UNIWERSYTET WSB MERITO SZCZECIN

wcześniej Wyższa Szkoła Bankowa

Bezpieczeństwo i ochrona cyberprzestrzeni

STUDIA PODYPLOMOWE

Program studiów

9	186	12	2
Liczba miesięcy nauki	Liczba godzin zajęć	Liczba zjazdów	Liczba semestrów

Społeczeństwo informacyjne (8 godz.)

- Podstawy funkcjonowania społeczeństwa informacyjnego
- Rola informacji i technologii w nowoczesnym świecie

Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO (32 godz.)

- Zadania i odpowiedzialność pełnomocnika
- Wymagania norm ISO 27001 i ISO 22301
- Cyberbezpieczeństwo a ochrona danych osobowych

Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001 (16 godz.)

- Planowanie i prowadzenie audytów wewnętrznych
- Dokumentacja i raportowanie audytów
- Doskonalenie systemu zarządzania bezpieczeństwem informacji

Organizacja Krajowego Systemu Cyberbezpieczeństwa (8 godz.)

- Struktura i zadania KSC
- Obowiązki operatorów usług kluczowych
- Współpraca z organami nadzoru

Organizacja i zadania Security Operations Center (8 godz.)

- Funkcje i modele SOC
- Monitorowanie bezpieczeństwa
- Reagowanie na zagrożenia

Prawno-karne aspekty cyberprzestępczości (8 godz.)

- Regulacje prawne dotyczące cyberprzestępstw
- Odpowiedzialność karna i administracyjna

- Przestępstwa komputerowe i dowody cyfrowe

Zarządzanie i obsługa incydentów cyberbezpieczeństwa (16 godz.)

- Procedury reagowania na incydenty
- Narzędzia wspierające obsługę incydentów
- Raportowanie i analiza incydentów

Postępowanie wyjaśniające i dochodzenie w przypadku incydentów (8 godz.)

- Zasady prowadzenia dochodzeń
- Dokumentowanie i analiza dowodów
- Współpraca z organami ścigania

Wykorzystanie Internetu jako narzędzia śledczego (16 godz.)

- OSINT – otwarte źródła informacji
- Monitorowanie aktywności w sieci
- Narzędzia do analizy śladów cyfrowych

Techniki analizy elektronicznego materiału dowodowego (32 godz.)

- Metody zabezpieczania dowodów cyfrowych
- Analiza dysków, pamięci i sieci
- Rekonstrukcja zdarzeń z danych cyfrowych

Metodyka przeprowadzania analizy śledczej (16 godz.)

- Etapy analizy śledczej
- Tworzenie hipotez i scenariuszy
- Raportowanie wyników analizy

Szacowanie ryzyka w systemach informatycznych (16 godz.)

- Identyfikacja zagrożeń i podatności
- Metody oceny ryzyka
- Zarządzanie ryzykiem w systemach IT

Egzamin (2 godz.)

- Test końcowy