Możliwość dofinansowania

SOPOCKA AKADEMIA NAUK STOSOWANYCH

SOPOCKA AKADEMIA NAUK STOSOWANYCH

Brak ocen dla tego dostawcy

Audyt bezpieczeństwa informacji - studia podyplomowe

Numer usługi 2025/11/21/187674/3163350

Sopot / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

Studia podyplomowe

200 h

14.03.2026 do 28.02.2027

6 500,00 PLN brutto

6 500,00 PLN netto

32,50 PLN brutto/h

32,50 PLN netto/h

Informacje podstawowe

Kategoria	Prawo i administracja / Ochrona informacji niejawnych
Grupa docelowa usługi	Studia przeznaczone są dla osób zamierzających zajmować się zawodowo bezpieczeństwem informacji, cyberbezpieczeństwem i ochroną prywatności, a także odpowiedzialnych za zaplanowanie oraz przeprowadzanie audytów w jednostkach sektora publicznego i prywatnego w tym zakresie.
Minimalna liczba uczestników	12
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	13-03-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	200
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	Kształcenie na studiach podyplomowych prowadzonych przez uczelnie

Cel

Cel edukacyjny

Wiedza i umiejętności praktyczne zdobyte w ramach studiów pozwolą absolwentom na samodzielne zbadanie czy proces zarządzania ryzykiem jest adekwatny do potencjalnych zagrożeń, zapewnia wystarczającą ochronę aktywów (zasobów) i informacji oraz czy system kontroli w obszarze całej infrastruktury informatycznej jest efektywny i skuteczny, zgodnie z przyjętymi standardami i kryteriami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Absolwent biegle porusza się w tematach: Cyberbezpieczeństwo Audyt wewnętrzny i metodyka przeprowadzania kontroli w obszarze IT Bezpieczne projektowanie systemów IT Zarządzanie ryzykiem w obszarze cyberbezpieczeństwa Normalizacja i standardy międzynarodowe w obszarze bezpieczeństwa informacji, cyberbezpieczeństwa i prywatności Kontynuacja działalności po awarii. Zarządzanie ciągłością działania Zarządzanie kryzysowe. Krajowy system cyberbezpieczeństwa Audyt infrastruktury teleinformatycznej Regulacje prawne obejmujące szeroko pojęte bezpieczeństwo informacji, prywatność i cyberbezpieczeństwo	Praca projektowa	Prezentacja

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

L.p.	BLOKI TEMATYCZNE	Liczba godzin	Prowadzący
1.	Cyberbezpieczeństwo – wprowadzenie • Podstawowe definicje i funkcje związane z obszarem cyberbezpieczeństwa oraz bezpieczeństwa informacji • Analiza najbardziej popularnych zagrożeń i podatności związanych z systemami teleinformatycznymi • Podatności związane z obszarem IT • Wprowadzenie do testów penetracyjnych	20	Piotr Błaszczeć
2.	Audyt wewnętrzny i metodyka przeprowadzania kontroli w obszarze IT • Planowanie strategiczne • Etapy tworzenia planu audytu • Identyfikacja obszarów ryzyka • Analiza ryzyka na potrzeby planowania • Audyt poza planem • Realizacja audytu IT – program audytu, techniki gromadzenia dowodów, próbkowanie i dokumentowanie wyników • Krajowe i międzynarodowe standardy audytu wewnętrznego • Znaczenie audytu IT w organizacji • Kodeks etyki audytora	20	Adam Kuczyński
3.	Bezpieczne projektowanie systemów IT • Planowanie i organizacja systemów IT • Architektura informatyczna i kierunek technulogiczny • Zarządzanie inwestycjami • Zarządzanie projektami IT	20	Artur Heliński
4.	Zarządzanie ryzykiem w obszarze cyberbezpieczeństwa • Metodyka zarządzania ryzykiem w zakresie bezpieczeństwa informacji, • Organizacja i odpowiedzialności w zakresie procesu oceny i szacowania ryzyka, • Szacowanie ryzyka – warsztaty praktyczne, • Tworzenie planów postępowania z ryzykiem • Informowanie o ryzyku, • Monitoring i przegląd ryzyka.	20	Artur Rudy

