EITCA/IS

Akademia Bezpieczeństwa Informatycznego

Zawartość programowa Akademii:

- EITC/IS/CF: Podstawy kryptografii (15h)
- EITC/IS/EEIS: Bezpieczeństwo informatyczne e-Gospodarki (15h)
- EITC/IS/SMMOS: Administracja i zarządzanie bezpieczeństwem w systemach Microsoft (15h)
- EITC/IS/OS: Bezpieczeństwo systemów operacyjnych (15h)
- EITC/CN/SCN1: Bezpieczne sieci komputerowe 1 (15h)
- EITC/CN/SCN2: Bezpieczne sieci komputerowe 2 (15h)
- EITC/IS/ACNS: Zaawansowane bezpieczeństwo sieci informatycznych (15h)
- EITC/IS/QCF: Kryptografia kwantowa (15h)
- EITC/IS/FAIS: Formalne aspekty bezpieczeństwa informacji (15h)
- EITC/IS/IST: Teoria bezpieczeństwa informatycznego (15h)
- EITC/QI/QIF: Informatyka kwantowa w kontekście bezpieczeństwa (15h)
- EITC/FC/CCT: Złożoność obliczeniowa jako podstawa bezpieczeństwa informacji (15h)

EITC/IS/CF

Podstawy kryptografii

Szczegółowa zawartość programowa kursu (15 godz.):

- Poufność
    - Techniki szyfrowania
        - Szyfry przestawieniowe
        - Szyfry podstawieniowe
        - Szyfry macierzowe
        - Klucze
        - XOR
        - OTP
- Wiarygodność
    - Techniki uwierzytelniania
        - Funkcje skrótowe (hashujące)
            - Dyskretny logarytm
            - Ciągi pseudolosowe
            - MD5
    - Integralność
- Kryptologia
    - Kryptografia
    - Kryptoanaliza
    - Steganografia
- Kryptosystemy
    - Asymetryczne (kryptosystemy klucza publicznego)
        - Problemy trudne (klasa problemów NP)
        - Algorytmy asymetryczne
        - Infrastruktura Klucza Publicznego
    - Symetryczne (kryptosystemy klucza prywatnego)
        - Algorytmy symetryczne
        - Dystrybucja klucza prywatnego
        - Kryptografia kwantowa
- Realizacje praktyczne algorytmów
    - Symetryczne
        - Szyfr Vernama
        - DES, IDEA, RC5, 3DES, AES (Rijndael), NASZ
    - Asymetryczne
        - RSA, DH, ElGamal
- Autoryzacja
- Realizacje autoryzacji (hasła, systemy biometryczne)

EITC/IS/EEIS

Bezpieczeństwo informatyczne e-Gospodarki

Szczegółowa zawartość programowa kursu (15 godz.):

- Zagrożenia informatyczne e-gospodarki
    - Zagrożenia celowe
    - Zagrożenia niecelowe
- Polityka bezpieczeństwa
    - Formalizacja przepływów informacji w organizacji
- Audyt bezpieczeństwa informatycznego
    - Wywiad w organizacji
    - Analiza bezpieczeństwa przepływów informacyjnych
    - Metody i narzędzia auditingowe
    - Model zagrożeń i metodologia STRIDE
- Walka z zagrożeniami
    - Wirusy komputerowe
    - Bezpieczne składowanie danych
    - Ochrona przed zagrożeniami sieciowymi
        - Zapory ogniowe
        - NAT i PAT
        - Serwery Proxy
        - Systemy IDS
        - Osobiste zapory ogniowe
- Kryptograficzna ochrona danych
    - Wykorzystanie kryptografii do ochrony danych
    - Certyfikacja i infrastruktura klucza publicznego (PKI)
    - Podpis elektroniczny
    - Protokół SSL
    - Wirtualne sieci prywatne
    - Bezpieczeństwo aplikacji i usług sieciowych

EITC/IS/SMMOS

Administracja i zarządzanie bezpieczeństwem w systemach Microsoft

Szczegółowa zawartość programowa kursu (15 godz.):

