



CYBERSECURITY

1. Misiunea programului de studii

Misiunea fundamentală a programului de studii de master *Cybersecurity* constă în formarea de specialiști capabili să protejeze informațiile și sistemele deținute de organizații și guverne împotriva amenințărilor cibernetice într-o lume tot mai interconectată digital. Acest program își propune să pregătească studenții pentru a deveni experți în protejarea sistemelor informatice și a rețelelor împotriva amenințărilor cibernetice, oferind studenților o bază solidă în tehnologiile și politicile de securitate cibernetică, precum și abilități practice de a gestiona și a reduce riscurile de securitate.

În vederea îndeplinirii misiunii asumate, programul de master *Cybersecurity* asigură dezvoltarea și formarea de competențe profesionale și transversale, utile pentru calificările obținute (descrise prin rezultatele învățării: cunoștințe, aptitudini, responsabilitate și autonomie), în concordanță cu standardele naționale și internaționale.

2. Obiectivele programului de studii

- Înțelegerea conceptelor și principiilor fundamentale ale securității cibernetice. Studenții vor învăța despre amenințările cibernetice, vulnerabilitățile sistemelor informatice și cum să protejeze sistemele de atacuri cibernetice;
- Dezvoltarea competenței în analiza riscurilor. Studenții vor învăța cum să identifice și să evalueze riscurile cibernetice și să dezvolte strategii de securitate adecvate pentru a reduce aceste riscuri;
- Protejarea datelor și a informațiilor. Studenții vor învăța cum să implementeze sisteme de securitate pentru a proteja datele și informațiile. Acest lucru poate include criptarea, autentificarea și controlul accesului;
- Detectarea și prevenirea amenințărilor cibernetice. Studenții vor învăța cum să detecteze și să prevină amenințările cibernetice, cum ar fi atacurile cu viruși sau cu phishing, prin utilizarea de instrumente de securitate avansate;
- Dezvoltarea unor abilități de analiză. Studenții vor învăța cum să efectueze analize de securitate și să identifice vulnerabilitățile sistemelor, astfel încât să poată fi dezvoltate soluții adecvate de securitate;
- Comunicarea și managementul incidentelor de securitate. Studenții vor învăța cum să comunice cu succes problemele de securitate și să dezvolte planuri de acțiune pentru a gestiona incidentele de securitate;
- Înțelegerea amenințărilor și vulnerabilităților cibernetice. Studenții vor învăța despre diferitele tipuri de amenințări cibernetice, cum ar fi hacking-ul, phishing-ul, malware-ul, atacurile DDOS și multe altele;
- Dezvoltarea abilităților tehnice necesare pentru a proteja informațiile și sistemele informatice împotriva atacurilor cibernetice. Acestea includ, printre altele, analiza datelor de securitate, criptografia, securitatea rețelelor, securitatea aplicațiilor și dezvoltarea de soluții de securitate cibernetică;
- Dezvoltarea abilităților de management și leadership. Acestea includ dezvoltarea de politici de securitate cibernetică, gestionarea riscurilor de securitate cibernetică, elaborarea de strategii de securitate cibernetică și coordonarea eforturilor de securitate cibernetică în organizație;
- Înțelegerea reglementărilor și standardelor de securitate cibernetică. Studenții vor fi familiarizați cu diferitele reglementări și standarde de securitate cibernetică, cum ar fi GDPR, NIST și ISO/IEC 27001;

- Dezvoltarea capacității de a lucra în echipe. Studentii vor avea ocazia să lucreze în echipe și să dezvolte abilități de comunicare și colaborare cu colegii;
- Dezvoltarea competențelor etice și legale. Acest obiectiv include învățarea despre normele și standardele etice și legale aplicabile în domeniul securității cibernetice, precum și despre impactul social și legal al atacurilor cibernetice;
- Dezvoltarea competențelor de management și leadership. Studenții vor învăța cum să conducă echipele de securitate cibernetică și cum să ia decizii strategice pentru a proteja organizațiile împotriva amenințărilor cibernetice.
- Crearea premiselor pentru a putea asigura echipe de lucru capabile să amelioreze gradul de securitate cibernetică pe plan local și național, conform realităților internaționale;
- Dezvoltarea de soluții de securitate inovatoare. Obiectivul final al programului de masterat este de a pregăti studenții să inoveze și să dezvolte noi soluții de securitate pentru a aborda provocările din ce în ce mai complexe ale securității cibernetice.

3. Premise și livrabile ale programului de studii

Programul de masterat *Cybersecurity* din domeniul de studii universitare de masterat Informatică, face parte din categoria programelor de master profesional fiind orientat preponderent spre pregătirea absolvenților interesați de concepte și soluții privind perfecționarea și aplicarea în practică a elementelor specifice securității cibernetice. Programul de studii asigură formarea de competențe cognitive, profesionale (instrumentale) și atitudinale (interpersonale) în concordanță cu standardele naționale și internaționale.

Competențele dezvoltate de către absolvenții acestui program de studii îi califică pentru următoarele ocupații, conform cu suplimentul la diplomă și înscrierea în RNCIS - expert în criminalistică informatică; 2529.6 - administrator de securitate în domeniul TIC; 2529.7 - consultant de securitate sisteme TIC; 2529.8 - manager de securitate sisteme TIC; 2529.9 - inginer tehnologii semantice.

