

EITC/IS/ISCF

Technologie bezpieczeństwa informatycznego

Szczegółowa zawartość programowa kursu (15 godz.):

- Wprowadzenie
 - Zagrożenia bezpieczeństwa informacji
 - Mechanizmy zabezpieczeń informacji
 - Zagrożenia celowe
 - Złośliwe oprogramowanie
 - Podszywanie się
 - Szpiegostwo
 - Przeciążanie systemu
 - Skanowanie
 - Zagrożenia niecelowe
 - Awaria sprzętu
 - Błędy ludzkie
 - Czynniki losowe
 - Szkodliwe oprogramowanie
 - Programy szpiegujące
 - Spyware
 - Adware
 - Programy antywirusowe
 - Rozpoznawanie zagrożeń
 - Analiza behawioralna
 - Analiza heurystyczna
 - Polityka bezpieczeństwa informatycznego
 - Obszary polityki bezpieczeństwa
 - Zabezpieczanie sprzętu
 - Kontrolowanie dostępu do informacji
 - Przetwarzanie dokumentów i informacji
 - Zakup i konserwacja oprogramowania komercyjnego
 - Walka a aktami cyberprzestępczości
 - Zachowywanie zgodności z regulacjami prawnymi
 - Planowanie ciągłości biznesu
 - Kontrola bezpieczeństwa informatycznego w handlu elektronicznym
 - Szkolenie personelu
 - Klasyfikacja informacji i danych
 - Zasady polityki bezpieczeństwa
 - Przykłady
 - Audyt bezpieczeństwa informatycznego
 - Czynności audytowe
 - Metody i narzędzia
 - Okoliczności przeprowadzania audytów bezpieczeństwa
 - Informatyczne narzędzia auditingowi
 - Skanery online
 - Kompleksowe oprogramowanie do zarządzania bezpieczeństwem
 - Wstęp do kryptografii
 - Historia zabezpieczania informacji
 - Przełomy w dziedzinie kryptografii
 - Szyfr Vernama
 - Enigma
 - DES

- RSA
- Kryptologia
 - Szyfrowanie
 - Deszyfrowanie
 - Kryptoanaliza systemów kryptografii
 - Odtwarzanie wiadomości z szyfrogramów
- Poufność danych i techniki szyfrowania
 - Szyfr podstawieniowy
 - Tworzenie szyfrogramu
 - Szyfr monoalfabetyczny
 - Szyfr Cezara
 - Szyfr polialfabetyczny
 - Szyfr Vigenere'a
- Systemy liczbowe, elementy logiki, szyfr przedstawieniowy, macierzowy, one-time pad
 - Systemy liczbowe
 - Zbiór reguł do zapisywania i reprezentowania liczb
 - System dziesiętny
 - System binarny
 - System addytywny
 - Rzymski zapis liczb
 - System pozycyjny
 - Znaki dla początkowych liczb
 - Funkcje logiczne
 - Funkcja OR (LUB)
 - Funkcja AND (ORAZ)
 - Funkcja NOT (NIE)
 - Funkcja XOR (exclusive OR)
 - Prawa DeMorgana
 - Obliczanie wyrażeń logicznych
 - Szyfr przedstawieniowy, macierzowy
 - Przeszycie liter w tekście
 - Odwrócenie napisu
 - Wprowadzenie tekstu do macierzy
 - One-time pad
 - Szyfrowanie tekstu jawnego kluczem losowym
- Kryptosystemy symetryczne i asymetryczne
 - Kryptosystemy symetryczne
 - Szyfrowanie wiadomości kluczem szyfrującym
 - Deszyfrowanie
 - Klucz tajny dla obu uczestników
 - Problem dystrybucji klucza
 - Problem skalowalności
 - Bezpieczeństwo algorytmu
 - Większa złożoność obliczeniowa to większe bezpieczeństwo
 - Kryptosystemy asymetryczne
 - Klucz publiczny i klucz prywatny
 - Zastosowanie w finansowych usługach elektronicznych
 - Powstanie podpisów cyfrowych
 - Idee kryptografii kwantowej
 - Rozwój kwantowej teorii informacji
 - Rozwiązanie problemu dystrybucji klucza
- Systemy biometryczne
 - Biometryka
 - Schemat systemu biometrycznego
 - Identyfikacja obiektu w systemach zabezpieczeń

- Cechy behawioralne
- Cechy fizyczne
- Klasyfikacja systemu
- Porównanie systemów
- Certyfikacja, funkcje hashujące, podpis cyfrowy, serwer Kerberos
 - Certyfikacja
 - Zastosowanie
 - Struktura certyfikatu
 - Funkcje hashujące
 - Przekształcanie ciągu znaków
 - Hash
 - Ciąg znaków zwracanych przez funkcję
 - Podpis cyfrowy
 - Zasada działania
 - Warunki na poprawność uwierzytelnienia wiadomości
 - Paradoks urodzinowy
 - Serwer Kerberos
 - Kontrola autentyczności
 - Przepustka
 - Zawartość przepustki
 - Bezpieczeństwo