

OPIS STUDIÓW:

Studia skierowane są głównie do osób zajmujących się szeroko rozumianą problematyką ochrony informacji i danych osobowych we wszystkich sektorach gospodarki (pracownicy przedsiębiorstw i firm, administracji państwowej i samorządowej, służb mundurowych), tj. do osób, które kierują lub przygotowują się do pracy w pionach ochrony danych osobowych i informacji niejawnych lub odpowiadają za politykę bezpieczeństwa w swoich jednostkach organizacyjnych, a w szczególności do osób zatrudnionych w charakterze pełnomocnika ds. ochrony informacji niejawnych, pełniących funkcję ABI oraz wszystkich zatrudnionych w pionach ochrony informacji niejawnych. Zapraszamy także pracowników kadr, PR, kierowników lub pracowników jednostek organizacyjnych, którzy obecnie lub w przyszłości zamierzają specjalizować się w zagadnieniach ochrony danych osobowych i prywatności.

Celem studiów jest podnoszenie kwalifikacji pracowników administracji samorządowej i rządowej, służb mundurowych, firm oraz przedsiębiorstw mających w swej działalności do czynienia z danymi osobowymi, informacjami prawnie chronionymi. Celem studiów jest także przygotowanie specjalistów do pełnienia funkcji Administratora Bezpieczeństwa Informacji (Inspektora Ochrony Danych Osobowych – w myśl planowanych regulacji UE) oraz wsparcie merytoryczne osób już zajmujących się tą problematyką. Warunkiem ukończenia studiów jest uzyskanie zaliczeń w trakcie trwania studiów, zakończone zdaniem egzaminu dyplomowego.

CZAS TRWANIA:

2 semestry (w tym jeden on-line) od 01.10 do 30.06, studia w trybie niestacjonarnym

ZAKRES KSZTAŁCENIA:

1. Wybrane elementy bezpieczeństwa narodowego.
2. Podstawy prawne ochrony informacji niejawnych.
3. Ochrona danych osobowych – podstawy teoretyczne i aspekty praktyczne.
4. Tworzenie dokumentacji z zakresu danych osobowych.
5. Praktyczne aspekty ochrony informacji niejawnych: bezpieczeństwo osobowe, bezpieczeństwo przemysłowe, bezpieczeństwo teleinformatyczne.
6. Standardy ochrony informacji niejawnych w NATO i UE.

7. Bezpieczeństwo informacji biznesowych. Teoretyczne i praktyczne aspekty ustanawiania i wdrażania tajemnicy przedsiębiorstwa.
8. Systemy zarządzania jakością i bezpieczeństwem informacji. Szacowanie i zarządzanie ryzykiem ochrony informacji niejawnych.
9. Funkcjonowanie kancelarii tajnych i niejawnych. Obieg dokumentów niejawnych.
10. Archiwizacja dokumentów.
11. Inwigilacja (nadzór) w społeczeństwie informacyjnym.
12. Zarządzanie bezpieczeństwem informacji w stanach kryzysowych/ekstremalnych.
13. Nowoczesne techniki technologii i ochrony informacji.