

GESTIUNEA SECURITĂȚII INFORMAȚIONALE
1. Date despre disciplină/modul

Facultatea	Calculatoare, Informatică și Microelectronică				
Departamentul	Ingineria software și automată				
Ciclul de studii	Studii de master, ciclul II				
Programul de studii	Securitate informațională				
Anul de studii	Semestrul	Tip de evaluare	Categoria formativă	Categoria de opționalitate	Credite ECTS
Anul I (<i>învățământ cu frecvență</i>)	I	E	F – unitate de curs fundamentală	O - unitate de curs obligatorie	5

2. Timpul total estimat

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

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Bazele securității informaționale, Managementul și auditul securității informaționale, Cadrul legal al securității informaționale, Infrațiuni informatice și tehnici de investigare, Programe malițioase și antivirus, Proiectarea sistemelor informaționale
Conform competențelor	Explicarea soluțiilor manageriale de securitate informațională prin utilizarea tehnicilor, conceptelor și principiilor din științele exacte și aplicative

4. Condiții de desfășurare a procesului educațional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector și calculator. Nu vor fi tolerate întârzierile studenților, precum și convorbirile telefonice în timpul cursului
Laborator/ seminar	Studenții vor perfecta rapoarte conform condițiilor impuse de indicațiile metodice. Pentru predarea cu întârziere a lucrării aceasta se depunceață cu 1pct./zi de întârziere

5. Competențe specifice acumulate

Competențe profesionale	C1 Operarea cu concepte și metode științifice în domeniul Securității informaționale C2 Cercetarea științifică privind aspectele organizaționale și informaționale ale securității C3 Modelarea sistemelor complexe de securitate și implementarea lor prin sisteme informatice C5 Managementul sistemelor de securitate în concordanța cu cerințele pieței
Competențe transversale	CT2. Preluarea diferitelor roluri în echipe de proiect și descrierea clară, concisă, verbală și în scris, în limba română și într-o limbă de circulație internațională, a rezultatelor din domeniul de activitate

6. Obiectivele disciplinei/modulului

Obiectivul general	Însușirea conceptelor, metodelor și politicilor de gestionare a riscurilor informaționale, de planificare, implementare, revizuire și monitorizare a SMSI.
Obiectivele specifice	Să înțeleagă și să descrie componentele sistemului de management al securității informaționale Să cunoască metodele de inventariere a activelor, identificarea vulnerabilităților și amenințărilor specifice organizației Să însușească și să utilizeze metodologiile de management al riscurilor informaționale Să cunoască modele de politici de securitate și modalități de implementare a lor în cadrul organizației Să aplice corect metodele de revizuire și de îmbunătățire a sistemului de management al securității informaționale

7. Conținutul disciplinei/modulului

Tematica activităților didactice	Numărul de ore
	învățământ cu frecvență
T.1. Cadrul de management al securității informației. Sistemului de Management al Securității Informaționale Noțiuni și concepte de bază. Standarde internaționale în domeniu: familia de standarde ISO 27000, NIST, PCI DSS. Relația între standarde și aplicabilitatea lor. Secțiunile standardului de securitate ISO / IEC 27002. Componentele și mecanismele unui SMSI. Managementul securității informaționale la nivel de stat: principii generale. Practica organizațiilor internaționale și a altor state	4
T.2. Politici, modele și programe de securitate Modele de securitate multinivel și multilaterale. Modelul Ball-LaPadula. Modelul Biba. Modele de politici de securitate. Exemple de politici de securitate. Aspecte practice ale politicii de securitate.	4
T.3. Analiza și evaluarea riscurilor de securitate. Metodologii și instrumente de analiza a riscurilor informaționale Noțiuni generale privind managementul riscurilor securității informaționale. Amenințări și vulnerabilități. Etapele procesului de analiză și evaluare riscuri conform ISO 27005. Evaluarea cantitativă și calitativă. Metodologia CRAMM. Metodologia MEHARI. Metodologia Ebios. Metodologia Octave. Metodologia IT-Grundschutz. Instrumentele GSTool, RiskWatch, Cramm, Ebios, Grif	4
T.4. Implementarea unui sistem de management al securității informaționale Modelul PDCA (Plan[Planificare]-Do[Implementare]-Check[Verificare]-Act[Corectare]). Etapele procesului de implementare a SMSI conform ISO 27001. Stabilirea obiectivelor și definirea sferei SMSI. Roluri și responsabilități.	4
T.5. Revizuirea și optimizarea sistemului de management al securității informaționale. Procedura de audit intern. Planul, Programul, Universul și Chestionar de audit. Raport de audit. Auditul activ și instrumente informatice de audit (CAATs). Procedura de acțiuni corective. Metode de optimizare utilizând teoria grafurilor, teoria probabilităților, procesele stochastice și metoda economică (ROSI).	4
Total curs:	20
LP.1.Sistemul de management al securității informației. Contextul organizației. Scopul și obiectivele SMSI	4
LL.2. Politici și proceduri de securitate Politica generală de securitate și politici specifice. Roluri și responsabilități. Fișe de post	4
LL.3. Managementul riscurilor informaționale Metodologia de gestionare a riscurilor informaționale. Inventarierea activelor sistemului informațional. Managementul vulnerabilităților și identificarea amenințărilor	4

