Możliwość dofinansowania

Akademia WSB

Zarządzanie cyberbezpieczeństwem - online

Numer usługi 2025/05/16/8729/2751826

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

Akademia WSB

4,4 / 5

1 046 ocen

zdalna w czasie rzeczywistym
Studia podyplomowe
166 h
11.10.2025 do 30.06.2026

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.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	04-10-2025
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 2023 r. poz. 742, 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

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

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: 0

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

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

Prowadzący

Liczba prowadzących: 2

1 z 2

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.

2 z 2

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.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują materiały z wytypowanych zajęć po ich realizacji.

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.

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

Sandra Szczygieł

E-mail krakow@wsb.edu.pl

Telefon (+48) 887 722 303