

Facilități

Cardul de student, care ține locul legitimației de student, asigură accesul la Bibliotecă, în căminele ULBS și la alte facilități oferite (wireless, copiere xerox etc.), precum și plata în cantinele și cafeteriile universității.

My Account include servicii de webmail, webspace și acces gratuit la internet wireless în tot campusul ULBS.

Website-ul este disponibil la adresa www.ulbsibiu.ro

Serviciul UMS oferă posibilitatea vizualizării online a situației școlare.

Platforma de e-learning facilitează interacțiunea online profesor-student, accesul la suporturile de curs aferente ș.a.

Biblioteca universității

Biblioteca deține aprox. 670.000 de unități documentare, 15.000 de volume periodice și abonamente la importante baze de date electronice. De asemenea, instituția dispune de un catalog online pentru cercetare bibliografică, de săli cu acces liber la raft, organizate pe domenii, într-un sediu nou și modern, precum și de 415 locuri pentru studiu, dotate cu echipamente de conectare la Internet, calculatoare, scanere, imprimante și multifuncționale.

Competențe

Competențe profesionale

C4. Îmbunătățirea performanțelor sistemelor hardware, software și de comunicații.

Competențe transversale

CT1. Comportarea onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei.

CT2. Identificarea, descrierea și derularea proceselor din managementul proiectelor, cu preluarea diferitelor roluri în echipă și descrierea clară și concisă, verbal și în scris, în limba română și într-o limbă de circulație internațională, a rezultatelor din domeniul de activitate.

CT3. Demonstrarea spiritului de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.

T: +40-(269) 21-79.28 F: +40-(269) 21-27.16 E: inginerie@ulbsibiu.ro W: inginerie.ulbsibiu.ro

Str. Emil Cioran, Nr.4, Sibiu, 550025, România



Facultatea de Inginerie

Securitatea Sistemelor Informatice

Program postuniversitar de specializare

Cyber security →

inginerie.ulbsibiu.ro



Universitate de stat acreditată
de către ARACIS cu calificativul
Grad de Încredere Ridicat

Universitatea „Lucian Blaga” din Sibiu este o universitate dinamică, iar aceasta se observă în întreaga sa istorie.

Edificată pe tradiția celor 230 de ani de învățământ superior sibian, Universitatea „Lucian Blaga” din Sibiu este, la ora actuală, una dintre cele mai performante universități din România.

Calitatea învățământului și a cercetării din ULBS este recunoscută și recompensată de organisme de evaluare ale statului român, ULBS fiind un centru academic de excelență și printre puținele universități din țară care au acreditat cercetarea științifică.

Promovând valori precum spiritual antreprenorial și inovativ, cercetarea de calitate și deschiderea, ULBS încurajează studenții să-și dezvolte creativitatea și potențialul, pregătindu-i și sprijinindu-i pentru dezvoltarea unei cariere de succes.

Facultatea de Inginerie

Facultatea de Inginerie este o școală politehnică cu o tradiție și experiență care au consacrat-o în țară și în lume.

Misiunea sa principală este aceea de a pregăti specialiști de nivel universitar în diverse domenii ale științelor ingineresti.

Reprezentând spiritul antreprenorial al Universității „Lucian Blaga” din Sibiu la cel mai înalt nivel, Facultatea de Inginerie are strânse colaborări cu principalii reprezentanți ai mediului de afaceri sibian, asigurând prin acestea atât o bază materială excelență și mediul propice pentru dezvoltarea abilităților practice ale studenților, cât și o resursă umană extrem de bine pregătită în raport cu necesitățile pieței muncii.

În plus, Facultatea de Inginerie dezvoltă o importantă activitate de cercetare pentru și în colaborare cu acești parteneri, ridicând nivelul educațional al facultății la standarde internaționale.

Structura pe module

Plan de învățământ

| Modul 1 | 5 săptămâni | ore C | L | Nr. credite | Forma de evaluare |
|---|--------------------|----------------------------|------------|-------------------------|-----------------------|
| Introducere în securitate cibernetică | | 10 | 10 | 2 | Examen |
| Securitatea cibernetică a sistemelor informatice | | 20 | 0 | 2 | Verificare pe parcurs |
| Elemente de legislație cibernetică | | 10 | 0 | 1 | Examen |
| Standarde și protocoale de securitate | | 10 | 10 | 2 | Examen |
| Sesiune de examinare | 1 săptămână | | | | |
| Modul 2 | 5 săptămâni | ore C | L | Nr. credite | Forma de evaluare |
| Elemente de criptografie | | 10 | 10 | 2 | Examen |
| Securitatea cibernetică a sistemelor informatice | | 20 | 0 | 2 | Verificare pe parcurs |
| Securitatea aplicațiilor Web | | 10 | 10 | 2 | Examen |
| Software malitios | | 10 | 10 | 2 | Examen |
| Sesiune de examinare | 1 săptămână | | | | |
| Modul 3 | 5 săptămâni | ore C | L | Nr. credite | Forma de evaluare |
| Securitatea cibernetică a dispozitivelor mobile | | 10 | 10 | 2 | Examen |
| Modalități de prevenție în spațiul virtual | | 10 | 0 | 1 | Verificare pe parcurs |
| Auditul sistemelor informatice și managementul riscurilor de securitate | | 10 | 10 | 2 | Examen |
| Tratarea incidentelor de securitate și investigarea datelor digitale | | 10 | 10 | 2 | Examen |
| Sesiune de examinare | 1 săptămână | Total | 200 | 20 | |
| Examen de absolvire | 1 săptămână | Taxa de școlarizare | | 3.000 lei / curs | |



În contextul actual, în care sistemele informatice sunt supuse la multiple amenințări, iar datele personale ale utilizatorilor sunt privite ca produse ce pot fi tranzacționate pe piață, este necesar ca la nivelul sistemelor informatice să fie asigurată o minimă securitate și să existe o informare a utilizatorilor în privința riscurilor existente. Astfel, securitatea cibernetică trebuie privită din perspectiva rolului pe care sistemul îl are în cadrul infrastructurii (cerere de servicii, oferire de servicii, echipamente de rețea), fiecare rol necesitând diferite soluții și metode de asigurare a securității.

