Sisteme Avansate de Securitate (Advanced Cybersecurity)

Descriere

Pregătirea de experți în domeniul securității cibernetice oferă cadrul necesar implementării corecte a instrumentelor de securitate la nivelul organizațiilor. Guvernanța electronică impune standarde de securitate cibernetică concomitent cu apariția, unor noi vulnerabilități, riscuri și amenințări la adresa securității organizațiilor. Necesitatea existenței unor experți în domeniul securității cibernetice se impune de la sine într-o societate în care informația electronică este atotcuprinzătoare.

Relevanță pentru piața muncii

Absolvenții programului de masterat activează în cadrul unor companii de prestigiu din țară și străinătate, în cadrul instituțiilor guvernamentale din România și Uniunea Europeană, care au responsabilități în domeniul securității cibernetice. Absolvenții pot alege o carieră în cercetare, prin studii doctorale în cadrul grupurilor de cercetare din UPB, cu rezultate excelent în ultimii ani (articole științifice, proiecte, colaborări, concursuri) sau a altor universități de prestigiu din țară sau străinătate.

Cunoștințe necesare

Programul Sisteme Avansate de Securitate (Advanced Cybersecurity) este recomandat absolvenților domeniului fundamental de Științe Inginerești, domeniului de studii universitare de licență Calculatoare și Tehnologia Informației și specialiștilor din domeniul Științei Calculatoarelor.

Competențe și abilități dobândite

Definirea specifică a conceptelor ce caracterizează securitatea cibernetică. Identificarea vulnerabilităților, riscurilor și amenințărilor de securitate cibernetică la nivelul organizației. Securizarea sistemelor la toate nivelurile: hardware, software, infrastructură, politici. Proiectarea și dezvoltarea de componente software și hardware ținând cont de riscurile de securitate la care sunt supuse. Specificul securității pentru sisteme de uz general, dispozitive mobile, sisteme cloud, dispozitive IoT. Proiectarea procedurilor de securitate și protecție cibernetică. Elaborarea politicii de securitate cibernetică în cadrul organizației. Elaborarea și implementarea planului de răspuns la incidente de securitate cibernetică.

Materii

Sem 1: Criptografie aplicată; Protocoale de securitate; Tehnologii de protecție a vieții private; Securitatea sistemelor informaționale; Cercetare

Sem 2: Securitatea în sistemele cloud și grid; Cyber defense și cyber intelligence. Tehnici de securitate cibernetică; Securitatea dispozitivelor mobile; Disciplină la alegere 1; Cercetare științifică și practică

Sem 3: Proiectarea dispozitivelor criptografice folosind FPGA; Managementul incidentelor de securitate cibernetică; Managementul securității informației; Disciplină la alegere 2; Cercetare științifică și practică

Sem 4: Cercetare științifică, practică de cercetare și elaborare disertație; Etică

Tehnologii folosite și cuvinte cheie

criptografie, inginerie inversă, exploatare, auditare, verificare software, cyberintelligence, malware, politici de securitate, standarde de securitate, strategii de securitate, online banking, privacy, PKI, forensics, monitorizare, Android, iOS, virtualizare, unit testing, SMSI

Teme de cercetare (exemple)

Investigarea scurgerilor de date private în iOS; Implementarea și analiza schemelor de mascare pe dispozitive tip SoC; Augmentarea securității unikernelurilor; Sisteme de detectare a intruziunilor (IDS) pentru rețele IoT; Programare folosind contracte în limbajul D; Securizarea sistemului AirDocs; Evaluarea securității aplicațiilor interconectate de tip smart home; Îmbunătățirea implementării bhyve pe arm64; Virtualizare eficientă folosind unikerneluri; Îmbunătățirea ruterelor de tip Onion (Tor)

Alte informații

Limba de predare: Engleză