UNIVERSITATEA POLITEHNICA DIN BUCUREŞTI
FACULTATEA DE AUTOMATICĂ ŞI CALCULATOARE
Splaiul Independenţei, nr. 313, sector 6, 060042 Bucureşti
Tel: 021-4029179; Fax: 021-410 1044; http://www.acs.pub.ro

Prezentarea programului de studii de masterat "Advanced Cybersecurity" (AC)

1. Misiunea programului AC

Programul de studii universitare de masterat **"Advanced Cybersecurity" (AC)** asigură pregătirea pe nivelul 7 al EQF (ciclul II Bologna – studii de masterat) pentru studenţii care au absolvit ciclul de licenţă al programului de studii Tehnologia informaţiei, din domeniul Calculatoare şi tehnologia informaţiei.

Programul de studii universitare de masterat **"Advanced Cybersecurity" (AC)** îşi asumă misiunea de a pregăti specialişti in domeniul Calculatoare şi Tehnologia Informaţiei, capabili de a utiliza cunoştinţe ştiinţifice, tehnice şi cultural-umaniste valoroase, de a contribui la progresul tehnologic, economic si social-cultural al societăţii româneşti şi al lumii contemporane şi de se integra în societatea cunoaşterii.

În contextul dezvoltării exponenţiale a Internet-ului şi a tehnologiilor aferente, conectivităţii şi a celei de-a patra revoluţie Industrială, competenţele legate de proiectarea şi implementarea securităţii cibernetice la nivel organizational, local sau regional sunt fundamentale.

Asigurarea unui set de politici si strategii de securitatea informaţiei precum şi de securitate cibernetică reprezintă un nivel de aşteptare uzual în cadrul organizaţiilor de orice natură (comercială, academică) şi de domeniul de activitate.

O bună pregătire a studenţilor, bazată pe prezentarea conceptelor legate de securitatea cibernetică, infrastructuri critice, securitate informaţională şi pe dobândirea de abilităţi în cadrul activităţilor practice, este o cerinţă de bază în cadrul contextului actual.

Participarea în cadrul unui astfel de program oferă deprinderi utile oricărei persoane cu veleităţi tehnice. Abilităţile de determinare a ameninţărilor, riscurilor şi vulnerabilităţilor de securitate cibernetică şi de gestionare rapidă şi eficientă a sistemelor in cazul unor incidente de securitate cibernetică, transmise în cadrul acestui program, sunt elemente reprezentative în cadrul spectrului tehnic al unui profesionist în domeniu.

Programul de masterat formează specialişti cu pregătire superioară pentru învăţământ, ştiinţă, şi activităţi economice într-un domeniu de mare actualitate şi cu ţintă pe termen lung. În concordanţă cu politica generală a universităţii, programul pregăteşte specialişti pentru integrarea rapidă pe piaţa muncii şi care vor contribui decisiv la dezvoltarea în România a societăţii cunoaşterii şi a conceptelor „smart". Societatea cunoaşterii reprezintă mai mult

decât societatea informaţională; ea este posibilă numai grefată pe societatea informaţională şi nu poate fi separată de aceasta. În acelaşi timp, ea este mai mult decât societatea informaţională prin rolul major care revine informaţiei–cunoaştere în societate.

Programul se adresează în principal studenţilor absolvenţi ai ciclului de licenţă dintr-o facultate de profil din domeniu dar poate fi urmat şi de studenţi absolvenţi ai unor facultăţi cu profil apropiat (de exemplu facultăţi cu profil de electronică şi telecomunicaţii), cursurile la alegere oferind posibilitatea selectării unor discipline complementare care să completeze pregătirea de bază a absolvenţilor unui ciclu de licenţă dintr-un profil apropiat.

Programul de master are o componentă orientată spre cercetare, Ştiinţa Serviciilor fiind un domeniu nou de cercetare, bazat pe sistemele distribuite de scară largă, pe aplicaţii complexe. Studenţii care vor urma cursurile acestui modul de master vor avea posibilitatea de ca colabora cu instituţii externe, autorităţi ale statului şi cu parteneri din industrie pentru elaborarea lucrării finale de disertaţie.