Uneori suntem prezenți în spațiul virtual, chiar dacă nu suntem conștienți de acest lucru, doar prin simplul fapt că deținem sau interacționăm cu echipamente "inteligente", care comunică GSM, bluetooth, WiFi sau NFC. Date pur statistice sau cu caracter confidențial, legate de persoane fizice și juridice sunt permanent generate, colecționate, stocate sau comercializate.

Desigur, există limitări legale care reglementează unele dintre aceste aspecte, dar dincolo de acțiunile și atribuțiile autorităților abilitate, este de datoria fiecăruia dintre noi să adoptăm o conduită preventivă în interacțiunea inevitabilă cu mediul virtual. Doar cunoscând valoarea urmelor informatice generate de fiecare dintre noi, precum și modul în care acestea pot fi utilizate fără acordul, dar mai ales în detrimentul nostru, vom putea prevedea în bună măsură posibile consecințe mai puțin dorite.

Domeniul securității cibernetică a început să capete noi dimensiuni odată cu creșterea gradului de automatizare a nivelului tehnologic și extinderea și amplificarea amenințărilor / atacurilor cibernetică. Administratorii de securitate din orice organizație au misunea dificilă de a încerca să facă față tuturor amenințărilor cibernetică cu care se confruntă și de a minimiza posibilitățile de compromitere a infrastructurii IT. În acest sens, este necesar a fi optimizat procesul de monitorizare a evenimentelor de securitate, în scopul prevenirii, detecției și răspunsului la incidentele de securitate cibernetică.

Scopul principal al acestui demers este formarea de specialiști în domeniul securității cibernetică, prin dezvoltarea unui program de studii la nivel postuniversitar. Propunerea dezvoltării unui program de studii postuniversitare vine în contextul tendințelor actuale de creștere a manifestării unor riscuri, vulnerabilități și amenințări în domeniul securității cibernetică la adresa organizațiilor și instituțiilor guvernamentale și private sau de interes strategic național.

Situația prezentată incumbă, pe de altă parte, o oportunitate deosebită pentru România, de constituire a unui corp profesional distinct, de specialiști în domeniul securității cibernetică, care să participe activ la creșterea industriei autohtone în domeniul Cyber Security, complementar industriei IT&C clasice, și implicit la creșterea securității naționale a României în acest domeniu. La nivelul pieței private și instituțiilor publice se constată o criză acută de specialiști în domeniul Cyber Security. Industria IT&C produce peste 6% din PIB-ul României. Industria Cyber Security, corect alimentată cu specialiști, poate contribui de asemenea semnificativ la PIB-ul țării.



Competențele dobândite la finalizarea cursului pot duce la ocuparea următoarelor posturi:

1. Manager securitatea informației / Chief Information Security Officer - CISO (cod COR 121118).

- Stabilește strategia și obiectivele în domeniul securității informației, armonizate cu strategia organizației;
- Stabilește cadrul de management al securității informației;
- Stabilește domeniul de securitate și managementul resurselor informaționale;
- Planifică sistemul de management al securității informației pe baza riscurilor și cerințelor;
- Managementul accesului la resurse și informații;
- Proiectează măsurile de securitate în procesele operaționale, IT&C și ale organizației în concordanță cu analiza de risc la securitatea informației;
- Consiliază conducerea organizației cu privire la sistemul de management al securității informațiilor;
- Gestionează incidentele de securitate a informației;
- Evaluează sistemul de management al securității informației;
- Aplică instrumentele și metodele de îmbunătățire a eficacității sistemului de management al securității informației.

2. Specialist în proceduri și instrumente de securitate a sistemelor informatice (cod COR 213908).

- Elaborează și aplică elemente din programul de securitate, inclusiv cele referitoare la securitatea fizică a datelor, asigură confidențialitatea informațiilor și disponibilitatea lor pentru persoanele în drept să le obțină și să le folosească;
- Identifică și evaluează vulnerabilitățile sistemului informatic, identifică amenințările potențiale, evaluează și prioritizează pierderile și acțiunile îndreptate către reducerea amenințărilor și a pierderilor de orice fel;
- Găsește răspunsurile la violările de securitate identificate și raportate;
- Proiectează politici și proceduri de securitate aplicabile sistemului informatic;
- Elaborează ghiduri de bună practică legate de cerințele de securitate ale sistemului informatic și de măsurile necesare pentru protejarea sistemului;
- Aplică standardele de securitate pentru rețele și calculatoare și validează din punctul de vedere al securității sistemul informatic (soluția IT&C aflată în funcțiune);
- Monitorizează / supraveghează aplicarea măsurilor de securitate proiectate pentru protejarea bunurilor fizice, a aplicațiilor și a altor produse software, a datelor și colecțiilor de date față de utilizarea neautorizată;
- Analizează și revizuieste amenințările, vulnerabilitățile, politicile, procedurile și instrumentele legate de asigurarea securității sistemului informatic;
- Elaborează rapoarte legate de asigurarea securității sistemului informatic, de gradul de aplicare a măsurilor de securitate stabilite, de vulnerabilitățile cunoscute și asumate.