- Instalacja systemu
    - Zagadnienia bezpiecznej instalacji oraz uaktualniania (upgrade)
    - Instalacja łatek bezpieczeństwa oraz dodatków Service Pack
- Konta użytkowników i uwierzytelnianie
    - Grupy użytkowników i uprawnienia
    - Współpraca z systemami silnego uwierzytelniania
- Konfiguracja systemu i urządzeń sprzętowych (m.in. drukarki)
    - System Plug&Play
    - Ręczna konfiguracja zasobów
- KONFIGURACJA SIECI
    - Protokoły (IP, TCP, UDP, etc.)
    - Usługi (DHCP, DNS, WINS, LmHOSTS)
    - Udostępnianie plików i drukarek
    - Wbudowany system firewall
    - Zdalny dostęp (Remote desktop)
- Konfiguracja domeny sieciowej
    - Active Directory
    - Bezpieczeństwo
- Konfiguracja usług IIS
    - Prawa dostępu
    - Zarządzanie usługami IIS
    - Serwery IIS
        - Serwer www
        - Serwer ftp
        - Udostępnianie danych w Internecie
- Zarządzanie dyskami
    - System NTFS
    - Przydział przestrzeni dyskowej użytkownikom
    - Bezpieczeństwo i udostępnianie
    - Kompresja
- Zintegrowane bezpieczeństwo systemu
    - Centrum Zabezpieczeń
    - Przywracanie Systemu
- Administracja systemem
    - Konsola zarządzania systemem MMC
- Backup i odtwarzanie systemu
    - Pliki rejestrów (zdjęcia i odtwarzanie)
    - Obraz systemu
- Sytuacje awaryjne
    - Obsługa Recovery Console
    - Dostęp do partycji NTFS
    - Odzyskiwanie haseł

EITC/IS/OS

Bezpieczeństwo systemów operacyjnych

Szczegółowa zawartość programowa kursu (15 godz.):

- Wprowadzenie do systemów operacyjnych
    - Miejsce, rola i zadania systemu operacyjnego w oprogramowaniu komputera
    - Klasyfikacja systemów operacyjnych
        - Klasyfikacja ze względu na sposób przetwarzania
        - Klasyfikacja ze względu na liczbę wykonywanych programów
        - Klasyfikacja ze względu na liczbę użytkowników
        - Inne rodzaje systemów operacyjnych
    - Zasada działania systemu operacyjnego
        - Cykl rozkazowy
        - Przerwania w systemie komputerowym
        - Zasady ochrony pamięci
        - Przerwanie zegarowe
- Procesy, zasoby, wątki
    - Obsługa procesów i zasobów
        - Podział operacji jądra systemu w zarządzaniu procesami i zasobami
        - Zarządcy
        - Cykl zmian stanów procesów i zasobów
        - Klasyfikacja zasobów
        - Kolejki procesów
        - Przełączanie kontekstu
        - Elementarne operacje na procesach
        - Elementarne operacje na zasobach
    - Wątki
        - Realizacja wątków
        - Przełączanie kontekstu wątków
        - Elementarne operacje na wątkach
    - Realizacja procesów/wątków w systemach Linux i Windows
        - Procesy/wątki w systemie Linux
        - Procesy/wątki w systemie Windows 2000/XP
- System plików – warstwa logiczna
    - Pliki w systemie operacyjnym
        - Zadania systemu operacyjnego
        - Atrybuty pliku
        - Typy plików
        - Struktura pliku
        - Metody dostępu do plików
        - Podstawowe operacje na plikach
    - Interfejs dostępu do pliku w systemie uniksopodobnym
    - Organizacja logiczna systemu plików
        - Podział na strefy
        - Operacje na katalogu
        - Struktura logiczna katalogów
- System plików – warstwa fizyczna
    - Przydział miejsca na dysku
        - Przydział ciągły
        - Przydział listowy (łańcuchowy)
        - Przydział indeksowy
    - Zarządzanie wolną przestrzenią

- Implementacja katalogu
- Przechowywanie podręczne w systemie plików
- Integralność systemu plików
- Synchronizacja dostępu do plików