2. Obiectivele programului

Programul de master **“Advanced Cybersecurity” (AC)** urmărește dezvoltarea competențelor profesionale și transversale ale cursanților conform Cadrului European al Calificărilor, pregătind speciali ti de înaltă calificare în domeniul securității cibernetice.

Din punct de vedere profesional, programul de master dezvoltă competențe inginerești privind identificarea vulnerabilităților, riscurilor și amenințărilor cibernetice, precum și competențe ştiinţifice privind realizarea de proiecte de cercetare în domeniu la nivel european. Masterul își propune și dezvoltarea autonomiei profesionale a cursanților și a capacității lor de interacțiune socială, competențe transversale esențiale dezvoltării ulterioare a carierei atât în mediul academic, cât și în mediul industriei IT&C.

Pe măsură ce societatea românească devine o societate a cunoașterii, o societate interdependentă și o societate ,,smart”, tehnologiile informației și ale comunicării vor ocupa un rol tot mai important în asigurarea succesului proiectelor economice, ştiinţifice şi chiar personale. Managementul incidentelor de securitate cibernetică și asigurarea securității informației este un domeniu a cărui relevanță pentru organizațiile contemporane crește continuu, odată cu nivelul de profesionalism necesar. Pe lângă competențe ştiinţifice şi inginereşti de înalt nivel, piața muncii solicită abilități de înțelegere și gestionare a riscurilor, de planificare eficientă a muncii, de estimare a costurilor și beneficiilor unei anumite soluții, de interacțiune în echipe mixte, confruntate cu sarcini complexe. Programul de master pregătește specialiști capabili de performanță inginerească și de inovare în găsirea soluțiilor tehnice și sociale, precum și în cercetarea științifică în domeniu.

Modulul vizează educarea unor specialişti cu înaltă pregătire într-un domeniu foarte actual şi important pentru cercetarea în tehnologia informaţiei, precum şi pentru valorificarea inovării în companiile de profil implicate în dezvoltarea unor produselor informatice cu un grad ridicat de complexitate.

Serviciile electronice constituie baza principalelor aplicaţii de TIC oferite utilizatorilor prin intermediul internetului. Astfel, provocarea cu care se confruntă un manager de securitate a informației/securitate cibernetică nu este doar aceea de monitorizare a sistemelor informationale și de asigurare a securității acestora, ci şi de a realiza integrarea in sisteme complexe, precum infrastructurile critice, care, la randul lor trebuie protejate, asigurand, astfel, securitatea cibernetică, ce devine parte integrantă a securității naționale. Programul acoperă principalele metode folosite pentru criptarea avansată a datelor, cele mai intalnite instrumente și metode de detective și gestionare a atacurilor cibernetice, principiile fundamentale ale securității cibernetice ale unei organizații, vazuta ca entitate de sine statătoare cât și ca parte integrantă a unui sistem intreconectat la nivel lonal, national si chiar regional.

O altă componentă importantă ce se regăseşte în cadrul programului o reprezintă oferirea de tehnici avansate de prevenție și detecție a atacurilor cibernetice, de realizare a auditurilor de securitate și de implementare a sistemelor de management al securității informației. În acest context studenţii au oportunitatea de a cerceta metodele specializate de analiză in profunzime (forensic), folosind echipamente şi unelte dedicate. Studenţii din cadrul acestui program de master vor interpreta impactul diverselor tipuri de atacuri asupra sistemelor informaționale integrate (calculatoare, dispozitive smart, rețele de comunicații etc) prin dezvoltarea uneltelor proprii de monitorizare, detecție și răspuns sau prin integrarea diverselor aplicaţii existente.

O direcţie majoră de cercetare pentru modulul de **“Advanced Cybersecurity” (AC)** o reprezintă crearea de aplicaţii pentru monitorizarea şi detectarea eventualelor anomalii în cadrul sistemelor informatice integrate. În această categorie intră, pe lângă utilizarea principalelor dispozitive sau programe software existente şi o importantă componentă de integrare a acestora, până la crearea de noi aplicaţii software care să corespundă unei anumite politici de imlementare a securității cibernetice pană la nivel de serviciu. Dată fiind evoluţia rapidă a domeniului serviciilor, programul pregăteşte masteranzii în vederea identificării noilor provocări, găsirii metodelor şi instrumentelor potrivite de soluționare, analizei şi îmbunătăţirii performantelor acestor sisteme complexe precum infrastructurile critice.

