

Zarządzanie cyberbezpieczeństwem. Certyfikat ISO 27001

STUDIA PODYPLOMOWE

Sposób realizacji: Hybrydowe

Obszar studiów: Administracja i bezpieczeństwo

Cechy: Od października • Polski

Miasto: Gdynia

To kierunek dla osób, które:

- chcą zdobyć zawód w dynamicznie rozwijającej się branży IT,
- myślą o przebranżowieniu i chcą szybko wejść do świata cyberbezpieczeństwa,
- pracują jako specjaliści i chcą poszerzyć kompetencje w zakresie bezpieczeństwa,
- pracują w IT i chcą zarządzać zespołami i wdrażać normy ISO 27001,
- cenią elastyczną naukę i chcą zdobywać certyfikaty w praktyczny sposób.



Informacje dodatkowe

Studia są dla osób, które chcą pracować w obszarze bezpieczeństwa IT i rozwijać się w cyberbezpieczeństwie. Poznasz podstawy ochrony sieci, systemów i aplikacji oraz rozpoczniesz ścieżkę do certyfikacji w zakresie uprawnień audytora.

2

partnerów kierunku

- Policja
- Szkoła Policji

Podczas zajęć skorzystasz z **Laboratorium Cyberbezpieczeństwa**, gdzie w praktyce poznasz techniki obrony przed atakami i scenariusze bezpieczeństwa IT.

Dostęp online

Wysoka jakość kształcenia. Wszystkie materiały dydaktyczne będą dostępne dla Ciebie online.

Praktyczny charakter studiów:

- część zajęć odbywa się w formie warsztatowej,
- prace projektowe wyłącznie zespołowe.

1

certyfikat specjalistyczny

Networking i rozwój kompetencji

Studia rozwijają kompetencje niezależnie od doświadczenia. Dzięki interaktywnym zajęciom i wymianie doświadczeń z innymi zyskasz **wiedzę, umiejętności i cenne kontakty**.

Kadra złożona z praktyków

Wśród wykładowców są **praktycy i eksperci** w wielu dziedzinach. Na zajęciach omawiają zjawiska i procesy na przykładach zaczerpniętych z własnej pracy.

Program studiów

9

Liczba miesięcy nauki

174

Liczba godzin zajęć

10

Liczba zjazdów

2

Liczba semestrów

Prawne aspekty zasobów informacyjnych w cyberprzestrzeni (40 godz.)

- Ramy systemu cyberbezpieczeństwa w Unii Europejskiej. Zadania państw członkowskich, zakres podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa (8 godz.)
- Obowiązki podmiotów kluczowych i ważnych, podmiotów działających w sektorach krytycznych, podmiotów publicznych (6 godz.)
- Organy właściwe do spraw cyberprzestępstwa (4 godz.)
- Sankcje karne w cyberprzestępczości (4 godz.)
- Prawne aspekty ochrony prywatności w sieci (4 godz.)
- Dowody elektroniczne, a przepisy kodeksu postępowania karnego (6 godz.)
- Postępowanie z incydemem informatycznym - środki zarządzania ryzykiem w



cyberbezpieczeństwie (8 godz.)

Organizacyjne aspekty zarządzania bezpieczeństwem cyberprzestrzeni (48 godz.)

- Funkcjonalne systemy bezpieczeństwa – bezpieczeństwo fizyczne i środowiskowe (8 godz.)
- Zagrożenia dla bezpieczeństwa w cyberprzestrzeni (8 godz.)
- Wymagania i metody szacowania ryzyka oraz zapewnienia ciągłości działania (10 godz.)
- Ochrona zasobów informacyjnych w systemach IT (8 godz.)
- Reagowanie na incydenty bezpieczeństwa IT (6 godz.)
- Wymagania i metody audytów systemów informatycznych (8 godz.)

Informatyczne aspekty cyberbezpieczeństwa (78 godz.)

- Bezpieczeństwo sieci komputerowych i telekomunikacyjnych (6 godz.)
- Identyfikowanie podatności w systemach teleinformatycznych (8 godz.)
- Metodyka testów penetracyjnych z elementami socjotechniki (10 godz.)
- Rozpoznanie w cyberprzestrzeni oraz analiza cyfrowych śladów (8 godz.)
- Przelamywanie zabezpieczeń klasycznych systemów operacyjnych i IoT (6 godz.)
- Technologie zabezpieczania i szyfrowania zasobów i informacji (8 godz.)
- Bezpieczeństwo systemów i aplikacji (6 godz.)
- Podstawy kryptografii (8 godz.)
- Wykorzystanie złośliwego oprogramowania (6 godz.)
- Skanowanie sieci i enumeracja systemów informatycznych (6 godz.)
- OSINT jako technika wywiadu i jego znaczenie dla bezpieczeństwa IT (6 godz.)

