INVESTIGAȚII DIGITALE ȘI RĂSPUNS LA INCIDENTE

1. Date despre disciplină/modul

Facultatea	Calculatoare, Informatică şi Microelectronică				
Departamentul	Inginerie Software şi Automatică				
Ciclul de studii	Ciclul II, Studii superioare de master				
Programul de studii	Securitate informațională				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
Anul I *(învățământ cu frecvenţă)*	I	E	F – uniate de curs de fundamentală	O - unitate de curs obligatorie	5

2. Timpul total estimat

Total ore în planul de învățământ		**Din care**				
		Ore auditoriale		**Lucrul individual**		
		Curs	**Practice**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicații**
Învățământ cu frecvență	**150**	20	20	-	60	50

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Accesul la disciplină este permis studenților care au parcurs disciplinele premergătoare conform structurii curriculare, având cunoștințe fundamentale în domeniul tehnologiei informației, securității informatice, și reglementărilor legale privind utilizarea sistemelor informatice. Este obligatoriu ca studenții să fi finalizat disciplinele introductive, precum „Introducere în securitatea informației” și „Aspecte generale ale sistemelor informatice.”
Conform competențelor	• Capacitatea de a analiza și înțelege structura și funcționarea sistemelor informatice. • Cunoașterea instrumentelor software utilizate pentru analiza și securizarea datelor. • Înțelegerea conceptelor de bază legate de investigarea incidentelor informatice și identificarea amenințărilor cibernetice. • Familiarizarea cu reglementările juridice și standardele aplicabile în domeniul criminalității informatice.

4. Condiții de desfășurare a procesului educațional pentru

Curs	Procesul educațional pentru curs se desfășoară într-o sală dotată cu echipamente multimedia, inclusiv proiector, sistem audio și acces la Internet, pentru a facilita prezentările și discuțiile interactive. Materialele didactice includ manuale, suporturi de curs, prezentări digitale și resurse accesibile pe platforme educaționale online. Metodele de predare se bazează pe implicarea activă a studenților prin întrebări, discuții și exemple practice relevante. Evaluarea se realizează prin teste formative, proiecte individuale sau de grup, precum și evaluări sumative care verifică cunoștințele acumulate. Participarea la curs este obligatorie în proporție de minim 75%.
Practice	Activitățile practice se desfășoară în laboratoare specializate, echipate cu calculatoare performante și software dedicat pentru investigarea criminalității informatice. Resursele utilizate includ ghiduri practice și scenarii simulate care permit aplicarea cunoștințelor în situații reale. Evaluarea se bazează pe rezultatele activităților practice, inclusiv rapoarte scrise, teste aplicative și prezentări finale. Participarea la activitățile practice este obligatorie, fiind necesară prezența la minim 75% dintre acestea și respectarea normelor de conduită profesională, cum ar fi confidențialitatea datelor.

5. Competențe specifice acumulate

Competențe profesionale	**CPM1: Sistemul informatic (SI) și alinierea strategiilor de afaceri** Coordonarea proceselor de investigare și implementare a soluțiilor inovative pentru combaterea criminalității informatice, prin integrarea cerințelor de securitate și alinierea acestora la obiectivele strategice. **CPM2: Managementul nivelului de servicii** Dezvoltarea unui plan strategic pentru monitorizarea și investigarea incidentelor informatice, asigurând respectarea standardelor de securitate și rezultatelor planificate. **CPM3: Elaborarea și proiectarea arhitecturii SI**