3. Competenţe profesionale şi transversale

Competenţele profesionale şi transversale definite pentru modulul de master **“Advanced Cybersecurity” (AC)** sunt rezultatul realizării obiectivului general şi contribuie la definirea calificărilor viitorilor absolvenţi. Acestea sunt:

Competenţe profesionale

C.1. Operarea cu concepte şi metode ştiinţifice în domeniul Calculatoare şi Tehnologia Informaţiei

C.2. Cercetare ştiinţifică privind securitatea sistemelor informatice complexe

C.3. Rezolvarea problemelor pe baza metodelor şi tehnologiilor de securizare a sistemelor informatice complexe

C.4. Identificarea vulnerabilităţilor, riscurilor şi ameninţărilor de securitate cibernetică la nivelul organizaţiei/infrastructurii critice

C.5. Conceperea, proiectarea si implementarea planurilor de securitate cibernetică la nivelul organizaţiei/infrastructurii critice

C.6. Proiectarea si implementarea planurilor de auditare, răspuns şi prevenţie la incidente de securitate cibernetică

Competenţe transversale

CT.1. Comportarea onorabilă, responsabilă, etică, în spiritul legii, pentru a asigura reputaţia profesiei

CT.2. Preluarea diferitelor roluri în echipe de proiect şi descrierea clară şi concisă, verbală şi în scris, în limba română şi într-o limbă de circulaţie internaţională, a rezultatelor din domeniul de activitate

CT.3. Demonstrarea spiritului de creativitate, iniţiativăşi acţiune, pentru actualizarea cunoştinţelor profesionale, economice şi de cultură organizaţională

4. Plan de învăţământ

Programul de master **"Advanced Cybersecurity" (AC)** conţine discipline inginereşti de specialitate din domeniul Calculatoare şi Tehnologia Informaţiei, care vizează educarea unor specialişti cu înaltă pregătire într-un domeniu foarte actual şi important pentru cercetarea în calculatoare şi tehnologia informaţiei, precum şi pentru valorificarea inovării în companiile de profil implicate în dezvoltarea unor produselor informatice cu un grad ridicat de complexitate.

Programul se desfăşoară în limba engleză.

Planul de învăţământ a fost întocmit în concordanţă cu Hotărârea de Guvern privind organizarea şi desfăşurarea studiilor universitare de masterat, în concordanţă cu Metodologia de evaluare externă elaborată de ARACIS, în concordanţă cu standardele specifice pentru programele de studii din domeniul fundamental ”Ştiinţe inginereşti” şi cu reglementările stabilite de Senatul UPB.

Programul este organizat pe 4 semestre a câte 14 săptămâni:

- 3 semestre cu activitate didactică, 16 ore didactice pe săptămână şi 12 ore de activitate individuală de cercetare;
- un semestru pentru cercetare si elaborarea lucrării de dizertaţie cu 16 ore de cercetare pe săptămână şi 12 ore pe săptămână pentru elaborarea lucrării de dizertaţie.

Disciplinele la alegere pot fi alese dintre disciplinele obligatorii ale celorlalte programe de master în domeniul Calculatoare şi Tehnologia Informaţiei, organizate de facultate. Se recomandă însă studenţilor, cu prioritate, alegerea unor anumite discipline în fiecare semestru. Cu acordul coordonatorului de program, disciplinele la alegere pot fi alese şi din programe înrudite, inclusiv programe din străinătate în cadrul mobilităţilor studenţilor, cu respectarea numărului de credite.

Modul de evaluare la fiecare disciplină în parte ţine cont de misiunea asumată, de cunoştinţele şi competenţele însuşite în urma parcurgerii disciplinei respective.

