieczeństwa.
Dzięki łączeniu praktyki orzeczniczej, wiedzy akademickiej i pracy eksperckiej w obszarze

informatyki śledczej, dr Marcin Szymczak posiada odpowiednie kwalifikacje i aktualne doświadczenie niezbędne do prowadzenia usług w zakresie prawa, ochrony danych cyfrowych oraz cyberbezpieczeństwa.

5 z 7

mgr Radosław Gnat

Doświadczony ekspert w obszarze bezpieczeństwa informacji i zarządzania usługami IT. W trakcie swojej kariery zawodowej pełnił różnorodne funkcje – od administratora systemów Windows, przez konsultanta ds. zgodności i architekta IT, aż po menedżera odpowiedzialnego za zarządzanie cyberbezpieczeństwem.
Obecnie związany z globalną organizacją GlaxoSmithKline, gdzie odpowiada za rozwój i wdrażanie strategii w zakresie cyberodporności oraz zarządzanie procesami bezpieczeństwa informacji na poziomie międzynarodowym. Dzięki bieżącej pracy w środowisku korporacyjnym o globalnym zasięgu posiada praktyczne i aktualne doświadczenie w implementacji standardów oraz najlepszych praktyk cyberbezpieczeństwa.
Spełnienie wymogów potencjału kadrowego:
• Doświadczenie zawodowe (ostatnie 5 lat): menedżer ds. cyberbezpieczeństwa w GSK, odpowiedzialny za procesy bezpieczeństwa i cyberodporność w skali globalnej.
• Kwalifikacje: absolwent Politechniki Poznańskiej oraz Wyższej Szkoły Bankowej, gdzie ukończył kierunki związane z zarządzaniem, psychologią biznesu i technologiami sieci komputerowych – wiedzę rozwija i wykorzystuje w bieżącej praktyce zawodowej.
mgr Radosław Gnat łączy kompetencje techniczne, doświadczenie menedżerskie i wiedzę akademicką, co zapewnia wysoką jakość realizacji usług w obszarze cyberbezpieczeństwa oraz zarządzania IT.

6 z 7

mgr inż Tomasz Banasik

Specjalista z ponad 20-letnim doświadczeniem w obszarze bezpieczeństwa informacji, teleinformatyki oraz audytów IT. Od 2014 r. Prezes Zarządu N-Serwis.pl Sp. z o.o., realizujący audyty i wdrożenia zgodne z wymaganiami ISO 27001, ISO 22301, ISO 24762, RODO, NIS2/DORA oraz Krajowego Systemu Cyberbezpieczeństwa.
Od 2018 r. wykładowca akademicki w zakresie analizy ryzyka, ciągłości działania, ochrony danych osobowych, cyberbezpieczeństwa i audytu systemów IT (Akademia WSB, Akademia WSAiB). Prowadzi szkolenia komercyjne w ww. obszarach oraz w zakresie informatyki śledczej, data forensics i zarządzania kryzysowego.
Posiada bogate kwalifikacje potwierdzone certyfikatami m.in.: Audytor Wiodący ISO 27001 i ISO 22301, Menedżer ryzyka ISO 31000, Compliance Officer, PRINCE2 Foundation, CompTIA Security+, MCSE, MCSA, MCITP, MCTS. Absolwent studiów inżynierskich z informatyki, magisterskich z zarządzania, MBA oraz licznych studiów podyplomowych (m.in. ABI, Project Management, Prawo w Biznesie).
Członek SABI, IIA Polska, Stowarzyszenia Instytutu Informatyki Śledczej oraz Klubu M

7 z 7

Przemysław Szczurek

Senior Manager ds. Bezpieczeństwa Informacji. Z branżą IT związany od ponad 12 lat. Obecnie pełni funkcję Senior Managera ds. Bezpieczeństwa Informacji w TUV NORD Polska, gdzie odpowiada za rozwój i sprzedaż usług związanych z normami: ISO 27001, ISO 20000, ISO 22301 oraz tematyką Ochrony Danych Osobowych i Cyberbezpieczeństwa. Posiada certyfikaty: Audytora Wiodącego ISO 27001, ISO 20000, Audytora Wewnętrznego ISO 22301, Incident Response Managera i Inspektora Ochrony Danych. Jest egzaminatorem w zakresie Systemu Zarządzania Bezpieczeństwem Informacji z ramienia TUV NORD Polska. Jako trener TUV NORD i wykładowca akademicki duży nacisk stawia na świadomość kadry.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują prezentacje z przeprowadzonych zajęć po ich realizacji.

Zawarto umowę z Wojewódzkim Urzędem Pracy w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu Zachodniopomorskie Bony Szkoleniowe

Warunki uczestnictwa

Kandydaci powinni posiadać co najmniej wyższe wykształcenie.

Warunkiem uczestnictwa w usłudze jest dokonanie wpłaty oplaty wpisowej w kwocie 300 zł, która jest dodatkową opłatą poza kosztem wskazanym w usłudze.

Zapis w BUR nie jest równoznaczny z przyjęciem na studia w Uczelni. Warunkiem przyjęcia na studia w Uczelni jest dokonanie rejestracji w systemie internetowej rekrutacji oraz złożenie kompletu dokumentów

Informacje dodatkowe

- Kandydaci powinni posiadać co najmniej wyższe wykształcenie.
- Czas trwania: 2 semestry.
- Podstawa zaliczenia: studia kończą się 2 egzaminami po każdym semestrze studiów.
- Dni odbywania się zajęć: dwa razy w miesiącu: soboty, niedziele.

Organizator studiów zastrzega sobie możliwość wprowadzenia zmian w programie studiów.

Aby ukończyć studia, należy uzyskać co najmniej 80% obecności na zajęciach. Obecność jest weryfikowana na podstawie list generowanych w aplikacji MS Teams oraz zrzutów ekranu.

Harmonogram zajęć pojawi się maksymalnie na tydzień przed rozpoczęciem studiów.

1 godzina zajęć w Akademii WSB = 45 min. zajęć dydaktycznych

Na 8h zajęć przewidziane łącznie 35minut przerwy zależenie od potrzeb grupy i wykładowcy wliczone w czas usługi.

Powyżej 8h zajęć 45 minut przerwy

Warunki techniczne

Usługa realizowana zdalnie poprzez platformy ClickMeeting, Zoom oraz MS Teams.

Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji: •Komputer stacjonarny/laptop z dostępem do Internetu

•Sprawny mikrofon i kamera internetowa (lub zintegrowane z laptopem)

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: download 8 mb/s, upload 8 mb/s, ping 15 ms

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: Zalecamy wykorzystanie aktualnej wersji przeglądarki CHROME (zarówno na komputerach z systemem operacyjnym Windows jak i Apple

Okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line: 7,5 h

Kontakt

Iwona Zębala

E-mail iwona.zebala@wsb.edu.pl

Telefon (+48) 322 959 395