Projekt (8 godz.)

- Seminarium podyplomowe (8 godz.)

Warunki przyjęcia

Aby zostać uczestnikiem studiów podyplomowych na Uniwersytecie WSB Merito, należy:

- mieć ukończone studia licencjackie, inżynierskie lub magisterskie,
- złożyć komplet dokumentów i spełnić wymogi rekrutacyjne,

Możliwości dofinansowania

- **Pierwsi zyskują najwięcej!** Im szybciej się zapiszesz, z tym większej zniżki skorzystasz.
- Oferujemy specjalne, **większe zniżki dla naszych absolwentów.**
- Możesz skorzystać z dofinansowania z **Bazy Usług Rozwojowych.**
- Pracodawca może dofinansować Ci studia,



- o przyjęciu decyduje kolejność zgłoszeń.

[Dowiedz się więcej](#)

otrzymując dodatkową zniżkę w ramach **Programu Firma**.

- Warto sprawdzić możliwości dofinansowania z **KFS**.

[Dowiedz się więcej](#)

Czego się nauczysz?

- Nauczysz się skutecznie **zabezpieczać sieci, systemy i aplikacje** w różnych środowiskach.
- Dowiesz się, jak przeprowadzać **audyty bezpieczeństwa** i wykrywać słabe punkty systemów.
- Poznasz **podstawy kryptografii** i sposoby ochrony danych przed dostępem niepowołanych osób.
- Zdobędziesz umiejętności, które pozwolą Ci **zapobiegać cyberatakom** i reagować na incydenty.
- Będziesz potrafić planować działania i wdrażać procedury zgodne z normą **ISO 27001**.
- Przećwiczysz nowoczesne techniki obrony w praktycznym **Laboratorium Cyberbezpieczeństwa**.

Ceny

Dla Kandydatów

1 rok

2 raty **2950 zł** ~~3200 zł~~ (2 x 2950 zł)
Najniższa cena z ostatnich 30 dni: 2760zł

10 rat **610 zł** ~~660 zł~~ (10 x 610 zł)
Najniższa cena z ostatnich 30 dni: 572zł

12 rat **513 zł** ~~555 zł~~ (12 x 513 zł)
Najniższa cena z ostatnich 30 dni: 481zł

Cena jednorazowa: **5800 zł** ~~6300 zł~~

Najniższa cena z ostatnich 30 dni: 5420zł

Dla naszych absolwentów

1 rok

2 raty **2750 zł** ~~3200 zł~~ (2 x 2750 zł)
Najniższa cena z ostatnich 30 dni: 2560zł

10 rat **570 zł** ~~660 zł~~ (10 x 570 zł)
Najniższa cena z ostatnich 30 dni: 532zł

12 rat **480 zł** ~~555 zł~~ (12 x 480 zł)
Najniższa cena z ostatnich 30 dni: 448zł

Cena jednorazowa: **5400 zł** ~~6300 zł~~

Najniższa cena z ostatnich 30 dni: 5020zł



Dla kandydatów z zagranicy

1 rok

2 raty **2950 zł** ~~3200 zł~~ (2 x 2950 zł)
Najniższa cena z ostatnich 30 dni: 2760zł

10 rat **610 zł** ~~660 zł~~ (10 x 610 zł)
Najniższa cena z ostatnich 30 dni: 572zł

12 rat **513 zł** ~~555 zł~~ (12 x 513 zł)
Najniższa cena z ostatnich 30 dni: 481zł

Cena jednorazowa: **5800 zł** ~~6300 zł~~

Najniższa cena z ostatnich 30 dni: 5420zł

Wykładowcy

dr Ernest Lichocki

- Jego zainteresowania naukowe obejmują cyberterrorizm, bezpieczeństwo teleinformacyjne i teleinformatyczne oraz bezpieczeństwo morskie, w tym Morską Infrastrukturę Krytyczną Państwa.
- Autor kilkunastu projektów wdrożonych w resortach MON i MSWiA. Jego prace wspierają rozwój systemów bezpieczeństwa i administracji, łącząc wiedzę ekspercką z praktyką.
- Autor i współautor ponad 40 publikacji związanych z bezpieczeństwem teleinformatycznym i bezpieczeństwem Infrastruktury Krytycznej Państwa.
- Posiada uprawnienia z zakresu bezpieczeństwa teleinformatycznego i teleinformacyjnego, w tym ochrony informacji niejawnych. Ukończył w kraju i za granicą ponad 20 kursów specjalistycznych.

dr Klaudia Skelnik

- Prodziekan Wydziału Prawa i Administracji Wyższa Szkoła Bankowa w Gdańsku, doktor nauk społecznych w dyscyplinie nauki o bezpieczeństwie, absolwent studiów MBA zarządzanie bezpieczeństwem.
- Doświadczenie zawodowe zdobyła głównie pełniąc wieloletnią służbę cywilną w Policji przede wszystkim w pionie ochrony informacji niejawnych głównie zajmując stanowiska związane z bezpieczeństwem.
- Realizowane projekty, audyty, wdrożenia: Jednostki Urzędu Miasta Gdańsk, Prywatne firmy księgowo, marketingowe, świadczące usługi sprzedażowe.