Tematica activităților didactice	Numărul de ore
	învățământ cu frecvență
LL.4. Evaluarea conformității SMSI. Instrumentul Microsoft Security Assessment Tool. Instrumentul CSET Stand Alone – evaluarea securității după alte modele și standarde. Declarația de aplicabilitate	4
LL.5. Revizuirea și optimizarea SMSI Rechizite de auditare SMSI. Instrumente informatice de audit (CAATs). Acțiuni corective	4
Total lucrări practice/seminare:	20

8. Referințe bibliografice

Principale	<ol style="list-style-type: none"> 1. Familia de standarde ISO 2700k – Sistemul de management al securității informaționale; 2. William Stallings, <i>Effective Cybersecurity A Guide to Using Best Practices and Standards</i>, 2019 Pearson Education; 3. Tudor BRAGARU, <i>Dezvoltarea și implementarea sistemului de management al securității informației (în baza ISO/IEC 27001): Ghidul participantului și suport de curs pentru instruirea tradițională, online și/sau la distanță: Complet de Resurse Educaționale Digitale (CRED)</i>. Chișinău, 2021; 4. Tudor BRAGARU, <i>Auditul sistemului de management al securității informației: Ghidul participantului și suport de curs pentru instruirea tradițională, online și/sau la distanță: Complet de Resurse Educaționale Digitale (CRED)</i>. Chișinău, 2021.
Suplimentare	<ol style="list-style-type: none"> 1. Dumitru Oprea, <i>Protecția și securitatea informațiilor</i>. Ed. II, Polirom, Iași, 2007. – 445 p. 2. Popa Sorin Eugen, <i>Securitatea sistemelor informatice</i>, Bacău, 2007. – 136 p. 3. Al. Astahov, <i>Искусство управления информационными рисками</i>, ДМК, Москва, 2010. – 316 p. 4. Nicolas Mayer, <i>Model-based Management of Information System Security Risk</i>, Namur, Belgium, 2009. – 295 p. 5. M.E. Whitman, H.J.Mattord, <i>Management of Information Security</i>, 3rd Edition, Course Technology, 2010. 6. A.Calder, S.Watkins, <i>A Manager's Guide to Data Security and ISO 27001/ISO27002</i>, 4th Edition, Kogan Page, 2008. 7. D.Landool, <i>The Security Risk Assessment Handbook</i>, Auerbach Publications, 2006.

9. Evaluare

Periodică		Curentă	Studiu individual	Proiect/teză	Examen
EP 1	EP 2				
Învățământ cu frecvență					
10%	10%	10%	30%	-	40%
Standard minim de performanță Prezența și activitățile la prelegeri și lucrări practice. Obținerea notei minime de „5” la fiecare dintre lucrări și examen					

10. Criterii de evaluare

Activitate	Componente evaluare	Metodă de evaluare, Criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
Învățământ cu frecvență				
Evaluare periodică I	Conținut teoretic, teme 1-3	Test pe MOODLE	100%	10%
Evaluare periodică II	Conținut teoretic, teme 4-5	Test pe MOODLE	100%	10%
Evaluare curentă	Lucrări practice	Discuții în cadrul lecțiilor practice	50%	10%
		Dosar completat cu Rapoarte pentru fiecare Studiu de caz în discuție	50%	
Studiul individual	SMSI	Prezentare/discurs public	100%	30%
Evaluarea finală	Conținut teoretic și practic	Test pe MOODLE. Notare conform baremului	100%	40%