



Kierunek: Zarządzanie bezpieczeństwem IT

Wiedza o stanie bezpieczeństwa firmy jest podstawą budowania bezpiecznej infrastruktury teleinformatycznej. Świadomość zagrożeń, płynących zarówno z zewnątrz, jak i wewnątrz firmy, a następnie przełożenie ich na aktualne środowisko IT organizacji, umożliwia dokonanie trafniejszego wyboru drogi rozwoju zabezpieczenia procesów biznesowych przedsiębiorstwa. Jest ona najczęściej określona w strategii i polityce bezpieczeństwa, jednak największym problemem dla większości organizacji jest przełożenie przyjętych regulacji na rzeczywiste środowisko teleinformatyczne.

Celem studiów jest przygotowanie słuchaczy do pełnienia menedżerskich funkcji w zakresie zarządzania bezpieczeństwem IT. Studia pozwolą na zdobycie profesjonalnej wiedzy w tematyce zarządzania bezpieczeństwem IT oraz przygotują do prowadzenia procesów audytowania i kontrolowania procesu bezpieczeństwa informacji w organizacji. W ramach programu słuchacze zapoznają się ze standardami związanymi z bezpieczeństwem informacji, w szczególności z wdrażaniem norm ISO.

Metodyka: Zajęcia prowadzone są w formie wykładów i ćwiczeń, ze szczególnym uwzględnieniem interaktywnych metod nauczania oraz pracy w laboratoriach komputerowych. Zajęcia prowadzone są przez specjalistów i praktyków z zakresu objętego tematyką studiów.

Adresatami studiów podyplomowych na kierunku „Zarządzanie bezpieczeństwem IT” są osoby posiadające wyższe wykształcenie i chcące zdobyć umiejętność w zakresie zarządzania bezpieczeństwem IT w organizacjach. Studia adresowane są w głównej mierze do osób piastujących menedżerskie lub kierownicze stanowiska, specjalistów i pracowników przedsiębiorstw, firm doradczych i IT, których pracownicy pragną pogłębić wiedzę z zakresu zarządzania bezpieczeństwem informacji.

Warunkiem udziału w szkoleniu jest podstawowa wiedza z zakresu informatyki, a zwłaszcza technicznych aspektów bezpieczeństwa teleinformatycznego.

TEMATYKA	Liczba godzin
BLOK WPROWADZAJĄCY	10
Wprowadzenie do problematyki bezpieczeństwa IT	10
BLOK UMIEJĘTNOŚCI ZAWODOWYCH	185
Podstawy zarządzania bezpieczeństwem IT	15
Zarządzanie zasobami IT	25
Techniczne aspekty bezpieczeństwa: Bezpieczeństwo osobowe	5
Techniczne aspekty bezpieczeństwa: Bezpieczeństwo fizyczne	5
Techniczne aspekty bezpieczeństwa: Zarządzanie ciągłością działania	5
Techniczne aspekty bezpieczeństwa: Zarządzanie incydentami związanymi z bezpieczeństwem informacji	10
Techniczne aspekty bezpieczeństwa: Zarządzanie sieciami oraz systemami teleinformatycznymi	10
Techniczne aspekty bezpieczeństwa: Kontrola dostępu i zarządzanie tożsamością	10
Pozyskiwanie, rozwój i utrzymanie systemów informatycznych	15



Audyt systemu zarządzania i audyt techniczny	45
Wymagania bezpieczeństwa w aplikacjach	5
Podstawy kryptografii i steganografii	5
Bezpieczeństwo prawne	15
Zarządzanie finansami	15
BLOK UMIEJĘTNOŚCI INTERPERSONALNYCH	20
Trening menedżerski	20
Seminarium dyplomowe	5
Łącznie	220