	Proiectarea și implementarea infrastructurilor de investigare digitală care să sprijine analiza criminalității informatice, utilizând metode și tehnologii avansate. **CPM4: Monitorizarea tendințelor tehnologice** Valorizarea tehnologiilor emergente pentru a identifica și preveni amenințările informatice, demonstrând adaptabilitate la noile tendințe. **CPM5: Proiectarea și dezvoltarea aplicațiilor** Aplicarea instrumentelor software pentru analizarea și investigarea criminalității informatice, optimizând procesele de colectare a probelor și realizând aplicații dedicate acestui scop. **CPM6: Schimbarea suportului** Asigurarea integrității datelor și evidențelor digitale prin soluții de stocare și recuperare adaptate necesităților investigațiilor. **CPM7: Furnizarea de servicii** Gestionarea serviciilor digitale și implementarea de soluții eficiente pentru protejarea și investigarea sistemelor informatice afectate de incidente. **CPM9: Îmbunătățirea proceselor** Optimizarea procedurilor de investigare și răspuns la incidente prin implementarea tehnologiilor moderne și a bunelor practici în domeniu.
Competenţe transversale	**CTM1: Autonomie și responsabilitate** Dezvoltarea capacității de a acționa autonom în situații complexe de investigare a criminalității informatice, asumându-și responsabilitatea pentru luarea deciziilor adecvate. **CTM2: Interacțiune socială** Colaborarea eficientă cu echipe multidisciplinare, inclusiv cu autoritățile legale și partenerii internaționali, în cadrul proceselor de investigare. **CTM3: Dezvoltare profesională și personală** Îmbunătățirea continuă a cunoștințelor și abilităților prin formare profesională și adaptare la noile provocări din domeniul criminalității informatice.

6. Obiectivele disciplinei/modulului

Obiectivul general	Dezvoltarea competențelor studenților în analiza, prevenirea, detectarea și investigarea criminalității informatice, prin utilizarea cadrului juridic, tehnic și metodologic specific, pentru a contribui la protecția infrastructurilor IT și la combaterea fenomenului de criminalitate cibernetică.
Obiectivele specifice	• Înțelegerea fenomenului de criminalitate informatică, inclusiv a reglementărilor juridice naționale și internaționale aplicabile. • Identificarea și analiza modurilor de operare utilizate frecvent în criminalitatea informatică. • Dezvoltarea abilităților practice de investigare criminalistică a infracțiunilor informatice, inclusiv percheziția calculatorului și cercetarea la fața locului. • Utilizarea tehnologiilor și metodelor moderne pentru investigarea traficului de rețea și a aplicațiilor de Internet. • Investigarea infracțiunilor specifice, cum ar fi utilizarea frauduloasă a instrumentelor de plată electronică, criminalitatea cibernetică prin intermediul telefoniei mobile și pornografia infantilă. • Aplicarea strategiilor de prevenire, detectare și răspuns la incidentele informatice, incluzând remedierea și recuperarea după incidente. • Cooperarea națională și internațională pentru combaterea criminalității informatice, inclusiv coordonarea cu autoritățile și instituțiile relevante. • Elaborarea documentației specifice, precum rapoartele de incident, pentru învățarea din experiențele anterioare și îmbunătățirea continuă a proceselor.

7. Conținutul disciplinei/modulului

Tematica activităților didactice	**Numărul de ore învățământ cu frecvență**
Tematica cursurilor	
T1. Aspecte introductive privind fenomenul de criminalitate informatică.	**2**
T2. Reglementarea juridică națională și internațională a criminalității informatice.	**2**
T3. Moduri de operare frecvente întâlnite în criminalitatea informatică.	**2**
T4. Aspecte metodologice privind investigarea criminalistică a infracțiunilor informatice.	**2**
T5. Particularități privind percheziția calculatorului și cercetarea la fața locului în cazul infracțiunilor informatice.	**2**
T6. Investigarea traficului de rețea și a aplicațiilor de Internet.	**2**
T7. Investigarea infracțiunilor informatice săvârșite prin utilizarea frauduloasă a instrumentelor de plată electronică.	**2**