5.	Normalizacja i standardy międzynarodowe w obszarze bezpieczeństwa informacji, cyberbezpieczeństwa i prywatności • ISO/IEC 27001 • ISO/IEC 27017 • ISO/IEC 27018 • ISO/IEC 27701 • Inne standardy dziedzinowe • Standardy NIST	40	Artur Gębicz
6.	Kontynuacja działalności po awarii. Zarządzanie ciągłością działania • Rule i odpowiedzialności • Plany awaryjne • Plany przywracania systemów po awarii • Testowanie planów awaryjnych • Odtwarzanie techniki teleinformatycznej po katastrofie.	8	Adam Kuczyński
7.	Zarządzanie kryzysowe. Krajowy system cyberbezpieczeństwa. • Działania w czasie kryzysu. • Działania lokalnych komórek CSIRT • Obowiązki operatorów usług kluczowych i dostawców usług cyfrowych • Organizacja systemu zarządzania cyberbezpieczeństwem • Architektura cyberbezpieczeństwa – określenie i powołanie struktur wewnętrznych • Współpraca z sektorowymi zespołami cyberbezpieczeństwa	8	Adam Kuczyński
	Audyt infrastruktury teleinformatycznej • Techniki przeprowadzania audytu infrastruktury informatycznej, • Podejście do mobilności i przetwarzania danych w chmurach obliczeniowych; • Techniki kontruli warstwy sieciowej, systemowej i aplikacyjnej, • Tworzenie audytowych list kontrolnych: CASE STUDY • Najczęściej występujące niezgodności i problemy identyfikowane w trakcie audytów.	20	Piotr Błaszczeć

9	Regulacje prawne obejmujące szeroko pojęte bezpieczeństwo informacji, prywatność i cyberbezpieczeństwo • Kodeks karny • Dyrektywa pulicyjna • Przestępstwa przeciwko ochronie informacji • Powiązanie RODO a obszar IT • Analiza projektów i nowelizacji przepisów o ochronie danych osobowych oraz obszaru cyberbezpieczeństwa • Prawa autorskie i zasady ochrony własności intelektualnej. • Krajowe Ramy Interoperacyjności. • Dowód elektroniczny na potrzeby postępowania sądowego w postępowaniach karnych oraz postępowaniach cywilnych. • Tajemnica przedsiębiorstwa i inne tajemnice prawnie chronione.	40	Stanisław Hady Głowiak
	SUMA godzin	**200**	

14-15.03.2026

11-12.04.2026

25-26.04.2026

09-10.05.2026

30-31.05.2026

20-21.06.2026

10-11.10.2026

21-22.11.2026

05-06.12.2026

09-10.01.2027

23-24.01.2027

Harmonogram

Liczba przedmiotów/zajęć: 2

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 2 Cyberbezpieczeństwo	Piotr Błaszczeć	14-03-2026	08:00	15:00	07:00	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
2 z 2 Cyberbezpieczeństwo	Piotr Błaszczeć	15-03-2026	08:00	15:00	07:00	Tak

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 500,00 PLN
Koszt przypadający na 1 uczestnika netto	6 500,00 PLN
Koszt osobogodziny brutto	32,50 PLN
Koszt osobogodziny netto	32,50 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

Stanisław Hady-Głowiak

Wieloletni pracownik administracji publicznej, audytor wiodący normy ISO/EIC 27001, radca prawny, autor wielu publikacji naukowych, branżowych, doświadczony Inspektor Ochrony Danych, absolwent studiów doktoranckich na Wydziale Prawa i Administracji Uniwersytetu Śląskiego – dr nauk prawnych, wykładowca prowadzący szkolenia i kursy oraz wykłady na uczelniach publicznych, ekspert ds. bezpieczeństwa informacji

2 z 2

Piotr Błaszczeć

Od kilkunastu lat ściśle zajmuje się tematyką związaną z bezpieczeństwem informacji. Od kilku lat współpracuje z jednostką certyfikacyjną CIS – Certification Security Services Sp. z o. o. Zajmuje się audytem, wdrożeniami systemów bezpieczeństwa, testami penetracyjnymi i analizą computer forensics. Przez kilkanaście lat pełnił funkcję CSO (Chief Security Officer) w jednej z agencji rządowych, a wcześniej w sektorze bankowym. Obecnie odpowiada za bezpieczeństwo informacji w grupie kapitałowej będącej jednym z największych graczy rynku e-commerce a także w ramach outsourcingu funkcji Inspektora ochrony danych nadzoruje bezpieczeństwo Spółek funkcjonujących w obszarze finansów i płatności mobilnej oraz służby zdrowia. Niezależny konsultant ds. bezpieczeństwa IT, biegły sądowy z zakresu przestępstw przy użyciu sprzętu i sieci komputerowych, audytor systemów IT, CICA (Certified Internal Controls Auditor), CISSO (Certified Information