- System plików – przegląd wybranych implementacji
  - CP/M
  - MS DOS i Windows 9x (FAT12/16/32)
  - ISO 9660
  - UNIX
  - NTFS
- Wprowadzenie do bezpieczeństwa systemów operacyjnych
  - Co to jest bezpieczny system?
  - Czynniki decydujące o znaczeniu bezpieczeństwa
  - Zagrożenia bezpieczeństwa
  - Ogólne problemy konstrukcji zabezpieczeń
  - Strategia bezpieczeństwa
  - Polityka bezpieczeństwa
  - Normy i zalecenia zarządzania bezpieczeństwem
- Podstawowe problemy bezpieczeństwa systemów operacyjnych
  - Wprowadzenie
  - Naruszenia bezpieczeństwa systemu operacyjnego
  - Rozpoznawanie systemu operacyjnego komputera ofiary
  - Uwierzytelnianie
  - Prawa dostępu do zasobów
    - Standard POSIX (Portable Operating System Interface) 1003.1
    - Standard POSIX 1003.1e/1003.2c
    - Listy dostępu ACL
  - Uprawnienia specjalne w systemie Unix
  - Malware
    - Wirusy i inne robactwo
  - Zamaskowane kanały komunikacji
- Uwierzytelnianie i kontrola dostępu
  - Ogólne założenie uwierzytelniania w systemie Linux
  - Prawa dostępu do plików w systemach uniksopodobnych
  - Mechanizm POSIX ACL w systemie Linux i Windows
    - Lokalna kontrola dostępu w systemie Linux
    - Lokalna kontrola dostępu w systemie Windows XP
  - Modularne systemy uwierzytelniania i kontroli dostępu
    - Mechanizm PAM
- Ograniczenia i delegacja uprawnień, domeny zaufania, kontrola dostępu zdalnego
  - Ograniczone środowiska wykonywania aplikacji, ograniczone powłoki systemu operacyjnego środowisk serwerowych, delegacja uprawnień
    - Mechanizm limitów
    - Mechanizm SUDO
    - Mechanizm SUID i SGID
  - Domeny zaufania, mechanizmy kontroli zdalnego dostępu
    - Zastosowanie domen zaufania
    - Polecenie rlogin w systemie Linux
    - Zabezpieczanie usług sieciowych programem tcpd
- Umacnianie ochrony systemu operacyjnego serwerowych środowisk MS Windows
  - Konta użytkowników
  - System plików
  - Szyfrowanie danych
    - Szyfrowanie na poziomie systemu plików
    - Archiwa z ochroną kryptograficzną

- Kryptograficzna ochrony poczty elektronicznej
- Środowisko sieciowe
  - Otoczenie sieciowe i udziały sieciowe
  - Ukrycie komputera w otoczeniu sieciowym
  - Połączenia sieciowe
  - Zapory sieciowe
- Podsumowanie

EITC/CN/SCN1

Bezpieczne sieci komputerowe 1

Szczegółowa zawartość programowa kursu (15 godz.):

- Wprowadzenie do komunikacji sieciowej
- Paradygmaty komunikacji sieciowej
    - Komutacja łącz
    - Komutacja pakietów
- Topologie sieci
    - Pierścień, gwiazda, P2P, sieci mieszane
    - Topologie sieciowe na różnych poziomach abstrakcji
- Warstwowy model komunikacji sieciowej
    - Model referencyjny ISO/OSI
    - Warstwy komunikacji (fizyczna, łącza, sieciowa, transportowa, sesji, prezentacji, aplikacji)
    - Model uproszczony TCP/IP
- Technologie i protokoły warstw medium komunikacyjnego
    - Standardy warstwy fizycznej i łącza danych: sieci LAN i standard Ethernet
    - Sieci rozległe WAN
    - Urządzenia sieciowe w warstwie fizycznej i łącza danych (karty sieciowe, repeatery, huby, mostki, switche)
    - Bezprzewodowe sieci LAN i MAN (Wi-Fi, WiMAX)
    - Sieci mobilne (1G, 2G, 3G)
        - Techniki multiplexingu: CMDA, FDMA, itd.
- Sieć Internet - protokoły warstwy sieciowej
    - Enkapsulacja i transmisja danych
    - Protokół IPv4 i adresacja
    - Podsieci i nadsieci
    - Protokół IPv6
    - Odwzorowanie IP-MAC
    - Adresy IP a nazwy symboliczne – system DNS
    - Protokół kontrolny ICMP
- Sieć Internet - protokoły transportowe
    - Transport danych w sieci Internet
    - Porty i gniazda
    - Protokół UDP i TCP
- Warstwa aplikacji - usługi sieciowe
    - Poczta elektroniczna - protokoły SMTP, POP3 i IMAP
    - Transfer plików - protokół FTP i NFS
    - Usługi informacyjne - protokół HTTP i NNTP