Klaudia Maciejewska

- Prawniczka i doktorantka Uniwersytetu Szczecińskiego w programie „Doktorat wdrożeniowy”. Specjalizuje się w prawie nowych technologii.
- Inspektor ochrony danych i mediator sądowy. Kierowniczką centrum B+R Currenda Lab w Currenda Sp. z o.o., łączy prawo z technologią.
- Nominowana przez Perspektywy Women in Tech do Top 100 kobiet w AI. Wyróżnienie potwierdza jej kompetencje w obszarze nowych technologii.



- Autorka publikacji o ochronie danych, AI i prawie technologii. Zajmuje się etyką AI oraz postępowaniem egzekucyjnym w ujęciu prawnym.

Dariusz Kłós

- Project Manager, Architect IT i współzałożyciel firmy teleinformatycznej. Od ponad 20 lat związany z informatyką, rozwiązaniami IT, architekturą oraz bezpieczeństwem.
- Ma ponad 10 lat doświadczenia konsultingowego we wdrażaniu nowych technologii w biznesie. Projektuje rozwiązania, nadzoruje zespoły i popularyzuje nowe technologie.
- Na co dzień zajmuje się projektowaniem i integracją mechanizmów zwiększających bezpieczeństwo oraz dynamikę hybrydowej infrastruktury IT i rozwiązań Cloud Computing.
- Posiada certyfikacje Citrix, Microsoft, VMWare, PRINCE2 i ITIL. Dzieli się wiedzą na szkoleniach, wykładach, konferencjach i warsztatach w Polsce oraz za granicą.

Grzegorz Piotrowski

- Specjalista od przeprowadzania zmian technologicznych i organizacyjnych. Od lat promuje praktyczne podejście do bezpieczeństwa IT oraz ochrony cyberprzestrzeni.
- Ma 25 lat doświadczenia zawodowego związanego z cyberprzestrzenią i jej zagrożeniami. Pracował dla firm międzynarodowych oraz polskich organizacji.
- W projektach dla takich marek jak Allianz, BASF, ING, Microsoft, O2 czy Telefonica dbał o podnoszenie standardów bezpieczeństwa IT i cyberbezpieczeństwa.
- Prelegent i ekspert wydarzeń technologicznych oraz cyberbezpieczeństwa. Jeden z pierwszych certyfikowanych hakerów w Polsce, trener IT i testów penetracyjnych.

Piotr Robakowski

- Wykładowca Uniwersytetu Gdańskiego i ekspert ds. bezpieczeństwa. Pracuje także jako główny specjalista ds. bezpieczeństwa i obronności w Uniwersyteckim Centrum Klinicznym.
- Pełni funkcję Inspektora Ochrony Danych w Gdyńskim Centrum Zdrowia oraz Prezesa Zarządu Pomorskiego Biura Inspektorów Ochrony Danych.
- Specjalizuje się w bezpieczeństwie, ochronie danych osobowych, bezpieczeństwie informacji, ochronie infrastruktury krytycznej i zarządzaniu kryzysowym.
- Posiada doświadczenie jako pełnomocnik i audytor SZBI ISO 27001/27032. Współpracuje ze strategicznymi firmami, tworząc projekty i trendy w bezpieczeństwie.

Przemysław Świeboda

- Ekspert ds. cyberbezpieczeństwa działający w strukturach Krajowego Systemu Cyberbezpieczeństwa. Etyczny haker, pentester oraz audytor, w tym wiodący normy ISO 27001.
- Prowadzi zajęcia z cyberbezpieczeństwa na studiach podyplomowych oraz I i II stopnia, m.in. na kierunkach Bezpieczeństwo Wewnętrzne i Administracja.
- Członek Grupy Roboczej ds. Sztucznej Inteligencji GRAI przy KPRM oraz Komitetu Technicznego ds. Sztucznej Inteligencji PKN jako reprezentant ISACA.



- Badacz bezpieczeństwa z uznanymi krytycznymi i wysokimi podatnościami w komercyjnych systemach bezpieczeństwa oraz serwisach rządowych i bankowych.