Systems Security Officer), audytor wiodący ISO 27001, ISO 20000, ISO 22301, EN 50600. Uczestnik i koordynator wielu projektów audytowych oraz postępowań kontrolnych realizowanych w organizacjach sektora prywatnego i publicznego. Trener realizujący zadania dla wielu firm z zakresu bezpieczeństwa informacji, audytu teleinformatycznego, danych osobowych, ochrony własności intelektualnej w sektorze nowych technologii oraz prawnych aspektów umów w IT.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy studiów otrzymują zestaw materiałów dydaktycznych udostępnionych na platformie eduPortal. Treści te są przygotowywane przez wykładowców i dostosowywane do tematyki prowadzonych zajęć.

Uczestnicy studiów mają dostęp do platformy Wirtualna Uczelnia, to wewnętrzna platforma komunikacyjna, stworzona w celu ograniczenia formalności oraz ułatwienia przepływu informacji między uczestnikami a uczelnią. Za jej pomocą przez całą dobę i z każdego miejsca na świecie uczestnicy mają dostęp do:

- harmonogramu zajęć,
- informacji na temat płatności,
- informacji dotyczących zmian w planach zajęć, ogłoszeń i aktualności.

Warunki uczestnictwa

Rekrutacja na studia podyplomowe odbywa się poprzez wypełnienie formularza online dostępnego na stronie: Rekrutacja online/Online Recruitment - Sopocka Akademia Nauk Stosowanych

Kryteria kwalifikacyjne do udziału w studiach:

- ukończone studia wyższe I lub II stopnia,
- spełnienie warunków określonych w procedurze rekrutacyjnej.
- Cena usługi **nie obejmuje opłaty wpisowej oraz opłaty za świadectwo**.
- **Usługa kształcenia świadczona przez SANS 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.**

Warunek zaliczenia studiów - uczestnictwo w **minimum 80% zajęć - badane na podstawie logowania do spotkania (wydruk listy z Teams) oraz list obecności (zajęcia stacjonarne).**

Informacje dodatkowe

Organizacja zajęć: zajęcia odbywają się 1-2 razy w miesiącu w soboty i niedziele (ok. 50 % zajęć w trybie online).

sobota – 08.00 – 15.00 (1 godz. lekcyjna = 45 min)

niedziela – 08.00 – 15.00 (1 godz. lekcyjna = 45 min)

Przerwy: 9.30 -9.45, 11.15 -11.30, 13.00-13.00

Forma zaliczenia studiów – praca projektowa.

Po ukończeniu studiów z wynikiem pozytywnym Absolwenci otrzymują:

1. Świadectwo ukończenia Studiów Podyplomowych nadawane przez SANS
2. Certyfikat Audytora nadawany przez Polski Instytut Kontroli Wewnętrznej
3. Prawo wpisu na Krajową Listę Audytorów, Kontrolerów i Specjalizacji Powiązanych prowadzoną przez PIKW
4. Bezterminowe, bezpłatne, kierunkowe wsparcie merytoryczne ze strony Rady Programowej PIKW w zakresie czynności, wykonywanych na stanowisku pracy, związanych z uzyskaną specjalizacją / patrz § 9 Regulaminu Krajowej Listy /

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:

- komputer wyposażony w głośniki i mikrofon (wbudowane lub zewnętrzne),
- stabilne połączenie z Internetem,
- słuchawki (zalecane, choć opcjonalne),
- kamera internetowa (opcjonalna, lecz przydatna podczas aktywnych form zajęć).

Adres

ul. Rzemieślnicza 5

81-855 Sopot

woj. pomorskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Izabela Bednarska

E-mail podyplomowe@sopocka.edu.pl

Telefon (+48) 509 655 417