EITC/CN/SCN2

Bezpieczne sieci komputerowe 2

Szczegółowa zawartość programowa kursu (15 godz.):

- Standard Ethernet
    - Podstawy działania
    - Ramka Ethernet
    - Protokół MAC
        - Protokół CSMA/CD
        - Błędy transmisji
        - Negocjowanie trybu pracy
    - Zasady budowy systemu Ethernet
        - Repeatery
        - Koncentratory (ang. hub)
        - Mosty (ang. bridge)
        - Przełączniki sieciowe (ang. switch)
        - Redundancja połączeń sieciowych
- Fizyczne media komunikacyjne
    - Kable elektryczne
        - Kable typu skrętka
        - Kabel współosiowy koncentryczny
        - Kategorie kabli miedzianych
        - Sieci oparte na kablu UTP
        - Elementy montażowe
    - Kable światłowodowe
        - Światłowód wielomodowy
        - Światłowód jednomodowy
        - Złącza światłowodowe
- Bezprzewodowe sieci WLAN
    - Pasma łączności radiowej
    - Podstawowe elementy sieci bezprzewodowych
    - Zalety sieci bezprzewodowych
    - Standardy 802.11
    - Zabezpieczenia sieci WLAN
        - WEP, TKIP, WPA, 802.1X, NAC
- Sieci rozległe WAN
    - Sieć Frame Relay
        - Frame Relay w modelu OSI
        - Sprawdzanie błędów w ramkach
        - Typowa infrastruktura sieci FR
        - Format ramki FR
        - Połączenia logiczne FR
        - Zależność szybkości transmisji danych w kanałach od wartości CIR i EIR
        - Sterownie przeciążeniami
        - Dane audio/video w sieciach FR
        - Protokół LMI
    - ATM Asynchronous Transfer Mode
        - Urządzenia ATM
        - Adresy ATM
        - Rodzaje połączeń
        - Budowa komórki
        - Model sieci ATM

- Interfejsy ATM
- Protokół ILMI
- Protokół PNNI
- ATM a sieci komputerowe
- Standard LANE
- Połączenia ATM w LANE 1.0
- LANE 2.0
- IP Over ATM
- Uzyskiwanie adresu IP
- Protokół ARP
- Protokół BOOTP
- Protokół DHCP
- DNS
- Historia systemu DNS
- Budowa i działanie systemu DNS
- Struktura nazw
- Serwery DNS
- Rozwiązywanie nazw DNS
- Konfiguracja resolvera DNS w systemach operacyjnych
- Konfiguracja serwera DNS
- Routing IP
- Routing statyczny
- Routing dynamiczny
- Podział ze względu na zasięg działania
- Podział ze względu na sposób wyznaczania trasy
- Przykłady protokołów routingu dynamicznego
- Wymagania dotyczące protokołów routingu
- Metryki routingu
- Protokół RIPv1
- Protokół RIPv2
- Sposoby unikania pętli routingu
- Protokół OSPF
- Protokół EIGRP
- Protokół BGP

EITC/IS/ACNS

Zaawansowane bezpieczeństwo sieci informatycznych

Szczegółowa zawartość programowa kursu (15 godz.):