Toate disciplinele de predare se încheie cu examen iar activităţile de cercetare ştiinţifică din fiecare semestru se încheie cu un raport de cercetare si o verificare care implică prezentarea raportului de cercetare individual şi a rezultatelor obţinute în activitatea de cercetare. În activitatea de cercetare, studenţii pot lucra la o temă individual sau în echipă. Îndrumătorii temelor de cercetare sunt cadrele didactice implicate în program, în special conducătorii de doctorat. În multe cazuri, temele de cercetare sunt legate de granturi de cercetare ale cadrelor didactice implicate în program.

Cod	**Disciplina**	**Sem**	**C**	**S**	**L**	**P**	**PC**	**Evaluare**
UPB.03.M1.O.08-01	Criptografie aplicată	**I**	2		2		5	E
UPB.03.M1.O.08-02	Protocoale de securitate	**I**	2		2		5	E
UPB.03.M1.A.08-03	Securitatea cibernetică a infrastructurilor critice	**I**	2			2	5	E
UPB.03.M1.A.08-04	Securitatea sistemelor informaționale	**I**	2		2		5	E
	Total activităţi didactice: 16 ore		**8**		**6**	**2**	**20**	
UPB.03.M1.A.08-05	**Cercetare: 12 ore**	**I**	**12**				**10**	P

	TOTAL	**I**	**28**				**30**	
UPB.03.M2.O.08-06	Securitatea în sistemele grid și cloud	**II**	2		2		5	E
UPB.03.M2.O.08-07	Cyberdefense și cyberintelligence. Tehnici de securitate cibernetica	**II**	2		2		5	E
UPB.03.M2.A.08-08	Securitatea dispozitivelor mobile	**II**	2		2		5	E
UPB.03.M2.A.08-09	Tehnologii de protecție a vieții private	**II**	2		2		5	E
	Total activităţi didactice: 16 ore		**8**		**8**	**-**	**20**	
UPB.03.M2.A.08-10	**Cercetare: 12 ore**	**II**	**12**				**10**	P
	TOTAL	**II**	**28**				**30**	
UPB.03.M3.O.08-11	Proiectarea dispozitivelor criptografice folosind FPGA	**III**	2		1	1	5	E
UPB.03.M3.O.08-12	Managementul incidentelor de securitate cibernetică	**III**	2			2	5	E
UPB.03.M3.O.08-13	Managementul securității informației	**III**	2		1	1	5	E
UPB.03.M3.O.08-14	Disciplina la alegere	**III**	2			2	5	E
	Total activităţi didactice: 16 ore		**8**		**2**	**6**	**20**	
UPB.03.M3.A.08-15	**Cercetare : 12 ore**	**III**	**12**				**10**	P
	TOTAL	**II**	**28**				**30**	
	Total activităţi didactice : 0 ore	**IV**						
UPB.03.M4.O.08-16	**Elaborare lucrare de disertaţie**	**IV**	**12**				**12**	**A/R**
UPB.03.M4.O.08-17	**Cercetare ştiintifică: 16 ore**	**IV**	**16**				**18**	**P**
	Total		**28**				**30**	

Evaluare: E-examen cu nota(1-10); V-verificare pe parcurs cu nota; P-proiect cu nota; A/R – verificare pe parcurs cu calificativul Admis sau Respins