Tematica activităților didactice	Numărul de ore învățământ cu frecvență
T8. Particularități ale investigării infracțiunilor informatice săvârșite prin intermediul telefoniei mobile.	**2**
T9. Particularități ale investigării infracțiunilor informatice din categoria pornografiei infantile.	**2**
T10. Cooperarea internațională și europeană în domeniul combaterii criminalității informatice	**2**
Total curs:	**20**
Tematica lucrărilor practice	
LP1. Prevenirea incidentelor: Implementarea unui set robust de politici de securitate și proceduri pentru a preveni incidentele IT. Utilizarea unor soluții de securitate informatică, cum ar fi firewalls, antivirus și sisteme de detecție a intruziunilor. Formarea personalului în privința practicilor de securitate cibernetică și a conștientizării asupra securității informațiilor.	**2**
LP2. Prevenirea incidentelor: Actualizări și patch-uri. Monitorizarea continuă a activității rețelei și a sistemelor IT. Controlul accesului. Backup și recuperare prin realizarea copiilor de rezervă regulate ale datelor. Evaluare și auditare regulată	**2**
LP3. Detectarea incidentelor: Implementarea unor mecanisme automate și manuale pentru a detecta activitățile suspecte sau neautorizate. Monitorizarea constantă a activității sistemului și a rețelei pentru a identifica semnalele de avertizare ale unui posibil incident.	**2**
LP4. Detectarea incidentelor: Utilizarea sistemelor de detecție a intruziunilor (IDS) și a sistemelor de prevenire a intruziunilor (IPS) privind detectarea și blocarea activităților neautorizate sau potențial dăunătoare în rețea sau în sistemul informatic. Monitorizarea și analiza log-urilor de sistem și de securitate privind activitățile neobișnuite sau suspecte care ar putea indica un incident de securitate.	**2**
LP5. Detectarea incidentelor: Utilizarea tehnologiilor de detecție a amenințărilor avansate. Implementarea unor soluții moderne de detecție a amenințărilor – analiza comportamentală, analiza de anomalii și tehnologiile bazate pe inteligență artificială și învățare automată.	**2**
LP6. Detectarea incidentelor: Monitorizarea și analiza traficului web privind identificarea site-urilor web infectate sau a altor surse de amenințare. Configurarea unor alerte și notificări automate pentru activități suspecte sau pentru evenimente semnificative privind reacția rapidă și eficientă în cazul unui incident.	**2**
LP7. Răspunsul la incidente: Designarea unei echipe de răspuns la incidente care să fie responsabilă cu gestionarea și remedierea incidentelor. Documentarea clară a procedurilor de răspuns la incidente, inclusiv etapele de notificare, escaladare și comunicare internă și externă. Izolarea rapidă a incidentului pentru a preveni răspândirea ulterioară a daunelor și a limita impactul asupra sistemelor și datelor	**2**
LP8. Investigarea și analiza incidentelor: Colectarea de probe și date relevante pentru a înțelege cauza și amploarea incidentului. Analiza detaliată a modului în care incidentul s-a produs și identificarea punctelor vulnerabile ale infrastructurii IT pentru a preveni incidente similare în viitor.	**2**
LP9. Remedierea și recuperarea: Aplicarea măsurilor corective necesare pentru a remedia problemele și pentru a restabili serviciile afectate. Actualizarea politicilor și procedurilor de securitate pentru a preveni incidente similare în viitor. Evaluarea și îmbunătățirea continuă a planului de răspuns la incidente în funcție de experiența acumulată din incidente anterioare.	**2**
LP10. Raportarea și învățarea din incidente: Furnizarea unui raport detaliat al incidentului către părțile interesate interne și, dacă este necesar, autorităților externe. Analiza procesului de răspuns la incidente pentru a identifica punctele tari și slabe și pentru a îmbunătăți planul și procedurile. Împărtășirea experienței și învățămintelor din incidente cu întreaga echipă pentru a îmbunătăți înțelegerea și pregătirea în fața viitoarelor amenințări.	**2**
Total lucrări practice:	**20**

8. Referințe bibliografice

Principale	1. National Institute of Standards and Technology, NIST Special Publication 800, NIST SP (800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise Revision 1), https://www.nist.gov/. 2. OWASP Foundation, OWASP Top Ten: The Ten Most Critical Web Application Security Risks, 2023, https://owasp.org/. 3. ISO/IEC 27000 family, Information security management, (ISO/IEC 27035:2020-2024 — Information technology — Information security incident management),