- Podstawowe problemy bezpieczeństwa sieci komputerowych
    - Warstwa sieciowa
    - Warstwa transportowa
    - Warstwa aplikacyjna
    - Typowe ataki na infrastrukturę sieciową
    - Ataki Denial of Service (DoS)
        - Przegląd ataków DoS
        - Metody obrony przed atakami DoS/DDoS
    - Mechanizmy bezpieczeństwa zdalnego dostępu
    - Narzędzia bezpieczeństwa
- Tunele wirtualne VPN
    - Konfiguracje sieci VPN
    - Protokół IPsec
        - Tryby pracy protokołów IPsec
        - Protokół AH (Authentication Header)
        - Protokół ESP (Encapsulating Security Payload)
        - Asocjacja bezpieczeństwa (Security Association)
        - Zarządzanie kluczami
        - Ograniczenia
        - IPsec w Windows
        - Bezpieczeństwo w IPv6
    - Propagowanie połączeń aplikacyjnych (port forwarding)
    - Tunele SSL
- Zapory sieciowe i translacja adresów
    - Podstawowe funkcje systemów firewall
    - Podstawowe komponenty systemów firewall
        - Router filtrujący
        - Komputer Twierdza
        - Strefa Zdemilitaryzowana
    - Translacja adresów – Network Address Translation (NAT)
    - Dodatkowa funkcjonalność zapór sieciowych
    - Problemy realizacji zapór sieciowych
- Metody atakowania aplikacji WWW i mechanizmy ich ochrony
    - Kradzież kodu źródłowego
    - Pola ukryte HTML
    - Zmienne Cookies
    - Path Traversal
    - SQL Injection
    - Przejęcie sesji
    - Denial of Service (DoS)
    - Podsumowanie
- Systemy programowych zapór sieciowych i systemy wykrywania włamań IDS
    - Programowe zapory sieciowe
    - Zapora sieciowa netfilter/iptables
        - Konfiguracja iptables
        - Translacja adresów
        - Moduły rozszerzające IPTABLES
        - Krótkie opisy celów (TARGETs)

        - Informacje dodatkowe
        - Przykłady
    - Wbudowana zapora osobista w systemach Windows
    - Systemy wykrywania włamań
    - System Snort
- Bezpieczna konfiguracja serwera HTTP na przykładzie Apache
    - Serwer Apache
    - Dziennik serwera Apache
    - Ścieżki logiczne i fizyczne
    - Dyrektywy blokowe
    - Ochrona dostępu wg adresów
    - Ochrona dostępu poprzez uwierzytelnianie użytkowników
    - Połączenia HTTPS
    - Podsumowanie
- Tworzenie sieci VPN w środowisku Linux i Windows
    - Zastosowania technologii VPN
    - Oprogramowanie OpenVPN
        - Podstawy działania
        - Połączenie VPN Linux - Linux z wykorzystaniem mechanizmu współdzielonego klucza
        - Połączenie VPN Linux - Linux z wykorzystaniem mechanizmu certyfikatów cyfrowych
        - Połączenie VPN Linux - Windows z wykorzystaniem mechanizmu współdzielonego klucza
        - Podsumowanie możliwości programu OpenVPN
    - Oprogramowanie Openswan
        - Protokół IPsec
        - Budowanie sieci VPN z użyciem oprogramowania Openswan
- Spoofing
    - Rodzaje spoofingu
        - IP spoofing (Internet Protocol spoofing)
        - Web spoofing
        - E-mail spoofing
        - DNS spoofing
        - Caller ID spoofing
        - SMS spoofing
    - IP spoofing – podstawy teoretyczne

EITC/IS/QCF

Kryptografia kwantowa

Szczegółowa zawartość programowa kursu (15 godz.):

- Klasyczne podejście do bezpiecznego przesyłania informacji
  - Ogólna koncepcja bezpiecznych kanałów informacyjnych
  - Kryptografia z kluczem prywatnym
  - Kryptografia z kluczem publicznym
  - Uwierzytelnianie
  - Kanały z szumem – detekcja i korekcja błędów
  - Słabości kryptografii klasycznej
- Koncepcja absolutnie bezpiecznych kanałów kwantowych
  - Informacja kwantowa
    - Podstawowe idee informacji kwantowej (pojęcie qbitu, twierdzenie No-Cloning)
    - Kwantowe przetwarzanie informacji w praktyce
  - Wykorzystanie mechaniki kwantowej do ochrony informacji klasycznej
- Kwantowa dystrybucja klucza
  - Kwantowa dystrybucja klucza bez splątania
    - Kluczowe własności spolaryzowanych fotonów
    - Protokół BB84
    - Protokół B92
  - Kwantowa dystrybucja klucza ze splątaniem
    - Splątanie kwantowe i twierdzenie Bella
    - Protokół splątaniowy Ekerta
- Bezpieczne kanały informacyjne z wykorzystaniem QKD
  - Potencjalne ataki na schemat kwantowej dystrybucji klucza
  - Kanały kwantowe z szumem
  - Wzmacnianie prywatności
  - Uwierzytelnianie
  - Kompletny schemat bezpiecznej komunikacji
  - Teoretyczna analiza bezpieczeństwa
- Praktyczne realizacje kryptografii kwantowej
  - Praktyczne realizacje kryptografii kwantowej
  - Sieć kwantowa DARPA
    - Struktura sieci
    - Zaimplementowane technologie
    - Warstwa programowa sieci
    - Rozszerzenia protokołu IPSec
  - Projekt SECOQC
  - Rozwiązania komercyjne
- Inne zastosowania i podsumowanie
  - Inne zastosowania mechaniki kwantowej w kryptografii
    - Zobowiązanie bitowe i kwantowy rzut monetą
    - Generatory liczb losowych
  - Nietypowe alternatywne próby uzyskania odpornych na podsłuch kanałów informacyjnych – protokół Kisha
  - Przyszłość kryptografii kwantowej
  - Podsumowanie