Cod	**Disciplina**	**Sem**	**C**	**S**	**L**	**P**	**PC**	**Evaluare**

UPB.03.M1.O.08-01	Applied Cryptography	**I**	2		2		5	E
UPB.03.M1.O.08-02	Security Protocols	**I**	2		2		5	E
UPB.03.M1.A.08-03	Critical Infrastructure Cybersecurity	**I**	2			2	5	E
UPB.03.M1.A.08-04	Security of Informational Systems	**I**	2		2		5	E
	Total activităţi didactice: 16 ore		**8**		**6**	**2**	**20**	
UPB.03.M1.A.08-05	**Research: 12 ore**	**I**	**12**				**10**	P
	TOTAL	**I**	**28**				**30**	
UPB.03.M2.O.08-06	Security in Cloud and Grid Computing	**II**	2		2		5	E
UPB.03.M2.O.08-07	Cyberdefense and Cyberintelligence. Cybersecurity Techniques	**II**	2		2		5	E
UPB.03.M2.A.08-08	Security of Mobile Devices	**II**	2		2		5	E
UPB.03.M2.A.08-09	Privacy Enhancing Technologies	**II**	2		2		5	E
	Total activităţi didactice: 16 ore		**8**		**8**	**-**	**20**	
UPB.03.M2.A.08-10	**Research: 12 ore**	**II**	**12**				**10**	P
	TOTAL	**II**	**28**				**30**	
UPB.03.M3.O.08-11	Cryptographic Devices Design using FPGA	**III**	2		1	1	5	E
UPB.03.M3.O.08-12	Cybersecurity Incidents Management	**III**	2			2	5	E
UPB.03.M3.O.08-13	Information Security Management	**III**	2		1	1	5	E
UPB.03.M3.O.08-14	Optional Course	**III**	2			2	5	E
	Total activităţi didactice: 16 ore		**8**		**2**	**6**	**20**	
UPB.03.M3.A.08-15	**Research : 12 ore**	**III**	**12**				**10**	P
	TOTAL	**II**	**28**				**30**	
	Total activităţi didactice : 0 ore	**IV**						

UPB.03.M4.O.08-16	**Development of Dissertation Thesis**	**IV**	**12**	**12**	**A/R**
UPB.03.M4.O.08-17	**Research: 16 ore**	**IV**	**16**	**18**	**P**
	Total		**28**	**30**	

Evaluare: E-examen cu nota(1-10); V-verificare pe parcurs cu nota; P-proiect cu nota; A/R – verificare pe parcurs cu calificativul Admis sau Respins

5. Activitatea de cercetare în cadrul programului

Studenţii angrenaţi în program beneficiază de un mediu de cercetare stimulativ şi sunt antrenaţi în activităţi de cercetare fundamentală şi aplicativă, inclusiv pe bază de granturi de cercetare, la nivel naţional şi internaţional. Cercetarea în Catedra de Calculatoare se orientează pe o serie de direcţii prioritare, printre care menţionăm: Sisteme bazate pe Grid pentru rezolvarea problemelor complexe, Sisteme distribuite pe scară larga, Sisteme de cunoştinţe bazate pe semantică, Sisteme multi-agent şi inteligenţă artificială, Sisteme de eLearning şi colaborative mobile.

Planul de cercetare al modulului de masterat **“Advanced Cybersecurity” (AC)**se încadrează în aceste direcţii prioritare de cercetare ale catedrei, cu focus pe cercetări din domeniul securităţii reţelelor, mai ales în dezvoltarea sau utilizarea aplicaţilor, pe extinderea resurselor folosite de către o aplicaţie prin paralelizarea acesteia, sau prin metode de arhitectura cu privire la auditarea şi securizarea calculatoarelor sau a reţelelor de calculatoare. Tematica specifică de cercetare este, evident, corelată cu diferitele granturi de cercetare la nivel naţional şi internaţional câştigate de cadrele didactice implicate în program.

Activitatea de cercetare prevăzuta modulul de master " **Advanced Cybersecurity” (AC)**" este axată pe aplicarea conceptelor și cunoștințelor teoretice din disciplinele studiate pentru soluționarea unor probleme concrete, apelând la tehnologii de ultimă oră. Principalele domenii de cercetare sunt: politicile în securizarea ruterelor și a switchurilor, prevenirea atacurilor de tip DoS, gestionarea dinamică a securității sistemelor locale virtuale, planificarea și implementarea serviciilor de rețea, limitarea și gestionarea riscurilor de securitate a rețelelor informatice.

Activitatea de cercetare are în vedere următoarele obiective principale:

- Familiarizarea masteranzilor cu metodele de cercetare științifică din domeniu și cu etapele realizării unui proiect de cercetare;
- Dezvoltarea competențelor masteranzilor de lucru în echipă în proiecte de cercetare;

- Deprinderea competenţelor necesare redactării şi prezentării publice a unui raport de cercetare.