4. Activitatea de predare

Cursuri	364 ore
Seminarii	-
Laboratoare	392 ore
Proiecte	-
Lucrări practice	75 ore

5. Evaluarea studenților

	Număr de evaluări/ani de studii			
Tip evaluare	Anul 1	Anul 2	TOTAL	%
Examene	8	8	16	84.21
Colocvii	1	2	3	15.79
Alte forme	-	-	-	-

6. Modalități de înscriere (condiții de acces). Condiții de înscriere în anul de studii următor. Condiții de promovare a unui an de studii.

La programul de studii de masterat *Cybersecurity* admiterea se bazează exclusiv pe competențele academice ale candidatului și nu se aplică criterii discriminatorii. Înscrierea la concursul de admitere se face numai pe baza diplomei de licență sau a altor acte de studii

echivalente. Pentru admitere se susține o probă orală evaluată cu admis/respins, o probă de competențe lingvistice evaluată cu admis/respins iar clasificarea candidaților admiși la proba orală se face integral pe baza notei obținute la examenul de licență. Regulamentul de admitere prezintă criteriile de admitere precum și cele de departajare a candidaților cu aceeași notă la examenul de licență.

Înscrierea în anul următor este condiționată de întrunirea condițiilor de promovare cuprinse în Regulamentul privind activitatea profesională a studenților.

7. Egalitatea de șanse

Recrutarea, admiterea, transferul și mobilitățile studenților la programul *Cybersecurity* se realizează transparent în conformitate cu legislația în vigoare și procedurile aprobate de Senatul ULBS. Admiterea se bazează exclusiv pe competențele academice ale candidatului și nu aplică niciun fel de criterii discriminatorii.

8. Sustenabilitatea programului

Din perspectiva sustenabilității ecologice, programul de studiu *Cybersecurity* promovează o utilizare eficientă a resurselor prin următoarele măsuri: configurarea formațiilor de studiu pentru minimalizarea consumurilor energetice aferente desfășurării activităților didactice dar cu asigurarea unei formări profesionale eficiente; încurajarea utilizării formatului electronic pentru teme, referate sau proiecte; utilizarea materialelor suport în format electronic.

De asemenea, deșeurile rezultate în urma activităților aplicative sunt gestionate conform normelor în vigoare și a sistemului de colectare a deșeurilor adoptat de ULBS.

Există o foarte mare nevoie de specialiști în informatică în ziua de astăzi. Odată cu avansul tehnologic rapid și dependența tot mai mare de tehnologie în diferite domenii, cererea pentru profesioniști în informatică a crescut semnificativ.

Formarea profesională prin programul de masterat *Cybersecurity* răspunde nevoilor societății conferind sustenabilitate dezvoltării sociale și economice.

9. Asigurarea flexibilizării instruirii. Condiționări.

Flexibilizarea programului de studii este asigurată prin discipline opționale și discipline facultative.

Disciplinele opționale sunt în număr de 6 grupate câte două în 3 pachete, din care studenții vor alege cel puțin una. Disciplinele opționale sunt propuse începând cu semestrul 2. Numărul mare de discipline opționale flexibilizează programul de studiu și permite obținerea de competențe pentru diferite debușee profesionale.

10. Metodologia de evaluare a competențelor la finalizarea studiilor

Condițiile de susținere a examenului de absolvire sunt prezentate în Metodologia de finalizare a studiilor aplicabilă, aprobată de Senatul Universității. Conform acestei metodologii, prezentarea la examenul de absolvire este condiționată de promovarea tuturor disciplinelor prevăzute în planul de învățământ.

EXAMENUL DE ABSOLVIRE

- 1 Perioada de întocmire a lucrării de disertație: semestrele 3-4;
- 2 Perioada de înscriere la examenul de absolvire - în cursul lunii iunie.
- 3 Perioada de susținere a examenului de licență: săptămâna 40 a anului II
- 4 Numărul de credite pentru susținerea examenului de disertație: 10 credite.

11. Pregătirea pentru ocuparea prin concurs a unui post în învățământ

Pentru ocuparea prin concurs a unui post în învățământ (gimnazial, liceal sau superior în domeniul de licență) absolventul trebuie să posede Certificatul de absolvire a unui program de studii pentru formarea psiho-pedagogică (care permite exercitarea profesiei didactice) coordonat de Departamentul pentru Pregătirea Cadrelor Didactice din cadrul ULBS (sau din cadrul altei universități).

Formarea psiho-pedagogică pentru obținerea Certificatului de absolvire se face în urma parcurgerii a două module:

- (1) Modul I (30 credite) - care se desfășoară suplimentar, în paralel cu studiile de licență sau în regim postuniversitar, la finalizarea căruia se obține Certificat de absolvire (modul I).
- (2) Modul II (30 credite) - care se desfășoară după absolvirea studiilor de licență, în paralel cu perioada studiilor de masterat sau în regim postuniversitar. Acesta se finalizează cu Certificat de absolvire (nivel de aprofundare).