EITC/IS/FAIS

Formalne aspekty bezpieczeństwa informacji

Szczegółowa zawartość programowa kursu (15 godz.):

- Wstęp do bezpieczeństwa i zagrożeń informatycznych
    - Bezpieczeństwo informatyczne i zagrożenia
    - Normy i polityki bezpieczeństwa
- Standardy i normy bezpieczeństwa informatycznego
    - ITIL (BS 15000, ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 27001:2005, ISO/IEC 27002:2005, Basel I, Basel II, BS 7799-1, BS 7799-2, BS 7799-3:2006, ISO/IEC 17799:2005)
    - Rekomendacja D GINB
    - Metodyka TISM
    - Metodyka OSSTM
    - PAS-56
    - PAS-77:2006
    - PAS 99 :2006
    - BS 25999
    - ISO 28000 - zarządzanie bezpieczeństwem łańcucha dostaw
    - COSO
    - COSO II
    - SOX
    - COBIT
    - ISO/IEC TR 18044
    - ISO/IEC 24762:2008
    - ISO/IEC 15408
    - ISO/IEC TR 13335
    - ISO 19011:2002
    - PN-I-02000:2002
    - ISO Guide 73:2002
- Uwarunkowania prawne
    - Ustawa o ochronie danych osobowych
    - Ustawa o statystyce publicznej
    - Ustawa o zwalczaniu nieuczciwej konkurencji
    - Ustawa o elektronicznych instrumentach płatniczych
    - Kodeks karny
    - Ustawa o ochronie informacji niejawnych
    - Ustawa – Prawo telekomunikacyjne
    - Ustawa – Prawo bankowe
    - Ustawa o narodowym zasobie archiwalnym i archiwach
    - Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne
    - Ustawa o świadczeniu usług drogą elektroniczną
    - Ustawa o ochronie osób i mienia
    - Ustawa o podpisie elektronicznym
    - Ustawa o ochronie baz danych
    - Ustawa o prawie autorskim i prawach pokrewnych
- Modele licencyjne oprogramowania
    - EULA
    - Projekt GNU (Gnu's Not Unix!)
        - Wolne oprogramowanie
        - Copyleft
        - Fundcja Wolnego Oprogramowania (Free Software Foundation)
        - GNU/Linux

        - Wolna dokumentacja
        - Open Source
        - Licencja GNU GPL
        - Licencja GFDL
    - Inne rodzaje licencji
        - Licencja BSD
        - Licencja X11
        - Licencja typu Linux
        - Licencja typu Public Domain
        - Licencja Demo
        - Licencja Freeware
        - Licencja Shareware
        - Licencja grupowa
        - Licencja Adware
        - Licencja Firmware
        - Licencja OEM
        - Licencja MOLP
        - Licencja BOX
- Audyt bezpieczeństwa informatycznego
    - Wprowadzenie
    - Zasady projektowania bezpiecznych systemów
    - Model STRIDE
        - Idea modelu STRIDE
        - Data Flow Diagrams
        - Budowanie modelu zagrożeń w metodologii STRIDE

EITC/IS/IST

Teoria bezpieczeństwa informatycznego

Szczegółowa zawartość programowa kursu (15 godz.):