Menţinerea excelenţei în cercetare este una din priorităţile Catedrei de Calculatoare, cercetarea ştiinţifică fiind orientată pe proiecte şi programe naţionale, europene şi internaţionale. Colectivul Catedrei de Calculatoare, impreună cu specialişti din cadrul ICI Bucureşti, se mândresc cu rezultate recunoscute pe plan internaţional in domenii precum sisteme distribuite, calcul ştiinţific, inteligenta artificiala si multe altele. Activitatea de cercetare din catedră se desfăşoară în cadrul unor laboratoare şi grupuri de cercetare care aparţin Centrului Naţional de Tehnologia Informaţiei.

Centrul Naţional de Tehnologia Informaţiei (CNTI) este parte a Universităţii Politehnica din Bucureşti şi este condus de către Catedra de Calculatoare. Misiunea centrului este de a promova activităţi de cercetare avansată şi inter-disciplinară, de a dezvolta noi paradigme şi direcţii de colaborare între cercetătorii din domeniul Tehnologiei Informaţiei şi cercetători din alte domenii, de a dezvolta potenţialul uman prin programe educaţionale adresate absolvenţilor Facultăţii de Automatică şi Calculatoare (Master, Doctorat, etc.), de a dezvolta o „cultură" locală în domeniul calculului de înaltă performanţă şi de a oferi comunităţilor academice şi din industrie din România accesul local şi la distanţă la o infrastructură puternică de calcul. CNTI dezvoltă proiecte de cercetare, la nivel naţional şi internaţional, în colaborare cu centre şi instituţii similare. El are parteneriate şi cu companii de profil în care facilitează inovarea şi transferul de tehnologie avansată.

Printre temele majore de cercetare ale CNTI, teme care se desfăşoară în cadrul laboratoarelor menţionate, amintim: servicii distribuite pentru agregarea si regăsirea informaţiei, modele de reprezentarea a datelor şi resurselor in sisteme distribuite, actualizarea automată a informaţiilor în baze de date distribuite, managementul în Sisteme Distribuite auto-adaptive, mecanisme de orchestrare si configurare pentru servicii in sisteme distribuite de mari dimensiuni, servicii de contextualizare pentru dispozitive mobile, mecanisme de asigurare a încrederii datelor schimbate în medii mobile, soluţii de agregare a informaţiilor de vizualizare a datelor geografice, sisteme colaborative sigure in medii de tip Cloud, acces sigur la resurse in sisteme Cloud.

In același context, Institutul national de cercetare-dezvoltare in informatică, ICI București, având rezultate remarcabile în activități de cercetare-dezvoltare in domeniul informaticii, detine cloud-ul guvernamental, pe baza caruia cursanți ai programului mastreal vor putea so cunoască sau să aprofundeze cunoștințe privitoare la tehnologii de ultimă generație.

De asemenea, ICI București detine un laborator „Digital forensics" dotat cu dispositive hardware și aplicații software de ultimă generație in domeniul investigațiilor digitale, al detecție posibilelor atacuri cibernetice.

Nu in ultimul rând, ICI Bucureşti pune la dispoziția cursanților un laborator de simulare a scenariilor de atac cybernetic și, intr-un viitor cat mai apropiat, un polygon cybernetic, in completarea cloud-ului guvernamental, pe care studenții să poată studia posibile atacuri cibernetice.

În concluzie, programul de studii universitare de masterat **"Advanced Cybersecurity" (AC)** reprezintă un program care oferă absolvenţilor o pregătire ştiinţifică şi tehnica modernă, de calitate şi competitivă, este perfect încadrat în politica Universităţii POLITEHNICA din Bucureşti și a Institutului national de cercetare-dezvoltare in informatică ICI Bucureşti, atât din punct de vedere al conţinutului şi structurii, cât şi din punct de vedere al aptitudinilor, competenţelor dobândite şi deschiderii naţionale şi internaţionale oferite studenţilor. Absolvenţii acestui program vor fi capabili de o integrare rapidă pe piaţa muncii şi de ocuparea unor poziţii cheie în industrie sau poziţii în învăţământ şi cercetare.