	https://www.iso.org/standard/iso-iec-27000-family. 4. National Cyber Security Centre (NCSC), Mitigating Malware and Ransomware Attacks, 2023, https://www.ncsc.gov.uk/. 5. The European Union Agency for Cybersecurity, ENISA Threat Landscape 2024, https://www.enisa.europa.eu/ 6. Anderson R., Security Engineering: A Guide to Building Dependable Distributed Systems (3rd Edition), Wiley, 2020. 7. Stallings W., Computer Security: Principles and Practice (5th Edition). Pearson, 2021. 8. Symantec Corporation, Internet Security Threat Report, 2023. 9. Northcutt, S., The Cybersecurity Handbook: Prepare for and Protect Against the Next Cyberattack, Wiley, 2021.
Suplimentare	10. William Villegas-Ch. 1, Ivan Ortiz-Garces and Santiago Sánchez-Viteri, Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus, Computers, 2021, https://www.mdpi.com/2073-431X/10/8/102. 11. Raghvinder S. Sangwan, Youakim Badr and Satish M. Srinivasan, Cybersecurity for AI Systems: A Survey. 2023, 166–190, https://www.mdpi.com/2624-800X/3/2/10 12. Maanak Gupta, Charankumar Akiri, et. all. From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy, IEEEAccess, Volume II, 2023. 13. Daniel Schlette, M. Caselli, G. Pernul, A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective, 2021. https://epub.uni-regensburg.de/52721/1/Accepted_CTI%20Survey_IEEE_COMST_public.pdf 14. Inger Anne Tøndel, Maria B. Line, Martin Gilje Jaatun, Information security incident management: Current practice as reported in the literature, 2020. https://www.sciencedirect.com/science/article/abs/pii/S0167404814000819?via%3Dihub

9. Utilizarea IA generativă

Permisiunea de utilizare	Utilizarea IA generative în cadrul temelor și proiectelor este permisă, cu condiția ca studenții să respecte următoarele reguli: • IA generativă poate fi utilizată pentru generarea de idei, structuri de text sau cod, dar toate materialele generate trebuie să fie revizuite și ajustate de către student pentru a se asigura că acestea corespund cerințelor academice. • Orice utilizare a IA generative trebuie să fie declarată în secțiunea de apendice a fiecărei lucrări, folosind fraza: "În timpul pregătirii acestei lucrări, autorul a utilizat [NUME INSTRUMENT / SERVICIU] în scopul [MOTIV]. După utilizarea acestui instrument/serviciu, autorul a revizuit și editat conținutul după cum a fost necesar și își asumă întreaga responsabilitate pentru conținutul lucrării."
Restricții de utilizare	Studenții nu trebuie să considere IA generativă ca o sursă de încredere pentru informații, deoarece nu oferă referințe clare sau surse documentate. • Nu este permisă citarea directă a conținutului generat de IA în lucrările academice ca și cum ar fi sursă primară. • Activitățile în care este interzis utilizarea IA generativă sunt specificare de profesor și sunt de regulă evaluări intermediare și finale sau care nu presupun activități de dezvoltare a competențîlor profesionale.

10. Evaluare

Periodică		**Curentă**	**Studiu individual**	**Proiect/teză**	**Examen**
EP 1	**EP 2**				
15%	15%	15%	15%		40%
Standard minim de performanţă Prezenţa şi activitatea la prelegeri şi lucrări practice. Obţinerea notei minime de „5” la fiecare dintre atestări şi lucrări practice.					

11. Criterii de evaluare

Activitate	**Componente evaluare**	**Metodă de evaluare, criterii de evaluare**	**Pondere în nota finală a activității**	**Ponderea în evaluarea disciplinei**
Evaluare periodică I	Conținut teoretic Teme 1-5	Test electronic pe platforma else.fcim.utm.md	100%	**15%**
Evaluare periodică II	Conținut teoretic Teme 5-10	Test electronic pe platforma else.fcim.utm.md	100%	**15%**

Activitate	Componente evaluare	Metodă de evaluare, criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
Evaluare curentă	Participare, lucrări practice, rapoarte	Participarea la activități, calitatea și acuratețea realizării lucrărilor practice, pregătirea și susținerea rapoartelor	100%	**15%**
Studiul individual	Studiu de caz privind metodologia de gestionare a incidentelor de securitate cibernetică.	Prezentare orală/discurs la studiului de caz în fața colegilor; evaluarea coerenței, clarității și documentării. Verificarea planului de răspuns la incidente cibernetice ca componentă esențială a gestionării securității informațiilor și a asigurării continuității afacerii în cadrul unei organizații, definind o structură și proceduri standardizate pentru a detecta, investiga și remedia incidentele de securitate și problemele de infrastructură IT.	100%	**15%**
Evaluarea finală	Conținut teoretic și practic	Test electronic pe platforma else.fcim.utm.md	100%	**40%**