- Definicja informacji (stan klasyczny, źródło wiadomości)
    - Jednostka (bit) i inne jednostki informacji
    - Miara (entropia Shannona)
    - Teoria grafów
    - Prawdopodobieństwo warunkowe
        - Twierdzenie Bayesa
- Ciągi losowe i ciągi pseudolosowe
    - Znaczenie losowości dla bezpieczeństwa
- Wprowadzenie do kodowania
    - Rodzaje kodów
    - Kody Humminga
    - Kompresja
        - Stratna
        - Bezstratna
    - Twierdzenia Shannona
- Kanały komunikacyjne
    - Kanały bezstratne
    - Kanały stratne
        - Rodzaje szumów informacyjnych
    - Procedury korekty błędów
- Podstawowe pojęcia informatyki (algorytm, algebra, język, gramatyka)
- Teoria złożoności obliczeniowej
    - Klasy problemów matematycznych
        - Klasa problemów wielomianowych (P)
        - Klasa problemów wykładniczych (NP)
    - Kontekst kryptografii asymetrycznej
- Modele obliczeniowe
    - Maszyny stanów (Turinga, DAS, NDAS)
        - Twierdzenie Churcha-Turinga
    - Algebra Boole'a i klasyczna teoria układów logicznych
        - Bramki klasyczne
        - Uniwersalność
        - Brak odwracalności binarnej informatyki
        - Realizacje algorytmów
    - Probabilistyczny model obliczeniowy
        - Klasa problemów NBP
        - Rozszerzone twierdzenie Churcha-Turinga
        - Realizacje algorytmów
    - Kwantowy model obliczeniowy
        - Klasa problemów NQP
        - Kwantowa teoria układów logicznych
        - Realizacje algorytmów
        - Fundamentalne zagrożenie kryptografii asymetrycznej
            - Kwantowa transformata Fouriera
            - Algorytm Shora i grupy Kitaeva

EITC/QI/QIF

Informatyka kwantowa w kontekście bezpieczeństwa

Szczegółowa zawartość programowa kursu (15 godz.):

- Wprowadzenie do mechaniki kwantowej
    - Formalizm informatyki kwantowej
        - Przestrzeń Hilberta
        - Funkcje falowe i wektory (ortogonalne i nieortogonalne)
        - Baza
        - Operatory unitarne i hermitowskie
        - Rozkład spektralny
        - Notacja Diraca
    - Postulaty
        - Stan kwantowy
        - Ewolucja unitarna i równanie Schrödingera
        - Pomiar kwantowy (rzutowanie von Neumana)
        - Iloczyn tensorowy i splątanie kwantowe
- Kwantowy paradygmat informacji
    - Definicja (stan kwantowy, źródła wiadomości)
    - Jednostka (qubit), sfera Blocha
    - Splątanie qubitów, stany Bella
    - Miara splątania i informacji kwantowej (entropia von Neumanna)
    - Pomiar kwantowy qubitów
- EPR i złamanie zasady realizmu lub lokalności
    - Nierówności Bella
    - Teleportacja kwantowa
- Kwantowa teoria obwodów
    - Bramki kwantowe
        - Bramki jednoqubitowe (Pauliego, Hadamarda, Fazy)
        - Bramki wieloqubitowe (CNOT, Toffola)
    - Zbiór uniwersalny (CNOT i bramki jednoqubitowe)
    - Odwracalność
    - Realizacja algorytmów kwantowych
        - Układ realizujący kwantową transformatę Fouriera – wykładnicze przyspieszenie
        - Układ realizujący teleportację kwantową
- Kwantowe aspekty bezpieczeństwa
    - Algorytm faktoryzacji Shora
    - Twierdzenia no-cloning, no-deleting, no-broadcasting
    - Kwantowa dystrybucja klucza QKD
- Realizacje praktyczne komputera kwantowego
    - Dekoherencja
    - Kryteria DiVincenzo
    - Technologia pułapkowanych jonów
    - Technologia NMR
    - Technologia kropek kwantowych
        - Orbitalne stopnie swobody
        - Spinowe stopnie swobody
    - Topologiczne stopnie swobody

EITC/FC/CCT

Złożoność obliczeniowa jako podstawa bezpieczeństwa informacji

Szczegółowa zawartość programowa kursu (15 godz.):

- Wprowadzenie i model obliczeniowy oparty o maszynę Turinga
    - Model obliczeń
    - Maszyna Turinga
        - Definicja formalna
        - Działanie
        - Reprezentacja
    - Język maszyny. Języki rekurencyjne i rekurencyjnie przeliczalne
    - Zapis programu i stanu maszyny
    - Zasoby potrzebne do obliczenia maszyny
    - Wielotaśmowa maszyna Turinga
    - Niedeterministyczna maszyna Turinga
- Inne modele dla złożoności
    - Maszyna RAM
        - Zestaw instrukcji
        - Działanie maszyny RAM
        - Rozpoznawanie języków
        - Złożoność obliczeniowa w modelu RAM
        - Porównanie czasu działania maszyny Turinga i maszyny RAM
        - Symulowanie maszyny RAM na wielotaśmowej maszynie Turinga
        - Porównanie złożoności pamięciowej w modelach obliczeniowych
    - Obwody logiczne
- Klasy złożoności obliczeniowej
    - Klasy złożoności czasowej i pamięciowej
    - Twierdzenia o liniowym przyspieszaniu i kompresji pamięci
    - Relacje między klasami, twierdzenie Savitcha
    - Dopełnienia klas
    - Twierdzenia o hierarchii czasowej i pamięciowej
- Redukcje, zupełność oraz problemy NP-zupełne
    - Redukcje wielomianowe, logarytmiczne i transformacje
        - Redukcje wielomianowe
        - Redukcje logarytmiczne
        - Transformacja wielomianowa w sensie Turinga
    - Zupełność
    - Klasa NP i NP-zupełność
        - Problem SAT
        - Charakteryzacja klasy NP w języku logiki
        - Egzystencjalne zdania drugiego rzędu a złożoność
        - Twierdzenie Fagina
    - Problem SAT
        - 3SAT
        - MAXSAT
    - NP-zupełne problemy grafowe
        - Pokrycie wierzchołkowe
        - Klika, zbiór niezależny
    - Problemy na zbiorach i liczbach
        - Trójdzielne skojarzenie i pokrycie zbiorami
        - Suma podzbioru i inne problemy liczbowe
- Algorytmy i schematy aproksymacji

- Problem optymalizacyjny
    - Problemy optymalizacyjne a problemy decyzyjne
    - Rozwiązania aproksymacyjne
  - Pokrycie wierzchołkowe NODE COVER
    - Algorytm zachłanny
    - Algorytm skojarzeniowy
  - Problem maksymalnego przekroju MAX CUT
  - Problem komiwojażera TSP
    - Wersja metryczna
  - Pakowanie BIN PACKING
    - 2-aproksymacja
  - Problem plecakowy KNAPSACK
  - Schematy aproksymacji
  - Schemat aproksymacji dla problemu KNAPSACK
  - Asymptotyczny PTAS dla BIN PACKING
  - L-redukcje
- Algorytmy probabilistyczne
  - Probabilistyczne klasy złożoności
    - Klasa ZPP
    - Klasa PP
    - KLASA BPP
  - Rozpoznawanie liczb pierwszych
    - Test Millera-Rabina
  - Generowanie bitów losowych
- Obliczenia równoległe
  - Modele obliczeń równoległych
    - PRAM
    - Obwody logiczne
  - Klasy złożoności
    - Model obwodów logicznych
    - Klasy w modelu PRAM
  - P-zupełność
  - Równoległość i randomizacja
- Problemy funkcyjne i złożoność zliczania
  - Problemy funkcyjne
    - Klasy FP i FNP
    - Klasa TFNP
  - Złożoność zliczania
    - Klasa 'hasz P' i twierdzenie Valianta
    - Klasa 'parzystość P'
- Pamięć logarytmiczna, hierarchia wielomianowa, pamięć wielomianowa i złożoność wykładnicza
  - Klasy L, NL i coNL
  - Twierdzenie Immermana-Szelepcsényi'ego
  - Klasy coNP i DP
  - Maszyny alternujące
  - Hierarchia wielomianowa
  - Klasa PSPACE
  - Problemy PSPACE-zupełne
    - Optymalizacja periodyczna
  - Złożoność wykładnicza
    - Problemy zwięzłe
    - Wyrażenia regularne
- Kryptografia a złożoność
  - Funkcje jednokierunkowe
  - Systemy dowodów interaktywnych